



Republic Bank (Barbados) Limited

PERSONAL DATA INCIDENT REPORT FORM

Purpose of the Personal Data Incident Report Form

This form is used to document and assess any incidents involving personal data. It helps the Bank identify potential risks, take appropriate action, and ensure compliance with data protection requirements.

A personal data incident is any event that affects the security or handling of personal data. This could include accidental disclosure, loss, or unauthorized access to personal data including a cyber incident or personal data breach.

Example: An email containing a customer's personal details is accidentally sent to the wrong recipient. Even though this may have been an honest mistake and not a deliberate breach, it is still considered a personal data breach because personal data was exposed in a way that was not intended.

Note: Personal Data is any information that can identify a person on its own or when combined with other information (names, contact information, identification numbers, IP address, etc.). Cyber Incident: any event that disrupts or threatens the security of a computer system, network, or digital information. Personal Data Breach: when personal data is accidentally or unlawfully lost, destroyed, changed, shared without permission, or accessed by someone who should not have it.

Need help? Contact the Data Privacy Officer (DPO) at inga.king@rfhl.com or ext. 4037. Required fields are marked with an asterisk ().*

Quick links: [Key Definitions](#) [Frequently Asked Questions](#) [Email the DPO](#)

Section 1: Reporting Individual

Note: Provide your name, role, department, and contact details in case further clarification is needed.

1. Name *

2. Position / Role *

3. Department *

4. Contact Information *

Email

Phone

Section 2: Incident Details

Note: Date of Incident and Date Discovered: specify when the incident occurred and when it was first noticed. Location of Incident: indicate whether it happened on-site, remotely, or externally. Description of Incident: clearly explain what happened, including how it was discovered.

5. Date of Incident (yyyy/mm/dd) and Time of Incident *

Date required. Time optional.

Date

Time

6. Date Incident was Discovered (yyyy/mm/dd) *

7. Location of Incident *

Branch

Department

If Other (Branch or Department), please specify

8. Description of Incident *

What happened? How was it discovered?

Example: "I noticed unusual activity on my work email account at 10 AM on [date]. I received a phishing email asking for my login details."

Section 3: Data Involved

Note: Categories of Personal Data Affected: list the types of data exposed. Number of Data Subjects Affected: estimate how many individuals may be impacted. A data subject is a person whose personal data is collected, stored, or used (customers, employees, or anyone whose data the Bank handles).

9. Categories of Personal Data Affected *

e.g. names, contact information, ID numbers. Provide relevant details of each category.

10. Number of Data Subjects Affected (if known) *

☐ Unknown

11. Does the incident involve Sensitive Personal Data? *

Note: Sensitive Personal Data means personal data on a data subject's racial or ethnic origin; political opinions; religious or similar beliefs; membership of a political body; trade union membership; genetic data; biometric data; sexual orientation or sexual life; financial record or position; criminal record; or proceedings for any offence. It could significantly affect an individual's privacy if misused.

☐ Yes ☐ No

If yes, please specify (select all that apply). Selecting No clears and locks these options:

- | | |
|---|--|
| ☐ Racial or ethnic origin | ☐ Political opinions |
| ☐ Religious or similar beliefs | ☐ Membership in a political organisation |
| ☐ Trade union membership | ☐ Genetic data |
| ☐ Biometric data (e.g. fingerprints, facial recognition) | ☐ Sexual orientation or sex life |
| ☐ Financial records or financial status | ☐ Criminal record, including any offences (committed or alleged), related legal proceedings, and the outcome or sentence imposed by a court |

Section 4: Incident Impact

Note: Potential Risks: explain how the incident could affect individuals (e.g. fraud, identity theft). Notification to Affected Individuals: note whether affected persons have been informed. Mitigation Measures Taken: detail steps taken to minimize harm (e.g. email recall, password reset).

12. Potential risks to individuals *

Select all that apply.

- | | |
|---|--|
| ☐ Identity theft | ☐ Financial fraud or loss |
| ☐ Unauthorised access to accounts | ☐ Reputational harm |
| ☐ Discrimination or unfair treatment | ☐ Loss of confidentiality/privacy |
| ☐ Emotional distress or anxiety | ☐ Phishing or social engineering risk |
| ☐ Misuse of personal information | ☐ Physical safety risk (where applicable) |
| ☐ Loss of employment or business opportunities | ☐ No significant risk identified |
| ☐ Other (please specify) | |

If Other, please specify

13. Have affected individual(s) been notified? *

Note: Affected individual: the person whose personal data is involved in the incident.

- ☐ Yes ☐ No

If yes, method of notification (select all that apply). Selecting No clears and locks these options:

- | | |
|---|--|
| ☐ Email | ☐ Telephone call |
| ☐ SMS/Text message | ☐ Postal mail |
| ☐ In-person | ☐ Secure online portal |
| ☐ Public notice | ☐ Authorised representative |
| ☐ Other (please specify) | |

If Other, please specify

Date of notification (yyyy/mm/dd) and further details

14. Mitigation measures taken *

Note: Mitigation measures are steps taken to reduce harm after a personal data incident. Detail steps taken to minimize harm (e.g. email recall, password reset). If unsure what action to take, consult the IT Security Team, Corporate Security Officer, or DPO.

- ☐ Yes ☐ No

If yes, detail the steps taken

Section 5: Containment and Recovery

Note: Containment: taking immediate steps to stop a personal data incident from getting worse (restricting access, recalling an email, disabling a compromised account). Recovery: actions to fix the issue and prevent recurrence. If unsure how to contain or recover, contact the IT Security Team, Corporate Security Officer, or DPO.

15. Has the incident been contained? *

- ☐ Yes ☐ No

If No, explain the ongoing risks below

16. Steps taken to recover affected data or systems

Section 6: Notification Requirements

Note: External Reporting: indicate if the incident has been reported to law enforcement or any other authority.

17. Has the incident been reported to other departments or external bodies? *

e.g. law enforcement, IT Security Team, Enterprise Risk.

☐ Yes ☐ No

If yes, select all that apply. Selecting No clears and locks these options:

- | | |
|--|---|
| ☐ Information Security | ☐ Cybersecurity Incident Response Team (CSIRT) |
| ☐ Data Privacy Officer | ☐ Legal Services |
| ☐ Enterprise Risk Department | ☐ Compliance Department |
| ☐ Senior Management / Executive Team | ☐ Human Resources |
| ☐ Law Enforcement (e.g. Police) | ☐ Regulator / Supervisory Authority (e.g. CBB) |
| ☐ Third-party service provider / vendor | ☐ Group / Parent Company |
| ☐ Other (please specify) | ☐ Not reported to any other department or body |

If Other, please specify

Section 7: Additional Information

18. Any other relevant details or documents? (Attach files if necessary)

Attach a document

Attached files travel with the saved PDF.

Section 8: Authorization

Note: Sign and date the form before submission.

To sign: type your name in the signature field, or use Adobe Acrobat / Reader Fill & Sign to apply your saved signature or Digital ID. When signed with a Digital ID, Adobe records the date and time of signing automatically.

19. Submitted By - Name *

Position / Role

Signature (sign in Adobe Reader: Digital ID, or Fill & Sign)

Date (yyyy/mm/dd)

20. Reviewed & Approved By (Supervisor / Manager) - Name

Must be a different person from the Submitter.

Position / Role

Signature (sign in Adobe Reader: Digital ID, or Fill & Sign)

Date (yyyy/mm/dd)

Section 9: Frequently Asked Questions & Key Definitions

Frequently Asked Questions (FAQ)

1. What should I do if I suspect a personal data incident?

Report the incident immediately using this form. If you are unsure about any details, provide as much information as possible.

2. Who can I contact if I need help completing the form?

You should contact the Data Privacy Officer (DPO) at inga.king@rfhl.com or ext. 4037 for guidance.

3. What happens after I submit this form?

After you submit the form, the Data Privacy Officer (DPO) will review the incident to assess its impact and determine the next steps.

Investigation: The DPO may gather more details to understand what happened and whether any risks exist.

Reporting Obligations: If the incident meets legal requirements, the Bank may need to report it to the Data Protection Commissioner, other regulators, or the Board of Directors within the required timeframe.

Mitigation Measures: Steps may be taken to limit harm, such as securing accounts, notifying affected individuals, or strengthening security measures to prevent future incidents.

The Bank will handle each case based on its severity, ensuring compliance with regulations while protecting personal data.

4. What are some examples of mitigation measures?

For Emails Sent to the Wrong Recipient: Contact the recipient and request that they delete the email immediately. Confirmation of deletion of emails by sender and recipient. If possible, recall the email (e.g. using Outlook's recall function). Notify the Data Privacy Officer (DPO) for further guidance.

For Lost or Stolen Devices (e.g. laptops, USBs, phones): Remotely wipe or lock the device if possible. Change account passwords linked to the device. Report the loss to IT security and the DPO.

For Unauthorized Access to Systems or Accounts: Reset passwords and enable multi-factor authentication. Delete the user profile. Revoke unauthorized access rights. Conduct a security review to identify vulnerabilities.

For Physical Documents Lost or Misplaced: Attempt to retrieve the document if safe and possible. Inform the relevant department and assess the impact. Secure remaining physical records to prevent further loss.

Key Definitions

Biometric Data: Information about your unique physical or behavioral characteristics that can be used to identify you, such as your fingerprints, facial features, or voice.

Containment: Taking immediate steps to stop a personal data incident from getting worse. This could include restricting access, recalling an email, or disabling a compromised account.

Cyber Incident: Any event that disrupts or threatens the security of a computer system, network, or digital information. For example, a hacker trying to break into a system or malware infecting a computer would be considered a cyber incident.

Data Subject: An individual whose personal data is collected, stored, or processed. For example, customers, employees, or any other individuals whose data is held by the Bank.

Mitigation measures: Steps taken to reduce harm after a personal data incident occurs. These actions help protect affected individuals and prevent further issues. They also help contain the incident, minimize risks, and reduce the likelihood of future occurrences.

Personal Data: Personal Data is any information that can identify a person on its own or when combined with other information. This can include names, contact information, identification numbers, IP address etc.

Personal Data Breach: A Personal Data Breach happens when personal data is accidentally or unlawfully lost, destroyed, changed, shared without permission, or accessed by someone who should not have it.

Personal Data Incident: Any event that affects the security or handling of personal data. This could include accidental disclosure, loss, or unauthorized access to personal data including a cyber incident or data breach.

Recovery: Involves actions to fix the issue and prevent it from happening again. This may include restoring lost data, strengthening security measures, or updating policies.

Sensitive Personal Data: Sensitive Personal Data means personal data consisting of information on a data subject's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a political body; membership of a trade union; genetic data; biometric data; sexual orientation or sexual life; financial record or position; criminal record; or proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings. This is data that could significantly affect an individual's privacy if misused.

Official Use Only

Comments (DPO)

Reviewed By (DPO): Name

Date (yyyy/mm/dd)

Validate and Email to DPO

Validate and Print / Save