HOLLKEN & ASSOCIATES

DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Data Privacy & Protection Program

For

Jacqueline Ann Hamilton

Attorney at Law

Polices & Procedure Manual

Last Updated 24.08.2023

By David Holland for Hollken & Associates

HOLLKEN & ASSOCIATES

DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Contents

HOLLKEN & ASSOCIATES

DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Intro & Disclaimer

Jamaica's Data Protection Act 2020 is an all-encompassing legislation designed to protect consumer data and places the responsibility on receiving, processing and storing their Data on your organization.

As of December 1, 2023 the new Data Protection Act (DPA) comes into force.

This program has been specifically designed to provide you with all the tools necessary to successfully register with IOC, and to ensure you are fully compliant .

Its important to note that this Data protection program is a fluid document and should be audited and updated frequently in order to be relevant to your current operating practices

Privacy By design : The DPA requires your organization to consider data protection as an integral part of your operation. This means that when ever you add or modify your processing activities, the Data Protection Act should always be considered before committing to executing new processing activities .

The DPA is an extensive new legislation that takes into consideration not only what data you process but also the data you transfer locally and internationally .

Therefore this hand book should be used as guideline and base tool to amend / improve as you become more knowledgeable and experienced with the DPA

HOLLKEN & ASSOCIATES
DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Data Controllers / Processors Contact information

Official Data Controller

Jacqueline Ann Hamilton

Suite 18A, Montego Freeport Shopping Centre
P.O. Box 145 Fontana
Montego Bay, Jamaica

Ph: 876-979-8200
Ph: 876-979-8184
Fax: 876-684-9974

jacqueline.ann.hamilton@gmail.com

Primary Data Processor

Christina Chin

Suite 18A, Montego Freeport Shopping Centre
P.O. Box 145 Fontana
Montego Bay, Jamaica

Ph: 876-979-8200
Ph: 876-979-8184
Fax: 876-684-9974

jacqueline.ann.hamilton@gmail.com

Data Privacy Policy Notice

HOLLKEN & ASSOCIATES
DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

IMPORTANT NOTE: This policy should be presented to all new clients and be posted on your website and available for ALL past and present clients to view at anytime

Effective Date: August 24, 2023

Thank you for placing your trust in Jacqueline A. Hamilton Attorney-at-Law ("we," "us," or "our"). We respect your privacy and are committed to protecting your personal information. This privacy policy explains how we collect, use, and disclose personal data when you interact with our legal services. Please read this policy carefully to understand our practices regarding your personal information and how we will treat it. By using our services, you consent to the collection and use of your personal data as described in this policy.

About the Information We Collect:

When you engage with our legal firm or visit our website, we may collect and store various types of information, including:

- **Personal Information:** This may include your name, contact details, Financial information, and any other information you provide to us voluntarily that connects you with the data we collect.
- **Device and Log Information:** We may collect information about the device you use to access our services, such as IP address, browser type, operating system, and log files.
- **Website Usage Information:** We may use cookies and similar technologies to collect information about your interactions with our website, such as pages visited, links clicked, and website navigation patterns.

Use of Information:

We may use the information we collect for the following purposes:

- Providing Legal Services: We may use your personal information to communicate with you, third party vendors such as government agencies and financial institutions , respond to inquiries, and provide legal advice and representation.
- Improving Our Services: We may analyze the information to enhance our services, monitor trends, and understand client preferences.
- Legal and Regulatory Compliance: We may use and disclose personal information as required by applicable laws, court orders, or government regulations.
- Marketing Communications: With your consent, we may send you newsletters, event invitations, and other promotional materials related to our legal services.

Data Sharing and Disclosure:

We understand the importance of keeping your personal information confidential. We will not sell, rent, trade, or otherwise disclose your personal information to third parties for their marketing purposes. However, we may share your information with authorized third parties for the following purposes:

- Service Providers: We may engage third-party service providers to perform various functions on our behalf, such as IT support, payment processing, and document management.
- Legal and Business Requirements: We may disclose your personal information to comply with legal obligations, protect our rights and interests.
- Consent: We may share your information with third parties only if you provide explicit consent to do so.

Data Security:

We take reasonable measures to protect your personal information from unauthorized access, disclosure, alteration, and destruction. However, please note that no transmission or storage method over the internet is 100% secure.

Data retention :

We retain your information in both digital and physical format only for the purposes of executing our legal services . Our policy is to keep your information for **8 Years** after your file has been closed where by we will either securely delete or destroy your information.

Your Rights:

You have the right to access, correct, update, and delete your personal information in accordance with the Jamaica Data Protection law . If you would like to exercise any of these rights, please contact the Data Controller Jacqueline A. Hamilton Attorney-at-Law at jacqueline.ann.hamilton@gmail.com

Changes to this Privacy Policy:

We may update this privacy policy from time to time. Any changes we make will be posted on our website. We encourage you to review this policy periodically to stay informed about how we collect, use, and protect your personal information.

Contact Us:

Jacqueline A. Hamilton
Attorney-at-Law
Suite 18A, Montego Freeport Shopping Centre
P.O. Box 145 Fontana
Montego Bay, Jamaica

HOLLKEN & ASSOCIATES
DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Ph: 876-979-8200
Ph: 876-979-8184
Fax: 876-684-9974
www.RealEstateLawJamaica.com

If you have any questions, concerns, or requests regarding this privacy policy or our data practices, please contact us at the above address

This privacy policy is effective as of the date mentioned above and supersedes any prior versions.

Data Consent Notice

HOLLKEN & ASSOCIATES
DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

IMPORTANT NOTE: This policy should be presented and signed by all new clients and old clients once they become active clients again.

Jacqueline Ann Hamilton - Attorney at Law

Data Protection Consent Form

Introduction

By signing this consent form, you acknowledge that you understand and agree to the collection, use, and processing of your personal data by **Jacqueline Ann Hamilton**
in accordance with applicable data protection laws and regulations.

Personal Data

Jacqueline Ann Hamilton may collect and process the following personal data:
- Full name
- Address
- Email address
- Phone number
- Date of birth
- Any other information necessary for the purposes outlined in this consent form.

Purpose of Data Collection

The personal data collected will be used for the following purposes:
- To execute legal services provided by us
- To comply with AML
- To Comply with regulatory requirements

Data Processing

Jacqueline Ann Hamilton may process your personal data by automated means or manually. We will take appropriate security measures to protect your personal data from unauthorized access, disclosure, alteration, or destruction.

Data Sharing

Your personal data may be shared with third parties under the following circumstances:
- To execute legal services

Data Retention

We will retain your personal data for as long as necessary to fulfill the purposes outlined in this consent form, unless a longer retention period is required or permitted by law.

Rights of Data Subjects

As a data subject, you have the following rights with respect to your personal data:
- Right to access and rectify your data
- Right to erase your data
- Right to restrict or object to the processing of your data
- Right to withdraw your consent at any time

Consent to Withdrawal

You have the right to withdraw your consent for the processing of your personal data at any time. To withdraw your consent or exercise any other rights, please contact us using the details provided bellow .

Contact Information

If you have any questions, concerns, or wish to exercise your rights regarding your personal data, please contact us at:

Jacqueline A. Hamilton - Attorney-at-Law, Suite 18A, Montego Freeport Shopping Centre
P.O. Box 145 Fontana
Montego Bay, Jamaica
Ph: 876-979-8200
Ph: 876-979-8184
Fax: 876-684-9974

jacqueline.ann.hamilton@gmail.com

By signing below, you confirm that you have read, understood, and consent to the terms outlined in this form.

Date:
Signature:
Name :

Data Subject Request Procedure

HOLLKEN & ASSOCIATES
DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

STEPS

1. **Acknowledgement:** Acknowledge receipt of the data request and provide a reference number or other identifier for the request.

2. **Verification:** Verify the identity of the requester and ensure that the request is legitimate

3. **Data Location:** Provide information on the location of the requested data, including any relevant data sources or systems

4. **Data Description:** Provide a description of the requested data, including the data types, formats, and any relevant context.

5. **Data Delivery:** Arrange for the secure delivery of the requested data to the requester, using appropriate security measures such as encryption and secure file transfer protocols

6. **Data Erasure:** If the request includes a request for erasure, ensure that the data is securely erased and no longer accessible.

7. **Follow-up:** Follow up with the requester to ensure that the data request has been fulfilled and that the requester is satisfied with the response.

8. **Data Request Logging:** Maintain a log of all data requests, including the requester's name, contact information, request details, response details, and any notable events or issues.

9. **Data Request Metrics:** Track and analyze data request metrics, such as the number of requests received, response times, and request types. Use this information to identify trends, optimize the data request process, and improve customer satisfaction.

10. **Data Request Communication:** Communicate with data subjects about their data requests through clear, concise, and transparent language. Provide information on Your data protection policies, applicable data protection laws, and the status of their requests.

11. **Data Request Training:** Provide regular training and awareness programs for employees on data protection laws, data subject rights, and the data request process.

12. **Data Request Compliance:** Ensure that all data requests are processed in compliance with applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other relevant laws.

13. **Data Request Security:** Implement appropriate security measures to protect personal data during the data request process, including encryption, secure communication channels, and access controls.

14. **Data Request Continuous Improvement:** Regularly review and update the data request process to ensure that it remains effective, efficient, and compliant with applicable data protection laws and regulations.

HOLLKEN & ASSOCIATES
DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Data Breach Response

Introduction

The purpose of this data breach response plan (DBRP) is to outline the steps and procedures that
Jacqueline A. Hamilton
Attorney-at-Law
follow in the event of a data breach. The plan is designed to help protect the organization, its employees, and its customers from the potentially harmful effects of a data breach.

Scope

This DBRP applies to all employees, contractors, and third-party vendors who handle sensitive data on behalf of Jacqueline A. Hamilton Attorney-at-Law It covers all types of data breaches, including but not limited to:

* Unauthorized access to sensitive data
* Unauthorized disclosure of sensitive data
* Loss or theft of devices containing sensitive data
* Unauthorized changes to sensitive data

Data Breach Identification and Reporting

Data breaches can be identified in a variety of ways, including but not limited to:

* Unusual activity on a system or network
* Unauthorized access to sensitive data
* Loss or theft of devices containing sensitive data
* Unauthorized changes to sensitive data

All employees, contractors, and third-party vendors are responsible for reporting any suspected data breaches to the DBRT immediately. The DBRT will then assess the situation and take appropriate action.

Data Breach Containment

The DBRT will take immediate steps to contain the data breach and prevent further damage. This may include:

* Isolating affected systems or networks
* Disconnecting affected systems from the internet
* Changing passwords and encryption keys
* Applying security patches and updates
* Collecting and preserving forensic evidence

Data Breach Investigation

The DBIT will conduct a thorough investigation of the data breach to determine the cause, scope, and impact of the breach. The investigation will include:

* Interviews with employees and contractors
* Analysis of system logs and data
* Review of security footage
* Forensic analysis of affected systems

Data Breach Notification

The DBRT will notify affected individuals and regulatory agencies in accordance with the DPA . The notification will include:

* Timely notice to affected individuals
* Timely notice to the ICO
* Information on the breach, including the type of data accessed or stolen, the number of individuals affected, and the steps being taken to address the breach

Data Breach Communication

The DBRT will develop a communication plan to inform stakeholders of the breach, including:

* Affected individuals
* Regulatory agencies
* Customers
* Partners
* Employees

Data Breach Post-Mortem

The DBRT will conduct a post-mortem analysis of the breach to identify lessons learned and areas for improvement. The analysis will include:

* Reviewing the effectiveness of the DBRP
* Identifying gaps in security controls
* Identifying areas for improvement in incident response
* Documenting lessons learned

Data Breach Prevention

The DBRT will implement measures to prevent future data breaches, including:

* Implementing additional security controls
* Conducting regular security audits

Data Retention Policy

Purpose

The purpose of this data retention policy is to ensure that Jacqueline Hamilton, Attorney-at-Law, retains data for an appropriate length of time, taking into account legal and business requirements, as well as the need to protect sensitive information.

Scope

This policy applies to all data created, received, or maintained by [Organization Name], including but not limited to:

* Customer data
* Employee data
* Financial data
* Marketing data
* Operational data
* Security data

Data Retention Schedule

The following data retention schedule outlines the minimum retention periods for different types of data. The retention periods are based on legal and business requirements, as well as the need to protect sensitive information.

Data Type	Retention Period
Customer data	5 years after last interaction
Employee data	7 years after employment ends
Financial data	7 years after fiscal year end
Marketing data	2 years after last interaction
Operational data	3 years after last interaction
Security data	1 year after last interaction

Data Retention Criteria

The following criteria will be used to determine the retention period for data that is not covered by the data retention schedule:

* **Legal requirements:** Data will be retained for the period required by law or regulation.
* **Business requirements:** Data will be retained for the period necessary to meet business needs and objectives.
* **Sensitive information:** Data that contains sensitive information, such as personal data or confidential business information, will be retained for a shorter period to minimize the risk of unauthorized access or disclosure.

Data Disposition

Data that is no longer required to be retained will be disposed of in a secure and appropriate manner. The following methods of data disposition are approved:

* Shredding
* Erasure
* Overwriting
* Secure deletion

Data Archiving

Data that is no longer actively used but is still required to be retained will be archived. The following data archiving methods are approved:

* Offsite storage
* Cloud storage
* Tape backup

Data Security

All data will be protected from unauthorized access, disclosure, or use. The following data security measures are approved:

* Encryption
* Access controls
* Authentication

* Auditing

Data Breach Notification

In the event of a data breach, Jacqueline Hamilton, Attorney-at-Law, will notify affected individuals and regulatory agencies in accordance with applicable laws and regulations. The notification will include:

* Timely notice to affected individuals
* Timely notice to regulatory agencies
* Information on the breach, including the type of data accessed or stolen, the number of individuals affected, and the steps being taken to address the breach

Data Retention Policy Review

This policy will be reviewed annually or as needed to ensure that it remains current and effective. The review will be conducted by Jacqueline Hamilton, Attorney-at-Law.

Compliance

All employees, contractors, and third-party vendors who handle data on behalf of [Organization Name] are required to comply with this policy. Failure to comply may result in disciplinary action, up to and including termination of employment or contract.

By implementing this data retention policy, Jacqueline Hamilton, Attorney-at-Law, aims to ensure that data is retained for an appropriate length of time, taking into account legal and business requirements, as well as the need to protect sensitive information.

Records of Data Impact Assessments

NONE

HOLLKEN & ASSOCIATES

DATA PRIVACY & PROTECTION COMPLIANCE SPECIALISTS

Further Data Protection Compliance Recommendations

- **Data Security Measures**

  Implement further technical & Organizational Measures to safeguard Personal data against Unauthorized access, Loss or Breaches.

  Conduct regular security assessments & vulnerability testing

- **Training & Awareness**

  Promote a culture of Privacy awareness

- **Vendor Management**
  Assess and monitor 3rd Party vendors data Protection Practices
  Include Data protection clauses in contracts with Vendors

- **Monitoring and Reporting**
  Implement a process to monitor data protection compliance and reporting to the IOC