

INFORMATION SECURITY AND DATA PRIVACY

POLICY

Version 1.0

Last Update: 15 November 2025

1. GENERAL

This Information Security Policy ("the Policy") establishes the framework by which MEDIAL N.V. ("the Company"), a licensed online gaming operator in Curaçao, protects the confidentiality, integrity, and availability of its information assets. The Policy applies company-wide and covers personal data, financial information, gaming records, and all related systems and processes.

The Policy ensures that the Company's handling of information is lawful, secure, and transparent, in line with:

- The National Ordinance on the Protection of Personal Data (NODP) of Curaçao;
- The General Data Protection Regulation (GDPR), where applicable to EU players;
- The National Ordinance on Games of Chance (NOGC) and Curaçao Gaming Authority (CGA) License Conditions;
- ISO/IEC 27001 (Information Security Management Systems); and
- Other relevant gaming compliance regulations.

The objectives of this Policy are to:

- Safeguard customer, employee, and company information against unauthorized access, misuse, loss, or corruption;
- Support compliance with regulatory requirements, including AML/CFT unusual transaction monitoring and Responsible Gaming obligations;
- Ensure resilience of gaming operations through robust technical, organizational, and cybersecurity measures; and
- Build trust with regulators, players, and business partners by demonstrating accountability, transparency, and strong governance.

This Policy applies to all employees, contractors, and third-party providers handling information on behalf of the Company. Compliance with this Policy is mandatory and subject to continuous monitoring, periodic audits, and annual review.

2. 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	Information which: · Is being processed by means of equipment operating automatically in response to instructions given for that purpose; · Is recorded with the intention that it should be processed by means of such equipment; · Is recorded as part of a filing system.
Data protection laws	· National ordinance on data protection (“NODP”) (Landsverordenening bescherming persoonsgegevens, National Gazette 2010, Consolidated text no. 84) - regulates the processing of personal data by both public and private entities in Curaçao. · General Data Protection Regulation (the “GDPR”) – a regulation of the European Union, which has 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 behavior in the European Union.
Data Subject	The natural person to whom personal data relates (e.g., players, employees, contractors).
DPL	Data Protection Lead
Encryption	The process of converting data into a coded form to prevent unauthorized access, using industry-standard algorithms.
Incident	Any actual or suspected event that compromises the confidentiality, integrity, or availability of Company information or systems (e.g., data breach, cyberattack, fraud attempt).
Information Asset	Any data, system, software, or infrastructure that supports the Company’s operations and requires protection against unauthorized access, alteration, loss, or disclosure.
Multi-Factor Authentication (MFA)	A security mechanism requiring two or more independent credentials (e.g., password & mobile verification) before granting access.
National data protection authority	· NODP - The Personal Data Protection Committee as referred to in article 42 of the National Ordinance Personal Data Protection; · GDPR - An independent public authority established by a Member state pursuant to article 51 of the GDPR (Article 4(21),

	GDPR). The authority is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.
Personal Data	Any information that identifies or can reasonably identify a natural person, directly or indirectly (e.g., name, ID number, IP address, location data, financial information).
Personal Data Protection Board (CBP Curaçao)	Curaçao's supervisory authority established to oversee compliance with the NODP (as of November 2025, the CBP has been formally established but is not yet fully operational.)
Processing	Any activity performed on personal data, including collection, storage, retrieval, use, disclosure, alignment, alteration, restriction, erasure, or destruction.
Processor	A natural or legal person which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.
Relevant Filing System	Any structured set of personal data accessible according to specific criteria, whether centralized, decentralized, or dispersed.
Sensitive Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data, or information about a person's sex life or sexual orientation. Where applicable, the GDPR definition applies only to EU-based players.
Vendor / Third Party	An external organization or service provider that processes or has access to Company data and must comply with contractual and regulatory requirements.

3. INFORMATION SECURITY OBJECTIVES AND PRINCIPLES

MEDIAL N.V. is committed to maintaining the confidentiality, integrity, and availability of information assets.

The Company's objectives are to:

- Protect player and company data from unauthorized access or disclosure.
- Ensure resilience of gaming platforms, systems, and services.
- Comply with all applicable laws and regulatory requirements, including the NODP, GDPR (where applicable), the National Ordinance on Games of Chance, and CGA license conditions.
- Maintain stakeholder trust through robust cybersecurity and data privacy practices.

3.1. INFORMATION ASSET INVENTORY

To ensure that information security controls remain appropriate, effective, and proportionate to the risks faced by the Company, MEDIAL N.V. maintains a structured approach to identifying, assessing, and managing information security risks.

The Company shall:

- Maintain an up-to-date inventory of all information assets, including systems, applications, databases, data repositories, and critical third-party services used in the operation of the gaming platform.
- Classify information assets based on sensitivity, regulatory importance, and business criticality.
- Conduct periodic information security risk assessments to identify threats, vulnerabilities, and potential impacts affecting the confidentiality, integrity, and availability of information assets.
- Implement and document appropriate risk-mitigation measures proportionate to the risks identified, taking into account operational feasibility, regulatory requirements, and business needs.
- Review and update the risk assessment at least annually, or sooner if there are material changes to systems, infrastructure, technology, regulatory obligations, or business operations.

4. ACCESS CONTROL & AUTHENTICATION

Access to player personal data and gaming records is strictly limited to authorized personnel whose duties require such access. Access to systems and data shall be granted on a “need-to-know” and “least privilege” basis. Multi-factor authentication (MFA) is mandatory for all privileged accounts and remote access.

Role-based access control shall be implemented for all systems handling player or financial data. Privileged accounts must be separately monitored, logged, and reviewed regularly by the Compliance and IT teams.

Terminated employees’ accounts must be disabled immediately upon termination.

The Company shall:

- Maintain access logs of all staff interactions with personal data;
- Require confidentiality agreements for all employees and contractors with data access;
- Prohibit disclosure of personal data to third parties except:
 - As required for regulatory compliance (e.g., CGA, AML/CFT reporting); or
 - Where mandated by law, with proper documentation.

5. GDPR PRINCIPLES

The GDPR sets out principles which the Company adhere to in relation to the Processing of Personal Data.

The Company also engages Processors to process Personal Data on its behalf, such Processors must, pursuant to the agreement entered into by both parties, comply with the principles in their processing of Personal Data on behalf of the Company.

When processing personal data, the Company follows the principles established under the GDPR and the NODP. External processors engaged by the Company must comply with these same principles under contractual agreement.

The seven key principles are:

- Lawfulness, Fairness, and Transparency – Data must be processed on a valid legal basis, handled fairly, and explained to individuals in clear terms.
- Purpose Limitation – Data is collected only for defined, legitimate business purposes (e.g., account creation, fraud prevention, payments, regulatory compliance) and not reused for incompatible purposes.
- Data Minimization – Only the minimum personal data necessary for each purpose is collected and retained.
- Accuracy – Personal data must be correct and updated when necessary; inaccurate data is corrected or deleted promptly.
- Storage Limitation – Data is kept no longer than required for business or legal purposes, unless archived securely for public interest, research, or statistical use.
- Integrity and Confidentiality – Data must be secured against unauthorized or unlawful use, loss, or damage with appropriate technical and organizational measures.
- Accountability – The Company is responsible for compliance and must be able to demonstrate it.

5.1. LAWFUL PROCESSING

Processing of personal data must always be based on a valid legal ground. Depending on the circumstances, this may include:

1. Consent – The player has given explicit agreement for their data to be processed for a stated purpose.
2. Contractual necessity – Data must be processed to provide services under a contract with the player (e.g., account management, processing wagers).
3. Legal obligation – Data is processed to comply with legal or regulatory requirements (e.g., AML/CFT laws, tax reporting).
4. Legitimate interests – Processing is necessary for the Company's legitimate business purposes (e.g., fraud detection, service improvement), provided players' rights are not overridden.

The Company shall consider the applicable legal basis for Processing Personal Data and apply each basis where relevant.

5.2. SENSITIVE PERSONAL DATA

Special categories of personal data, such as health information or political views, are subject to stricter protections. These may only be processed if:

- The player has given explicit consent;
- The processing is required by law (e.g., employment obligations);
- It is necessary to protect the player's vital interests;
- The data has been made public by the player;
- It is required for legal claims, public health, or other specific grounds permitted by GDPR.

5.3. CONSENT

Consent must be freely given, specific, informed, and unambiguous. It requires a clear affirmative action, not silence or pre-ticked boxes. The Company must record when and how consent was given.

Players can withdraw consent at any time, and the Company must stop processing for that purpose once consent is withdrawn.

6. RIGHTS OF THE DATA SUBJECT

Players (data subjects) have several rights regarding their personal data:

- Right to be informed – Players must be told how their data is collected, used, shared, and retained in a clear and accessible way.
- Right of access – Players can request a copy of their personal data. Responses must be provided free of charge (except in abusive cases) and within one month.
- Right to rectification – Incorrect or incomplete data must be corrected promptly.
- Right to erasure ("right to be forgotten") – In certain circumstances, players can request deletion of their data.
- Right to restrict processing – Players can request that their data be stored but not actively processed.
- Right to data portability – Players can request their data in a commonly used, machine-readable format.
- Right to object – Players may object to processing based on legitimate interests or direct marketing.
- Rights related to automated decision-making – Players have the right not to be subject to decisions made solely by automated processes without human oversight, except where allowed by law or explicit consent.

Where rights in the NODP differ from GDPR, the NODP rights will apply to non-EU data subjects.

7. ACCOUNTABILITY AND GOVERNANCE

The Company ensures compliance with data protection and information security obligations by:

- Maintaining internal records of all personal data processing activities (Processing Register).
- Conducting Risk Assessments when new technologies or high-risk processing activities are introduced.
- Providing all employees with initial and annual refresher training on data protection, confidentiality, and breach reporting.
- Requiring employees to acknowledge and sign confidentiality and data protection undertakings.

The Company shall ensure that all employees involved in the processing of personal data:

- Receive initial and annual refresher training on data protection, breach reporting, and confidentiality;
- Understand their responsibilities under GDPR, NODP, and the National Ordinance on Games of Chance; and
- Acknowledge and sign confidentiality and data protection undertakings as part of their employment.

7.1. RECORDS KEEPING AND RETENTION

The Company maintains clear and legally compliant retention periods for all categories of records, in line with Curaçao AML/CFT and gaming laws. After this period, data will be securely deleted or anonymized unless required for ongoing investigations or legal obligations.

Personal data shall be retained only for as long as necessary to fulfil the purposes for which it was collected, or to meet legal, regulatory, and contractual obligations.

Unless a longer period is required for ongoing investigations, regulatory inquiries, litigation, fraud prevention, or to meet statutory obligations, the following minimum retention periods apply:

Category	Details	Retention Period
Player Identification and KYC Documentation	KYC files, identity verification data, due diligence records, and supporting documents related to player onboarding and monitoring.	At least five (5) years following the player's last transaction or the closure of the player's account.
Gaming and Transaction Records	All records relating to wagers, bets, game results, account balances, deposits, withdrawals, session logs, gameplay history, and system-generated gaming data.	Five (5) years.
Financial, Accounting, and Tax Records	Financial statements, accounting ledgers, transaction records, payment processor statements, and statutory tax-related documents.	Five (5) years or any longer period mandated by applicable financial or tax laws.
Player Communications and Complaints Records	Records of customer support interactions, internal complaint logs, dispute correspondence, and related supporting documentation	Five (5) years.
Security, System, and Access Logs	System access logs, authentication logs, incident logs, and security monitoring records.	At least one (1) year, unless otherwise required for operational continuity, forensics, or regulatory investigation. Where logs form part of gaming system audits, they shall be retained for five (5) years.
Responsible Gaming and Player Protection Records	Records relating to self-exclusion, RG interventions, affordability assessments, and monitoring of player behavior.	Five (5) years.
Vendor and Third-Party Processing Records	Contracts, due diligence reports, and data processing agreements.	For the duration of the relationship and for five (5) years thereafter.

7.2. DATA PROTECTION IMPACT ASSESSMENTS

Data protection impact assessments are a tool which the Company uses to assist when identifying the most effective way to comply with the GDPR and to meet individuals' expectations of privacy. The Company requires a data protection impact assessment to be undertaken when:

- Using new technologies; and
- The Processing of Personal Data is likely to result in a high risk to the rights and freedoms of individuals
- Processing that is likely to result in high risk includes, but is not limited to:
- Systematic and extensive Processing activities, including profiling and where decisions that have legal effects – or similarly negative effects – on individuals;
- Large scale processing of special categories of Personal Data in relation to criminal convictions or offences

7.3. DATA STORAGE AND SERVER LOCATION

The Company shall ensure that all critical digital records, including players' personal data, gaming transaction data, and financial records, are stored on a Tier-IV certified data center located in Curaçao, in compliance with the Curaçao NOGC and the CGA License Conditions.

These records shall be accessible to the CGA at all times upon request for audit, inspection, or investigation purposes.

In addition, the Company maintains technical and organizational measures to protect stored data against unauthorized access, accidental loss, or damage.

7.4. ENCRYPTION AND DATA SECURITY

All player personal data, financial information, and gaming records shall be encrypted at rest and in transit where appropriate. Encryption keys shall be managed securely with restricted access and regular rotation. Applications and systems are subject to secure coding standards, vulnerability scanning, and periodic penetration testing.

8. TRANSFER OF DATA

When transferring personal data outside of Curaçao, the Company shall ensure that:

- The transfer is necessary for the performance of services requested by the player or for the functioning of the gaming platform;
- The recipient processes the data securely and only for the authorized purpose;
- Appropriate contractual or technical safeguards are in place to prevent unauthorized access, disclosure, or misuse; and
- The transfer does not conflict with any applicable Curaçao legal or regulatory obligations, including CGA access and audit requirements.

Where the personal data of individuals located in the European Union is transferred to a country outside the EU/EEA, the Company shall comply with Chapter V of the GDPR:

- Transfers to countries approved by the European Commission as “adequate” are permitted.
- Transfers to other countries require additional safeguards such as standard contractual clauses, binding corporate rules, or explicit player consent.

For all international transfers of personal data, regardless of jurisdiction, the Company shall:

- Ensure that third-country recipients implement security measures consistent with industry standards and the Company’s contractual requirements;
- Limit transfers to what is necessary for the stated and lawful business purpose;
- Prohibit onward transfers by the recipient unless authorized in writing; and
- Maintain records of cross-border transfers as part of the Company’s processing documentation

8.1. TRANSFERS SUBJECT TO APPROPRIATE SAFEGUARDS

The Company may also transfer Personal Data where the organization receiving the Personal Data has provided adequate safeguards. Individuals’ rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- A legally binding agreement between public authorities and bodies;
- Binding corporate rules;
- Standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- Standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- Compliance with an approved code of conduct approved by a supervisory authority;
- Certification under an approved certification mechanism as provided for in the GDPR;
- Contractual clauses agreed and authorized by the competent supervisory authority; or
- Provisions inserted in to administrative arrangements between public authorities or bodies authorized by the competent supervisory authority

8.2. THIRD PARTY AND VENDOR RISK MANAGEMENT

All third-party service providers handling Company and Player data must undergo security due diligence before onboarding.

Data Processing Agreements must explicitly require compliance with GDPR, NODP, and CGA security standards.

Critical vendors, such as payment processors, hosting providers, must provide annual certifications, as defined by their profile and where necessary, including but not limited to ISO 27001, PCI DSS, or equivalent industry-standard measures.

Vendor performance and compliance shall be reviewed regularly.

9. DATA BREACH NOTIFICATION

All data breaches must be reported internally to the Board as soon as possible.

Breaches affecting personal data will be reported to the CGA as soon as reasonably possible, and to EU supervisory authorities within 72 hours where GDPR applies, with a full incident report including: nature of the breach, data affected, immediate actions taken, and planned corrective measures. Where required by GDPR, affected players will also be notified.

All breaches are logged and followed up with corrective actions.

10. INCIDENT RESPONSE PLAN

The Company shall maintain a documented Incident Response Plan covering:

- **Detection:** All staff must immediately report suspected security incidents.
- **Assessment:** A dedicated Incident Response Team (IRT), assigned by the Board, shall classify incidents by severity.
- **Containment & Eradication:** Immediate measures must be taken to prevent further damage.
- **Notification:** Regulatory reporting obligations to the CGA, FIU, affected players, where applicable, must be fulfilled within prescribed timelines.
- **Recovery:** Systems must be restored from secure backups.
- **Post-Incident Review:** Root cause analysis and corrective actions shall be documented.
- **Annual incident response drills** shall be conducted to test readiness.

11. POLICY REVIEW

This Policy is reviewed annually or sooner if required by significant changes in laws or regulations, major security incidents, or updates to technology or business operations.