Agreement on the processing of personal data in accordance with Art. 28 (3) of the EU-GDPR between

- Customer - and **- Contractor -**

Actionbound GmbH
Bahnhofstraße 82
82383 Hohenpeißenberg
Germany

§ 1 Scope, duration and specification of contract processing of Data

The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the following Data:

Nr	Purpose	Data subjects	Data categories	Recipients	Transfers to a third country	Limits for erasure
1	Account creation	a) Customers b) Bound creator c) Bound player	Email address, user names (or pseudonym)	Financial accounting, Sales, Support	Not intended	upon termination of the account, upon revocation, upon instruction

2	Usage of Software, Creation of Bound	Bound creator	Login data, if applicable: media data, data of users or creators voluntarily entered by the creator	Support, Bound creator, Bound player	Not intended	upon termination of the account, upon revocation, upon instruction
3	Usage of the app and Bounds	a) Bound creator b) Bound player	E-mail address (voluntary), Data provided by the Bound creator, media (image, sound), geodata	Support, Bound creator, Bound player	Not intended	upon termination of the account, upon revocation, upon instruction
4	Evaluation and provision of game results	Bound player	E-mail address (voluntary), Data provided by the Bound player, media (image, sound)	Support, Bound creator, Bound player	Not intended	upon termination of the account, upon revocation, upon instruction
5	Log files for system monitoring, prevention of abuse	Website visitors, App user	IP address	Administration	Not intended	1 week

Except where this annex stipulates obligations beyond the term of the Agreement, the term of this annex shall be the term of the Agreement.

§ 2 Scope of application and responsibilities

(1) Supplier shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Within the scope of this annex, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(2) Company's individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Company shall, subsequently, be entitled to, in writing or in a machine-readable format, modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Company shall, without undue delay, confirm in writing or in text form any instruction issued orally.

§ 3 Supplier's obligations

(1) Except where expressly permitted by Article 28 (3)(a) of the GDPR, Supplier shall process data subjects' Data only within the scope of the statement of work and the instructions issued by Company. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

(2) Supplier shall, within Supplier's scope of responsibility, organise supplier's internal organisation so it satisfies the specific requirements of data protection. Supplier shall implement technical and organisational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organisational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk.

With regard to compliance with the protective measures and safeguards agreed upon and their verified effectiveness, parties refer to the implemented appropriate technical and organisational measures as proof of the appropriate guarantees, as documented in exhibit 1 hereto.

Supplier reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

(3) Supplier shall support Company, insofar as is agreed upon by the parties, and where possible for Supplier, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR. The parties are free to agree upon a remuneration for such support in the agreement.

(4) Supplier warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is

subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
(5) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility.
Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.
(6) Supplier shall notify to Company the point of contact for any issues related to data protection arising out of or in connection with the Agreement.
(7) Supplier warrants that Supplier fulfills its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
(8) Supplier shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Supplier shall, based on Company's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Company. The parties are free to agree upon a remuneration for such support in the agreement.
In specific cases designated by Company, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement. The parties are free to agree upon a remuneration for such support in the agreement.
(9) Supplier shall, upon termination of Contract Processing and upon Company's instruction, return all Data, carrier media and other materials to Company or delete the same. In case of testing and discarded material no instruction shall be required. Company shall bear any extra cost caused by deviating requirements in returning or deleting data.
(10) Where a data subject asserts any claims against Company in accordance with Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible. The parties are free to agree upon a remuneration for such support in the agreement.

§ 4 Company's obligations

(1) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.

(2) Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with Article 82 of the GDPR. The parties are free to agree upon a remuneration for such support in the agreement.
(3) Company shall notify to Supplier the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

§ 5 Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction insofar as agreed upon. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Options for documentation

(1) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this exhibit by appropriate measures. Company and Supplier agree that proof has been produced by exhibit 1: implemented list of appropriate technical and organisational measures acc. to Art. 32 GDPR.
(2) Where, in individual cases, audits and inspections by Company or an auditor appointed by Company are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Supplier's operations, upon prior notice, and observing an appropriate notice period. Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Supplier shall be entitled to rejecting auditors which are competitors of Supplier.
(3) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7 Subcontractors

(1) Company hereby consents to Supplier's use of subcontractors 1&1 Internet SE; Amazon Web Services, Inc.; Google LLC. Supplier shall, prior to the use or replacement of subcontractors, inform Company thereof.
Company shall be entitled to contradict any change notified by Supplier within a reasonable period of time and for materially important reasons. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists, and failing an amicable resolution of this matter by the parties, Company shall be entitled to terminating the Agreement.
(2) A subcontractor relationship shall be subject to such consent of Supplier commissioning further supplier or subcontractors with the performance agreed upon in the Agreement, in whole or in part. Supplier shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.
(3) Where Supplier commissions subcontractors, Supplier shall be responsible for ensuring that Supplier's obligations on data protection resulting from the Agreement and this exhibit are valid and binding upon subcontractor.

§ 8 Obligations to inform, mandatory written form, choice of law

(1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the GDPR.
(2) No modification of this annex and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(3) In case of any conflict, the data protection regulations of this annex shall take precedence over the regulations of the original Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.
(4) This annex is subject to the laws of Germany.

§ 9 Liability and damages

Company and Supplier shall be liable to data subject in accordance with Article 82 of the GDPR. The regulations on the parties' liability contained in the Agreement shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.

Date _____

Signatures

_____

Simon Zwick

Exhibit 1: list of appropriate technical and organisational measures acc. to Art. 32 GDPR
Exhibit 2: list of approved Subcontractors

Documentation of the technical and organizational measures for data protection compliance

Actionbound GmbH, henceforth called “Actionbound”

Physical Access Control

Prevent unauthorized persons from gaining access to the data processing systems.

Regarding the premises where data is processed, it is necessary to distinguish between the data centers and the corporate office.

Data Centers
The data centers are operated by Hetzner Online GmbH, 1&1 Internet SE and Amazon Webservices, Inc.. Amazon Web Services is contractually obligated to process all data at the data processing centering in the Frankfurt am Main metropolitan area. The data center operators each have an agreement for order data processing.
Access to the data centers is secured by the operators of the data centers. The normal, high standards of access control for industrial data processing have been contractually guaranteed and was considered when service providers were selected. Documentation can be provided by Actionbound as requested.

Corporate Office
The corporate office are the rooms used as the Berlin office and Hohenpeißenberg headquarters of Actionbound. Individual associates who have proven themselves to be especially trustworthy are also permitted to work from other locations (e.g. while on a business trip). Associates in managerial positions, who have proven to be especially reliable, have also been permitted to work in a lockable home office on a case-by-case basis. All employees are obliged in writing to maintain confidentiality and to comply with the data protection requirements under the General Data Protection Regulation. It has been ensured through a directive to all associates that the corporate office may not contain any unencrypted organizational or customer data, nor may any organizational or customer data be taken out of the corporate office.

For this reason, there is also no requirement for special access control at the corporate offices. The security measures employed are standard for commercial spaces, e.g. a locked door with a key registry and security shutters.

Logical Access Control

Prevent unauthorized persons from using data processing systems.

Data Centers
The servers in the data center store both organizational and customer data centrally. Access control to these servers is therefore of particular importance.

The servers in the data centers can be administered with corresponding user accounts. The administration of the servers takes place via the internet, using an encrypted protocol with access via 4096 bit RSA keys. These keys are known only to the management and are changed regularly.

Associates' Computers
Access to associates' computers is controlled via user accounts. Every associate has an individual user account both for their local computer and for the administrative software, with which controlled access to user and organizational data is possible in a customer support context (see data access control). Employees are obliged to use passwords as recommended by the Federal Office for Information Security. The transmission between the data centers to the employees' computers is encrypted.

Data Access Control

Ensure that only authorized persons can access data, and that the data may not be read, changed, copied, or deleted without authorization.

Access to customer data is only possible for trained associates in the sales, accounting, and support departments, as well as for the management. This is ensured by the special allocation of authorizations by the management to the employees.

Actionbound has a written agreement with each associate that ensures that data will not be read, copied, changed, or removed without authorization.

Data Transfer Control

Ensure that data cannot be read, copied, changed, or deleted in the process of transmission/ transport.

Actionbound ensures data transfer control through the storage location of customer and organizational data in data centers, as well as through restrictions on access to this storage location. Unauthorized reading, copying, changing, or deleting of data saved in the data center by the operators of the data center is contractually excluded. For the purposes of transmission data are encrypted, as is discussed above, under Data Access Control.

Data Entry Control

Ensure that it is possible to retrospectively determine whether data was changed or deleted, as well as who changed or deleted it.

To ensure the data entry control, associates' actions in the customer administration is protocolled. The data from this protocol can be used at any time to determine which associate undertook each entry or change. Duplicates of the log file are backed up geo-redundantly.

Control of Processing Instructions

Ensure that data that are processed on contract can only be processed in accordance with the instructions of the contractee

A written contract with all data processors ensures that order data processing occurs only in accordance with Actionbounds' instructions. Use or transfer of the data by associates of the data processing center is contractually excluded.

Availability Control

Ensure that data are protected from accidental destruction or loss.

The availability of data is ensured using a multi-layered security concept. The first layer is the server itself, which is equipped with mirroring hard-drives (RAID). There is therefore no data loss when one hard drive fails. Defective hard drives can be exchanged without disrupting service using a so-called “Hot-Plug” system. The status of the RAID system is observed regularly and the operators of the data center are commissioned with the replacement of a hard drive in the case of a disruption.

The second layer is that the data are also held on a second server at the data processing center, so that access is ensured in the case of disruption of the primary server.

As a third security level, the data is compressed daily and encrypted according to the established state of the art and transferred to a separate, spatially separate backup data center.

The data center offers fully airconditioned security rooms that offer protection from gas, water, and fire. The additional storage location in a back-up data center ensures that data will not be compromised even in the event of the most significant accidents that might be anticipated, e.g. the crash of an airplane into the first data center.

Separation Control

Ensure that data stored for different purposes are processed separately.

Data that are stored for different purposes (e.g. licenses, Bound creations, Bound results) are saved in different data bases . The test, quality assurance and production systems run on different instances with completely completely separate databases. The databases are logically separated from the application layer. The synchronization of the databases is ensured by replication.

Approved subcontractors

Actionbound GmbH commissions the following subcontractors under the condition of a contractual agreement according to Art. 28 par. 2 - 4 EU-DSGVO.

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
DE-GermanyDeutschland
(Datacenter Nürnberg and Falkenstein)

1&1 IONOS SE
Elgendorfer Str. 57
56410 Montabaur
DE-Germany
(Datacenter Karlsruhe)

AWS EMEA SARL
38 avenue John F. Kennedy,
L-1855 Luxembourg
(Datacenter Frankfurt am Main)

Document Status: 29.03.2023