Annex to the GTC
"mobivention prediction game for companies"

on data processing within the meaning of Art. 28 para. 3 of the General Data Protection Regulation (GDPR).

Preamble
This annex specifies the obligations of the contracting parties to data protection, which result from the GTC of 4 August 2025 in their details described order processing. It applies to all activities related to the contract and in which employees of the Contractor or persons authorised by the Contractor process personal data ("data") of the Client.

§ 1 Subject matter, duration and specification of the commissioned processing
The subject matter and duration of the contract as well as the type and purpose of the processing are specified in the contract. In particular, the following data are part of the data processing:

- Type of data: Surname, first name, user name, email address, tips on the matches of the 2026 FIFA Men's World Cup, championship tip, bonus questions, points for the tips and display in the ranking, activation of tip reminder, consent to the use of the email address for marketing purposes (only if the option is activated for public prediction games for use by clients), personal number (optional for upload in private prediction games)
- Type and purpose of data processing: Participation in the Prediction Game for companies
- Categories of data subjects: Depending on how the Prediction Game is organised, the data subjects may include employees, external parties (e.g. customers, suppliers, etc.) or both groups.

The term of this appendix is based on the term of the contract, unless the provisions of this appendix impose additional obligations.

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.

§ 2 Scope of application and responsibility
(1) The Contractor shall process personal data on behalf of the Client. This includes activities that are specified in the contract and in the service description. Within the scope of this contract, the Client is solely responsible for compliance with the statutory provisions of data protection laws, in particular for the lawfulness of data transfer to the Contractor and for the lawfulness of data processing ("controller" within the meaning of Art. 4 No. 7 GDPR).

(2) The instructions shall initially be set out in the contract and may subsequently be amended, supplemented or replaced by the Client in writing or in an electronic format (text form) to the body designated by the Contractor by means of individual instructions (individual instruction). Instructions that are not provided for in the contract shall be treated as a request for a change in performance. Verbal instructions must be confirmed immediately in writing or in text form.

§ 3 Obligations of the Contractor
(1) The Contractor may only process data of data subjects within the scope of the order and the instructions of the Client, unless there is an exceptional case within the meaning of Article 28 para. 3 a) GDPR. The Contractor shall inform the Client immediately if it is of the opinion

that an instruction violates applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Client.

(2) The Contractor shall design the internal organisation in its area of responsibility in such a way that it meets the special requirements of data protection. It shall take technical and organisational measures for the appropriate protection of the Client's data that meet the requirements of the General Data Protection Regulation (Art. 32 GDPR). The Contractor shall take technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing in the long term. The client is aware of these technical and organisational measures and is responsible for ensuring that they offer an appropriate level of protection for the risks of the data to be processed.

The Contractor reserves the right to change the security measures taken, although it must be ensured that the contractually agreed level of protection is not fallen short of.

(3) The Contractor shall support the Client within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set out in Art. 33 to 36 GDPR.

(4) The Contractor warrants that the employees involved in the processing of the Client's data and other persons working for the Contractor are prohibited from processing the data outside of the instructions. Furthermore, the Contractor warrants that the persons authorised to process the personal data have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality. The duty of confidentiality/secrecy shall continue to exist even after termination of the order.

(5) The Contractor shall inform the Client immediately if it becomes aware of any breaches of the protection of the Client's personal data.

The Contractor shall take the necessary measures to secure the data and to minimise possible adverse consequences for the persons concerned and shall immediately consult with the Client in this regard.

(6) The Contractor shall inform the Client of the contact person for data protection issues arising within the scope of the contract.

(7) The Contractor warrants to comply with its obligations under Art. 32 para. 1 lit. d) GDPR to implement a procedure to regularly review the effectiveness of the technical and organisational measures to ensure the security of the processing.

(8) The Contractor shall rectify or erase the contractual data if instructed to do so by the Client. If deletion in compliance with data protection regulations or a corresponding restriction of data processing is not possible, the Contractor shall undertake the destruction of data carriers and other materials in compliance with data protection regulations on the basis of an individual order by the Client or shall return these data carriers to the Client, unless already agreed in the contract.

In special cases to be determined by the Client, storage or handover shall take place; remuneration and protective measures for this shall be agreed separately, unless already agreed in the contract.

(9) Data, data carriers and all other materials must either be returned or deleted at the request of the client after the end of the order. If additional costs are incurred due to deviating specifications for the return or deletion of the data, these shall be borne by the client.

(10) In the event of a claim against the Client by a data subject with regard to any claims under Art. 82 GDPR, the Contractor undertakes to support the Client in the defence of the claim within the scope of its possibilities.

§ 4 Obligations of the client
(1) The Client shall inform the Contractor immediately and in full if it discovers errors or irregularities in the results of the order with regard to data protection regulations.

(2) In the event of a claim against the Client by a data subject with regard to any claims under Art. 82 GDPR, Section 3 (10) shall apply accordingly.

(3) The Client shall inform the Contractor of the contact person for data protection issues arising within the scope of the contract.

§ 5 Enquiries from data subjects
(1) If a data subject contacts the Contractor with requests for rectification, erasure or information, the Contractor shall refer the data subject to the Client, provided that the data subject can be assigned to the Client according to the information provided by the data subject. The Contractor shall forward the data subject's request to the Client without delay. The Contractor shall support the Client within the scope of its possibilities upon instruction. The Contractor shall not be liable if the request of the data subject is not answered by the Client, is not answered correctly or is not answered on time.

§ 6 Possibilities of proof
(1) The Contractor shall provide the Client with evidence of compliance with the obligations set out in this contract by suitable means.

(2) Should inspections by the Client or an inspector commissioned by the Client be necessary in individual cases, these shall be carried out during normal business hours without disrupting operations after notification, taking into account a reasonable lead time. The Contractor may make this dependent on prior notification with a reasonable lead time and on the signing of a confidentiality agreement with regard to the data of other customers and the technical and organisational measures that have been put in place. If the auditor commissioned by the Client is in a competitive relationship with the Contractor, the Contractor shall have the right to object to this.

(3) Should a data protection supervisory authority or another sovereign supervisory authority of the client carry out an inspection, paragraph 2 shall apply accordingly. It is not necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality where a breach is punishable under the German Criminal Code.

§ Section 7 Subcontractors (other processors)
(1) The use of subcontractors as additional processors is permitted if the client has been informed and has not objected.

(2) A subcontractor relationship requiring consent exists if the Contractor commissions other contractors to perform all or part of the services agreed in the contract. The Contractor shall enter into agreements with these third parties to the extent necessary in order to ensure appropriate data protection and information security measures.

The contractually agreed services or the partial services described below will be carried out with the involvement of the following subcontractors:

Name and address of the subcontractors / description of the partial services:

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen / Hosting of the data on cloud servers in Nuremberg or Falkenstein, Germany

- IONOS SE Elgendorfer Str. 57 56410 Montabaur / of the data on cloud servers in Frankfurt / Main area, Germany
- Mailjet SAS, 4 rue Jules Lefebvre, 75009 Paris, France / Email service for welcome emails, registration confirmations and typing reminders

The client authorises the contractor to use subcontractors. If subcontractors are engaged or replaced, the Contractor shall inform the Client by e-mail and by publishing the information at the following link: https://tippspiel-fuer-unternehmen.com/Dokumente/AVV.pdf.

The client may object to the change - within a reasonable period of time - for good cause - to the office designated by the client. If no objection is made within the deadline, consent to the change shall be deemed to have been given. If there is an important reason under data protection law and if it is not possible for the parties to reach an amicable solution, the Client and the Contractor shall be granted a special right of cancellation.

(3) If the Contractor places orders with subcontractors, it shall be incumbent on the Contractor to transfer its data protection obligations under this contract to the subcontractor.

§ 8 Duty to inform, written form clause, choice of law

(1) Should the Client's data be jeopardised by seizure or confiscation, by insolvency or composition proceedings or by other events or measures by third parties, the Contractor shall inform the Client of this immediately. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the "controller" within the meaning of the General Data Protection Regulation.

(2) Amendments and supplements to this Annex and all its components - including any assurances made by the Contractor - require a written agreement, which may also be made in an electronic format (text form), and an express reference to the fact that it is an amendment or supplement to these Terms and Conditions. This also applies to the waiver of this formal requirement.

(3) In the event of any contradictions, the provisions of this appendix on data protection shall take precedence over the provisions of the contract. Should individual parts of this Annex be invalid, this shall not affect the validity of the rest of the Annex.

(4) German law shall apply.

§9 Liability and compensation

A liability provision agreed between the parties in the service contract (main contract for the provision of services) also applies to commissioned processing, unless expressly agreed otherwise).

Annex on technical and organisational measures in accordance with Art. 32 GDPR

Security and data protection play an important role for us at all levels. This applies both within the company and in backend and frontend development.

It goes without saying that data communication takes place exclusively via HTTPS encryption. Security-relevant data is only stored locally in encrypted form. The level of security used in each case always depends on the application and the individual protection needs of the customer and the user and can be discussed and realised individually.

The requirements and measures to fulfil these are described in detail below.

1. access control

1.1 Requirement:
Unauthorised persons must be denied access to data processing systems that are used to process personal data.

1.2 Measures:

- Door key with electronic chip
- Keys only issued against signature and only to permanent employees
- Locked doors and windows
- Logging of entries and exits in the computer rooms
- Visitor regulations
- Access control for external persons

2. access control

2.1 Requirement:
Data processing systems must be prevented from being used by unauthorised persons.

2.2 Measures:

- Access to servers only with authorised SSH keys, workstations are password-protected
- Logging of access to the IT system that operates the app
- Implementation of user administration including rights assignment in accordance with the client's role and rights concept. Passwords are always stored in encrypted form (bcrypt)
- Data carriers are encrypted according to the state of the art

3. transfer control

3.1 Requirement:
It must be ensured that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which bodies personal data is intended to be transmitted by data transmission facilities.

Personal data may not be disclosed to third parties without authorisation. Accidental disclosure to unauthorised third parties must be ruled out.

3.2 Measures:

- Encrypted data transfer (SSH and VNC)
- Communication between the app and the server backend is only transport-encrypted (SSL)
- Password request according to password policy
- Data protection-compliant deletion
- Use of up-to-date antivirus software
- Logging of data connections

4. input control

4.1 Requirement:
It must be ensured that it is subsequently possible to check and determine whether and by whom personal data has been entered into, changed or removed from data processing systems.

4.2 Measures:

- Identification and authentication of authorised persons
- Logging of accesses and changes
- Regular evaluation of the logs (random checks)

5. order control

5.1 Requirement:
It must be ensured that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

5.2 Measures:

- Identification and authentication of authorised persons
- Logging of actions
- Verification by means of audits
- Regular evaluation of the logs (random checks)

6. availability control

6.1 Requirement:
It must be ensured that personal data is protected against accidental destruction or loss.

6.2 Measures:

- Daily backup of the databases
- Use of cloud infrastructure to ensure smooth operation and to be able to react quickly to possible failures
- Use of redundant hardware
- Mirroring of servers

- Protection of servers by means of UPS, firewall, etc.
- Disaster prevention & recovery plan with regular audits and exercises

7. separation control

7.1 Requirement:
It must be ensured that data collected for different purposes can be processed separately.

7.2 Measures:

- Separation of the client's data from the contractor's data and other clients
- Strict separation of test and live system