PremiumTrust Bank

Data Protection Impact Assessment Procedure

Classification: Internal

April 2023

Document Number: PTB/ICS/23/0016

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.

Table of Content

1. Introduction/Purpose

Efficient information management requires adequate accountability structure, policy and procedure documents, trained staff, and an effective governance process. The procedure document sets out PremiumTrust's approach for conducting a Data Protection Impact Assessment (DPIA).

The purpose of this document is to address any concerns and risks involved in processing/sharing of personal data, complying with the requirement of data protection by design and default, ensuring that the rights and freedom of individuals are not compromised, and mitigating any risks identified.

2. Scope

All projects that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a Data Protection Impact Assessment (DPIA).

3. Responsibilities

3.1 Data Protection Officer

- The Data Protection Officer (DPO) is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.
- The Data Protection Officer (DPO) is responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

3.2 Risk Owner

- Risk Owner(s) is/are responsible for implementing any privacy risk solutions identified.
- The risk owner is also responsible for checking that appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

4. Procedure

4.1 Identify the Need for a DPIA

The Data Protection Officer (DPO) identifies the need for a DPIA at the start of each project, assessing the project and type of personal data involved, or processing activity, against the screening questions set out in the DPIA tool workbook.

As specified in the NDPR framework, an impact assessment shall be required where the proposed processing involves:

a) evaluation or scoring (profiling).
b) automated decision-making with legal or similar significant effect
c) systematic monitoring
d) when sensitive or highly Personal Data is involved
e) when Personal Data Processing relates to vulnerable or differently-abled data subjects; and
f) when considering the deployment of innovative processes or application of new technological or organizational solutions.

If there is uncertainty regarding whether it is appropriate to carry out a data protection impact assessment for a specific project, by default the project team should err on the side of caution and ensure that one is performed. The Data Protection Officer may also be consulted for clarification.

4.2 Document the Purpose and Use of Personal Data

PremiumTrust Bank records key information about all personal data processed for each project in the DPIA Tool workbook. This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level definitions below).

PremiumTrust captures the type of processing activity associated with the personal data being processed as part of the project in the DPIA Tool workbook. These are categorized as:

- Collection
- Transmission
- Storage
- Access
- Deletion

PremiumTrust establishes on what lawful basis the data is being processed and its appropriate retention period in line with the business continuity plan.

PremiumTrust identifies the category of data processed, whether it is personal, special or that of a child, and the format of the data.

PremiumTrust identifies who has access to the data (individuals, teams, third-parties, or data processors) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and/or if it is trans-border processing.

4.3 Identify and Define the Risks

PremiumTrust identifies the privacy risks for each process activity. The identification of risks will be performed by a combination of group discussion and interview with interested parties.

Such interested parties will normally include (where possible):

- Manager(s) responsible for each activity
- Representatives of the people that normally carry out each aspect of the activity.
- Providers of the inputs to the activity (including, where appropriate, the data subject)
- Recipients of the outputs of the activity
- Appropriate third parties with relevant knowledge
- Representatives of those providing supporting services and resources to the activity
- Any other party that is felt to provide useful input to the risk identification process.

Identified risks will be recorded with as full a description as possible that allows the likelihood and impact of the risk to be assessed. Each risk should also be allocated an owner.

4.4 Analyse Privacy Risks

4.4.1 Determine the Likelihood

PremiumTrust estimates the likelihood of a risk occurring. The Bank would also consider whether it has happened before either in its organisation or similar organisations in the same industry or location and whether there exists enough motive, opportunity, and capability for a threat to be realised.

The likelihood of each risk would be graded on a numerical scale of 1 (low) to 3 (high). General guidance for the meaning of each grade is given in table 1 below.

When assessing the likelihood of a risk, existing controls should be considered. This may require an assessment to be made as to the effectiveness of existing controls.

GRADE	DESCRIPTION	SUMMARY
1	Low	Has never happened before and there is no reason to think it is any more likely now
2	Medium	There is a possibility that it could happen, but it probably won't
3	High	On balance, the risk is more likely to happen than not

Table 1 Likelihood criteria

The rationale for allocating the grade given would be recorded to aid understanding and allow repeatability in future assessments.

4.4.2 Determine the Impact

PremiumTrust estimates the impact that the risk could have on the rights and freedoms of the data subject. The Bank would also consider existing controls that lessen the impact, as long as these controls are seen to be effective.

The impact of each risk should be graded on a numerical scale of **1** (low) to **3** (**high**). General guidance for the meaning of each grade is given in table 2.

GRADE	DESCRIPTION	SUMMARY
1	Low	Data subjects will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)
2	Medium	Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, discrimination, subpoena, extra costs, denial of access to business services, fear, stress, physical ailments, lack of understanding etc.).
3	High	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death etc.).

Table 2 impact criteria

4.4.3 Determine the Risk Score

Using the criteria shown in table 2, following the likelihood and impact grading, a score is calculated for each risk by multiplying the two numbers. Producing a calculated risk score, PremiumTrust identifies the risk to the rights and freedoms of data subjects as shown in table 4.

	3	3	6	9
Likeli hood	**2**	2	4	6
	1	1	2	3
		1	**2**	**3**
			Impact	

Table 3 likelihood impact matrix

Risk Level	From	To	NDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk

Table 4: Risks to rights and freedoms of data subjects

The classification of each risk will be recorded as input to the risk evaluation stage of the process.

3.5 Risk Evaluation

PremiumTrust decides which risks can be accepted and which ones need to be treated. This should consider the risk acceptance criteria established for this specific risk assessment (see Risks to rights and freedoms of data subjects, above).

PremiumTrust will prioritize analysed risks for risk treatment based on the risk score and classification established above.

3.6 Risk Treatment

PremiumTrust identifies solutions to privacy risks to reduce either the likelihood or impact (or both) of each risk to bring it within acceptable bounds, assigns a risk treatment owner, and sets a target date for completion.

The following options may be applied to the treatment of the risks that have been agreed to be unacceptable:

- **Modify the risk** - apply appropriate controls to lessen the likelihood and/or impact of the risk
- **Avoid the risk** by taking action that means it no longer applies
- **Share the risk** with another party, e.g., insurer or vendor/supplier.

The evaluation of the treatment options will result in the production of the Data Protection Impact Assessment (DPIA) report which will detail:

- A description of the proposed processing operations and the personal data involved.
- The purposes of the processing including, where applicable the legitimate interest of the controller of the personal data as defined by the NDPR.
- An assessment of the necessity and proportionality of the processing
- The results of the assessment of the risks to the rights and freedoms of the data subjects
- Whether each risk is recommended for acceptance or treatment
- Priority of risks for treatment
- Risk owners.
- Recommended treatment option
- Control(s) to be implemented.
- Responsibility for the identified actions
- Timescales for actions
- Residual risk levels after the controls have been implemented.

3.7 Obtain Management Approval

Management will approve the data protection impact assessment. In addition to overall management approval, PremiumTrust risk owner, in consultation with Data Protection Officer (DPO), signs off the acceptance or treatment of each risk.

Once the risk treatment plan has been approved, the necessary actions should be tracked and completed as part of the day-to-day control of the project.

3.8 Regular Review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business process, such as introduction or new or changed IT services.