First published in the Government *Gazette*, Electronic Edition, on 29 January 2021 at 5 pm.

No. S 64

PERSONAL DATA PROTECTION ACT 2012 (ACT 26 OF 2012)

PERSONAL DATA PROTECTION (NOTIFICATION OF DATA BREACHES) REGULATIONS 2021

ARRANGEMENT OF REGULATIONS

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

THE SCHEDULE — *continued*

(*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 or to the care of a fit person under the VAA;

(*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 in which an individual or a vulnerable adult mentioned in sub-paragraph (*a*), (*b*) or (*c*) is committed, or the location of such a place of temporary care and protection or place of safety; or

(*e*) a fit person under whose care an individual or a vulnerable adult mentioned in sub-paragraph (*a*), (*b*) or (*c*) is placed, or the location of the premises of such a fit person.

7. Any private key of or relating to the individual that is used or may be used —

(*a*) to create a secure electronic record or secure electronic signature;

(*b*) to verify the integrity of a secure electronic record; or

(*c*) to verify the authenticity or integrity of a secure electronic signature.

8. The net worth of the individual.

9. The deposit of moneys by the individual with any organisation.

10. The withdrawal by the individual of moneys deposited with any organisation.

11. The granting by an organisation of advances, loans and other facilities by which the individual, being a customer of the organisation, has access to funds or financial guarantees.

12. The incurring by the organisation of any liabilities other than those mentioned in paragraph 11 on behalf of the individual.

THE SCHEDULE — *continued*

13. The payment of any moneys, or transfer of any property, by any person to the individual, including the amount of the moneys paid or the value of the property transferred, as the case may be.

14. The creditworthiness of the individual.

15. The individual's investment in any capital markets products.

16. The existence, and amount due or outstanding, of any debt —

    (*a*) owed by the individual to an organisation; or

    (*b*) owed by an organisation to the individual.

17. Any of the following:

    (*a*) the terms and conditions of any accident and health policy or life policy (called in this item the applicable policy) of which the individual is the policy owner or under which the individual is a beneficiary;

    (*b*) the premium payable by the policy owner under the applicable policy;

    (*c*) the benefits payable to any beneficiary under the applicable policy;

    (*d*) any information relating to any claim on, or payment under, the applicable policy, including the condition of the health of the individual and the diagnosis, treatment, prevention or alleviation of any ailment, condition, disability, disease, disorder or injury that the individual has suffered or is suffering from;

    (*e*) any other information that the individual is the policy owner of, or a beneficiary under, an applicable policy.

18. The assessment, diagnosis, treatment, prevention or alleviation by a health professional of any of the following affecting the individual:

    (*a*) any sexually-transmitted disease such as Chlamydial Genital Infection, Gonorrhoea and Syphilis;

    (*b*) Human Immunodeficiency Virus Infection;

    (*c*) schizophrenia or delusional disorder;

    (*d*) substance abuse and addiction, including drug addiction and alcoholism.

19. The provision of treatment to the individual for or in respect of —

    (*a*) the donation or receipt of a human egg or human sperm; or

    (*b*) any contraceptive operation or procedure or abortion.

THE SCHEDULE — *continued*

20. Any of the following:

    (*a*) subject to section 4(4)(*b*) of the Act, the donation and removal of any organ from the body of the deceased individual for the purpose of its transplantation into the body of another individual;

    (*b*) the donation and removal of any specified organ from the individual, being a living organ donor, for the purpose of its transplantation into the body of another individual;

    (*c*) the transplantation of any organ mentioned in sub-paragraph (*a*) or (*b*) into the body of the individual.

21. Subject to section 4(4)(*b*) of the Act, the suicide or attempted suicide of the individual.

22. Domestic abuse, child abuse or sexual abuse involving or alleged to involve the individual.

23. Any of the following:

    (*a*) information that the individual is or had been adopted pursuant to an adoption order made under the Adoption of Children Act (Cap. 4), or is or had been the subject of an application for an adoption order;

    (*b*) the identity of the natural father or mother of the individual;

    (*c*) the identity of the adoptive father or mother of the individual;

    (*d*) the identity of any applicant for an adoption order;

    (*e*) the identity of any person whose consent is necessary under that Act for an adoption order to be made, whether or not the court has dispensed with the consent of that person in accordance with that Act;

    (*f*) any other information that the individual is or had been an adopted child or relating to the adoption of the individual.

PART 2

1. The prescribed personal data or classes of personal data set out in Part 1 excludes —

    (*a*) subject to paragraph 2, any personal data that is publicly available; and

    (*b*) any personal data that is disclosed to the extent that is required or permitted under any written law.

2. The personal data mentioned in paragraph 1(*a*) must not be publicly available solely because of any data breach.

THE SCHEDULE — *continued*

3. In this Schedule —

"abuse", "fit person", "neglect", "place of safety", "place of temporary care and protection", "self-neglect" and "vulnerable adult" have the meanings given by section 2(1) of the VAA;

"accident and health policy", "life policy" and "policy owner" have the meanings given by the First Schedule to the Insurance Act (Cap. 142);

"capital markets products" has the meaning given by section 2(1) of the Securities and Futures Act (Cap. 289);

"child or young person" means a person below 18 years of age;

"credit card" and "charge card" have the meanings given by section 56 of the Banking Act;

"CYPA" means the Children and Young Persons Act (Cap. 38);

"electronic record", "secure electronic record" and "secure electronic signature" have the meanings given by section 2(1) of the Electronic Transactions Act (Cap. 88);

"health professional" means —

(*a*) a registered medical practitioner under the Medical Registration Act (Cap. 174); or

(*b*) a registered dentist under the Dental Registration Act (Cap. 76);

"investment in any capital markets product" includes any of the following:

(*a*) the nature, quantity and value of any capital markets products purchased or sold by the individual;

(*b*) the nature and value of any capital markets products held by or in the name of the individual;

"net worth" of an individual includes any of the following:

(*a*) the amount of any moneys, and value of any property, in which the individual has a legal or beneficial interest;

(*b*) the amount of any debts and other liabilities owed by the individual to any person;

"private key" includes a private key within the meaning given by paragraph 1(1) of the Third Schedule to the Electronic Transactions Act;

"property" includes any thing in action and any interest in real or personal property;

"protector" has the meaning given by section 2(1) of the CYPA;

THE SCHEDULE — *continued*

"specified organ" has the meaning given by section 2 of the Human Organ Transplant Act (Cap. 131A);

"VAA" means the Vulnerable Adults Act 2018 (Act 27 of 2018).

Made on 28 January 2021.

CHAN YENG KIT
Chairman,
Info-communications Media
Development Authority,
Singapore.

[AG/LEGIS/SL/227A/2020/1 Vol. 1]