



Data Protection Policy

Evoplay Entertainment B.V.

DATA PROTECTION POLICY

1. THE INTRODUCTION.

This Privacy Policy (hereinafter the "Policy") establishes the rules of Evoplay Entertainment B.V., the company incorporated in Curaçao, with its registered number 146580, with its registered address at Fransche Bloemweg 4, Willemstad, Curacao (hereinafter the "Company", "We", "Us", "Our") in relation to the processing of personal data. All other documents on the processing of personal data shall be compliant with this Policy.

For the purposes of this Policy, the word "data" shall also mean "personal data" as defined by Article 4(1) of the GDPR, unless the context means otherwise.

The Company's EU company is Evoplay Entertainment LTD, the company incorporated in the Republic of Cyprus, with its registered number HE 406912, with its registered address at Spyrou Kyprianou, 79, Protopapas bldg., 2nd floor, Flat/Office 201, Limassol, Cyprus, 3076 (hereinafter the "EU Company").

2. LEGAL BASES OF THIS POLICY.

This Policy has been prepared in compliance with the following:

Legal documents:

- ✓ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the "GDPR");
- ✓ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "Directive 95/46/EC");
- ✓ Article 29 Working Party/European Data Protection Board (hereinafter the "EDPB") guidelines and opinions (whichever is more actual) relating to the interpretation of the GDPR and Directive 95/46/EC;
- ✓ Rulings or decisions of the Court of Justice of the European Union relating to the interpretation of the GDPR and Directive 95/46/EC.

Other documents and materials:

- ✓ A Guide to Privacy by Design of the Spanish data protection supervisory authority: Agencia Española de Protección de Datos (AEPD);
- ✓ Privacy by Design, The 7 Foundational Principles by Ann Cavoukian;

- ✓ Teletrust and ENISA Guideline "State of Art" on the technical and organisational measures under Article 32 of the GDPR (hereinafter the "Teletrust Guideline").

All the terms and definitions used in this Policy shall correspond to the meanings given to them in the documents and materials specified in this Provision.

3. PERSONAL DATA PROCESSING PRINCIPLES.

The Company processes personal data in accordance with the Principles enshrined in Article 5(1) of the GDPR.

The Principles under Article 5(1) of the GDPR and the ways of their delivery	
The Principle	How the Principle is delivered
The Principle of lawfulness, fairness and transparency.	✓ Publication and making available of Privacy Policies/Notices under Articles of 13/14 of the GDPR. ✓ Exercise of data subjects' rights.
The Principle of Purpose Limitation.	The management of data processing activities.
The Principle of Data Minimisation.	
The Principle of Storage Limitation.	
The Principle of Integrity and Confidentiality.	✓ Bringing the Company into compliance with Teletrust Guideline; ✓ Privacy by Design and by Default; ✓ Implementation of Information Security Policies.

4. PUBLICATION OF PRIVACY POLICIES UNDER ARTICLES 13/14 OF THE GDPR.

4.1. Privacy Policies for job candidates and employees of the Company.

For the processing of job candidates' personal data, the Candidate Privacy Policy applies. Each candidate can observe a copy of the Candidate Privacy Policy before the submission of his or her job application to the Company.

If a job candidate is hired to a position, his or her personal data collected under the Candidate Privacy Policy is retained by the Company as a part of his or her employee records. In other cases, the candidate's data are deleted, unless either he or she has given a consent under Article 6(1)(a)

of the GDPR for further processing or (in some rare cases) the data shall be stored for protection from the former candidate's claims.

For the processing of personal data of employees, the Employee Privacy Policy is applied. Each employee of the Company can observe the Employee Privacy Policy in the Company's Wiki.

4.2. Privacy Policies for the Players of the Company's Games.

The Company publishes the Games Privacy Policy in the interface of the Games.

4.3. Privacy Policies for the employees and representatives of the Company's Counterparties.

The Counterparties of the Company are solely responsible for notification of its employees and representatives about the processing of personal data by the Company. This is achieved by proper contractual provisions achieved between the Company and Counterparties when signing the agreements on data processing.

4.4. Privacy Policies for marketing activities.

For marketing activities, the Company publishes Privacy Policies on its Websites and/or other landing pages.

5. MANAGEMENT OF DATA PROCESSING ACTIVITIES.

The Company manages its data processing activities. This management consists of the following:

5.1. Procedures before the launch of the processing activity.

Step 1. In 2 (two) weeks before the start of any processing activity, the responsible department sends to the legal department a description of the processing activity which contains the following:

- ✓ A description of the processing activity, accompanied with so-called "lifecycle" (if applicable);
- ✓ Data subjects whose personal data will be processed;
- ✓ The source of personal data;
- ✓ The purpose or purposes of the processing;
- ✓ How long personal data will be stored;
- ✓ With whom personal data will be shared and on where the data created or received in course of the processing will be stored.

Step 2. The legal department, within two weeks, evaluates whether this processing activity complies with the GDPR or any other data protection laws:

- ✓ If such processing activity is likely to result in a high risk to the rights and freedoms of natural persons, the legal department carries out the data protection impact assessment. If during the data protection impact assessment it is found that submitted processing activity

would result in a high risk, the Company shall consult with its leading supervisory authority about the processing. After the consultation, the processing activity is launched only after the approval from the supervisory authority.

- ✓ If the retention period of personal data processed is excessive, a reasonable retention period is determined (unless determined by the applicable law).
- ✓ The processing activity is also evaluated whether the data collected are indeed necessary for a declared purpose. Is the data proposed for the collection is excessive for the purpose, the collection of personal data shall be limited only for those data which are necessary for the declared purpose.
- ✓ The recipients of personal data. The recipients of personal data are also evaluated. If they are external, the legal department ensures that proper agreements governing personal data processing are in place.
- ✓ If the processing is/are to be based on legitimate interest, the legal department performs legitimate interest assessment.

Step 3. When Step 2 is finished, the legal department performs the following actions:

- ✓ Chooses a legal basis for the processing (if has not been chosen before).
- ✓ Includes this processing activity into the record of processing activities as required by Article 30 of the GDPR.
- ✓ If the processing requires notification of data subjects under Articles 13/14, the legal department prepares special policies/notices on data processing or amend existent ones.

5.2. The Record of processing activities.

The Company keeps the record of processing activities under Article 30 of the GDPR.

5.3. Anonymization of the information.

When the main purpose of the processing is reached, and there are no restrictions both by the applicable law or by the conditions of the processing, personal data are anonymized.

6. TECHNICAL AND ORGANIZATIONAL MEASURES.

The Company applies the following technical and organisational measures:

6.1. Technical measures (as specified in the Teletrust Guideline):

- ✓ Cryptographic procedures;
- ✓ Encryption of files and folders;
- ✓ Disk encryption;
- ✓ E-mail encryption;
- ✓ Use of VPNs;
- ✓ Mobile Device Management.

6.2. Organisational measures:

- ✓ Clear desk and clear screen Policy;
- ✓ Password Policy;
- ✓ Usage of Internal messenger policy;
- ✓ Corporate VPN Policy;
- ✓ Office Security Policy;
- ✓ Mobile device and teleworking Policy:
 - Usage only the Company's devices Policy;
 - Usage only approved software Policy.

6.3. Internal Informational Security Policies:

- ✓ Information Security Policy;
- ✓ Access control Policy;
- ✓ The incident management process Policy;
- ✓ Human Resource Security.

7. ACTIONS IN CASE OF THE PERSONAL DATA BREACH.

The Company's actions in case of the personal data breach are described in the table below.

The nature of the risk	Actions
The personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.	✓ Internal self-audit.
The personal data breach is likely to result in a risk to the rights and freedoms of natural persons.	✓ Notification of supervisory authority within 72 hours after becoming aware of the personal data breach. ✓ Mitigation of risk procedures; ✓ Internal self-audit.
The personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.	✓ Notification of supervisory authority and data subjects within 72 hours after becoming aware of the personal data breach. ✓ Mitigation of risk procedures; ✓ Sending the instructions on how to mitigate the risks to the data subjects and further cooperation with them; ✓ Internal self-audit.



8. LEAD SUPERVISORY AUTHORITY AND DATA SUBJECTS' RIGHTS.

8.1. Lead supervisory authority. The Company's lead supervisory authority is the Cyprus Commissioner for Personal Data Protection. The Website of the Commissioner's Office <http://www.dataprotection.gov.cy/>.

8.2. Exercise of data subjects' rights. If a data subject wants to exercise his or her rights under the GDPR, he or she needs to contact the Company via the e-mail address privacy@evoplay.games.

9. AGREEMENTS AND ROLES WITH COUNTERPARTIES.

9.1. Appointing processors for the processing of personal data.

The Company appoints processors for the processing of personal data when the counterparty processes personal data solely under its documented instructions. It can be hosting companies, some analytics companies, and some service providers.

9.2. When the Company acts as a processor. If a data subject wants to exercise his or her rights under GDPR,

The Company acts a processor when the business relationships with the Company will process personal data only on behalf of the counterparty and under the counterparty's documented instructions.

9.3 Joint Controllershship.

The Company acts as a joint controller with counterparties when:

- ✓ They jointly determine the means and purposes of the processing;
- ✓ Their decisions on the processing of personal data are converging.

10. PRIVACY BY DESIGN AND BY DEFAULT.

When engineering, constructing or reconstructing any programs, interfaces, or websites the Company implements the principles of Privacy by Design:

10.1. *Proactive not Reactive; Preventative not Remedial*. This principle is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen.

10.2. *Privacy as the Default Setting*. This principle consists in the delivery of the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, his or her privacy still remains intact.

10.3. *Privacy Embedded into Design*. Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

10.4. *Full Functionality – Positive-Sum, not Zero-Sum.* Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as "privacy vs. security", demonstrating that it is possible, and far more desirable, to have both.

10.5. *End-to-End Security – Full Lifecycle Protection.* Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

10.6. *Visibility and Transparency – Keep it Open.* Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike.

10.7. *Respect for User Privacy – Keep it User-Centric.* Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

11. REVISIONS OF THIS POLICY.

This Policy is subject to revision each year. In addition, this Policy may be revised in the following cases:

- ✓ Changes in applicable data protection legislation;
- ✓ Changes in the corporate structure of the Company;
- ✓ Changes in the business profile of the Company;
- ✓ There are found sufficient deficiencies of this Policy or Company's data protection rules;
- ✓ In other cases when the situation may require a revision of the document.