Preamble

Die Crowdfox GmbH (“Crowdfox”) and the Customer conclude a contract for SaaS services (“Main Contract”) and have agreed that this Data Processing Agreement (“DPA”) shall become part of the Main Contract as an annex to the Main Contract. This agreement shall enter into force when the Main Agreement becomes effective and does not require any further signature to become effective. Rights and obligations under this contract are only derived if the customer has concluded the main contract with Crowdfox.

Table of contents

I. General Conditions

1. Crowdfox processes personal data as a processor (“Contractor”) for the customer as the controller (“Client”, collectively “Parties”) in the manner described in this contract on behalf of the controller in accordance with the following provisions.
2. This DPA governs the rights and obligations of the parties in the context of the processing of personal data on behalf. This DPA is designed in such a way that it complies with the provisions of the applicable General Data Protection Regulation (“GDPR”), the German Federal Data Protection Act and the relevant state data protection laws.
3. This DPA applies to such activities in which the Contractor, employees of the Contractor or subcontractors commissioned by the Contractor process personal data of the Client in the context of the main contract within the meaning of Art. 28 GDPR.
4. Terms used in this DPA are to be understood in accordance with their definition in the GDPR.
5. This agreement replaces all previous data protection agreements and DPAs or DPA contracts between the parties.
6. In the event of contradictions between the Main Contract and this DPA, the DPA shall take precedence as a more specific regulation in data protection matters.

II. Purpose of the processing and the type of personal data

Crowdfox processes the following personal data as part of the scope of services under the Main Contract:

- Communication data (e.g. e-mail address),
- user data (e.g. IP address)
- Business address data of the user (e.g. address of a location)

III. Processing Activities

Processing activity is the storage of personal data to fulfill the obligations arising from the Main Contract.

IV. Categories of data subjects

The categories of data subjects are employees of the Client.

V. Obligations of the Client

1. Within the scope of this DPA, the Client shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the Contractor and for the lawfulness of the processing. This also applies with regard to the subject matter, scope, type and purpose of the data processing regulated in this agreement, the description of the data concerned and the protection of the rights of the data subjects.
2. In particular, the client is responsible for ensuring that the technical and organizational measures (“TOM”) taken by the contractor for this processing provide an adequate level of protection for the risks of the processed data. For its part, the Contractor is responsible for

complying with these TOMs.

3. The client must inform the contractor immediately and in full if it discovers errors or irregularities with regard to the processing of data protection regulations.
4. If necessary, the Client shall provide the Contractor with the contact person for data protection issues arising within the scope of this DPA.
5. Further rights and obligations arise from the following provisions of this DPA and the GDPR as well as the associated statutory provisions.

VI. Quality assurance and other obligations of the Contractor

In addition to complying with the provisions of this contract, the Contractor has statutory obligations pursuant to Art. 28 to 33 GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

1. Written appointment of a data protection officer who performs his or her duties in accordance with Art. 38 and 39 GDPR.
2. The maintenance of confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Contractor shall only use employees who have been obliged to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may only process this data in accordance with the instructions of the Client, including the powers granted in this contract, unless they are legally obliged to process it.
3. The implementation of and compliance with all technical and organizational measures required for this order in accordance with Art. 28 para. 3 sentence 2 lit. c, Art. 32 GDPR.
4. The Client and the Contractor shall cooperate with the supervisory authority in the performance of their tasks upon request.
5. The immediate information of the client about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies if a competent authority investigates the processing of personal data in the context of an administrative offense or criminal proceedings relating to the processing of personal data at the contractor's premises.
6. To the extent that the Client is subject to an inspection by the supervisory authority, misdemeanor or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Client to the best of its ability.
7. The Contractor shall regularly monitor the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the

protection of the rights of the data subject is guaranteed.

8. Verifiability of the technical and organizational measures taken vis-à-vis the client.

VII. Technical and organizational measures

1. taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Contractor shall implement appropriate TOM in such a manner that the processing of personal data meets the requirements of the applicable data protection law, in particular the GDPR and this Agreement.
2. For this purpose and in accordance with Article 32 GDPR, the contractor shall adequately document the specific measures and submit them to the client upon request.
3. The TOMs change with technical progress and are constantly evolving. In this context, the Contractor may take suitable alternative measures. However, the security level of the aforementioned measures may not fall below the level agreed in this contract without the consent of the Client.
4. The TOMs implemented by the Contractor at the time of this Data Protection Agreement are listed in Annex 1 to this DPA.

VIII. Transfer of personal data

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. GDPR are met. However, if these requirements are met, there must be important reasons under data protection law to refuse consent.

IX. Subcontractors (Subprocessors)

1. Subcontractors within the meaning of this regulation are those services providers that are directly related to the provision of the main service and process personal data in the process. This does not include ancillary services which the contractor uses, e.g. as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and data security of the Client's data, even in the case of outsourced ancillary services.
2. The commissioning of Subcontractors for the processing or use of personal data is only permitted with the approval of the client. For the subcontractors listed in Annex 2 at the time of the conclusion of the contract, this authorization shall be deemed to have been granted. The Client shall grant the Contractor general authorization to make use of further subcontractors. However, it may object to such changes, whereby this may not be done without good cause under data protection law. The Contractor shall inform the Client in text form by active notification (e.g. e-mail) if it intends to use additional or substitute subcontractors. The objection to the intended change must be submitted to the contractor

in text form (e.g. to datenschutz@crowdfox.com) within 14 days of the information about the change being made available. In the event of an objection, the Contractor may, at its own discretion, provide the service without the intended change or - if the provision of the service without the intended change is unreasonable for the Contractor - discontinue the service to the Client within 4 weeks of receipt of the objection and terminate the main contract without notice and with immediate effect.

3. The transfer of the client's personal data to the subcontractor and the subcontractor's initial activities are only permitted once all requirements for subcontracting have been met.

4. If the Contractor places orders with subcontractors, the Contractor shall be responsible for transferring its data protection obligations under this contract to the subcontractors and concluding a contractual agreement with them in accordance with Art. 28 para. 2-4 GDPR. In particular, the Contractor shall ensure that the subcontractor's TOMs meet the level of protection of the TOMs under this DPA.

X. Information and Control Rights of the Client

1. The Client shall have the right to carry out inspections or have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of random checks, which must be notified in good time.

2. The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations under Art. 28 GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

3. It is agreed that both parties shall bear the personnel costs incurred for the inspection to enable the client to carry out inspections. The costs for third party inspectors appointed by the client shall be borne in full by the client.

4. The contractor has the right to refuse the on-site inspection without cause if and as long as it provides evidence of the fulfillment of its obligations, in particular the implementation of the TOM and its effectiveness, by means of suitable evidence. Suitable evidence may in particular be approved codes of conduct within the meaning of Art. 40 GDPR or an approved certification procedure within the meaning of Art. 42 GDPR. Both parties agree that the submission of certificates or reports from independent bodies (e.g. IT security officer, data protection officer), a conclusive data security concept or suitable certification through an IT security and data protection audit are also recognized as suitable evidence.

XI. Notification of breaches by the Contractor

1. The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes:

   - Ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as

well as the predicted likelihood and severity of a potential breach through security vulnerabilities and enable the immediate detection of relevant breach events.
- The obligation to report personal data breaches to the client without delay the obligation to support the client in the context of its duty to inform the data subject and to provide the client with all relevant information in this context without delay.
- Supporting the client for its data protection impact assessment.
- Supporting the client in the context of prior consultations with the supervisory authority.

2. The Contractor may claim remuneration for support services that are not included in the service description or are not attributable to misconduct on the part of the Contractor.

XII. Authority of the Client to issue instructions

1. The contractor may not rectify, erase or restrict the processing of data processed on behalf of the client without authorization, but only in accordance with documented instructions from the client. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay. The Contractor shall not be liable if the data subject's request is not answered by the Client, or is not answered correctly or on time, and this is solely the fault of the Client.

2. The Contractor must inform the Client immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

XIII. Deletion and return of Personal data

1. Copies or duplicates of the data shall not be created without the knowledge of the client. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data required to comply with statutory retention obligations.

2. After completion of the contractually agreed work or earlier at the request of the client - at the latest upon termination of the main contract - the contractor shall hand over to the client all documents, processing and usage results and data stocks that have come into its possession in connection with the contractual relationship or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material. The deletion log must be submitted on request.

3. Documentation that serves as proof of the order and proper data processing shall be retained by the Contractor beyond the end of the contract in accordance with the respective retention periods. The Contractor may hand them over to the Client at the end of the contract in order to discharge the Client.

XIV. Liability

1. Reference is made to Art. 82 GDPR.

2. In all other cases, the Client shall be fully liable internally for the damage and shall indemnify the Contractor against any claims of the data subject or third parties asserted

against the Contractor in connection with the commissioned processing on first demand.

3. The client shall bear the burden of proof that damage is not the result of a circumstance for which it is responsible.

4. Any exclusions of liability in this contract shall not apply in the event of intent or gross negligence or in the event of damage to life, body or health.

XV. Duration of the DPA

The term of this DPA corresponds to the term of the main contract.

XVI. Other provisions

Amendments and supplements to this agreement and all its components - including any assurances made by the Contractor - must be made in writing in accordance with the GDPR, which may also be in an electronic format, and must expressly state that it is an amendment or supplement to these terms and conditions. This also applies to the waiver of this formal requirement. Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

XVII. Anhänge

Annax 1: Technical and organizational measures

Annax 2: Subcontractors

Annax 1: Technical and organizational measures

Confidentiality

Confidentiality includes the points “measures of access control of data processing centres”, “measures of access control of data processing systems”, “measures for access control of personal data in data processing systems” and “measures separation control”.

- **Measures of access control of data processing centres**
  Access controls of data processing centres are measures that are suitable for preventing unauthorized persons from gaining access to data processing centres with which personal data is processed or used.

Technical Measures	Organizational Measures
Alarm-System	Key regulation and list
Automatic access control system	Reception and Porters
Biometric access locks	Visitor Book and log of visits
Chip cards/transponder systems	Careful selection of cleaning service
Manual locking system	Visitors accompanied by employees
Security locks	Careful selection of security staff
Locking system with code lock	
Doors with knob on the outside	
Doorbell system with camera	
Video surveillance of entrances	

- **Measures of access control of data processing systems**
  Access controls of data processing systems are measures that are suitable for preventing data processing systems from being used by unauthorized persons. Access control refers to the unauthorized prevention of the use of systems.

Technical Measures	Organizational Measures
Login with user name + password	Managing user authorization
Encryption of notebooks and tablets	Creating user profiles
Anti-virus software server	Central passwords assignment
Anti-Virus-software clients	„Secure Password“ policy
Anti-Virus-Software mobile devices	„Clean Desk“ policy
Firewall	„Delete/Destroy“ policy
Intrusion Detection Systems	„General Data Protection“ policy and/or “Security Policy”
Mobile Device Management	Mobile Device Policy
Use of VPN for remote access	
Encryption of data carries	

Automatic desktop lock

- **Measures for access control of personal data in data processing systems**
  Access controls of personal data in data processing systems are measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical Measures	Organizational Measures
File shredder (at least level 3, cross cut)	Use of authorization concepts
Logging of access to applications, specifically when entering, changing and deleting data	Access rights are not assigned directly, but the necessary rights groups are assigned to certain user groups
Physical deletion of data carriers	Minimum number of administrators
	Management of user rights by administrators

- **Measure of separation control**
  Separation controls are measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logically and physically separating the data.

Technical Measures	Organizational Measures
Separation of productive and test enviroment	Control via authorization concept
Physical separation (systems/databases/data carriers)	Definition of database rights
Multi-client capability of relevant applications	Categorization of data types

Pseudonymization

Pseudonymization is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organizational measures.

Organizational Measures
Internal instruction to anonymize/pseudonymize personal data wherever possible

Integrity

Integrity includes “transfer control” and “input control measures”.

- **Transfer Control**
  Transfer control means measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during their

transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

Technical Measures	Organizational Measures
E-Mail encryption	Disclosure in anonymized or pseudonymized form
Use of VPN	Overview of regular retrieval and transmission processes
Logging of accesses and retrievals	
Provision via encrypted connections connections such as sftp, https	

- **Input Control Measures**

  Input control refers to measures that ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed from data processing systems.

Technical Measures	Organizational Measures
Technical logging of the entry, modification and deletion of data	Overview of which programs can be used to enter, change or delete which data.
Manual or automated control of the logs	Clear responsibilities for deletions
	Assignment of rights for input, modification and deletion of data on the basis of an authorization concept
	Retention of forms from which data has been transferred to automated processing

Availability ans Resilience

- **Availability Control and Resilience Control**

  Availability control refers to measures that ensure that personal data is protected against accidental destruction or loss.

Technical Measures	Organizational Measures
Fire and smoke detection systems	Backup & recovery concept
Server room fire extinguisher	Control of the backup process
Server room monitoring temperature and humidity	Regular data recovery tests and logging of the results
Air-Conditioned server room	Storage of the backup media in a secure location outside the server room
UPS (Uninterruptible power supply	Separate partitions for operating systems and data

Protective socket strips Server room	Existence of an emergency plan
RAID system/hard disk mirroring	
Video surveillance server room	
Alarm message for unauthorized access to server room	

Procedures for regular review, assessment and evaluation

- **Data Protection Management**

Technical Measures	**Organizational Measures**
Software solutions for data protection management are in use	external Data Protection Officer Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 5 93047 Regensburg Tel.: 0941-298693-0 Fax: 0941-298693-16 Mail: info@projekt29.de Web: www.projekt29.de
Central documentation of all data protection procedures and regulations with access for employees as required/authorized	Employees trained and committed to confidentiality/data secrecy
Security certification according to ISO 27001	Regular sensitization of employees at least annually
A review of the effectiveness of the technical protective measures is carried out at least once a year	external Chief of Information Security Officer: Name / Firma Kontakt: Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 5 93047 Regensburg Tel.: 0941-298693-0 Fax: 0941-298693-16 Mail: info@projekt29.de Web: www.projekt29.de
	The data protection impact assessment (DPIA) is carried out if required
	The organization complies with the information obligations under Art. 13 and 14 GDPR

- **Incident-Response-Management**
  Support in responding to security breaches.

Technical Measures	Organizational Measures
Use of firewall and regular updating	Documented process for detecting and reporting reporting of security incidents/data mishaps (also with regard to reporting obligations to the supervisory authority)
Use of spam filters and regular updating	Documented procedure for Dealing with security incidents
Use of virus scanner and regular updating	Involvement of DPO and CISO in security incidents and data breaches
Intrusion Detection System (IDS)	Documentation of security incidents and data breaches, e.g. via ticket system
Intrusion Prevention System (IPS)	Formal process and responsibilities for the follow-up of security incidents incidents and data breaches

- **Privacy-friendly default settings**
  Privacy by design / Privacy by default.

Technical Measures
No more personal data is collected than it is necessary for the respective purpose

- **Order control (outsourcing to third parties)**
  Order control refers to measures that ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Organizational Measures
Prior examination of the safety measures the safety measures taken by the contractor measures taken by the contractor and their documentation
Selection of the contractor under due diligence (especially with regard to with regard to data protection and data security
Conclusion of the necessary agreement for order processing or EU standard
contractual clauses
Written instructions to the contractor
Obligation of the contractor's employees employees to maintain data secrecy
Obligation to appoint a data protection protection officer by the contractor if there is an obligation to appoint
Agreement of effective control rights vis-à-vis the contractor
Regulation on the use of further sub contractors

Ensuring the destruction of data after completion of the order

Crowdfox GmbH
Im Mediapark 8a
50670 Cologne
CEO: Dirk Schäfer

Contact:
+49 221 165359-38
professional@crowdfox.com
www.crowdfox.pro

Bank:
Commerzbank Bergisch Gladbach
IBAN: DE42370400440277726600
BIC: COBADEFFXXX

Tax Number: DE297246515
Local court: Cologne, HRB 81982
Regsitered Office:
Germany, Cologne

Annax 2: Subcontractors

The following subcontractors/Subprocessors may be commissioned by Crowdfox to process personal data in the Crowdfox customer's area of responsibility.

The purpose of the processing, the processing activity, the categories of data subjects and the categories of personal data are set out in the DPA, unless otherwise stated in this Annex.

Subcontractor/Subprocessor	**Adress**	**Context of Processing**
firstcolo GmbH	Kruppstraße 105, 60388 Frankfurt am Main	Provision of data centers, server hosting
Microsoft Ireland Operations Ltd.	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521, Ireland	Provision of data centers, server hosting
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy 1855 Luxembourg	Provision of data centers, server hosting