NIOPLAY DATA PROTECTION POLICY

Effective Date: *March 2nd, 2025*

1. Introduction

NIOPLAY is committed to maintaining the highest standards of data protection and security for its players. This Data Protection Policy outlines the measures taken to safeguard personal information, prevent unauthorized access, and ensure compliance with applicable data protection regulations, including but not limited to the **California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).**

This document serves as an internal guideline for data protection while complementing NIOPLAY's publicly available ***Privacy Policy.***

---

2. Scope of this Policy

This policy applies to:

- All **player data** collected and processed by NIOPLAY.
- Data collected from employees, vendors, and third-party service providers.
- Information stored and transmitted via NIOPLAY's platform, including website and mobile applications.
- Security controls governing data access, storage, and breach response procedures.

3. Data Collection & Processing

NIOPLAY collects, processes, and stores **Personally Identifiable Information (PII)** and other player-related data solely for gaming operations, compliance, and fraud prevention.

Types of data collected:

- **Player Registration Data** (Name, Date of Birth, Residential Address, Email, Phone Number, Last Four Digits of SSN).
- **Identity Verification Data** (Government-issued ID, Proof of Address, Selfie Verification through GeoComply).
- **Financial Data** (Payment method details for deposits and withdrawals, including ACH and Debit Card transactions).
- **Geolocation Data** (Used for regulatory compliance and fraud prevention).
- **Gaming Activity Data** (Transaction logs, winnings, self-exclusion records, Responsible Gaming tool usage).

---

4. Data Security & Protection Measures

To ensure the security of user data, NIOPLAY implements the following measures:

4.1 Encryption & Secure Data Storage

- **All sensitive player data is encrypted** using AES-256 encryption during storage.
- Data in transit is protected via **SSL/TLS encryption** to prevent unauthorized interception.
- PII is stored on secure, access-controlled servers with industry-standard security protections.

4.2 Access Controls & Employee Restrictions

- Only authorized personnel with a **legitimate business need** can access sensitive player data.
- Role-based access controls (RBAC) are enforced to **limit employee access** to necessary data only.
- Multi-factor authentication (MFA) is required for internal system logins.
- Employee access logs are regularly audited to detect unauthorized activity.

4.3 Data Minimization & Retention Policy

- NIOPLAY only collects the **minimum required information** to provide services and comply with regulations.

- Player PII is retained for **five years** after account closure to comply with AML and financial reporting obligations.
- After the retention period, data is permanently deleted or anonymized to prevent unauthorized use.

4.4 Third-Party Data Sharing & Security Controls

- NIOPLAY shares player data only with **regulated third-party vendors**, including:
  - **GeoComply** (Identity verification and geolocation compliance)
  - **Approvely / Payment Processors** (Transaction processing & fraud monitoring)
  - **Lexicon Bank** (Player funds safeguarding)
- All third-party partners undergo **security vetting and contractual compliance agreements** to uphold strict data protection standards.

4.5 Incident Response & Data Breach Handling

NIOPLAY has a formal **Incident Response Plan** in place to detect, contain, and report data breaches:

- **Automated monitoring tools** detect potential breaches and unauthorized access attempts.
- In the event of a breach, affected users and regulatory bodies are notified within **72 hours**.
- Forensic investigations are conducted to identify and remediate vulnerabilities.

---

5. Compliance & Regulatory Oversight

5.1 Compliance with Global Data Protection Laws

NIOPLAY ensures compliance with **data privacy laws**, including:

- **CCPA & CPRA** (U.S. California residents' data rights)
- **PIPEDA** (Canada’s privacy regulation)
- **GDPR (General Data Protection Regulation)** (Should NIOPLAY expand to European markets in the future)

5.2 User Rights & Data Control

Players have the following rights regarding their personal data:

- **Access & Correction:** Players can request access to their stored data and correct inaccuracies.
- **Opt-Out & Deletion:** Players can request account closure and deletion of personal data, subject to compliance and AML retention laws.
- **Data Portability:** Players may request a copy of their personal data in a structured format.

Requests related to data rights can be submitted via email at: support@nioplay.net.

---

6. Internal Training & Employee Responsibilities

All NIOPLAY employees undergo **mandatory data protection training**, including:

- Recognizing and reporting potential data breaches.
- Secure handling of player PII.
- Compliance with responsible gaming, AML, and financial regulations.

*Employees found in violation of data protection policies face **immediate suspension and potential termination.***

---

7. Updates to this Policy

This Data Protection Policy will be reviewed **annually** and updated as necessary to comply with new laws, industry standards, and technological advancements.

*For any inquiries regarding this policy, please contact our **Data Protection Officer** at **compliance@nioplay.net**.*

NIOPLAY – Protecting Player Data, Ensuring Fair Play.