Guidelines for Risk Assessment and Personal Data Breach Notification Khon Kaen University

Prepared by The Secretariat of the Personal Data Protection Committee
Khon Kaen University

Translate by Gemini-2.5-pro

Preface

These Guidelines for Risk Assessment and Personal Data Breach Notification serve as a practical guide for the consideration of the Khon Kaen University Personal Data Protection Committee and the University's Data Protection Officer (DPO). They are intended to direct the process of notifying the Office of the Personal Data Protection Committee (PDPC) and the data subjects of personal data breaches, in accordance with the Personal Data Protection Act, B.E. 2562 (2019). This document compiles the principles, methods, and procedures for risk assessment and breach notification, along with relevant laws and announcements from the Personal Data Protection Committee, to establish a standard of practice. This will ensure that the University's personal data protection operations comply with legal requirements and are executed effectively.

The Secretariat of the Khon Kaen University Personal Data Protection Committee sincerely hopes that these Guidelines will prove beneficial to all relevant personnel.

Secretariat of the Personal Data Protection Committee

Khon Kaen University

Table of Contents

Translate by Gemini-2.5-pro

Guidelines for Risk Assessment and Personal Data Breach Notification

Part 1: Introduction

Background

The infringement of personal data privacy rights continues to be a prevalent issue. Such personal data breaches cause significant distress, annoyance, and damage to data subjects. Furthermore, technological advancements have made the collection, use, or disclosure of personal data in a manner that constitutes a breach easy, convenient, and swift. Subsequently, the Personal Data Protection Act, B.E. 2562 (2019) was enacted to establish principles, mechanisms, and measures for regulating the protection of personal data. Regarding personal data breach notification, Section 37 (4) of the aforementioned Act requires the Data Controller to notify the Office of the Personal Data Protection Committee of a personal data breach without undue delay and within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The Data Controller must also notify the data subject of the breach and the remedial measures without undue delay. The notification process, including any exemptions, must adhere to the rules and methods prescribed by the Personal Data Protection Committee. Consequently, the Committee issued the "Announcement of the Personal Data Protection Committee Re: Rules and Methods for Personal Data Breach Notification, B.E. 2565 (2022)." This Announcement sets out key details and procedures that Data Controllers must follow when a breach occurs. This includes details to consider in the risk assessment, the process for notifying the data subject, and other information beneficial to Data Controllers.

To ensure that Khon Kaen University's personal data protection operations are conducted correctly and orderly, the Secretariat of the Khon Kaen University Personal Data Control Committee, in its capacity as the supporting body for the Committee's operations—which is responsible for establishing rules, methods, practices, or other actions to govern the collection, use, or disclosure of personal data by Khon Kaen University in compliance with the Personal Data Protection Act, B.E. 2562 (2019) has therefore compiled examples of risk assessments and methods for personal data breach notification. These are intended to serve as a comparative guide for operations and for managing potential personal data breach incidents that may occur within the university in the future.

Objectives

To serve as a guideline for the risk assessment and notification of personal data breaches for the Khon Kaen University Personal Data Control Committee and the Data Protection Officer (DPO) of Khon Kaen University. Additionally, it aims to provide operational guidance for personnel within the university whose duties involve notifying such incidents to the Office of the Personal Data Protection Committee and the data subjects, in accordance with the law.

Scope and Missions

These guidelines for risk assessment and personal data breach notification cover the personal data protection responsibilities of the university in the event of a potential breach of personal data of other individuals that is under the control of the university. The Khon Kaen University Personal Data Control Committee is responsible for assessing the risk and notifying the Office of the Personal Data Protection Committee and the data subjects of the extent to which the personal data breach poses a risk to the rights and freedoms of the individual data subject.

Definitions

"University" means Khon Kaen University.

"Office" means the Office of the Personal Data Protection Committee, or PDPC.

"Personal Data Control Committee" means the Khon Kaen University Personal Data Control Committee.

"Data Protection Officer" means the Data Protection Officer of Khon Kaen University.

"Data Controller" means the Khon Kaen University Personal Data Control Committee, which has the authority to make decisions regarding the collection, use, or disclosure of personal data.

"Personal Data Breach" means a breach of security measures that leads to the unauthorized or unlawful loss, access, use, alteration, modification, or disclosure of personal data, whether caused intentionally, willfully, or negligently; committed without authorization or unlawfully; or resulting from a computer-related offense, a cybersecurity threat, an error or defect, or any other cause.

Expected Benefits

The Khon Kaen University Personal Data Control Committee, the Data Protection Officer (DPO) of Khon Kaen University, and personnel within the university whose duties involve personal data protection will understand the guidelines for assessing risk and notifying the Office of the Personal Data Protection Committee and data subjects of personal data breaches, in accordance with the law.

Part 2: Risk Assessment and Notification of Personal Data Breaches

“Personal Data Breach” means a breach of security measures that leads to the loss, access, use, alteration, modification, or disclosure of personal data without authorization or unlawfully, whether caused by intention, willfulness, or negligence; committed without authorization or unlawfully; or resulting from a computer-related offense, a cybersecurity threat, an error or defect, or any other cause.

Furthermore, the "Announcement of the Personal Data Protection Committee Re: Rules and Methods for Personal Data Breach Notification, B.E. 2565 (2022)" specifies the personal data breach incidents that the Data Controller is required to notify to the Office of the Personal Data Protection Committee or the data subject under the Personal Data Protection Act. Such breaches may arise from the actions of the Data Controller itself, the Data Processor acting on the instruction or behalf of the Data Controller in relation to the collection, use, or disclosure of personal data, related persons of the said Data Controller or Data Processor, other individuals, or other factors. Each personal data breach incident may involve one or more of the following types of breaches:

(1) Confidentiality Breach: Involves the access to or disclosure of personal data without authorization or unlawfully, or resulting from an error, defect, or accident.

(2) Integrity Breach: Involves the unauthorized or unlawful alteration or modification of personal data, rendering it inaccurate, incomplete, or not whole, or resulting from an error, defect, or accident.

(3) Availability Breach: Results in the inability to access personal data or the destruction of personal data, rendering the personal data unavailable for normal use.

Examples of Risk Assessment for Personal Data Breaches

The following details are examples for assessing the risk of a personal data breach to determine the extent to which the incident may affect the rights and freedoms of an individual.

In each example, the rationale and a risk assessment are provided to determine whether the incident requires notification to the Office of the Personal Data Protection Committee or the data subject.

No.	Incident	Notify the Office of the PDPC	Notify the Data Subject	Remarks
1	A faculty, division, or agency, acting as the Data Controller, stores a backup of personal data on a USB drive that is encrypted with reliable technology. Subsequently, the said USB drive is lost.	Notification not required	Notification not required	Low risk. Since the data has been encrypted with reliable technological measures, the data is inaccessible. The loss of the USB drive, therefore, poses no risk to the data subject.
2	A faculty, division, or agency, acting as the Data Controller, provides an online service for storing personal data. Subsequently, a cybersecurity threat occurs, resulting in a personal data leak from the Data Controller's computer system.	Notification required	Notification required	Because the personal data is in a usable state and can be used to identify individuals, the cybersecurity threat could lead to problems and impacts that cause damage to a large number of data subjects.

No.	Incident	Notify the Office of the PDPC	Notify the Data Subject	Remarks
3	The electrical system of the Call Center of a faculty, division, or agency, acting as the Data Controller, malfunctions due to a temporary power outage. This causes the computer systems and equipment to be temporarily unable to provide service.	Notification not required	Notification not required	The personal data is temporarily unavailable due to a technological issue. Once the electrical system is restored, the data becomes accessible again. Therefore, it is not considered a personal data breach that poses a risk to the rights and freedoms of the individual.
4	A faculty, division, or agency, acting as the Data Controller, is subject to a cybersecurity threat in the form of a ransomware attack. Personal data is encrypted by the attacker (hacker), and with no backup available, the data becomes inaccessible and unusable.	Notification required	Notification required	Since the personal data is identifiable, the ransomware attack renders the data unusable, and no backup exists. Furthermore, this could cause damage to the operations of the Data Controller and to the data subjects themselves. Therefore, notification of the incident is required.

No.	Incident	Notify the Office of the PDPC	Notify the Data Subject	Remarks
5	A faculty, division, or agency receives a report from a university staff member about receiving an invoice for an unknown individual. Within 24 hours, an investigation reveals a personal data leak involving 10 individuals.	Notification required	Notification required, specifically for the 10 individuals whose personal data was on the bank's invoice.	As the data was confirmed to have been leaked, the initial impact is limited to the individuals who were billed. However, the faculty, division, or agency, as the Data Controller, must conduct a further investigation to determine if the data of any other individuals was also leaked. If so, additional notification is required.
6	A hospital providing patient services is attacked by a cybersecurity threat. The names of patients, their passwords, and medical histories are accessed and subsequently posted on the internet.	Notification required, as patient medical history is sensitive personal data that can be used to identify individuals.	Notification required for all affected patients whose data was leaked online. As this is sensitive personal data, malicious actors could use it to commit illegal acts or adversely affect the rights and freedoms of the data subjects.	The data leak on the internet resulted from an attack that constitutes an offense under the Computer Crime Act. The leaked data includes the names, health information, and other critical data of the patients who used the service. Therefore, it is necessary to notify the data subjects due to the high risk that this information could be used for illegal transactions.

No.	Incident	Notify the Office of the PDPC	Notify the Data Subject	Remarks
7	A Web Hosting service provider, contracted as a Data Processor for a Data Controller, experiences a software error in its access authorization program, preventing users from accessing the service.	Notification is required. The Data Processor must inform the Data Controller, who must then notify the Office of the Personal Data Protection Committee (PDPC), as the incident has a considerable impact on a group of customers who are unable to access their personal data.	The Data Controller is not required to notify the data subjects, as they have not been adversely affected because the issue is currently limited to service unavailability and no significant problem has yet occurred.	Initially, this is merely a software error preventing access to personal data, and the investigation has not yet revealed any cybersecurity threat. However, the Data Controller and the Data Processor must conduct a further factual investigation. If it is discovered that the service was attacked by a cybersecurity threat, the Web Hosting provider must promptly notify the Data Controller, and the Data Controller must then promptly notify both the Office of the Personal Data Protection Committee and the data subjects.
8	A hospital is subjected to a cybersecurity threat. A hacker attack renders patient records inaccessible for 30 hours.	Notification required, as patient medical history is sensitive personal data that can be used to identify the individual.	Notification required. As this is sensitive personal data, malicious actors could use it to commit illegal acts or adversely affect the rights and freedoms of the data subjects.	As the breached data includes health information, which is sensitive personal data, notification and further data investigation are necessary.

No.	Incident	Notify the Office of the PDPC	Notify the Data Subject	Remarks
9	A school erroneously sends the data of numerous students via email to its logistics service contractor, instead of to the students' parents.	Notification required.	Notification required.	The data transmission was unencrypted and involved the personal data of many individuals, which may include both general and sensitive personal data. The recipient could potentially misuse this information improperly and cause harm.
10	A direct marketing company sends an email to 100 individuals (students or personnel), but due to an error, places all their email addresses in the "To" or "Cc" field. This results in each recipient seeing the personal data of others.	Notification is required, as this involves the transmission of data belonging to a large number of data subjects. However, if the data was encrypted using reliable technology, notification may be exempted.	Notification is required, as the personal data in the email could subsequently be used to cause harm to the data subjects.	The determination of whether to notify the data subjects may depend on the volume and nature of the personal data disclosed. If all of the data was encrypted, it may be considered a low-risk incident, and notification would not be necessary.

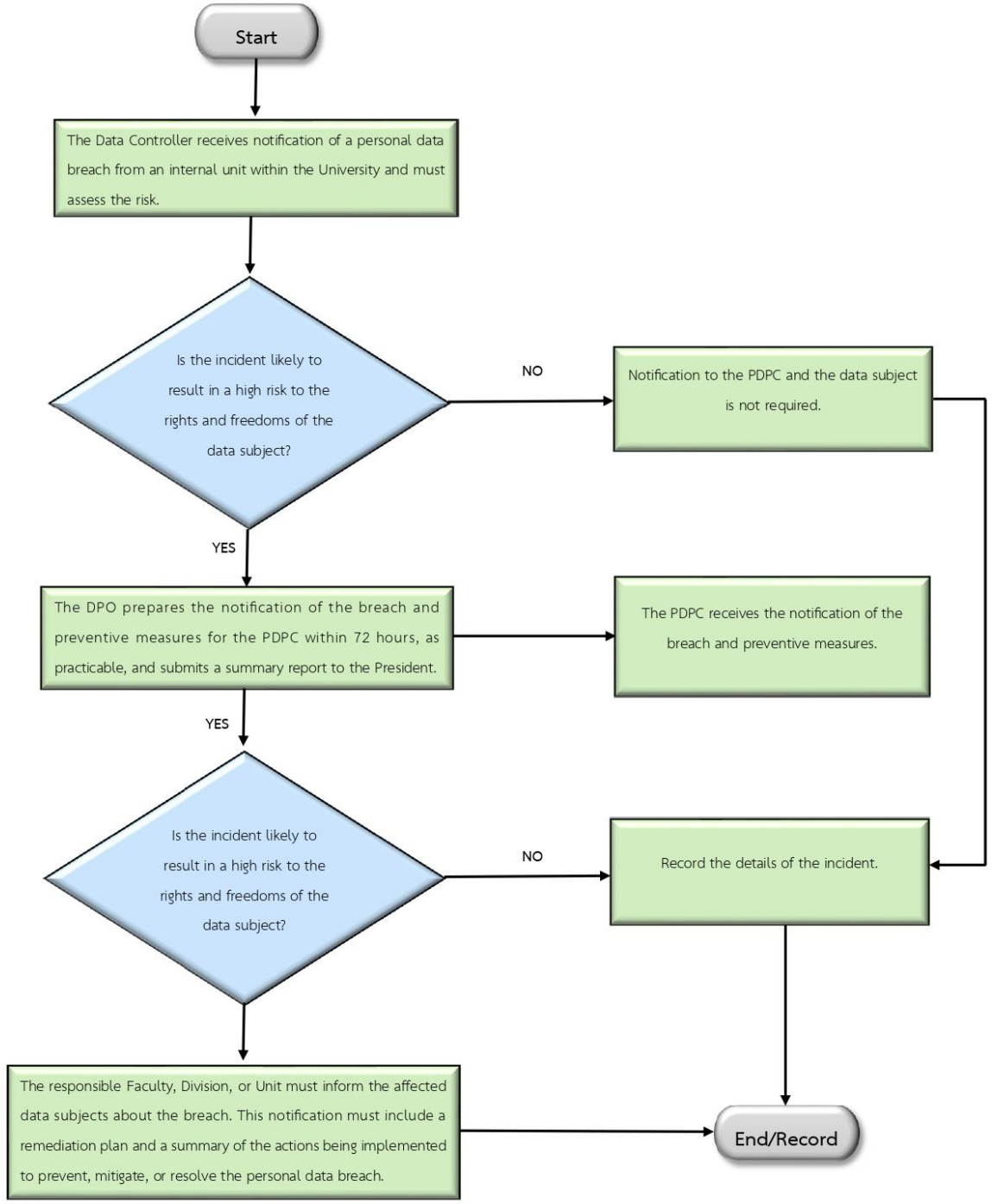
Note: The 10 preceding examples of risk assessment for personal data breaches are provided as guidelines only. The criteria for conducting a risk assessment must be based on the specific facts and relevant factors of each individual case.

Furthermore, once a personal data breach incident has been reported to the Office of the Personal Data Protection Committee (PDPC) or the data subjects, the respective faculty, division, or agency must record the details of the breach. This record must include a summary analysis of the incident, lessons learned, and corrective action plans. This process serves as a guideline to prevent further damage and includes notifying or advising relevant parties to act in accordance with the established plans or procedures.

Translate by Gemini-2.5-pro

Operational Flowchart

Procedure for Managing Personal Data Breach Incidents under the Possession or Control of Khon Kaen University



Procedure for Handling Personal Data Breach Incidents at Khon Kaen University

Translate by Gemini-2.5-pro

Part 3: Appendices

Relevant Laws, Regulations, and Notifications

a. Personal Data Protection Act, B.E. 2562 (2019)

b. Notification of the Personal Data Protection Committee
the Criteria and Procedures for Notification of Personal Data Breach, B.E. 2565 (2022)

c. Notification of the Personal Data Protection Committee
Electronic Channels for Reporting Personal Data Breaches by Data Controllers B.E. 2568 (2025)