

Personal Data Protection (Notification of Data Breaches) Regulations 2021

Table of Contents

Enacting Formula

1 Citation and commencement

2 Definitions

3 Data breach resulting in significant harm to individuals

4 Data breach of significant scale

5 Notification to Commission

6 Notification to affected individuals

THE SCHEDULE Prescribed personal data and prescribed circumstances under section 26B(2) of Act

No. S 64

PERSONAL DATA PROTECTION ACT 2012 (ACT 26 OF 2012)

PERSONAL DATA PROTECTION (NOTIFICATION OF DATA BREACHES) REGULATIONS 2021

In exercise of the powers conferred by section 65 of the Personal Data Protection Act 2012, the Personal Data Protection Commission, with the approval of the Minister for Communications and Information, makes the following Regulations:

Citation and commencement

1. These Regulations are the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and come into operation on 1 February 2021.

Definitions

2. In these Regulations, unless the context otherwise requires —

“bank” has the meaning given by section 2(1) of the Banking Act (Cap. 19);

“finance company” has the meaning given by section 2 of the Finance Companies Act (Cap. 108);

“identification number”, in relation to an individual, means an identity card number, a passport number or the number of any other document of identity issued by a government as evidence of the individual’s nationality or residence, and includes a foreign identification number.

Data breach resulting in significant harm to individuals

3.—(1) For the purposes of section 26B(2) of the Act, a data breach is deemed to result in significant harm to an individual if the data breach relates to —

- (a) the individual’s full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual set out in Part 1 of the Schedule, subject to Part 2 of the Schedule; or
- (b) all of the following personal data relating to an individual’s account with an organisation:
 - (i) the individual’s account identifier, such as an account name or number;
 - (ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual’s account.

(2) In paragraph (1)(b), “account identifier” includes a number assigned to any account the individual has with an organisation that is a bank or finance company.

Data breach of significant scale

4. For the purposes of section 26B(3)(a) of the Act, the prescribed number of affected individuals is 500.

Notification to Commission

5.—(1) For the purposes of section 26D(3) of the Act, the notification by an organisation to the Commission of a notifiable data breach under section 26D(1) of the Act must include all of the following information:

- (a) the date on which and the circumstances in which the organisation first became aware that the data breach had occurred;
- (b) a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment under section 26C(2) or (3)(b) of the Act that the data breach is a notifiable data breach;
- (c) information on how the notifiable data breach occurred;
- (d) the number of affected individuals affected by the notifiable data breach;
- (e) the personal data or classes of personal data affected by the notifiable data breach;
- (f) the potential harm to the affected individuals as a result of the notifiable data breach;
- (g) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Commission of the occurrence of the notifiable data breach —
 - (i) to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and
 - (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
- (h) information on the organisation's plan (if any) to inform, on or after notifying the Commission of the occurrence of the notifiable data breach, all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach;
- (i) the business contact information of at least one authorised representative of the organisation.

(2) If the organisation notifies the Commission of the notifiable data breach after the expiry of the period specified in section 26D(1) of the Act, the notification to the Commission must additionally specify the reasons for the late notification and include any supporting evidence.

(3) Where, despite section 26D(2) of the Act, the organisation does not intend to

notify any affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) of the Act of the occurrence of that data breach, the notification to the Commission must additionally specify the grounds (whether under the Act or other written law) for not notifying the affected individual.

(4) The notification by the organisation to the Commission must be in the form and manner specified on the Commission's website at www.pdpc.gov.sg.

Notification to affected individuals

6. For the purposes of section 26D(3) of the Act, the notification by an organisation to an affected individual affected by a notifiable data breach under section 26D(2) of the Act must contain all of the following information:

- (a) the circumstances in which the organisation first became aware that the notifiable data breach had occurred;
- (b) the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach;
- (c) the potential harm to the affected individual as a result of the notifiable data breach;
- (d) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual —
 - (i) to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and
 - (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
- (e) the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach;
- (f) the business contact information of at least one authorised representative of the organisation.

THE SCHEDULE

Regulation 3(1)(a)

PRESCRIBED PERSONAL DATA AND PRESCRIBED
CIRCUMSTANCES UNDER SECTION 26B(2) OF ACT

PART 1

1. The amount of any wages, salary, fee, commission, bonus, gratuity, allowance or other remuneration paid or payable to the individual by any person, whether under a contract of service or a contract for services.
2. The income of the individual from the sale of any goods or property.
3. The number of any credit card, charge card or debit card issued to or in the name of the individual.
4. The number assigned to any account the individual has with any organisation that is a bank or finance company.
5. Any information that identifies, or is likely to lead to the identification of, the individual as a child or young person who —
 - (a) is or had been the subject of any investigation under the CYPA;
 - (b) is or had been arrested, on or after 1 July 2020, for an offence committed under any written law;
 - (c) is or had been taken into care or custody by the Director-General of Social Welfare, a protector, any officer generally or specially authorised in that behalf in writing by the Director-General or protector or a police officer under the CYPA;
 - (d) is attending or had attended a family programme in relation to an application to be made under section 50 of the CYPA;
 - (e) is or was the subject of an order made by a court under the CYPA; or
 - (f) is or had been concerned in any proceedings in any court or on appeal from any court, whether the individual is the person against or in respect of whom the proceedings are taken or a witness in those proceedings.
6. Any information that identifies, or is likely to lead to the identification of —
 - (a) the individual who has been or is the subject of any investigation, examination, assessment or treatment under the VAA relating to whether the individual is a vulnerable adult experiencing or at risk of abuse, neglect or self-neglect;
 - (b) the individual as a vulnerable adult who has been committed to a place of temporary care and protection or place of safety designated under section 19(1) of the VAA or to the care of a fit person under the VAA; [\[S 735/2021 wef 01/10/2021\]](#)
 - (c) the individual as a vulnerable adult who is the subject of an order made by a court under the VAA;
 - (d) a place of temporary care and protection or place of safety designated under