

Data Processing Agreement

The following Data Processing Agreement (DPA) within the meaning of Art. 28 (3) GDPR governs the obligations and rights under data protection law between

the controller (Art. 4 (7) GDPR) of data processing:

Name and address

Geb. got Game, Schreiner Str. 22 c/o wine&gut, 10247 Berlin

hereinafter referred to as the: controller

and the processor (Art. 4 (8) GDPR):

Startnext GmbH, represented by the managing director Mr Denis Bartelt, Grundstraße 1, D-01326 Dresden

hereinafter referred to as the: processor

in connection with the service contract [Data Privacy Statement](#). The content complies with the Commission's standard contractual clauses according to Art. 28 (6), (7) GDPR of 04.06.2021 (C 2021) 3701 final.

SECTION I

Clause 1: Purpose and scope

- a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.
- b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.
- c) These Clauses apply to the processing of personal data as specified in Annex II.
- d) Annexes I to IV are an integral part of the Clauses.
- e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2: Invariability of the Clauses

- a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3: Interpretation

- a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5: Docking clause

- a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6: Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7: Obligations of the Parties

7.1 Instructions

- a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

- a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Documentation and compliance

- a) The Parties shall be able to demonstrate compliance with these Clauses.
- b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.6 Use of sub-processors

- a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
- b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

- d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.7 International transfers

- a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8: Assistance to the controller

- a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - a. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - b. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - c. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - d. the obligations according to Article 32 Regulation (EU) 2016/679/..
- d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9: Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:
 - 1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 2. the likely consequences of the personal data breach;
 - 3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

in complying, pursuant to Article 34 Regulation (EU) 2016/679/, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- b) the details of a contact point where more information concerning the personal data breach can be obtained;
- c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /.

SECTION III – FINAL PROVISIONS

Clause 10: Non-compliance with the Clauses and termination

- a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

- b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
- the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I – LIST OF PARTIES

Controller: Starter

Processor: Startnext GmbH, Grundstraße 1, 01326 Dresden

Name, position and contact details of the contact person:

Tino Kreßner, Data Protection Coordinator, datenschutz@startnext.com

Name and contact details of the Data Protection Officer

Kemal Webersohn

WS Datenschutz GmbH, Dircksenstraße 51, 10178 Berlin

Telefon: 030 88 72 07 88

E-Mail: startnext@ws-datenschutz.de

ANNEX II – DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- Buyer (Supporter), Users

Categories of personal data processed

- First name, surname, address, e-mail address, IP address

Nature of the processing

- The type of processing is the collection and provision of personal data of supporters of the starter

Purpose(s) for which the personal data is processed on behalf of the controller

- The respective starter of a crowdfunding project is the client and concludes a contract with the contractor Startnext as part of the platform use of Startnext.com. The data is stored and processed

exclusively for the purposes resulting from the registration in compliance with the relevant statutory data protection provisions

Duration of the processing

- The information in the questionnaire refers to deletion periods, but the duration of the processing must also be specified.

ANNEX III – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Confidentiality (Art. 32 para. 1 lit. b GDPR)

Physical Access control

No unauthorized access to data processing facilities: electronic key system with logged issue and return, separate locking groups corresponding to established security zones, electric door openers, alarm system, data protection-compliant perimetry monitoring (video system).

All visitors are accompanied personally.

There is a regulated workflow for approving, managing and deleting access authorizations. The management or its representatives periodically (at least annually) check the necessity of access media for employees and initiate the necessary steps.

IT systems for the public provision of online platforms are operated exclusively in secure third-party data centers. In the case of data transfers to (sub-)processors, the specific technical and organizational measures that the (sub-)processor must take to support the controller must also be described.

Data Access control

No unauthorized system use: unique user IDs with secure passwords, IP blocking, encryption of data carriers. Further technical safeguards are provided by firewalls and proxy servers in the contractor's systems.

Availability control

No unauthorized reading, copying, modification or removal within the system: authorization concepts and needs-based access rights, logging of access.

Each employee may only access the systems necessary for his or her work and the required data with the authorization assigned to him or her.

All of the contractor's employees are subject to certain verification routines when they are hired and are bound in writing to data secrecy (GDPR) and confidentiality.

Separation control

Separate processing of data collected for different purposes: Separation of test and product systems, functional separation of test and production data, separation of data sets for other customers.

Pseudonymization and encryption (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

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

Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

No unauthorized reading, copying, modification or removal during electronic transmission or transport: encryption, virtual private networks (VPN), electronic signature, transport security (transmission protocol): TLS 1.2

The integrity of personal data during storage and transfer within the IT systems and IT applications is ensured by plausibility checks and/or verification procedures. Firewall systems and constantly updated virus software secure communication on the Internet in addition to Secure Socket Layer (SSL) encryption and the use of VPN technology.

Input control

Determining whether and by whom personal data has been entered, changed or removed from data processing systems: Logging, document management.

The strict implementation of the role concept means that each user only has the rights they need to carry out their work tasks. In addition, administrator access is documented as follows: SSH log and protocol data for administrator access via shell.

Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Availability control

Protection against accidental or willful destruction or loss: backup strategy, patch management; virus protection; firewall.

Maintenance and troubleshooting: regular maintenance of the production systems ensures high availability of the technical systems. This is ensured by appropriate service contracts

Data storage: redundant data storage on storage systems using RAID technology; creation of backups; secure storage of backup copies

Organizational measures: Emergency plans; implementation of emergency drills

Emergency power: essential systems are equipped with uninterruptible power supplies (UPS).

Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Order control

No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g: Clear contract design, formalized order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.

It is ensured in the IT systems that the data provided is only processed in accordance with the instructions of the respective client and in particular that it is not passed on to unauthorized third parties. The same applies to order-related information; this is only provided to the client or in accordance with the client's instructions

ANNEX IV – LIST OF SUB-PROCESSORS

The current list of sub-processors approved by the controller pursuant to section 7.6 a) is available und <https://www.startnext.com/about/terms-of-use/privacy.html>.

Insofar as the subcontracting and processing of data by one of the listed subprocessors is accompanied by a transfer of data by the subprocessor to a third country, the controller hereby issues the necessary instructions relating to the corresponding transfer process and the processing of the data by the subprocessor.

The requirements of Section 7.6 lit. a) apply to the amendment of the list of sub-processors.