JDPA Compliance Checklist

for Small and Medium-Sized Enterprises

A step-by-step checklist covering all 8 Standards of the Jamaica Data Protection Act 2020

Prepared by GHS Data Security Limited

admin@ghsdatasecurity.com | ghsdatasecurity.com

Mandeville, Manchester, Jamaica

How to Use This Checklist

This checklist is designed to help small and medium-sized enterprises (SMEs) in Jamaica assess their compliance with the Jamaica Data Protection Act 2020 (JDPA). Work through each section, tick off the items you have in place, and note the gaps. Use the results to prioritise your compliance activities.

The checklist is organised around the 8 Standards of the JDPA. Each standard includes a set of practical requirements that apply to most SMEs. Some requirements may not apply to your specific business; mark those as N/A.

Organisation Name:	
Date of Assessment:	
Completed By:	
Role / Title:	

Standard 1: Fairness and Lawfulness

- ■ You have identified a lawful basis for processing each type of personal data you hold
- ■ You have a published Privacy Notice that explains how you collect and use personal data
- ■ Your Privacy Notice is easily accessible (e.g., on your website, in your premises)
- ■ You obtain consent where required, and that consent is freely given, specific, and informed
- ■ You keep records of when and how consent was obtained
- ■ You do not use personal data for purposes that the data subject would not reasonably expect

Notes / Actions Required:	

Standard 2: Purpose Limitation

- ■ You have documented the specific purpose for each type of personal data you collect
- ■ You do not use personal data for purposes beyond what was originally specified
- ■ If you need to use data for a new purpose, you obtain fresh consent or identify a new lawful basis
- ■ Marketing communications are only sent to individuals who have opted in

Notes / Actions Required:	

Standard 3: Data Minimisation

- ■ You only collect the minimum personal data necessary for each stated purpose
- ■ You have reviewed your forms and data collection processes to remove unnecessary fields
- ■ You do not collect sensitive personal data unless strictly necessary and legally justified
- ■ You do not retain personal data 'just in case' it might be useful later

Notes / Actions Required:	

Standard 4: Accuracy

- ■ You have processes in place to verify the accuracy of personal data at the point of collection
- ■ You provide a way for data subjects to update their information
- ■ You periodically review stored data for accuracy and correct or delete inaccurate records
- ■ You keep audit trails of changes made to personal data

Notes / Actions Required:	

Standard 5: Storage Limitation

- ■ You have a documented Data Retention Schedule that specifies how long each type of data is kept
- ■ You regularly review and purge data that has exceeded its retention period
- ■ You securely destroy or anonymise personal data when it is no longer needed
- ■ You do not retain personal data indefinitely without a lawful reason
- ■ Employee records are retained in accordance with Jamaican employment law requirements

Notes / Actions Required:	

Standard 6: Rights of Data Subjects

- ■ You have a process for handling Data Subject Access Requests (DSARs)
- ■ You can respond to DSARs within the timeframe required by the JDPA
- ■ You have a process for handling requests for correction of personal data
- ■ You have a process for handling requests for deletion of personal data
- ■ You have a process for handling objections to processing
- ■ Staff members who receive data subject requests know how to escalate them

Notes / Actions Required:	

Standard 7: Security Measures

- ☐ You have implemented appropriate technical measures (encryption, firewalls, access controls)
- ☐ You have implemented organisational measures (policies, training, incident procedures)
- ☐ You restrict access to personal data to only those employees who need it
- ☐ You use strong passwords and multi-factor authentication where possible
- ☐ You have a documented Data Breach Response Plan
- ☐ You can detect and report a data breach to the OIC within 72 hours
- ☐ You conduct regular security assessments or audits
- ☐ You securely dispose of physical records containing personal data (shredding, etc.)
- ☐ You back up personal data regularly and test your backup restoration process

Notes / Actions Required:	

Standard 8: International Transfers

- ☐ You have identified all instances where personal data is transferred outside Jamaica
- ☐ You have assessed whether the receiving country provides adequate data protection
- ☐ You have appropriate safeguards in place for cross-border transfers (contracts, encryption)
- ☐ You have conducted a Transfer Impact Assessment for each international transfer
- ☐ Your cloud service agreements include data processing terms that meet JDPA requirements
- ☐ You know the physical location of your data for all cloud-hosted services

Notes / Actions Required:	

General Compliance Requirements

- ☐ You are registered as a Data Controller with the OIC
- ☐ Your OIC registration is current and has been renewed for the current registration year
- ☐ You have a completed Record of Processing Activities (ROPA)
- ☐ You have appointed a Data Protection Officer or engaged a Fractional DPO
- ☐ You have conducted a Data Protection Impact Assessment (DPIA) for high-risk processing
- ☐ All staff who handle personal data have received data protection training
- ☐ You have data processing agreements with all third-party processors
- ☐ You have a documented process for responding to OIC enquiries or investigations
- ☐ Your Board / senior management reviews data protection compliance at least annually

---

Need help filling the gaps? Contact GHS Data Security for a free Gap Analysis.

admin@ghsdatasecurity.com | ghsdatasecurity.com