HONEYCOMBERS

Data Breach Management and Response Plan using C.A.R.E. (4 Steps)

STEP 1: CONTAINING THE DATA BREACH TO PREVENT FURTHER COMPROMISE OF PERSONAL DATA

1. The Data Protection Officer (DPO) and the CEO should be notified of all suspected/confirmed data breaches immediately upon detection.

2. Upon being notified, the DPO and/or the CEO shall conduct an initial assessment of the data breach to determine the severity of the data breach. The initial assessment should include (but not be limited to) the following:

- Cause of the data breach and whether the breach is still ongoing
- Number of affected individuals
- Type(s) of personal data involved
- The affected systems and/or services
- Whether help is required to contain the breach

3. After the initial assessment, actions should be taken to:

- Stop the identified practices that led to the data breach
- Establish whether the lost data can be recovered and steps that can be taken to minimise any harm or impact caused by the data breach (e.g. remotely disabling a lost notebook containing personal data of individuals)
- Isolate the compromised system/service from the Internet or network, or shut down the compromised system/service if necessary
- Prevent further unauthorised access to the system/service
- Reset passwords if accounts and passwords have been compromised
- Isolate the causes of the data breach in the system/service, and where applicable, change the access rights to the compromised system/service

4. The details of the data breach and post-breach response(s) will be recorded in email communications between the reporter and the DPO and CEO.

5. The Company shall alert the:

Police, if criminal activity (e.g. hacking, theft or unauthorised system access by an employee) is suspected, and to preserve evidence for investigation

Cyber Security Agency of Singapore through the Singapore Computer Emergency Response Team (SingCERT) for cyberattacks

STEP 2: ASSESSING THE DATA BREACH BY GATHERING THE FACTS AND EVALUATING THE RISKS, INCLUDING THE HARM TO AFFECTED INDIVIDUALS

1. Upon containment of the data breach, the Company shall conduct an in-depth assessment within 30 days from when the Company first becomes aware of a potential data breach.

2. If the in-depth assessment reveals that the data breach is likely to result in significant harm or impact to the affected individuals, the Company shall notify the PDPC within 72 hours and the affected individuals as soon as practicable.

3. Where the Company is uncertain if affected individuals need to be notified, the Company shall report to the PDPC and seek clarification.

4. If the data breach involves the accidental disclosure of personal data to a trusted third party, the Company shall take steps to request that the third party delete the personal data that was accidentally disclosed and secure the third party's compliance with its request.

STEP 3: REPORTING THE DATA BREACH TO THE PERSONAL DATA PROTECTION COMMISSION (PDPC) AND/OR AFFECTED INDIVIDUALS, IF NECESSARY

1. The Centre shall notify the PDPC and/or affected individuals when the data breach is:
    - likely to result in significant harm or impact to the individuals to whom the information relates; or
    - of a significant scale (i.e. data breach involves personal data of 500 or more individuals)

2. Information to be included in the notice to the PDPC:
    - Extent of the data breach;
    - Type(s) and volume of personal data involved;
    - Cause or suspected cause of the breach;
    - Whether the breach has been rectified;
    - Measures and processes that the organisation had put in place at the time of the breach;
    - Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so; and
    - Contact details of person(s) whom the PDPC could contact for further information or clarification.

Submit the notification at https://eservice.pdpc. gov.sg/case/db or call 6377 3131 during working hours.

3. Information to be included in the notice to the affected individuals:
    - How and when the data breach occurred;
    - Types of personal data involved in the data breach;

- What the organisation has done or will be doing in response to the risks brought about by the data breach;
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- Contact details and how affected individuals can reach the Company for further information or assistance (e.g. helpline numbers, e-mail addresses or websites); and/or
- Where applicable, what type of harm/impact the individual may suffer from the compromised data

The DPO or CEO shall send email the notice to the affected individuals. Refer to ANNEX A for template.

STEP 4: EVALUATING HONEYCOMBER'S RESPONSE TO THE DATA BREACH INCIDENT AND CONSIDER THE ACTIONS WHICH CAN BE TAKEN TO PREVENT FUTURE DATA BREACHES.

1. The Company shall review and take action to improve its personal data handling practices and prevent the reoccurrence of similar data breaches.

2. Actions may include the following:
- Implementation/continuing efforts of the remediation actions
- Identification of areas of weakness and taking action to strengthen them
- Effectiveness of the organisation's data breach response(s)
- Corrective actions to be taken

ANNEX A - SAMPLE MAIL

Dear [NAME]:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that [may involve/involves] your personal information.

[[Between/On] [IDENTIFY TIME PERIOD OF BREACH], [SUMMARISE BREACH INCIDENT].] The data accessed [may have included/included] personal information such as [IDENTIFY TYPES OF PERSONAL INFORMATION AT ISSUE]. [To our knowledge, the data accessed did not include any [IDENTIFY TYPES OF PERSONAL INFORMATION NOT INVOLVED]].

We value your privacy and deeply regret that this incident occurred. We are conducting a thorough review of the potentially affected [records/computer system/IDENTIFY OTHER], [and will notify you if there are any significant developments]. We have implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of the Company's valued [clients/employees/IDENTIFY GROUP OF AFFECTED INDIVIDUALS].

[The Company also is working closely with the Personal Data Protection Commission (PDPC) to ensure the incident is properly addressed.]

For further information and assistance, please contact our Data Protection Officer at 8779 0890 during working days, between 09:30AM and 06:30PM or visit our website at thehoneycombers.com.

Sincerely,

[Name of DPO or CEO]
[Designation]

References:

- Personal Data Protection (Notification of Data Breaches) Regulations 2021
- https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.ashx?la=en