PremiumTrust Bank

Personal Data Breach Notification Procedure

Classification: Internal
April 2023
Document Number: PTB/ICS/23/0011
Status: Approved

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
March 2023	V1.0	Document creation	Information & Cyber Security Group

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Contents

1 Introduction 4
2 Personal data breach notification procedure 5
2.1 The controller(s) of the personal data 5
2.2 The supervisory authority 5
2.2.1 Deciding whether to notify the supervisory authority 6
2.2.2 How to notify the supervisory authority 7
2.3 Data subjects 7
2.3.1 Deciding whether to notify data subjects 8
2.3.2 How to notify data subjects 8

Tables

Table 1: Supervisory authority contact details 6

1 Introduction

This procedure is intended to be used when an incident of some kind has occurred that has resulted in, or is believed to have resulted in, a loss of personal data. This document should be used in conjunction with the Information Security Policy Manual, which describes the overall process of reacting to an incident affecting the information security of PremiumTrust Bank Limited.

It is a requirement of the Nigeria Data Protection Regulation (NDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. If the 72-hour target is not met, reasons for the delay must be given.

In the situation where we are acting as a processor, there is an obligation to inform the data controller(s) of the personal data about the breach "without undue delay".

Where an incident affects personal data for which we are a controller, a decision must be taken regarding the extent, timing, and content of communication with data subjects. The NDPR requires that communication must happen "without undue delay" if the breach is likely to result in "a high risk to the rights and freedoms of natural persons".

The actions set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding what to do. However, it is intended that the steps set out here will prove useful in ensuring that our obligations under the NDPR are fulfilled.

This procedure should be considered in conjunction with the following related documents:

- Information Security Incident Response Procedure
- NDPR Controller-Processor Agreement Policy
- Data Protection Impact Assessment Process
- Records Retention and Protection Policy
- Data Protection Policy

2 Personal data breach notification procedure

Once it has been decided that a breach of personal data has occurred, there are three parties who may be required by the NDPR to be informed. These are:

1. The controller(s) of the personal data
2. The supervisory authority
3. The data subjects affected.

It is not a foregone conclusion that the breach must be notified; this depends upon an assessment of the risk that the breach represents to "the rights and freedoms of natural persons". The following sections describe how this decision must be taken and what to do if notification is required.

2.1 The controller(s) of the personal data

Where PremiumTrust is acting as a processor of personal data on behalf of one or more controllers, there is an obligation to inform each controller about the breach "without undue delay". It will then be up to the controller to decide whether it needs to be reported, and to take subsequent actions.

In order to allow the controller to meet the requirements of the NDPR, PremiumTrust will need to provide the following information to them:

- The date and time that the breach was discovered.
- The date and time that the breach is believed to have occurred.
- The data items included e.g. name, address, bank details, biometrics.
- The volume of data involved.
- The number of data subjects affected.
- The nature of the breach e.g. theft, accidental destruction
- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used.
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The actions that have been taken to manage the impact of the breach.
- Contact details of the person handling the breach within our organisation
- Any other factors that are deemed to be relevant.

Where more than one controller is involved, care must be taken to ensure that only information about each individual controller's personal data is provided.

2.2 The supervisory authority

Where PremiumTrust is the controller of the personal data involved, the supervisory authority may need to be informed. The supervisory authority contact details for the purposes of the NDPR for PremiumTrust is as follows:

NAME	Nigeria Data Protection Bureau (NDPB)
ADDRESS	No. 5, Donau Crescent, off Amazon Street, Maitama, Abuja, Nigeria
TELEPHONE	+234 (0) 916 061 5551
EMAIL	info@ndpb.gov.ng

Table 1: Supervisory authority contact details.

2.2.1 Deciding whether to notify the supervisory authority

The NDPR states that a personal data breach shall be notified to the supervisory authority "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". This requires that the organisation assesses the level of risk before deciding whether to notify.

Factors to be considered as part of this risk assessment should include:

- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used.
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The data items included e.g. name, address, bank details, biometrics.
- The volume of data involved.
- The number of data subjects affected.
- The nature of the breach e.g. theft, accidental destruction
- Any other factors that are deemed to be relevant.

Parties involved in this risk assessment may include representatives from the following areas, depending on the nature and circumstances of the personal data breach:

- Senior management
- Business area(s)
- Technology
- Information security
- Legal
- Data protection officer

The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by top management. The result of the risk assessment should include one of the following conclusions:

1. The personal data breach does not require notification.

2. The personal data breach requires notification to the supervisory authority only.
3. The personal data breach requires notification both to the supervisory authority and to the affected data subjects.

These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

2.2.2 How to notify the supervisory authority

If it is decided to notify the supervisory authority, the NDPR requires that this be done "without undue delay and, where feasible, not less than 72 hours after having become aware of it". If there are legitimate reasons for not having given the notification within the required timescale, these reasons must be given as part of the notification.

The notification should be given via appropriate secure means to the body listed in Table 1, using the form Personal Data Breach Notification Form as a template.

The following information must be given as part of the notification:

1. The nature of the personal data breach, including, where possible:
    a. Categories and approximate number of data subjects concerned.
    b. Categories and approximate number of personal data records concerned.
2. Name and contact details of the data protection officer or other contact point where more information may be obtained.
3. A description of the likely consequences of the personal data breach
4. A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.
5. If the notification falls outside of the 72-hour window, the reasons why it was not submitted earlier.

Written confirmation should be obtained from the supervisory authority that the personal data breach notification has been received, including the date and time at which it was received. Where necessary, the NDPR allows the information to be provided in phases without undue further delay.

Documentation of the personal data breach, including its effects and the remedial action taken, will be produced as part of the Information Security Policy Manual.

2.3 Data subjects

Where PremiumTrust is the controller of the personal data involved, the affected data subjects may also need to be informed.

2.3.1 Deciding Whether to Notify Data Subjects

The NDPR states that a personal data breach shall be notified to the data subject "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons".

The risk assessment carried out earlier in this procedure will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the NDPR.

Notification to affected data subjects is also not mandated by the NDPR where it "would involve disproportionate effort". However, in this case a form of public communication should be used instead.

Again, this may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

2.3.2 How to Notify Data Subjects

Once it has been decided that the breach justifies communication to the data subjects affected, the NDPR requires that this be done without undue delay.

The communication to the affected data subjects "shall describe in clear and plain language the nature of the personal data breach" and must also cover:

1. Name and contact details of the Data Protection Officer or other contact point where more information may be obtained.
2. A description of the likely consequences of the personal data breach
3. A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

In addition to the points required by the NDPR, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.

In most cases it will be appropriate to notify affected data subjects via email or in order to ensure that the message has been received and that they have an opportunity to take any action required.