Playtech - Group Personal Data Protection and Privacy Policy

April 2021

PUBLIC

Preface

Purpose

This Policy governs all data privacy issues. It defines standards for processing, storing, and transferring personal data within and outside the Group to ensure adequate protection for data subjects. Compliance with the Policy is mandatory.

Scope

In the case of conflict, national and international obligations shall prevail over the Policy. Every recipient of data must therefore understand the obligations that apply to his/her field of responsibility and ensure compliance with them. However, where data privacy requirements under national or international law are less strict than under the Policy, the Policy shall prevail.

Each Group entity is responsible for complying with national requirements and for communication with national data protection regulators. The transfer of personal data to government authorities and agencies is only permissible in accordance with the respective applicable national laws.

Whenever a corporate unit has reason to believe that applicable national requirements prevent it from fulfilling its obligations under the Policy, it must seek immediate guidance from the Group Data Protection Office. The Group Data Protection Office will then determine the matter, and notify the respective national data protection authority as and when needed.

Intended Audience

Public.

Contents

1 Introduction and Context

Playtech Group of companies ("the Group") is committed to collecting and processing all forms of data in a legally compliant manner. All entities' international and national operations shall comply with the legal requirements applicable in each country and region in which they operate. Moreover, we are committed to implementing adequate protection of data not just within the Group but also by our business partners.

This Group Policy on Data Protection and Personal Data Privacy ("the Policy"), when applied in conjunction with the Information Security Policies, is designed to ensure that all Group companies meet these requirements. This Policy has been agreed with the Playtech Board of Directors.

Each company within the Group is committed to safeguarding the personal rights of any individual whose personal data it deals with – including data of its employees, players, individuals employed by suppliers, licensees and other contractual partners, interested persons and other data subjects, regardless of how such personal data is collected. Accordingly, the Group has issued the following Policy. It relates to data protection and personal data privacy and is binding on each entity within the Group.

2 General Principles for Processing Personal Data

The Group is committed to complying with the principles that personal information:

- Shall be processed fairly and lawfully and in a transparent manner;
- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes;
- Shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed;
- Shall be accurate and, where necessary, kept up-to-date;
- Shall not be kept for longer than is necessary for that purpose or purposes;
- Shall be processed in accordance with the rights of data subjects under national or international laws;
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information; and
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

In addition, each group company shall ensure that:

- It has appointed a Data Champion locally;

- All employees managing and handling personal information complete appropriate data protection training (within the first three months on starting with the company and refreshed annually thereafter);
- Its employees understand that they are contractually responsible for adhering to data protection requirements and policies and commit to treating personal data as confidential;
- Methods of handling personal information are regularly reviewed and any changes assessed and evaluated together with the Group Data Protection Office.

Each Playtech company shall identify whether this entity has to be registered with a data protection supervisory authority and if so, advise the Group Data Protection Office accordingly.

3 Processing of Special Categories of Personal Data and Personal Data Relating to Criminal Issues

Special categories of personal data and personal data relating to for example criminal issues or bank data are especially Sensitive data (see Terminology in 0 for the full list of this kind of data). and the Group is committed to applying a high degree of protection to it. Any processing of special categories of personal data shall be consulted on with the Group Data Protection Office.

4 Data Processing via Third Parties

In circumstances where a Group entity acts as a data controller and intends to contract with a firm whose activity makes it a data processor, the following shall apply:

- The data processor must guarantee the technical and organisational security measures needed for the processing of personal data and must provide sufficient guarantees in respect to the protection of the rights of all data subjects impacted by the contract.
- The processing of personal data must be governed by a written and signed agreement (Data Processing or Model Clause Agreement) in which the rights and duties of the data controller and the data processor are clearly set out.
- The data processor must be contractually obliged to process personal data only within the scope of the contract and according to the data controller's instructions. Personal data may not be processed for any other purpose.
- The data controller remains the legal owner of the personal data and the contact partner for data subjects.

5 Sharing of Personal Data

When sharing with a third party personal data within the country in which data was initially collected, compliance with the existing legal requirements of the respective country shall be

ensured. Transfer of personal data across national and international borders is only permissible if such data is properly protected and if the group companies that process the data can give an adequate guarantee that the privacy of the individuals whose data is transmitted is being protected.

Sharing of personal data within the European Economic Area (EEA) is generally permitted if the data is processed in line with the requirements of this corporate policy.

6 Transfer of Personal Data from the EEA to Third Countries

The transfer of personal data from an EEA country to a third country is permitted only if:

- the data subject is aware and has given his/her consent; or
- the transfer of personal data is necessary for the performance of a contract between the data subject and the data controller; and
- the data receiving party provides sufficient guarantees and contractual, technical and operational protection within the meaning of this Policy.

Any Group entity transferring personal data shall take appropriate measures in case of violations of this policy by the recipient. These provisions must be included in the contract. If the recipient is not a Group entity, the contracting entity shall ensure that the recipient complies with this Policy in addition to Group data security standards.

7 Rights of the Data Subject

The Group is committed to safeguarding the rights of all data subjects whose data is processed by any of its entities or business partners. This includes:

- Right to be informed about data processing in advance, in a concise, transparent, intelligible and easily accessible form, using clear and plain language,
- Right to access to a copy of personal data processed,
- Right to rectification of incorrect data,
- Right to object to or request restriction of processing (where the company has no overriding interest in the processing),
- Right to erasure, requesting deletion of their data (where no further requirement exists to process the data),
- Right to data portability (where processing is based on consent or performance of a contract),
- Right in principle not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her,
- Right to raise concerns or complain to the competent supervisory authority.

The Group is committed to ensuring that whenever personal data is processed, affected individuals can exercise their rights in line with legal requirements. The respective rights will be indicated within the relevant privacy notice.

8 Procedural Rules- Implementation within the Playtech Group

Group companies, as data controllers, shall ensure compliance with the principles set out in this Policy. Group management shall ensure implementation of this Policy, including in particular providing information to employees. The Group Data Protection Office together with their local representatives are committed to supporting the Group in all data protection matters, including where necessary through specific additional training. The Group is committed to enforcing the general principles of this Policy and any violation may result in consequences under criminal, civil or employment law.

9 Security measures

The Group takes information security very seriously and is committed to ensuring that personal data is stored securely using modern software that is kept up-to-date taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Access to personal data shall be limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information.

The Group is committed to ensuring that personal data is retained only as long as necessary, and that when personal data is deleted this is done securely and such that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions shall be in place.

10 Roles and Responsibilities

Every employee

Every employee is responsible for adhering to this Policy and shall be supported by Line Management in case of any questions or concerns.

Line Management

Every member of management within the company shall ensure that

- any data processing activities within their remit complies with this Policy,
- their team are aware of this Policy and comply accordingly and
- any extra training requirements are identified and remedied.

Any questions should be raised with the Group Data Protection Office.

Chief Privacy Officer, Group Data Protection Office and local Data Champions

The Playtech Board has appointed the Chief Privacy Officer (CPO) to monitor compliance with this Policy. The CPO will be supported by the Group Data Protection Office and local Data Champions as appointed.

Local Data Champions are responsible for developing local data protection policies and for ensuring compliance with local data protection requirements; they must also co-operate closely with the Group Data Protection Office and inform them of any regulatory complaints and breaches of data protection regulations in line with the policies and procedures on security incident reporting. Group Senior Management shall support the CPO and his/her local representatives in the exercise of their duties.

The Group is fully committed to cooperating, on request, with the relevant supervisory authority in the performance of its tasks. Data protection supervisory authorities should direct any enquiries to the Group Data Protection Office (Privacy@Playtech.com).

Executive Board

The Executive Board is responsible for overall legal compliance and for putting in place appropriate governance structures for the business to be able to demonstrate compliance management.

11 Data Breaches

In the event of a breach of security leading to a personal data incident through the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the relevant line manager responsible for the business area where the incident occurred shall inform the Group Data Protection Office as soon as possible and latest within 24 hours of becoming aware, to ensure that any actual or suspected incidents can be investigated and addressed in a timely manner. If the breach of personal data meets the requirements for reporting to the respective supervisory authority and/or data subjects, the Group Data Protection Office fulfils this obligation within 72 hours from the personal data breach.

12 Amendment of the Corporate Policy and Continued Application

The Group Corporate Compliance team reserves the right to amend this Policy as necessary, for instance to comply with changes to statutes, regulations, requirements of data protection agencies or internal Group procedures. Where required by law, the Group Corporate Compliance team will submit any amended version for regulatory review.

Should this Policy become invalid, irrespective of the reasons or cause of such invalidity, all Group entities are bound by this Policy in relation to any personal data transferred prior to the date of such invalidity, unless the Policy has been replaced.

13 Relationship to other Company Policies

In the event that other company privacy policies conflict with this Policy, this Policy takes precedence.

14 Contact

In case of any questions either in regards to this policy or any other data protection matter, the Group Data Protection Office can be contacted on Privacy@Playtech.com.

15 Appendix A – Terminology

The following terminology is used in the document:

- **Consent** – Is any freely given and unambiguous declaration by the data subject that he/she accepts the processing of his/her personal data. Consent may be subject to particular requirements arising from respective national laws. Consent is one of six legal bases on which personal data may be processed, i.e. not every data processing activity must be based on consent (e.g. where legal requirements must be fulfilled).
- **Data processor** – Is the individual or legal entity that processes personal data on behalf of a data controller (such as licensees).
- **Data controller** – Is either a licensee or the legally independent Playtech Group entity that decides the purposes and means of processing personal data.
- **Data protection/privacy** – Is the sum of all actions taken to protect the personal rights of data subjects when handling their personal data.
- **Data subjects** – Are individuals whose personal data are processed within the Playtech Group, including current, future and former employees, players, employees of suppliers and other contractual partners and any other data subjects.
- **Data Champions** – Have a specialist role that incorporates processes, policies, guidelines and responsibilities for administering Playtech's entire data in compliance with policy and/or regulatory obligations at local level. A data champion may share some responsibilities with the Group Data Protection Office. The replacement of a data champion has to be agreed with the Group Data Protection Office.
- **Personal data** – Are any information relating to an identified or identifiable living individual. An individual is identifiable if he/she can be directly or indirectly identified, for example, by assigning a reference number.
- **Processing of personal data** – Is any automated or non-automated operation or set of operations performed in respect of personal data – such as collection, recording, storage, adaptation, alteration, selection, retrieval, use, transmission, blocking, deletion or erasure. This definition will also apply to the word "processed" when used in this context.
- **Sensitive data** – particularly sensitive personal data categories are defined as "special categories of personal data" and include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, biometric or genetic data, trade union membership, health and sexual orientation or data about someone's sex life. In Playtech we treat those categories of data as well as other data categories such as financial records and criminal records as "confidential".
- **EEA** – Includes all EU countries and in addition, non-EU countries Iceland, Liechtenstein, and Norway.

- **Third party** – Is every individual or legal entity that are outside of Playtech, (for example, every external business partner).

  Transfer of personal data – Is the forwarding of personal data, its distribution, or all other forms of transfer to third parties. In particular where data transfer relates to transfers outside the EEA, this must be subject to adequate safeguards (e.g. only to countries that have been identified as having data protection standards equivalent to GDPR, or subject to contractual safeguards (e.g. Standard Contractual Clauses). The Group Data Protection Office will support with identifying adequate safeguards to be implemented This definition also applies analogously to the words "transferred" and "transferring" when used in this context.

16 Appendix B – Employee Privacy Notice

Internal document. Available in case of legitimate requests.