Risk Assessment Guidelines and report a personal data violation version 1.0

Office of the Personal Data Protection Commission

15 December 2022

This Guideline for Risk Assessment and Notification of Personal Data Violation is created To be a guideline for the consideration of the data controller in reporting personal data breach incidents. To the Office of the Personal Data Protection Commission and the owner of the personal data

The Personal Data Protection Act B.E. is obligated to notify the Personal Data Protection Commission of the case of a personal data breach without delay within 72 hours from the date of knowledge of the cause to the best extent possible unless there is no such violation Risks affecting the rights and liberties of individuals Where violations have a high risk of repercussions to the rights and liberties of individuals to notify the owner of the personal data about the violation along with the guidelines Remedy without delay as well. **2565 (2022),** which clause 4 describes the types of data breaches and clause 12 specifies various factors that the personal data controller may use in Assessment of risks that will affect the rights and liberties of individuals are kept. The Office of the Personal Data Protection Commission therefore has prepared a sample risk assessment of violations. Personal data as a guide for the personal data controller to learn more

Note: Examples of such risk assessments of personal data breaches are only guidelines for risk assessment. Criteria for considering risk assessment must be based on facts based on relevant factors on a case-by-case basis

Document revisions (Version history)

version	date	Note
version 1.0	December 15, 2022	Examples of risk assessment guidelines in Notification of personal data breach to the Office Personal Data Protection Committee and Owner personal information

Example of risk assessment of personal data breach The following

is an example of a risk assessment approach for reporting violations. personal data to the Office of the Personal Data Protection Commission and the data subject about the extent to which a breach of personal data risks affecting the rights and liberties of individuals

In each case, the reasons and examples of risk assessment are explained. must notify the personal data breach to the Office of the Personal Data Protection Commission or the data subject personal or not

example	notify the office board Protection of personal data	Notify the owner of the personal data	reason
1. Data Controller Store personal data backed up in a USB Drive by Encrypted with technology Trusted. Later, the USB Drive is lost.	without notification	do not inform	low risk because when It is encrypted with measures reliable technology Such data cannot be activated, USB Drive loss is not a risk. with the owner of personal data due to personal information It is in working
2. Data Controller provide personal information storage services In the online system later born Cyber threats result in the leakage of personal information. from the computer system Data Controller	notify	notify	condition. and can identify individuals. Cyber may cause problems and effects that damage to owner a lot of personal information
3. Electrical system in call center of the controller of personal data interrupted by a temporary power outage resulting in the computer system and computer equipment	do not inform	do not inform	Such personal information is not in the state this Oh, yes. this work due to technological problems when the electrical system back as before

example	notify the office board Protection of personal information	Notify the owner of the personal data	reason
Data Controller Service is temporarily unavailable.			such personal data can be used, therefore it is not considered It's a data breach. Individuals at risk will affect the rights and freedom of person
4. The controller of personal data is cyber threats by Attacked by ransomware, personal data all of the data controllers Personal information is encrypted by a hacker and without backup hence unable to access and use the data. such	notify	notify	due to personal information in a condition that can Identifiable people and being attacked by ransomware cause such information is not in available state and no backup data may also be cause damage to The business of the controller of personal data, including the owner. Personal information must be notified. cause
5. The bank has been contacted by A bank customer said that he had received an invoice for collection of Unknown person, controller of personal data Inspected within 24 hours, it was found that there was a leak of personal information. 10 cases	notify	need to inform only 10 personal data subjects who are called Collect money according to the invoice of bank	Because such information is The leaked information actually Initially, there were only The person who is billed according to the invoice. However, the bank as the data controller must conduct an inspection In addition, if there is any other person information leak outside

example	notify the office board Protection of personal information	Notify the owner of the personal data	reason
			or not, if found, must inform further
6. Data Controller Providing online trading services throughout the country. Personal information is attacked by cyber threats by List of service users, passwords and purchase history Goods are accessed and taken posted on the internet	notify	must notify the customer of the controller of personal data In the area where information has been leaked on Internet	b suck lot m the flowing on Internet attack is an offense against the law. on offense Regarding computers, the leaked data included names of and important information of service users Therefore, it is necessary to notify Owner of personal data because there is a high risk that information Such will be used
7. Websites of Web Hosting Service Providers that are contracted to process Personal data from the controller personal data There was a problem with the program error in Checking access rights makes the service user unable to access the service enough customers because of	must notify the controller personal information for the controller personal information Notify the office because there is Group effect can such problems no customer group can reach personal information	The controller of personal data does not have to inform Owner of personal data not received effect because there is still no problem	to conduct illegal transactions. Initially, it's just a mistake. of programs that allow access Personal information is not from The investigation did not appear to have cyber threats in any way. Individuals and Processors Personal information must be verified. Additional facts if found The system has been attacked by threats. via cyber service provider website Web Hosting must notify the controller of personal data and controller of personal data

example	notify the office board Protection of personal information	Notify the owner of the personal data	reason
			must hurry to notify the whole office and the owner of personal data
8. A hospital was hit by a disaster. Cyber threats by attacking the system from a hacker. make the patient's history not can be accessed for 30 hours	must notify because historical data of patient as information personal with sensitive and able to identify individuals	notify due to information personal with sensitivity Those who do not wish well may applied to commit an offense or have impact on rights and freedom of owner of personal data	due to data breach Such information, including health information, is personal information. Sensitivity is therefore necessary. Report incidents and investigate additional information.
9. A school crashed. Error sending data. large number of students by e-mail go a d. this u a R in Provide transportation services. school not parent student	notify	notify	due to the transmission of such information There is no encryption and personal information of large numbers of individuals, which may include general personal and sensitive personal data which the contractor may bring information and can cause damage
10. A company does direct marketing by sending information.	must be notified because It is a data transmission	have to inform because the information	Determining whether to notify cause to the owner of personal data

example	notify the office board Protection of personal	Notify the owner of the personal data	reason
personal information to each recipient, but with error, so the address of 100 people who received the email into the To or Cc slots, making The recipient of the email sees the email containing the information. other person's personal	**information** of the owner of the information So many individuals need report, but if such information is encrypted by reliable technology, it may be exempt from notify	personal in such e-mail may be applied and cause damage to the owner of personal data later	or not, it may depend on the quantity of the personal data sent and the nature of the data. If the data is encrypted As mentioned all, it may be considered low risk. No need to report

Note: Examples of such risk assessments of personal data breaches are only guidelines for risk assessment. Criteria for considering risk assessment must be based on facts based on relevant factors on a case-by-case basis

Announcement of the Personal Data Protection Committee on

Criteria and Procedures for Reporting Personal Data Breach Incidents B.E. 2565

By virtue of Section 16 (4) in conjunction with Section 37 (4) of the Personal Data Protection Act 2019 Personal Data Protection Committee hereby issued an announcement as follows:

1 This announcement is called “Announcement of the Personal Data Protection Committee on Criteria and Procedures for Reporting Personal Data Breach Incidents B.E. 2565”

Clause 2 This announcement shall come into force from the date of its publication in the

Government Gazette. Clause 3 In this announcement, “Personal Data Breach” means a violation of security measures that causes loss, access, use, change, correction or disclosure of information. personal without authority or wrongly whether due to intent, willfulness, negligence, Unauthorized or wrongful acts involving computer crimes cyber threat Mistakes, glitches or accidents or any other cause. “Office” means

the Office of the Personal Data Protection Committee. “Committee” means

the Personal Data Protection Committee. Clause 4 Personal Data

Breach that the Personal Data Controller is obligated to notify To the office or the owner of the personal data under the Personal Data Protection Act, consisting of causes caused by breaches of security measures that cause loss, access, use, change, correction or disclosure of personal data without authorization. authoritative or wrongful Whether due to willfulness, willfulness, negligence, unauthorized or wrongful action,

computer fault cyber threat Mistakes, glitches or accidents or any other reason which may be caused by the actions of the controller of the personal data itself Personal Data Processor who deals with the collection, use or disclosure of personal data in accordance with the request orders or on behalf of the controller that personal data as well as employees, employees, contractors, agents or related persons of the controller personal data or the processor of such personal data or another person or other factors Each personal data breach may be related to a particular type of breach. or several types as follows

(1) Violation of personal data confidentiality (Confidentiality Breach), which has access to or disclose personal information without authority or wrongfully or arising from an error or accident

(2) Integrity Breach of Personal Data where the Personal Data has been altered to be inaccurate, incomplete or incomplete without authority, wrongful or due to error. (3) Violation of the availability of personal data. (Availability

Breach) which makes the personal data inaccessible or there is the destruction of the personal data causing the personal data to not be in the The condition is ready for normal use. whether

verbally, in writing or by other means electronically or the controller of personal data himself or herself whether there is or is likely to be The reason for the breach of personal information The personal data controller must take the following actions:

(1) assess the credibility of such information; and investigate facts about violations preliminary personal data without delay to the extent practicable that there are reasonable grounds to believe that there has been an infringement personal data? The controller of personal data should conducting a review of therapeutic measures Security of personal information both organizational measures organizational measures and technical measures, which may include physical measures in relation to such personal data. Both in relation to the data controller itself. proceed with the collection, use or disclosure of personal data in accordance with the instructions or on behalf of the controller of such personal data as well as employees, employees, contractors, agents or related persons of data controllers or data processors thereof. In order for the personal data controller to confirm whether a personal data breach has occurred or not, the personal data controller must consider details from relevant facts. including risk assessment (2) if, during the

investigation of the personal data breach under (1), it is found that there is a high risk that it will affect the rights and liberties of individuals Let the personal data controller do it himself or instruct the data processor or related person to do so. to prevent, suppress or correct the personal data breach so that the personal data breach ends or the personal data breach does not have further impacts (3) Considering the facts under (1), it appears that there is a

reasonable ground to believe that there is a data breach. real personal Instruct the personal data controller to notify the Office of the violation office without delay within seventy-two hours from the date of knowledge of the cause as far as is practicable, except that such violation is not at risk. that will affect the rights and liberties of individuals

(4) in the event that such personal data breach has a high risk of affecting the rights and freedom of the person to the personal data controller to notify the data subject of the breach along with guidelines for remedies without delay as well

(5) taking action in accordance with necessary measures; necessary and appropriate to suspend, respond, remedy or recover from such personal data breach. Including preventing and reducing the impact of the incident. future similar breaches of personal data This includes reviewing security measures. in order to have appropriate security efficiency, taking into account the level of risk based on technological factors, context, environment, acceptable standards for for agencies or Businesses of the same or similar type or nature Nature and purpose of collection, use and disclosure of personal data required resources and the possibility of Clause 6. In notifying the Personal Data Breach incident to the Office, the Personal Data Administrator must proceed to notify the Personal Data Breach in writing. or notified through the

method electronically or by any other methods as specified by the SEC Office. Individuals must specify the substance (1) information as brief as can be identified about the nature and type of infringement; personal information may describe the nature and quantity of the number of personal data subjects or the nature and number of records (records) of the personal data involved in the breach; and how to contact the Personal Data

Protection Officer in the event with personal data protection officers or contact names and the contact method of the person in charge personal data entrusted to Coordinator and provide additional information.

(3) information about potential impacts arising from personal data breach incidents; (4)

information about measures taken or will be used by the personal data controller to prevent, suppress, or remedy personal data breach incidents. or remedy the damage It may use personnel, process or technology measures. or any other measures Clause 7 In case of necessity causing the notification of personal

data breach to be delayed more than seventy-two hours since the incident Whether arising from a preliminary investigation, taking action to prevent, suppress, or correct a necessary cause of personal data breach, or any other necessity that cannot be prevented, the personal data controller may request S The SEC Office may consider waiving the offense from delaying the notification of the personal data breach by requiring the data controller to explain the reason of necessity. necessary and relevant details to display show that there is a reason It is an unavoidable necessity that makes This may cause a delay in notifying the incident of personal data breach, which must be notified to the SEC Office as soon as possible, provided that it must not exceed fifteen days from the date of knowledge of the incident.

The SEC Office may later inform the Personal Data Controller to clarify reasons or additional facts, and if the SEC Office considers it appropriate to exempt the offense from delayed notification of personal data breach due to a necessary cause, it shall be deemed that the Personal Data Controller Personal data controllers are exempt from processing. proceed to notify data breach to the SEC Office as specified in Section 37

(4) notifying the SEC Office of personal data breach The Office is not an excuse to exclude duties or liabilities. of the data controller under the specific laws related to that business or other laws

Clause 8 In the event that the Data Controller has an agreement with the Data Processor to control perform duties of the personal data processor in accordance with the law on protection of personal information or assign or order the Personal Data Processor to collect, use or disclose personal data in accordance with the request orders or on their own behalf Data Controller It must be stated in the relevant agreement or contract that the personal data processor is obliged to notify. breach of personal data to the data controller without delay within seventy-two hours from the date of The Personal Data Processor is aware of the cause as much as it is able to do as well. Clause 9 The Personal Data Controller may raise an exception to notify the Office of Personal

Data Breach for consideration. If the personal data controller can prove that the data breach that person There is no risk of affecting the rights and freedoms of individuals. This includes cases where information personal data according to the breach of that personal data It is non-personally identifiable information to the owner. personal information or that personal data is no longer usable due to adequate technological measures or other reliable reasons in raising such exceptions The personal data controller has a duty to provide information or send documents or Evidence of reasons for exemption This

includes details about security measures. The security of personal data or any other data shall be considered by the SEC Office. violation of has already received the SEC Office or is in the process of preparing to notify the SEC Office if the data controller After checking the facts, it was

Clause found that Such a breach of personal data has a high risk of repercussions. to the rights and liberties of individuals The personal data controller shall notify the data subject of the personal data breach together with the following essence to the affected data subject as much as possible.

without delay

(1) Brief information about the nature of the personal data breach (2) Name

and address of contact and the contact method of the personal data protection officer or individual that the personal data controller assigns to do coordinator

(3) information about potential impacts on the Personal Data Owner from the Personal Data Breach

incident; and brief information about the measures that the personal data controller has taken or will take in order to prevent, suppress or remedy the infringement personal information It may use personnel, process or technology measures. or any other necessary and appropriate measures including advice information on measures that the personal data subject may take additional actions to prevent, suppress or remedy the infringement of personal data or remedy the damage

Clause 11 In notifying the Personal Data Breach incident to the affected Personal Data Owner if he or she is unable to proceed Individual notification in writing or by means electronically because there is no means of contact or for any other necessity. The cause of the violation to the owner of personal data is a group. Or notify publicly through public media, social media or by electronic means or any other means that the subject of the affected personal data. Or the general public can access such notifications. Reporting violations to personal data subjects as

a group or notified in general must not cause damage or impact to the owner of the personal data. for breach of personal data that there is a risk of How much

does it affect the rights and liberties of individuals? The personal data controller may consider the following factors: (1) the nature and type of personal data breach; (2) the nature or category of personal

data involved in the breach; (3) the amount of personal

data involved. with abuse which may be considered by the number of

owners

personal data or the number of records (records) of personal data involved in the breach

(4) the nature, type or status of the subject of the personal data affected, including the fact that the subject of the affected personal data It includes minors, the handicapped, the incompetent. incompetent person or vulnerable persons (vulnerable persons) who lack the ability to (5) The severity of the impact and damage that occurred or may occur to the owner of the data.

personal from personal data breach and the effectiveness of the measures taken by the personal data controller. Or it will be used to prevent, suppress, or remedy a personal data breach. or remedy the damage To mitigate impacts and damages that occur or may occur to the owner of the personal data.

(6) widespread impact on business or operations action of the data controller or to the public from a personal data breach

(7) characteristics of the Personal Data collection system involved in the breach and relevant security measures of the Data Controller or Data Processor. both as organizational measures (8) the legal status of the personal data controller as a natural person or a legal entity; including the size and nature of the data controller's business.

Clause

Announced on December 6, 2016 5 Thienchai Na
Nakhon Chairman
of the Personal Data Protection Committee

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗

ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

telephone: 1111 or 02-142-1033 or 02-141-6993

Facebook: https://www.facebook.com/pdpc.th

Website: http://www.pdpc.or.th

E-mail office: pdpc@mdes.go.th