

DATA SHARING AGREEMENT

(Between Independent Data Controllers for Alternative Dispute Resolution)

This Data Sharing Agreement ("Agreement") is made and entered into on 03.06.2026

("Effective Date") by and between:

- (1) Promotech N.V., a company incorporated in Curaçao, company number 165167 whose registered address is at Seru Loraweg 17 C, Curaçao, incorporated 06.10.2023 (the "Operator").
- (2) EGIS – FZCO, a company incorporated in Dubai with trade licence number 22105 whose registered address is at Unit 22105-001, IFZA Business Park, DDP, Dubai, United Arab Emirates (the "Provider").

EGIS – FZCO and Promotech N.V. are hereinafter jointly referred to as the "Parties" and each individually as a "Party".

1. PURPOSE AND SCOPE

1.1. The purpose of this Agreement is to set out the terms and conditions under which the Parties, acting as independent Data Controllers, share and process certain categories of personal data for the purpose of facilitating, managing, and resolving disputes through alternative dispute resolution (ADR) mechanisms related to gaming, betting, and associated services provided by Operator and/or its partners.

1.2. Each Party acts as a separate and independent Controller with respect to any Personal Data it processes under this Agreement. The Parties do not act as joint controllers, and neither Party shall process personal data on behalf of the other.

2. DEFINITIONS

The terms used in this Agreement shall have the following meanings:

- "Applicable Laws" means the EU General Data Protection Regulation (2016/679), relevant Member State laws implementing it, and any other applicable data protection legislation.
- "Personal Data", "Processing", "Controller", "Data Subject", and "Supervisory Authority" have the meanings given in the GDPR.
- "Dispute Data" means any Personal Data exchanged between the Parties in the context of ADR procedures.

- “Personal Data Breach” means any unauthorized or unlawful processing, access, loss, or destruction of shared Personal Data.
- “Restricted Transfer” means a transfer of Personal Data to a third country outside the EEA not covered by an adequacy decision.

3. PRINCIPLES AND LAWFULNESS

3.1. Each Party shall determine and document its own lawful basis for processing under Article 6 (and, if applicable, Article 9) GDPR.

3.2. Each Party shall ensure transparency towards Data Subjects, including notification that Personal Data may be shared with another controller for ADR purposes.

3.3. The Parties shall share Personal Data in a manner consistent with data minimization, accuracy, and purpose limitation principles.

4. DATA SHARING ARRANGEMENTS

4.1. The Parties agree to share only the minimum amount of Personal Data necessary for the ADR purpose.

4.2. Categories of Personal Data that may be shared include, but are not limited to:

- Basic identification data (name, surname, username, country of registration);
- Contact details (email address, phone number);
- Account and transaction data related to the dispute (betting or gaming history, payments, timestamps, device data, etc.);
- Correspondence and complaint-related communication;
- Outcome or resolution data of the ADR process.

4.3. The Parties agree to use Personal Data exclusively for the ADR process and not for any secondary or incompatible purpose.

4.4. The Parties agree to exchange data using secure transmission channels, including encrypted communication or VPN tunnels, and to maintain an audit trail of all exchanges.

4.5. The scope, purpose, and duration of processing are described in Annex I.

5. SECURITY AND CONFIDENTIALITY

5.1. Each Party shall implement appropriate technical and organizational measures to protect Personal Data shared under this Agreement, ensuring a level of security appropriate to the risk, as required under Article 32 GDPR.

5.2. Such measures shall include, at a minimum:

- encryption and pseudonymization of transferred data;
- strict access control and authentication;
- audit logging of access and modification;
- secure data transmission protocols;
- confidentiality obligations for staff involved in ADR processing.

5.3. Agreed measures are listed in Annex II.

6. DATA SUBJECT RIGHTS

6.1. Independent responsibility.

Each Party is independently responsible for fulfilling its own obligations as a Data Controller in relation to Data Subject rights under Articles 12–23 GDPR, including the right of access, rectification, erasure, restriction, portability, objection, and rights related to automated decision-making.

6.2. Misrouted requests.

If either Party receives a Data Subject Request (“DSR”) that wholly or mainly concerns data controlled by the other Party, it shall:

- forward the request to the appropriate Party without undue delay and no later than five (5) business days from receipt; and
- inform the Data Subject that the request has been redirected and provide the relevant contact details of the receiving Party.

6.3. Cooperation in complex cases.

Where handling a DSR requires information held by the other Party, both Parties shall cooperate in good faith and exchange only the minimum information necessary to respond.

- Preliminary acknowledgement between Parties: within 5 business days.
- Full provision of relevant extracts or metadata (logs, account data, transaction references, ADR case identifiers): within 10 business days, if technically feasible.

6.4. Response timeframe to the Data Subject.

Each Party shall respond to the Data Subject without undue delay and in any event within one (1) month of receipt of the request.

Where necessary due to complexity or volume, this period may be extended by up to two (2) additional months in accordance with Article 12(3) GDPR, with notification to the Data Subject of the reasons for delay.

6.5. Access (Art. 15) and Portability (Art. 20).

Each Party shall, where applicable, provide:

- confirmation as to whether personal data concerning the individual are being processed;
- categories of data, purposes, recipients, and retention criteria;
- a copy of the personal data being processed; and
- for portability, data in a structured, commonly used, machine-readable format, to the extent technically feasible and without adversely affecting the rights and freedoms of others.

6.6. Rectification, erasure, and restriction (Arts. 16–18).

- Where accuracy of data is contested, the relevant Party shall restrict processing for verification.
- Deletion shall not apply insofar as retention is necessary for the establishment, exercise, or defence of legal claims, or for compliance with a legal obligation within the ADR framework; in such cases, processing shall be limited (“restriction mode”).

6.7. Objection (Art. 21) and automated decision-making (Art. 22).

- Data Subjects may object to processing based on legitimate interests. The Party shall cease such processing unless it demonstrates compelling legitimate grounds overriding the interests of the Data Subject (including necessity for ADR proceedings).
- No solely automated decisions producing legal or similarly significant effects are made within ADR processes unless accompanied by appropriate safeguards as required by the GDPR.

6.8. Verification and logging.

Each Party shall take reasonable steps to verify the identity and authority of Data Subjects or authorised representatives before fulfilling requests.

Each Party shall maintain a log of DSRs, including date, nature of request, decision, and time to completion.

6.9. Supervisory Authority communication.

If either Party is contacted by a Supervisory Authority in relation to a Data Subject’s complaint or request relevant to this Agreement, the Parties shall cooperate in good faith and share relevant information to ensure consistency and compliance.

6.10. Contact points.

Each Party shall maintain a dedicated contact channel (email or portal) for Data Subject Requests and complaints and notify the other Party of any change without undue delay.

Contact points are listed in Annex I.

7. PERSONAL DATA BREACH

7.1. Each Party shall notify the other without undue delay (and no later than 48 hours) after becoming aware of any Personal Data Breach affecting data shared under this Agreement.

7.2. The Parties shall cooperate in good faith in assessing, mitigating, and documenting the breach and in fulfilling any reporting or notification obligations to Supervisory Authorities or affected Data Subjects.

8. INTERNATIONAL DATA TRANSFERS

8.1. Where Personal Data is transferred outside the EEA, the transferring Party shall ensure that an adequate safeguard under Chapter V of the GDPR applies, including Standard Contractual Clauses or an adequacy decision.

8.2. No data shall be transferred to a jurisdiction lacking adequate data protection guarantees without prior written agreement between the Parties.

9. RETENTION AND DELETION

9.1. Each Party shall retain shared Personal Data only for as long as necessary to fulfil the ADR purpose and comply with legal or regulatory obligations.

9.2. Upon completion of the ADR process or expiry of retention periods, each Party shall securely delete or anonymize the data.

10. COOPERATION AND ACCOUNTABILITY

10.1. The Parties shall cooperate as reasonably necessary to ensure compliance with the GDPR, including in relation to audits, DPIAs, or investigations by Supervisory Authorities.

10.2. Neither Party shall be responsible for any acts or omissions of the other in relation to the processing of Personal Data, except to the extent caused by its own breach of this Agreement or the GDPR.

11. GOVERNING LAW AND DISPUTE RESOLUTION

11.1. This Agreement shall be governed by and construed in accordance with the laws of a Member State of the European Union - Cyprus.

11.2. Any disputes arising out of or in connection with this Agreement shall be resolved through amicable negotiation, and if not possible, through alternative dispute resolution mechanisms agreed upon by the Parties.

12. TERM AND TERMINATION

12.1. This Agreement shall enter into force on the Effective Date and remain in effect for as long as the Parties exchange Personal Data for the ADR purpose.

12.2. Either Party may terminate this Agreement upon thirty (30) days' written notice. Upon termination, all shared data shall be deleted or anonymized unless retention is required by law.

13. MISCELLANEOUS

13.1. No provision of this Agreement creates a joint controllership or processor relationship.

13.2. This Agreement constitutes the entire understanding between the Parties and supersedes any prior arrangements relating to the same subject matter.

13.3. Amendments to this Agreement must be made in writing and signed by both Parties.

Signed by (SMES) Solutions for
Management and Employment
Support N.V.

By: Vivian Victoria Ersilia

For and on behalf of (**Operator**)



Signed by **Hazem Eldine** for and on
behalf of EGIS - FZCO (**Provider**)

H Eldine

Director

Date: 03.06.2026

ANNEX I — DETAILS OF DATA SHARING

Field	Description
Purpose of Processing	Management and resolution of disputes (ADR) related to gaming/betting services
Categories of Data Subjects	Players, complainants, claimants, and related account holders
Types of Personal Data	Identification, contact, transactional, communication, and resolution data
Legal Basis	Legitimate interests (Art. 6(1)(f) GDPR) and contractual necessity (Art. 6(1)(b))
Frequency of Data Sharing	On a case-by-case basis as disputes arise
Retention Period	Duration of ADR + 12 months
Security Measures	Encryption, pseudonymization, role-based access, audit logs, secure transfer
Transfer Mechanism	SCCs or equivalent under Chapter V GDPR, if applicable

Signed by (SMES) Solutions for
Management and Employment
Support N.V.

By: Vivian Victoria Ersilia

For and on behalf of (**Operator**)



Signed by **Hazem Eldine** for and on
behalf of EGIS - FZCO (**Provider**)

H Eldine
.....

Director

Date: 03.06.2026

ANNEX II — SECURITY MEASURES

1. Access control: Users access only data necessary for ADR case handling; privileged rights are restricted and reviewed quarterly.
2. Encryption: All Personal Data is encrypted in transit (TLS 1.3) and at rest (AES-256).
3. Logging and monitoring: System and access logs are retained for a minimum of 12 months and regularly reviewed.
4. Incident management: Breaches or suspected incidents are reported within 48 hours; records maintained.
5. Supplier oversight: Third-party ADR platforms, if used, must ensure equivalent security controls.
6. Data backup and deletion: Secure backups maintained; automated deletion after retention period.

Signed by (SMES) Solutions for
Management and Employment
Support N.V.

By: Vivian Victoria Ersilia

For and on behalf of (**Operator**)



Signed by **Hazem Eldine** for and on
behalf of EGIS - FZCO (**Provider**)

H Eldine
.....

Director

Date: 03.06.2026