Stunlock Studios AB

GENERAL DATA PROTECTION POLICY

Stunlock Studios AB, ("**Stunlock**") has implemented this General Data Protection Policy ("**General Data Protection Policy**") in order to establish a standard for the protection of any Personal Data when Processed by employees, contractors and agents of Stunlock ("**Employees**"). This General Data Protection Policy focuses on the legal requirements established by the General Data Protection Regulation ("**GDPR**"), as well as contact persons. Where local data privacy or protection law establishes greater protections for personal data, such local law applies. All capitalized terms and definitions herein shall have the same meaning as in the GDPR.

1. Scope and Objective. This General Data Protection Policy has, as applicable, been implemented by any affiliate or subsidiary of the Stunlock (each affiliate or subsidiary referred to as "**Company**") to establish and standardize a level of data protection compliance. Employees are obliged to comply with this General Data Protection Policy whenever they Process Personal Data in connection with or in the context of the performance of their work duties for Company.

2. Core Data Protection Requirements. The Company and each of its Employees need to ensure that they always comply with the following Core Data Protection Requirements when Processing Personal Data.

2.1 Key Principles. Each Employee must ensure that Personal Data is

(i) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

(iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay ('accuracy');

(v) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed unless specifically authorized by law; ('storage limitation'); and

(v) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

2.2 Legal Basis for Processing Personal Data. All Processing of Personal Data shall rely on at least one legal basis pursuant to Art. 6 of the GDPR.

2.3 Information Requirements. The Company shall ensure that data subjects are informed pursuant to Art. 13-14 of the GDPR.

2.4 Confidentiality. All Employees must be committed to keeping any Personal Data confidential and not to disclose any Personal Data to unauthorized third parties (within the Company or outside of the Company).

2.5 Disclosure to Service Providers. Service Providers (external third parties as well as Company's affiliate providing services to Company) may have access to Personal Data. In this case, Company must ensure that (i) such access is limited to the Personal Data which is absolutely necessary (need-to-know-principle), (ii) the Service Provider is diligently chosen, considering in particular the technical and organizational security measures provided by the Service Provider, and (iii) appropriate data processing clauses contained in a relevant service agreement or a separate data processing agreement is in place.

2.6 Data Subject's Rights. The Data Subjects whose Personal Data is Processed by the Company may have certain rights to request (1) access to their Personal Data, (2) rectification of their Personal Data, (3) erasure of their Personal Data, (4) restriction of Processing of their Personal Data, (5) portability of their Personal Data, (6) objection to the Processing of their Personal Data (including object to profiling), and (7) objection to automated decision making (including profiling). In case the Company receives such a request, the Data Protection Officer is responsible for responding to such requests and the *GDPR Data Subject Request Policy* shall be adhered to.

2.7 Technical and Organizational Security Measures. With regard to the level of risk and sensitivity of the Personal Data at hand, the Company will take appropriate technical and organizational measures to protect the Personal Data, against loss, unauthorized access, use, destruction, modification or disclosure. Taking into account state-of-the-art measures, costs, nature, scope, context and Processing purposes as well as the rights and freedoms of the Data Subjects, this may include in particular the pseudonymization and encryption of Personal Data, measures to ensure confidentiality, integrity, availability and resilience, measures to restore the Personal Data in a timely manner in the event of a security incident, and processes for regularly testing, assessing and evaluating the effectiveness of the security measures. All Employees are responsible for ensuring that any personal data that Stunlock holds and which they Process, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Stunlock to receive that information and has entered into a confidentiality agreement through a contract between all parties involved.

Processing of Personal Data ‘off-site’ presents a potentially greater risk of loss, theft or damage to Personal Data. Staff must be specifically authorised to process data off-site.

Access rules to certain personal data is described below:

- Employee contracts and documentation shall be kept in a secure location in Company's offices, and all Personal Data shall be treated with the highest security and must be kept:
    - in a lockable room with controlled access; and/or
    - in a locked drawer or filing cabinet; and/or
    - if computerized, password protected in line with corporate requirements; and/or
    - stored on (removable) computer media which are encrypted.

  Such Employee data may only be accessed by personnel who hold a set of keys to the locked bookshelf where the information is stored. Only the CFO of the Company and the Business Controller shall have access to these sets of keys and the keys are to always be kept at a secure location.
- Player data linked to a game account shall only be accessed on a strictly necessary basis, i.e. by Employees that need such access in order to conduct their work duties, and shall be protected by a double authentication method, consisting of a personal password and a Multi-Factor-Authentication (MFA).
- Email addresses obtained from Customer Support services shall only be accessed by the Customer Support Representative and the account manager, who has access to the Company's email accounts.

When assessing implementation of appropriate technical safety measures, appropriate persons within the Company will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Stunlock.

When assessing implementation of appropriate organizational safety measures the DPO will consider the following:

- The appropriate training levels of Stunlock Employees;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the
- workplace;

- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EU/EEA.

Information regarding the technical and organizational security measures can be found in the *Records of Processing pursuant to Art. 30 of the GDPR*.

2.8 Data Transfer. Personal Data must not be transferred to countries that do not provide an adequate level of data protection from a European data protection law perspective ("Restricted Countries") unless adequate safeguards have been adduced. Further information regarding such adequate safeguards are found in the *Records of Processing pursuant to Art. 30 of the GDPR*, which shall always be kept up to date.

2.9 Data Protection Impact Assessment (DPIA). The owner of the Processing activity shall be responsible to identify the need for a DPIA and to comply with the *Data Protection Impact Assessment Procedure.* The Data Protection Officer is responsible for performing necessary checks to establish the need for conducting a DPIA, the Head of Risk and Data Protection Officer are responsible for checking that appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing, and the Risk Owner is responsible for implementing any privacy risk solutions identified in accordance with the *Data Protection Impact Assessment Procedure.*

2.10 Data Protection by Design/by Default. The Company shall, both at the time of the determination of the means for a processing activity and at the time of the processing activity itself, implement appropriate technical and organizational measures, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR. The Company shall implement appropriate technical and organizational measures for ensuring that only Personal Data which are necessary for each specific purpose of the Processing are Processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the retention time and their accessibility. In particular, such measures shall ensure that by default Personal Data are not unnecessarily made accessible.

2.11 Keeping Documentation up-to-date. When developing or considering a new Processing activity, the owner of the Processing activity shall inform The Company DPO, Ruth Dominguez, and shall provide her with all necessary information in order to keep the related data protection documentation up-to-date, including the *Records of Processing pursuant to Art. 30 of the GDPR*.

2.12 Training. All Employees shall participate in data protection training to become familiar with applicable data protection laws, this General Data Protection Policy, and any supplementing policies, instructions and guidelines. Such training shall be documented.

3. Responsibilities of all Employees. All Employees of the Company are responsible for complying with this General Data Protection Policy, and any supplementing policies, instructions and guidelines. In particular, each Employee shall: (i) meet his or her confidentiality obligations with respect to Personal Data; (ii) Process Personal Data only to the extent necessary to perform his or her work duties; (iii) undertake any assigned data protection training; (iv) promptly report any breach of the General Data Protection Policy by contacting his or her direct or functional manager or Stunlock's DPO; and (v) ensure that any Personal Data he or she provides to the Company is true, accurate and up-to-date.

4. Responsibility for development of GDPR procedures.

Top Management and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practices within the Company; responsibilities are set out in individual job descriptions.

4.1 Data Protection Officer

The DPO is tasked with the duties set out in the GDPR. The DPO:

(i) should be a member of the senior management team;

(ii) reports to Stunlock's Board of Directors;

(iii) shall advise and inform Employees about data protection legislation and good practice;

(iv) shall monitor development and implementation of the data protection procedures as required by this General Data Protection Policy and any other instructions;

(v) shall monitor security and risk management in relation to Personal Data; and

(vi) shall be the first point of call for Employees seeking clarification on any aspect of Stunlock's data protection compliance.

4. Questions

Any questions relating to the General Data Protection Policy should be directed to Stunlock's DPO at dataprotection@stunlockstudios.com.

[California Privacy Rights. California law in some cases entitle California residents to ask us for a notice describing what categories of personal information Stunlock collects, from what sources, for what purpose and with whom Stunlock shares such information. California law also in some cases provide California residents with rights to request access to and deletion of certain personal information, to know whether personal information is shared, and to opt out of the “sale” of personal information. To understand how we honor these California rights, to make requests regarding these rights if they apply, please visit our **California Privacy Notice and Policy**.]

This Policy may be updated by Company as required.

Effective Date: 29-06-2021