

GBL SOLUTIONS N.V.

**INFORMATION SECURITY
POLICY**

Document Information:

Approval	Board of Directors
Scope	Company - Wide
Effective Date	October 2, 2025
Next Review Date	October 2, 2026

Version History:

Date	Version	Summary Changes	Approved by: Mrs. Vivian Victoria Ersilia On behalf of SMES
October 2, 2025	1.0	Policy Implementation	

Table of Contents

Table of Contents.....	3
Definitions.....	4
Introduction.....	5
Information Security Objectives and Principles.....	5
Access Control & Authentication.....	5
GDPR Principles.....	6
Lawful Processing.....	6
Sensitive Personal Data.....	6
Consent.....	6
Rights of the Data Subject.....	7
Accountability and Governance.....	7
Records Keeping and Retention.....	7
Data Protection Impact Assessment.....	7
Data Storage and Server Location.....	7
Encryption and Data Security.....	8
Transfer of Data.....	8
Transfers Subject to Appropriate Safeguards.....	8
Third Party and Vendor Risk Management.....	8
Data Breach Notification.....	8
Incident Response Plan.....	8
Policy Review.....	9

DEFINITIONS

“BUSINESS CONTINUITY” The capability of the Company to maintain or quickly resume critical operations following a disruption.

“Confidential Information” Any non- public information belonging to the Company, its players, or its partners, including commercial, financial, technical, or operational data.

“Controller” The entity that determines the purposes for which and the manner in which any personal data are, or are to be, processed, is regarded as the data controller under applicable data protection laws.

“Data” Any recorded information subject to electronic or manual processing, relevant to the Company’s operations.

“Data Protection Laws” National Ordinance on the Protection of Personal Data (NODP, Curaçao Gazette 2010, no. 84). EU General Data Protection Regulation (GDPR), insofar as applicable to EU-based customers.

“Data Subject” Any individual whose personal information is collected or processed (e.g., players, employees, contractors).

“DPO” Data Protection Officer.

“Encryption” Conversion of data into secure coded form to restrict unauthorized access.

“Incident” Any event that compromises confidentiality, integrity, or availability of Company information.

“Information Asset” Any system, database, file, or technology critical to the Company’s operations.

“Multi-Factor Authentication (MFA)” Two or more independent verification factors before granting access.

“Processor” Any natural or legal person processing data on behalf of the Company.

“Sensitive Personal Data” Data relating to racial/ethnic origin, health, political/religious beliefs, biometric identifiers, or sexual orientation.

“Vendor/Third Party” External providers with access to Company data under contractual safeguards.

INTRODUCTION

This Information Security Policy sets out the framework by which GBL Solutions N.V., a licensed online gaming operator in Curaçao, protects the confidentiality, integrity, and availability of its information resources. It applies across all areas of the Company and covers personal data, financial records, gaming activity, and the technological infrastructure that supports them.

The Policy ensures that GBL Solutions N.V. manages information securely and transparently in accordance with Curaçao's National Ordinance on Data Protection (NODP), the General Data Protection Regulation (where applicable to EU customers), the National Ordinance on Games of Chance and the conditions set by the Curaçao Gaming Authority (CGA). It also incorporates standards under ISO/IEC 27001 as the baseline framework for information security governance, PCI DSS requirements for handling payment data, and other obligations relating to anti-money laundering, counter-terrorist financing, and responsible gaming.

The objectives of this Policy are to protect Company, employee, and customer information against misuse, unauthorized access, and accidental loss, to ensure the resilience and continuity of gaming operations through strong security measures, and to demonstrate accountability and transparency to regulators, players, and partners.

INFORMATION SECURITY OBJECTIVES AND PRINCIPLES

GBL Solutions N.V. is committed to safeguarding its information assets. The Company's objectives are to prevent unauthorized access to data, ensure the continuity and resilience of its platforms and services, comply with all applicable laws and regulatory requirements, and maintain the trust of its stakeholders through effective security and privacy practices.

ACCESS CONTROL AND AUTHENTICATION

Access to Company systems is granted only where strictly necessary for business purposes. The principle of least privilege applies at all times. All privileged accounts and any remote access must be secured by multi-factor authentication. Access to sensitive platforms, including those processing player and financial data, is subject to role-based controls. All privileged account usage is logged and subject to quarterly review. Employee accounts must be disabled within twenty-four hours of termination.

All staff and contractors who have access to confidential information must sign Non-Disclosure Agreement. No personal data may be disclosed to third parties except as required by law or regulation, or under documented and authorized agreements.

GDPR AND NODP PRINCIPLES

The Company follows the seven core data protection principles established under the NODP and GDPR. These require that personal data is processed lawfully, fairly, and transparently; that it is collected for defined purposes and not reused for incompatible purposes; that only the minimum necessary data is collected; that data is accurate and kept up to date; that data is not stored longer than necessary; that appropriate technical and organizational security measures are applied; and that the Company is accountable for demonstrating compliance.

All external processors engaged by the Company must agree contractually to comply with these same principles.

LAWFUL PROCESSING

Processing of personal data shall only take place where a valid legal ground exists. This may include the consent of the individual, the necessity of processing for the performance of a contract, compliance with legal obligations, the protection of vital interests, the carrying out of tasks in the public interest, or the pursuit of the Company's legitimate interests provided the rights of individuals are not overridden.

SENSITIVE PERSONAL DATA

Information falling within special categories of personal data may only be processed under stricter legal conditions. This includes explicit consent by the individual, compliance with employment or legal obligations, the protection of vital interests, the individual's own decision to make the data public, or requirements relating to legal claims, public health, or other permitted grounds.

CONSENT

Whenever consent is relied upon as the basis for processing, it must be freely given, specific, informed, and based on clear affirmative action. Consent must be documented and individuals may withdraw their consent at any time.

RIGHTS OF THE DATA SUBJECT

Data subjects have the right to be informed of how their information is processed, to request access to their personal data, to correct inaccurate records, to request erasure of data in certain circumstances, to restrict processing, to request portability of their data in machine-readable form, to object to processing based on legitimate interests or direct marketing, and to avoid being subject to automated decision-making without human oversight unless permitted by law.

ACCOUNTABILITY AND GOVERNANCE

The Company ensures compliance with its data protection obligations through the maintenance of internal records of all processing activities, the conduct of Data Protection Impact Assessments where new technologies or high-risk processing are introduced, the provision of initial and refresher training for all employees, and the requirement that all staff sign confidentiality and data protection undertakings as part of their employment.

RECORDS KEEPING AND RETENTION

GBL Solutions N.V. maintains complete records of player registrations, KYC documentation, financial transactions, and communications relating to gaming activities. These records are retained for a minimum of five years following the last transaction, in line with Curaçao's AML/CFT and gaming legislation, after which they are securely deleted or anonymized unless retention is legally required.

DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments are carried out when the Company considers new technologies or processes that may pose a high risk to the rights and freedoms of individuals. This includes large-scale processing of sensitive personal data or automated decision-making that has legal or significant effects on individuals.

DATA STORAGE AND SERVER LOCATION

All critical records, including customer personal data, gaming transactions, and financial information, will be stored in a Tier-IV certified data center located in Curaçao. These records must remain accessible at all times to the Curaçao Gaming Authority for inspection or audit purposes.

ENCRYPTION AND DATA SECURITY

Personal and financial data are protected through encryption, with secure key management and regular key rotation. Systems and applications are developed and maintained according to secure coding standards. Vulnerability scanning and penetration testing are performed on a regular basis.

TRANSFER OF DATA

Personal data may only be transferred outside Curaçao or the EU where appropriate safeguards exist. This includes transfers to jurisdictions recognized as adequate by the European Commission, or transfers supported by mechanisms such as standard contractual clauses, binding corporate rules, or explicit consent.

THIRD-PARTY AND VENDOR RISK MANAGEMENT

All external service providers that process Company data are subject to security due diligence before onboarding. Contracts must include data protection obligations aligned with NODP, GDPR, and CGA standards. Critical vendors such as hosting providers and payment processors are required to provide annual certifications such as ISO 27001 or PCI DSS, and their compliance is reviewed on a regular basis.

DATA BREACH NOTIFICATION

Any data breach must be reported immediately to the Board of Directors. Incidents affecting personal data must also be reported to the Curaçao Gaming Authority within twenty-four hours, accompanied by a full report of the breach, the categories of data involved, the corrective measures taken, and the plan for further mitigation. Where required by law, affected individuals will also be notified.

INCIDENT RESPONSE PLAN

The Company maintains a formal incident response plan. This includes immediate reporting and detection of incidents, classification of severity by the Incident Response Team, containment and eradication of the threat, timely notification of regulators and affected parties, recovery of systems from secure backups, and post-incident review to identify root causes and corrective actions. The Company also conducts annual incident response drills to ensure readiness.

POLICY REVIEW

This Policy will be reviewed annually, or earlier if required due to significant changes in law, regulations, or business operations, or in the event of a major security incident.

Approved by the Board of Directors of GBL Solutions N.V.



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

Managing Director

20.10.2025

CONFIDENTIAL