



78CEF Hagley Park Road,  
Kingston 10, Jamaica, W.I.  
Tel: (876) 758-5601; 630-1353  
Fax: (876) 758-7594; 758-4904  
Email: info@bgjc.gov.jm  
Web: www.bgjc.gov.jm

September 13, 2023

**CIRCULAR LETTER TO:**

**ALL GAMING MACHINE OPERATORS - GAMING LOUNGES**

- Chief Executive Officers
- Chief Operating Officers
- Nominated Employees
- Compliance Officers
- Other Principal Senior Officers
- Other Relevant Personnel

**REF: CIR-006-09-2023**

***Data Privacy and Anti-Money Laundering Requirements in the Gaming Sector***

---

The information provided within this circular is for general information purposes only. You are encouraged to confirm any information from or through the Office of the Information Commissioner (OIC) and review all information regarding your obligations under the Data Protection Act (DPA). Gaming operators should consult with appropriate professionals of the OIC for advice concerning specifics of the DPA.

**I. INTRODUCTION**

**A. Overview of the Gaming Industry:**

The gaming industry in Jamaica has experienced substantial growth in recent years, drawing the attention of both local and international visitors. This industry collects vast amounts of sensitive data, including personal information, financial details, and gaming activity records. This abundance of data renders it an appealing target for criminals with various motives. Given its significance as a key contributor to the country's economy, it becomes imperative for this sector to uphold rigorous standards of integrity and trustworthiness. The primary objective of this policy paper is to address data protection and anti-money laundering (AML) concerns within the gaming sector, with the ultimate goal of safeguarding customer information and thwarting illicit financial activities.

## **B. Importance of Data Privacy and AML Compliance:**

Data privacy and AML compliance are critical components of the gaming sector's operations. Ensuring the confidentiality, integrity, and availability of customer data is essential to maintaining the trust of patrons and protecting their sensitive information. Simultaneously, stringent AML measures are necessary to prevent the infiltration of criminal funds into the sector, thereby safeguarding the reputation of the gaming industry and Jamaica's financial system.

## **C. Purpose of the Circular:**

This circular aims to alert all gaming operators in Jamaica of some of their responsibilities under the DPA regulated by the Office of the Information Commissioner. The Betting, Gaming, and Lotteries Commission (BGLC), expects gaming operators to take these into consideration given the principles outlined to uphold their legal obligations, protect customer data, and contribute to the overall safety and stability of the gaming sector.

## **II. DATA PRIVACY IN THE GAMING SECTOR**

### **A. Understanding Data Privacy:**

- **Definition and Scope:**

Data privacy refers to the protection of personal information collected from individuals during their interactions with gaming operators. This includes data such as names, addresses, contact details, financial information, and other identifiable information. The scope of data privacy encompasses the entire data lifecycle, from collection to processing, storage, and eventual disposal.

- **Data Controller:**

Data controllers are people or entities, including gaming operators, that decide how to treat the personal information of data subjects<sup>1</sup>.

---

<sup>1</sup> Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

- **Types of Personal Information Collected:**

Gaming operators typically gather various types of personal information from customers, such as identification documents, financial transaction records, and customer preferences. Additionally, they may collect data from surveillance systems, loyalty programs, and online interactions.

- **Legal and Regulatory Frameworks:**

Jamaica has recently introduced the Data Protection Act (DPA) of 2020, a significant piece of legislation that governs the handling of personal data by both organizations and individuals operating within the country. This legislation meticulously outlines the general scope, standards, and oversight mechanisms for handling personal data, thereby empowering all sectors including the gaming operators to enhance their personal data protection measures.

Every identifiable Jamaican individual is recognized as a data subject and, under this Act, is endowed with several fundamental rights. These rights encompass but are not limited to, the right to be informed about the processing of their data, including the purpose and recipients of such processing. Additionally, individuals possess the right to seek compensation for any harm or suffering incurred as a result of a data controller's infringement of the Act.

It is imperative to note that Jamaican gaming operators must not only adhere to the Data Protection Act but also remain compliant with other relevant international data protection regulations, such as the General Data Protection Regulation (GDPR), particularly when interacting with customers from regions covered by these regulations.

## **B. Data Collection and Processing Practices:**

- **Customer Information Collection**

Gaming operators should clearly communicate the purpose of data collection to customers and only collect data that is necessary for legitimate business purposes. For example, collecting identification information is crucial for age verification and preventing underage gambling.

- **Purpose of Data Processing:**

Data should be processed only for specified purposes and not used for activities beyond the original intention. For instance, customer data gathered for loyalty programs should not be used for marketing purposes without explicit consent.

- **Consent and Transparency:**

Gaming operators must obtain informed and explicit consent from customers before processing their data. Transparency in data processing practices involves providing customers with clear and easily accessible privacy policies and information about their rights.

### **C. Data Retention and Deletion Policies:**

- **Retention Periods for Customer Data:**

Operators should establish appropriate retention periods for customer data, considering legal requirements and business needs. For instance, financial transaction records might be retained for a specific period for audit and AML purposes.

- **Secure Data Deletion Methods:**

When customer data is no longer needed, secure deletion methods should be employed to prevent unauthorized access. This may involve overwriting, encryption, or physical destruction of data.

### **D. Cross-Border Data Transfers:**

- **Transfer Mechanisms and Adequacy Agreements<sup>2</sup>:**

If personal data is transferred outside Jamaica, operators must ensure compliance with cross-border transfer regulations. Adequacy agreements or other transfer mechanisms, such as standard contractual clauses, may be necessary to maintain data protection standards.

- **Third-Party Data Processors and Subprocessors:**

When engaging third-party data processors, gaming operators should conduct due diligence to ensure these entities also adhere to adequate and relevant data protection and security standards.

### **E. Data Subject Rights and Requests:**

- **Procedures for Handling Data Subject Requests:**

---

<sup>2</sup> Adequacy agreements are a formal means of recognising that personal data exported from one jurisdiction to another will be subject to comparable data protection standards in the country where the importer is based.

Operators must establish procedures to handle data subject rights requests promptly. These requests may include access to personal data, rectification, erasure, and restriction of processing.

- **Timelines and Documentation:**

Gaming operators should respond to data subject requests within the timeframe mandated by the relevant data protection laws. Additionally, operators must maintain detailed documentation of these requests and the actions taken in response.

### **III. ANTI-MONEY LAUNDERING REQUIREMENTS AND DATA PROTECTION**

#### **A. Anti-Money Laundering (AML) Compliance in the Gaming Sector:**

- **Regulatory Landscape:**

Gaming operators in Jamaica are subject to the Proceeds of Crime Act (POCA) and must adhere to AML regulations and guidance issued by the relevant authorities. This includes appointing an AML Compliance Officer to oversee AML efforts.

- **AML Compliance Officer Role and Responsibilities:**

The AML Compliance Officer is responsible for developing, implementing, and monitoring the gaming operator's AML program. They should ensure ongoing training of staff and timely reporting of suspicious transactions to the Financial Investigations Division (FID).

#### **B. Integrating Data Protection with AML:**

- **Managing AML Data and Data Protection:**

While implementing AML measures, gaming operators must also consider data privacy. AML data, such as suspicious transaction reports, customer due diligence and customer transactions must be securely stored and accessed only by authorized personnel to prevent data breaches.

- **Safeguarding Customer Data during AML Checks:**

When conducting customer due diligence and enhanced due diligence for high-risk customers, operators should handle sensitive data with utmost care, adhering to data protection principles.

## **IV. ESTABLISHING A DATA BREACH PROTOCOL IN GAMING OPERATIONS**

### **A. Recognizing Data Breach Risks:**

- **Common Data Breach Vulnerabilities in Gaming Operators:**

Operators face various data breach risks, including cyber-attacks, insider threats, and physical theft of data storage devices. Recognizing these vulnerabilities is crucial for developing effective data breach response plans.

- **Potential Consequences of Data Breaches:**

Data breaches can lead to reputational damage, financial losses, legal consequences, and regulatory penalties. Addressing breaches promptly can mitigate these potential consequences.

### **B. Creating a Data Breach Response Team:**

- **Roles and Responsibilities of Team Members:**

The Data Breach Response Team should include representatives from the IT, legal, management, and communications departments. Each member must have clear roles and responsibilities during a data breach incident.

- **Training and Readiness:**

Team members should undergo regular training and simulations to ensure they are prepared to respond effectively to data breaches.

### **C. Developing a Data Breach Response Plan:**

- **Preparing a Detailed Response Plan:**

The Data Breach Response Plan should outline step-by-step procedures for identifying, containing, and mitigating data breaches. It should also specify how to assess the severity of breaches and report incidents to regulatory authorities.

- **Incident Documentation and Communication:**

The plan should emphasize the importance of documenting all actions taken during the data breach incident. Additionally, it should outline how and when to communicate with affected individuals, regulators, and other stakeholders.

## **D. Customer Notification and Support:**

- Timelines and Procedures for Customer Notification:

Operators must promptly notify affected customers of data breaches, providing them with clear and concise information about the incident, potential risks, and measures taken to protect their data.

- Providing Assistance and Support to Affected Customers:

Operators should offer support to affected customers, such as credit monitoring services or assistance in mitigating the impact of the breach on their personal and financial well-being.

## **E. Post-Breach Analysis and Improvement:**

- Identifying Lessons Learned:

After addressing the data breach, operators should conduct a post-incident analysis to identify weaknesses and areas for improvement in their data protection and AML protocols.

- Implementing Security Measures and Best Practices:

Based on the lessons learned, operators should implement security measures and best practices to enhance data protection and prevent future breaches.

## **WHAT IS REQUIRED NOW?**

### **Responsibilities of Data Controllers (Gaming Machine Operators)**

#### **1. Register with the Information Commissioner**

All gaming operators must submit to the Information Commissioner the following information:

- The data controller's Registration Particulars (the Commissioner must be kept informed of any changes in those Particulars);
- A general description of measures to be taken by the data controller to ensure compliance with the seventh data protection standard, that is, to ensure appropriate technical and organizational measures are taken –
  - (i) against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

- (ii) to ensure that the Commissioner is notified, without any undue delay, of any breach of the data controller's security measures which affect or may affect any personal data; and
- (iii) where applicable, a statement of fact that the Particulars provided do not include Particulars in relation to –
  - a) personal data processed; or
  - b) data controller, of a particular description, specified by the Minister, to be excluded from the requirement to submit Registration Particulars, by Order published in the *Gazette*.

Registration Particulars to be submitted to the Commissioner include the following:

- The data controller's name, address, and other relevant contact information;
- Where the data controller has appointed a data controller representative, the name, address, and other relevant contact information of the data controller representative;
- The name, address, and other relevant contact information of the data protection officer appointed by the data controller;
- A description of the personal data being, or to be, processed by or on behalf of the data controller and the category or categories of data subjects to which they relate;
- A description of the purpose or purposes for which the personal data are being, or are to be, processed;
- A description of any recipient or recipients to whom the data controller intends, or may wish, to disclose the personal data;
- The names of any State or territories outside of Jamaica to which the data controller directly or indirectly transfers or intends or may wish directly or indirectly to transfer, the personal data; and
- Any other information about the data controller is required in regulations issued by the Commissioner.

The addresses of data controllers and data controller representatives are –

- a) In the case of a registered company, its registered office; and
- b) In the case of an entity other than a registered company carrying on a business, is that entity's principal place of business in Jamaica.



Additionally, registration is to be accompanied by a registration fee.

A data controller is also required to pay a prescribed annual fee for the maintenance of the required Registration Particulars of the data controller in the Commissioner's Register. No entry shall be retained in the Register for longer than twelve months, except on the payment of the prescribed annual fee.

## **2. Appoint a Data Protection Officer**

Under the Act's provisions, each gaming operator is mandated to designate a qualified individual as a Data Protection Officer (DPO). This appointed officer must fulfil specific criteria: they must either be a Jamaican resident, represent a business that is established and registered in Jamaica, or be an individual with a recognized professional practice based in Jamaica.

The primary responsibility of the DPO is to:

- a) **Advice:** guide organizations in crafting and implementing data protection policies and procedures, while also educating staff about data-related risks and responsibilities. Additionally, serve as the liaison with the Information Commissioner to address DPA-related issues.
- b) **Data Protection Impact Assessments (DPIAs):** lead DPIAs for high-risk data processing activities, assessing privacy impacts and proposing risk-mitigation strategies.
- c) **Monitoring:** routinely oversee data processing to ensure compliance and recommend corrective measures as needed.
- d) **Data Breach Management:** investigate and manage data breaches, facilitate communication with affected individuals, report to the Information Commissioner, and suggest preventive measures.

## **3. Prepare to Submit the Data Protection Impact Assessment**

Data controllers, including gaming operators, are mandated to submit a Data Protection Impact Assessment to the Commissioner within ninety (90) days following the conclusion of each calendar year. This assessment is required to encompass the following key details:

- A description of planned personal data processing, its purposes, and any relevant legitimate interests pursued by the data controller.

- An evaluation of the necessity and proportionality<sup>3</sup> of processing in relation to these purposes.
- Measures to anticipate and address risks, including safeguards, security measures, and mechanisms to ensure compliance with the Data Protection Act compliance, while considering the rights and interests of data subjects and others concerned.

#### 4. Comply with Data Protection Standards

The Act outlines eight fundamental requirements that data controllers must adhere to when processing personal data:

- **Fair and Lawful Processing:** Personal data processing is permitted only with the data subject's consent, which should remain valid unless revoked. For sensitive data, written consent is mandatory.
- **Collect for Specified Lawful Purposes:** Data should only be gathered for explicit, legitimate purposes, and any subsequent treatment must align with these original intentions.
- **Data Quality:** Processed personal data must be relevant, adequate, and limited to what's necessary for its intended purpose.
- **Accurate and Current:** Data must be maintained accurately and kept up-to-date.
- **Limited Retention:** When personal data is no longer needed, it must be appropriately disposed of.
- **Processed in accordance with the Rights of Data Subjects:** Personal data handling must respect data subjects' rights, including access, information, rectification, restriction, consent withdrawal, and objection to automated decision-making for marketing.
- **Protected by Appropriate Technical and Organizational Measures:** Robust technical and organizational safeguards should be in place to prevent unauthorized or unlawful processing and to protect against accidental data loss or damage.
- **International Transfers:** Personal data should not be transferred outside Jamaica unless the receiving territory also offers adequate protection for personal data processing.

---

<sup>3</sup> Lawful basis for processing data

## 5. Report a Contravention of a Data Protection Standard or Breach of Security Measure

Starting from December 1, 2023, gaming operators must adhere to specific reporting obligations concerning personal data breaches and contraventions of data protection standards. When they become aware of such incidents, they are required to report them to the Commissioner within 72 hours.

These reports should include:

- A factual account of the breach or contravention.
- A description of the breach, including details about the affected data subjects, and the types and quantity of personal data involved.
- Details about the measures taken or planned to mitigate the potential adverse consequences of the breach.
- Information about the outcomes of the breach.
- Contact details for the Data Protection Officer.

In addition to notifying the Commissioner, data controllers must also inform each affected data subject about the nature of the breach, the measures taken or to be taken to mitigate its effects and provide contact information for the Data Protection Officer. This dual notification process ensures transparency and allows data subjects to take any necessary actions to protect their interests in the event of a breach or contravention.

## 6. Enforcement Mechanism

Non-compliance with these obligations carries significant consequences for data controllers, including:

- **Enforcement Notices:** The Commissioner may serve the data controller with an Enforcement Notice, Assessment Notice, Information Notice, or Fixed Penalty Notice.
- **Criminal Prosecution:**
  - Individual Responsibility: Individuals may face imprisonment or fines.
  - Corporate Entities: Corporate bodies could be fined up to 4% of their annual gross worldwide turnover.
- **Civil Suits:** Individuals who suffer harm due to a data controller's contravention of the Act's requirements have the right to seek compensation for the damages they incur through a civil suit against the data controller.

These repercussions underscore the imperative of strict adherence to data protection regulations and the seriousness with which non-compliance is regarded under the law.

## V. CONCLUSION:

Data privacy and AML compliance are essential for maintaining the integrity and trust of the gaming sector, as well as protecting customers and the financial system from illicit activities. Data protection and AML requirements are continually evolving. Gaming operators must remain proactive in adapting their policies and practices to meet changing regulations and emerging threats, ensuring the gaming sector remains a safe and secure environment for all.


The goal of this **REF: CIR-006-09-2023** is:

- to ensure the gaming operator understands their obligations as it relates to data protection and anti-money laundering requirements;
- to improve staff knowledge to enhance the application of the measures;
- to ensure the gaming operator is in the best position to prevent the gaming lounge from unlawfully collecting, processing, storing and/or disposing of customer information; and
- to ensure compliance with the Data Protection Act and the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019.

Please be guided accordingly.

For further information please contact: The Office of the Information Commissioner  
The Masonic Building (2<sup>nd</sup> Floor)  
45-47 Barbados Avenue, Kingston 5  
(876) 920-4390  
info@oic.gov.jm

Yours sincerely,



.....

Laurie Wiggan (Mrs.)

Director, Compliance & Regulatory

**BETTING, GAMING & LOTTERIES COMMISSION**