


*Personal Data Breach Report Form*



Regarding the Personal Data Protection Act, B.E. 2562, a controller must send a notification of any unauthenticated data processing to Personal Data Protection Committee within 72 hours after each unauthenticated processing occurred, except for no risk on the rights and liberty of the data subject. To support the verification processes of Personal Data Protection Officer, please specify the concerned details of the unauthenticated data processing as much as possible, the company will follow up all and later inform you with the result of the consideration.

You will be able to specify the details of the breach of personal information as you can by filling and submitting this form in person, or giving the delegation to the company, and sending the form through this email: [compliancerm@prospectrm.com](mailto:compliancerm@prospectrm.com) , however, within the period of 24 hours since the fact of the breach of personal information.

Details of whistle- blower of personal data breach report

Name - Surname \_\_\_\_\_

Telephone Number \_\_\_\_\_

E-mail \_\_\_\_\_

Address \_\_\_\_\_

- Found personal data breach by the data subject       Reported personal data breach by agent  
(Attached with signed power of attorney<sup>1</sup>)

The company reserves the right to query or ask for additional documents from the whistle- blower of personal data breach, in case of received unclear information and cannot clearly show that the applicant is the owner of the information or who has the right to submit the application, the company may reject your application.

Detail of personal data breach

1. Date & time of received personal data breach report Date \_\_\_\_\_ Time \_\_\_\_\_
2. Date & time of found personal data breach      Date \_\_\_\_\_ Time \_\_\_\_\_
3. Date & time of started personal data breach      Date \_\_\_\_\_ Time \_\_\_\_\_

Applicant's signature: \_\_\_\_\_ Date: \_\_\_\_\_

<sup>1</sup> Mandatory documents consist of 1) Signed power of attorney with revenue stamp 2) Valid copy of identification document issued by government department of grantor such as copy of identification card or passport.

4. Details of personal data breach (Please specify more info such as identity thief/ unauthorized access to personal data/ unauthorized data portability/ lost electronic devices with recorded personal data/ unauthorized data modification)

---

---

---

---

---

5. Place of found personal data breach (Please describe, i.e., inside department, in front of office)

---

---

6. Types of data subject (Please select)

- |   |  |
|---|--|
| <input type="checkbox"/> Trust unitholder and involved            | <input type="checkbox"/> Company's director/ executive |
| <input type="checkbox"/> Partner, tenant and involved             | <input type="checkbox"/> Company's employee            |
| <input type="checkbox"/> Consultant and involved                  | <input type="checkbox"/> Outsider                      |
| <input type="checkbox"/> Company's contractual staff/<br>employee | <input type="checkbox"/> Not applicable                |

7. Estimated number of victims (Please select)

- 1 – 9 persons     10 – 50 persons     51– 100 persons     Minimum 100 persons  
 No specific detail at the moment

8. Types of personal data breach (Please select)

- |  |  |
|--|--|
| <input type="checkbox"/> General info i.e., name- surname, address, phone number, email, date of birth, education, info of shareholding - director | <input type="checkbox"/> Sensitive info i.e., race, blood type, health conditions, criminal record, biological info, sexual preference |
| <input type="checkbox"/> Official documents i.e., identity card, passport, driving license, civil servant card                                     | <input type="checkbox"/> Documents issued by private organization i.e., employee card, membership card, credit card, business card     |
| <input type="checkbox"/> Financial statement   | <input type="checkbox"/> Family info of informant  |
| <input type="checkbox"/> Others (Please specify) .....   |  |
| <input type="checkbox"/> Not applicable  |  |

Applicant's signature: \_\_\_\_\_ Date: \_\_\_\_\_

9. How did you know about the personal data breach? (Please describe, i.e., received notification from the data subject/ found unusual Log File by unauthorized person/ lost devices).

---

---

10. Short description of personal data breach (Please specify types of personal data breach for better understanding of the case, including more details of data types as much as possible).

---

---

---

---

---

---

---

---

11. Details of information technology system and involved electronic devices (If any, such as personal mobile phone, including short description of data protection system, i.e., data access info or file backup in the company's system).

---

---

---

---

12. Please describe the risk of personal data (Please indicate, i.e., viewers may access and use that info without authorization).

---

---

---

---

Applicant's signature: \_\_\_\_\_ Date: \_\_\_\_\_

13. Estimate of risk for data subject (Please consider risk criterion according to the given footnote)

- High risk                       Medium risk                       Low risk                       No risk  
 Not applicable

14. Description of taken actions to remedy the infringement (Please specify the concerned measurement to solve the problem, i.e., changing password or searching for the lost devices).

Cause of problem \_\_\_\_\_  
\_\_\_\_\_

Short- term solution \_\_\_\_\_  
\_\_\_\_\_

Long- term solution \_\_\_\_\_  
\_\_\_\_\_

Recurrence prevention and solution Plan \_\_\_\_\_  
\_\_\_\_\_

Responsible department for above plan \_\_\_\_\_

15. Infringement report for the data subject

- Successfully notified the data subject                       On process for notifying the data subject  
 On considering process for notifying the data subject                       Not to notify the data subject  
subject

In case that the company rejects your request, you will be able to send your complaint through Personal Data Protection Committee at Personal Data Protection Committee Office, Office of the Permanent Secretary, Ministry of Digital Economy and Society, telephone: 1033-142-02, or e-mail: [pdpc@mdes.go.th](mailto:pdpc@mdes.go.th)

#### Acknowledgement and consent

You have clearly read and acknowledged the details of this request, and assured that all information given to the company is truth and correctness, you fully understand that the verification of authorization, identification, and place are essential procedures for considering your request according to your rights. If there is mistake intentionally, you may be prosecuted by law. The company might ask for your additional information in order to completely verify and process all according to your request.

In this regards, you hereby signed below:

Applicant's signature: \_\_\_\_\_ Date: \_\_\_\_\_

For officer only

For the Personal Data Protection Officer

Date of received request	:	_____
Date of recorded request	:	_____
Result of consideration	:	_____
<input type="checkbox"/> Proceeded request	Date of proceeded request	_____
	Operated by	_____
<input type="checkbox"/> Rejected request		
Reasons of rejection (If any)	:	_____
Recorded by	:	_____ Date _____
Acknowledgement letter no.	:	_____ Date _____
Processing fees (If any)	:	_____
Date of received processing fees	:	_____

**Occurred problem or feasible effects from the above infringement**

Those incidences are related to data control, data processing, cookies, data access, disclosure, modification and/ or personal data disclosure or not  Yes  No

Those incidences have significantly an effect on the data subject  Yes  No

**Reporting involved agencies**

1. Reporting company's data protection agency  Reported  No
2. Reporting company's top management  Reported  No
3. Reporting officer/ Police's daily record  Reported  No
4. Reporting the data subject\*  Notification had been sent Date /Time \_\_\_\_\_  
 On process for notifying the data subject  
 Company or trust decided not to notify the data subject  
 On considering process of the company and/ or trust  
 Others (Please specify) \_\_\_\_\_
5. Report Personal Data Protection Committee\*  Reported Date/Time \_\_\_\_\_  No  
(Government organization founded according to the Personal Data Protection Act, B.E. 2562)

\* Remark: In case of leakage of personal data, it must notify the data subject and the Personal Data Protection Committee within 72 hours.

Consideration of risk factors for rating risk's level according to these below risk criterion

Risk scores	Risk levels
0	No risk
1 – 7	Low risk
8 – 14	Medium risk
15 – 21	High risk

Risk factors:

Assessment topic	Risk scores			
	0	1	2	3
Number of data subjects that maybe affected	No data subject will be affected, such as leakage of only statistic data or outdate info.	Knowing exact number of data subjects, not over 10 persons.	Expecting that there may be more than 10 data subjects to be affected.	More than 10 data subjects will be affected, or no exact number can be expected.
Types of leaked information	Non- identity info, such as anonymous info, overall of statistic data, and other info that is not under the personal data protection law, i.e., death info, activities info of any family	Personal data that must be proved for identity (Not including sensitive data) with employee code, address, or phone number.	Personal data that immediately proves the identity such as name of data subject, photo or video.	Sensitive data, i.e., race, political preferences, religion, sexual behavior, criminal record, health report, disability, biological info.
Time of leakage found	Immediately after leakage occurred	Within 24 hours after the leakage occurred	Between 24 hours to 72 hours after the leakage occurred	Over 72 hours after the leakage occurred
Access to the company's employee data when identity theft occurred.	Employees can normally access to their personal data.	Employees cannot access their partial data temporarily.	Employees cannot access all kinds of data temporarily.	Employees cannot access all kinds of data permanently.
Damages on data when identity theft or unauthenticated access	No modification or no damage	The data is modified, but is not yet used by anyone,	The data is modified and may be used without modification	The data is modified and may be used without modification

Assessment topic	Risk scores			
	0	1	2	3
occurred due to any errors of involved company's employee.		and the company still has a backup file to be used.	alert, however the company still has a backup file to be used	alert, and the company has no backup file.
Scope of leakage of data	There is no disclosure of the data that was authentically accessed.	The leaked information may be disclosed to any unauthorized person within the company, but there is no evidence of unauthenticated data processing, i.e., lost document within the company's area, or deprecated electronic devices without removed data.	The data was disclosed or accessed easily by an outsider who can be identified, such as sending email to wrong address with attached personal document, but the receiver couldn't open the file, or it required technical support to access the info.	The data was disclosed and accessed by unexpected number of outsiders, such as public sharing or selling customers data/ trust unitholders to others.
Effects from leakage of data that may occurred on data subject.	No effect on data subject as it is public info before the leakage found, or the prevention measurement is already set before any damages occurred.	Expecting no effect on data subject, but it may cause some troubles on data subject when re-filling all info in the system is required, or the leaked data is not important for data subject.	It may cause any indirect effects on rights, assets, health, such as anxiety or concern.	It may cause any direct problems that might not be solved easily, such as income from dismissal, rejection of receiving some services, prosecuted action, health problem or severe or chronic illness, or death