

Continent Gaming N.V.

Data protection policy

Internal version

IT Security, August 2025

Summary

1. Introduction.....	2
2. Data protection laws (DPL).....	2
3. Definitions	2
4. Data protection principles.....	3
5. General provisions.....	3
6. Lawful purposes.....	4
7. Data minimization and Accuracy	4
8. Archiving / removal	4
9. Security	4
10. Online privacy	5
11. Security during interaction with third parties.....	5
12. Training.....	5
13. Breach and Enforcement.....	6

1. Introduction

- 1) This Data Protection Policy is the overarching policy for data security and protection for Continent Gaming N.V.
- 2) The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation, the common law duty of confidentiality and all other relevant national legislation.
- 3) This policy covers:
 - data protection principles and commitment to common law and legislative compliance;
 - procedures for data protection by design and by default.

2. Data protection laws (DPL)

- 1) National ordinance personal data protection (Landsverordening bescherming persoonsgegevens, National Gazette 2010, Consolidated text no. 84) “(National Ordinance Personal Data Protection”);
- 2) General Data Protection Regulation (the “GDPR”) – a regulation of the European Union which became effective on May 25, 2018 – may have implications for a data controller / data processor as the extra-territorial reach of the GDPR is not only relevant to businesses established in the European Union but also to international businesses established in Curaçao which offer goods or services to individuals in the European Union or monitor their behaviour in the European Union.

3. Definitions

- 1) According to the Explanatory Memorandum on the National Ordinance Personal Data Protection the term personal data has a broad meaning. This does not only concern data that can identify a person but concerns any data that can be associated with a particular person; it is foreseeable that under certain circumstances data can be traced to one person through systematic comparison and lengthy investigations. Personal identifiable confidential data is therefore not only limited to home address, email address, telephone number, membership number and/or identity number.
- 2) Sensitive Personal Data - A person’s religion or belief, race, political views, health, sexual life as well as personal data concerning membership of a trade union.
- 3) National data protection authority - The Personal Data Protection Committee as referred to in article 42 of the National Ordinance Personal Data Protection.
- 4) Collection: a natural or legal person, public authority, agency or other body which who has control over a person registration.

- 5) Processor: a natural or legal person, public authority, agency or other body which who owns all or part of the has equipment in his possession, with which a personal registration of which he is not the holder.

4. Data protection principles

- 1) The Organisation is committed to processing data in accordance with its responsibilities under DPL.
- 2) DPL requires that personal data shall be:
 - processed lawfully, fairly and in a transparent manner in relation to individuals;
 - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;
 - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 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;
 - 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the DPA in order to safeguard the rights and freedoms of individuals; and
 - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. General provisions

- 1) This policy applies to all personal data processed by the Organisation.
- 2) The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.
- 3) This policy shall be reviewed at least annually.

6. Lawful purposes

- 1) All data processed by the Organisation must be done on one of the following lawful bases:
 - consent,
 - contract,
 - legal obligation,
 - vital interests,
 - public task or
 - legitimate
 - interests.
- 2) The Organisation shall note the appropriate lawful basis:
 - where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data;
 - Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

7. Data minimization and Accuracy

- 1) The Organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 2) The Organisation shall take reasonable steps to ensure personal data is accurate.
- 3) Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8. Archiving / removal

- 1) To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- 2) The archiving policy shall consider what data should/must be retained, for how long, and why.

9. Security

- 1) The Organisation shall ensure that personal data is stored securely using modern software that is kept-up to date.
- 2) Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

- 3) When personal data is deleted, this should be done safely such that the data is irrecoverable.
- 4) Appropriate back-up and disaster recovery solutions shall be in place.

10. Online privacy

- 1) Cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users' data as long as they receive consent or if they have a legitimate interest.
- 2) Location data, the GDPR will apply if the data collector collects the location data from the device and if it can be used to identify a person.
If the data is anonymized such that it cannot be linked to a person, then the GDPR will not apply. However, if the location data is processed with other data related to a user, the device or the user's behavior, or is used in a manner to single out individuals from others, then it will be "personal data" and fall within the scope of the GDPR even if traditional identifiers such as name, address etc. are not known.

11. Security during interaction with third parties

- 1) In each case of interaction with third parties implement measures to mitigate security risks related to a third party. To mitigate the risk of a breach in customers data confidentiality verify third party's trustworthiness and ensure boundaries of the third party's responsibility for the customers data security.
- 2) Additionally, we conduct periodic assessments and audits to ensure that all third parties comply with our security requirements and industry best practices. This ongoing oversight helps maintain the integrity and confidentiality of customer data throughout our service ecosystem.

12. Training

- 1) If the Company's employees are not aware of their security responsibilities, the efficiency of the implemented security controls could decrease. Therefore, an atmosphere of responsible attitude to the customers data is the basis for the effective implementation of the security controls. To build the proper atmosphere, awareness of the Company's employees is regularly raised and includes regular reminders to employees about security processes and procedures implemented within the Company.
- 2) All new employees undergo mandatory security training as part of their onboarding process to ensure they understand our policies and procedures from day one.

13. Breach and Enforcement

- 1) In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach National data protection authority.
- 2) Pursuant to article 54 the responsible party who acts in contravention of the provisions of or pursuant to Article 4(3) may be penalized by the Curaçao committee of data protection with a financial penalty in the maximum amount of Naf. 10,000.00 (USD. 5,714.29. 2).