


☐

I'm not robot


reCAPTCHA

Continue

On this web page, Singapore PDPC provides links to advisory guidelines, including provisions relating to non-sound, consent to marketing goals and other obligations and interpretations of key terms in PDPC. - (1) In this Act, unless context requires otherwise: Removed under Act 22 2016 wef 01/10/2016 advisory committee means an advisory committee appointed under Article 7; The Appeals Committee means the Appeals Committee for Data Protection appointed under Article 33 (4); The Appeals Panel refers to the Data Protection Appeals Panel established under article 33 (1); The designated day means the start date of the iii-vi parts. an authorized official in relation to the exercise of any authority or performance of any function or responsibilities under any provision of this act means a person who, under section 38 of the Media Development Authority Act 2016, has been delegated to exercise of that authority or responsibilities under that provision; Act 22 of 2016 wef 01/10/2016 means the Office for the Development of Information and Communication Media, established under section 3 of the Information and Communication Media Development Act 2016; Act 22 2016 wef 01/10/2016 benefit plan means insurance policy, pension plan, annuity, fund plan or other similar plan; business includes the activities of any organization, whether it is carried out for profit or is carried out on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity; Business contact information means the name, name or name of the position, business phone number, business address, email address or business fax number and any other similar information about a person not provided by a person solely for his or her personal purposes; In accordance with the Act of 22 of 2016. No. 01/10/2016The Chief Executive Director, in relation to the Authority, means that the Chief Executive Is appointed under section 40 (2) of the Media Development Authority Act 2016, and includes any person acting in that capacity; Act 22 of 2016 wef 01/10/2016 means that a person appointed as the Commission for the Protection of Personal Data under Article 5 is responsible for administering the Act; Act 22 of 2016 wef 01/10/2016 refers to the Commissioner for the Protection of Personal Data appointed under Article 8 (1i) and includes any Deputy Commissioner for the Protection of Personal Data or Assistant Commissioner for The Protection of Personal Data appointed under Article 8 (1) (b); Act 22 2016 wef Credit Bureau means an organization that (a) provides credit reports for profit or profit; or (b) provides credit reports on a normal, non-commercial basis as an auxiliary part of the portion of the For profit or profit; a credit report means a communication, whether in written, oral or other form, provided to an organization to assess an individual's creditworthiness in connection with a transaction between an organization and a person; A data intermediary means an organization that processes personal data on behalf of another organization but does not include an employee of another organization. The document includes information recorded in any form; household means related to home or family; an educational institution means any organization that provides education, including education, training or training, whether in itself or in cooperation or in cooperation with any other person; The employee includes a volunteer; Employment includes work in unpaid voluntary work relationships; an appraisal purpose means (a) to determine the suitability, right or qualification of the person to whom the data -(i) for employment or for appointment, (ii) for promotion or employment or to continue work or office; (iii) for suspension from work or position; (iv) for admission to an educational institution; (v) for awarding contracts, awards, scholarships, honours or other similar benefits; or (vi) to provide financial or social assistance or appropriate health services under any scheme run by a government agency; (b) To determine whether to continue, modify or cancel a contract, award, scholarship, scholarship, honour or other similar benefit; (c) To decide whether a person or property should be insured or whether or not to renew the insurance of a person or property; or (d) for other similar purposes that may be prescribed by the Minister; An individual means an individual, whether alive or dead; The inspector means the person appointed by the inspector under article 8(1) (b); Act 22 of 2016 wef 01/10/2016 means an investigation related to a breach of the agreement; (b) violation of any written law or any standard of professional conduct or other requirement imposed by any regulatory authority in the exercise of its powers in accordance with any written law; or (c) circumstances or conduct that may result in remedies or assistance being available under any law; national interests include national defence, national security, public security, maintenance of basic services and international affairs; The organization includes any individual, company, association or body of persons, corporate or unincorporated, regardless of whether formed or recognized under Singapore law; or (b) resident, or having an office or place data means data, whether true or not, is about the person who can be identified -a) from this data; or (b) from this data and other information that the organization has or may have access to; the prescribed health authority means a health authority prescribed for the purpose of the fourth timetable by the Minister, who is responsible for health; prescribed by the law enforcement agency, which is responsible for investigating offences or charging offenders in accordance with written law prescribed for the purposes of section 21 (4) and the fourth timetable by the Minister responsible for these powers; private trust means trust for one or more designated individuals who are friends or family members, from settlor; proceedings mean any civil, criminal or administrative proceedings by a court, tribunal or regulatory authority relating to an allegation of breach of the agreement; (b) Violation of any written law or any standard of professional conduct or other requirement imposed by any regulatory authority in exercising its authority in accordance with any written law; or (c) a improper or violation of a duty that requires a remedy under any law; Processing for personal data means conducting any transaction or set of transactions with respect to personal data and includes any of the following: (b)holding; (c)holding; (c)organization, adaptation or change; (d) retrieval; (e)combination; (f)transmission; (g)erasure or destruction; The public institution includes (a) the Government, including any ministry, department, institution or public body; Any tribunal appointed under any written law; or (c) any statutory body listed under subsection (2); publicly available for personal information about a person means personal data that is generally available to the public and includes personal data that can be met by reasonably expected funds at the location or event where the person appears; and (b), which is open to the public; the relevant body means the Commission, the Appeals Board or any appeal committee; Act 22 of 2016 wef 01/10/2016 includes a judicial or quasi-judicial body or disciplinary, arbitration or mediation body. (2) The Minister may, by notice in the newspaper, specify any statutory body established under public law for public function to be a public institution for the purposes of the act. The Data Protection Act 2012 (No. 26 of 2012) (PDPA) is Singapore's main data protection legislation governing the collection, use and disclosure of individuals' data organizations. Prior to the adoption of PDPA, Singapore did not have a comprehensive law regulating the protection of personal data. Processing personal data in regulated to some extent by a patchwork of laws, including, common law, sector specific legislation and various self-regulated or joint regulatory codes. These existing industry data protection systems will continue to work with PDPA. PDPA was adopted by the Singapore Parliament on October 15, 2012 and implemented in three phases. The first phase of the general provisions came into force on January 2, 2013. These provisions relate to the scope and interpretation of THE PDPA; creation of the Personal Data Protection Commission (PDPC), the body that manages and enforces THEPA; Creation of a Data Protection Advisory Committee; creation of PDPC (DNC) do-Not-Call registers and other general PDPA provisions. In the second phase, provisions relating to the DNC registry take effect on January 2, 2014. In the third and final phase, the main provisions relating to the protection of personal data (the Data Protection Regulations), in particular Parts III-IV PDPA, will come into force on 2 July 2014. In addition to PDPA, the following supporting legislation has been issued to date: 1.2. The PDPC guidelines have issued a number of advisory guidelines that, while not legally binding on any party, provide greater clarity as to how PDPC can interpret PDPA provisions. Some examples include the Advisory Guidelines on Key Concepts in the Data Protection Act (Basic Concept Guidelines); Advisory guidelines on the Personal Data Protection Act on specific topics; Advisory guidelines for enforcement of data protection regulations; and, more recently, the Data Protection Guide to THE Development of ICT Systems. All recommendations and guides are available through the PDPC website. Since 2016, PDPC has published a number of enforcement solutions that are useful in illustrating how PDPA will be applied. These enforcement solutions are usually available through the PDPC website. Below is an overview of some of the latest enforcement decisions. As of 20 June 2019, the PDPC has issued a total of 90 decision-making grounds for 114 organizations, with the vast majority of them concerned violations of the Protection Obligation. The most common types of data breaches involve the deliberate disclosure of personal data; Inadequate technical security arrangements; Poor physical safety measures Errors in mass email and/or communication and insufficient data protection policies. To date, the highest financial penalties imposed on organizations are SGD 250,000 (about 166,260 euros) and SGD 750,000 (about 498,790 euros) respectively at SingHealth Services Pte Ltd and Integrated Health Information Systems Pte Ltd for the pdpa. (See. Re Singapore Health Health Pte Ltd and another 2019 SGPDPC 3). This unprecedented data breach, caused by a cyberattack on SingHealth's patient database system, resulted in the personal data of approximately 1.5 million patients being compromised. PDPA has also been tried in Singapore's courts. On February 19, 2019, the State Court dismissed a lawsuit brought by the Singapore Swimming Club for defamation and violation of the PDPA. Although there is no written basis for the decision, the case is important, as it appears that this is the first time that Singaporean courts have been asked to consider a violation of PDPA, and the PDPC has not taken any action on any alleged VIOLATIONS of PDPA. In addition to these enforcement decisions, PDPC also publishes an annual data protection digest, which is a compilation that includes PDPC's decision-making grounds, a summary of unpublished cases where unconfirmed violations have been detected, and a collection of data protection articles provided by data protection professionals. 2. SCOPE APPLICATION 2.1. Who do laws/regi apply to? PDPA usually applies to all organizations with respect to the personal data they collect, use and/or disclose. However, the following categories of organizations are exempt from PDPA: persons acting in a personal or domestic capacity; Employees who work in the organization; Government agencies or organizations acting on behalf of a government agency to collect, use or disclose personal data; or any other organization or personal data, or classes of organizations or personal data, as required by the relevant legislation. PDPA sets a basic standard for the protection of personal data in the private sector and will act together (and not repeal) existing laws and regulations. The PDPA stipulates that the data protection system does not affect any rights or obligations under the law and that other written laws will prevail in the event of any inconsistency. For example, bank secrecy laws under the Banking Act (Chapter 19) of 1971 (revised) regulate customer information obtained by banks. What types of treatments are covered/released? Government agencies are not subject to PDPA requirements because they have their own set of data protection rules that all public servants must comply with. Organizations acting on behalf of a government agency in connection with the collection, use or disclosure of personal data are also excluded from the Data Protection Regulations, although they continue to be subject to obligations under other laws and their contract with the relevant government agency. PDPA also organizations that do not have individuals in Singapore, as long as these organizations collect, use, or disclose data data Singapore. For example, organizations located abroad that collect data from individuals in Singapore through online channels or platforms will be subject to data protection provisions. It should be noted that related organizations within the organization are not excluded from the use of PDPA; an organization that transfers personal data to its parent company or subsidiary will be subject to data protection provisions. In addition, organizations involved in the cross-border transfer of personal data from Singapore to foreign locations are also subject to data protection provisions. Data brokers (defined in section 8 below) are partially excluded from the Data Protection Regulations and have PDPA obligations only regarding: protection of personal data found or controlled by them, by taking reasonable security measures to prevent unauthorized access, collection, use, disclosure, copying, modification, removal or similar risks; and the storage of personal data, the termination of the storage of documents containing personal data, or the removal of funds by which personal data may be linked to specific individuals (e.g., the destruction or anonymization of personal data) as soon as it is reasonable to assume that the purpose for which personal data was collected no longer serves its storage, and retention is no longer necessary for legal or business purposes. 3. DATA PROTECTION AUTHORITY REGULATORY BODY 3.1. THE main data protection regulator PDPC is the regulatory body responsible for administering and enforcing PDPA. It is a statutory body under the Ministry of Communications and Information and is part of the converged telecommunications and media regulator, The Media Development Office Infocomm ('IMDA'). 3.2. The core powers, responsibilities and responsibilities of pdPC's core powers, responsibilities and responsibilities are as follows: to raise awareness of data protection in Singapore; Providing advisory, advisory, technical, management or other specialized data protection services; Advise the Government on all data protection issues; Represent the government at the international level on data protection issues; research and research, promotion of data protection education, including the organization and conduct of seminars, seminars and symposiums related to it, and support for other organizations conducting such activities; Managing technical cooperation and data-sharing with other organizations, including foreign data protection authorities and international or intergovernmental organizations, on their own behalf or on behalf of the Government; And enforcing PDPA perform the functions assigned to the PDPC in accordance with any any Written law and engage in such other activities and perform functions such as minister may authorize or appoint a PDPC on an order published in the newspaper. 4. KEY DEFINITION Personal data BASIC CONCEPTS: Personal data according to PDPA refers to all data, true or not, about the person who can be identified from this data, or on those data and other information to which the organization has or may have access. This applies regardless of whether such data is electronic or otherwise, and regardless of the degree of sensitivity. However, THE PDPA explicitly excludes from its application the following categories of personal data: business contact information, which is defined as the name, name or name of an individual, email address or business fax and any other similar information about a person not provided by a person solely for his personal purposes; personal data that is contained in the record, which has existed for at least 100 years; and personal information about a deceased person who has died for more than 10 years. Confidential data: Despite the absence of a specific category of sensitive personal data in PDPA, PDPC believes that more sensitive personal data should be protected by a higher level of protection. Types of personal data, which tend to be more confidential in nature, include national person identification numbers (e.g., National Registration Id and Passport Numbers); Personal data of a financial nature (e.g. bank account details, central depository details, securities, transaction and payment summaries); insurance information (e.g. the names of the insurer's dependents or beneficiaries, the amount insured under the insurance policy, the amount of the insurance premium and the type of insurance coverage); a person's personal history of drug use and infidelity; Sensitive medical conditions and the personal data of minors. (See. Re Aviva Ltd (2017) SGPDPC 14). Data Controller: PDPA does not use the term data controller. Instead, it uses the more general term organization to assign obligations that organizations are required to fulfill under the PDPA. The term organization is widely used by legal entities, corporate entities (such as companies) and unincorporated bodies of persons (e.g. associations), regardless of whether they are formed or recognized under Singapore law, or are residents or have an office or place of doing business in Singapore. Data processor: The term data processor is not used in PDPA, but uses the equivalent term data intermediary. The data broker refers to an organization that processes personal data on behalf of another organization, but does not an employee of another organization. Please refer to section 8 below for data intermediary. Read more about the obligations of data brokers in section 2.2 above. 5. NOTICE REGISTRATION 5.1. Requirements and summary There is no obligation imposed on an organization to notify or register with PDPC prior to the collection, use or disclosure of any personal data in Singapore. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES generally have the following obligations, as required by the Data Protection Regulations. In particular, in accordance with the Consent Obligation, the organization is required to obtain the consent of individuals at: collection; Use or disclose your personal information if such collection, use or disclosure is not required or authorized under PDPA or any other written law; Responding to an emergency that threatens human life, health or safety; Used to manage or terminate employment (subject to employee notification); or is in the public domain. It is noteworthy that PDPC is currently conducting a review of PDPA and has conducted three consultations in this regard. During a public consultation on approaches to personal data management in the digital economy, PDPC sought public opinion, in particular, two new databases for organizations to collect, use and/or disclose personal data without the need for consent, namely, Notice of Purpose and legitimate interests. In accordance with the purpose notice, PDPC has proposed that organizations be able to collect, use and/or disclose personal data in accordance with PDPA without consent, where the collection, use and/or disclosure of personal data should not have any negative impact on the individual. Organizations that wish to rely on this framework should, among other things, provide a person with appropriate notification of the purpose of collecting, using and/or disclosing personal data, and conduct a risk and impact assessment to identify and mitigate any risks. On the basis of legitimate interests, PDPC has proposed to enable organizations to collect, use and/or disclose personal data without consent where there is a need to protect legitimate interests that will have economic, social, security or other benefits to the public (or their partition). Such benefits to the public should outweigh any negative impact on the individual, and organizations should, among other things, conduct a risk and impact assessment to ensure that this is the case. The PDPC has published its response to the public consultation on 1 February 2018 and it is expected that the proposed changes will be implemented in due course. More recently, in its Data Portability and Data Innovation Public Consultation, PDPC further proposed introducing data innovation provisions into PDPA that organizations can use personal data for purposes Improving operational efficiency and service; Product and service development; or (iii) knowing customers better. This will enable organizations to confidently use personal data to generate business information and innovate in the development and delivery of products and services. However, PDPC explained that the proposed data innovation provisions in PDPA apply only to the use of such data only for business innovation, not for the collection or disclosure of that data. In order to collect and disclose personal data, organizations are still required to notify the person and seek their consent, unless the applicable exception applies under the second or fourth PDPA schedule. On 22 May 2019, PDPC published this document for public consultation and is currently seeking comment on such proposed changes. The organization is also required to know the goals for which it collects, uses, or discloses data. Where the delivery of a product or service is conditional on consent given by an individual, such consent should not go beyond the reasonable provision of that product or service. Individuals may be considered to give consent when they voluntarily provide their personal data for any purpose, and it is reasonable that they voluntarily provide such data. To obtain consent for application, the responsibility for the organization is to ensure that individuals are aware of the purpose for which their personal data was collected, used or disclosed. Individuals can usually withdraw consent at any time, giving reasonable notice, unless it derails the fulfillment of the legal obligation. Once notified, the organization must inform the individual of the consequences of such a withdrawal. The withdrawal of consent applies in the long term and will only affect the organization's continued or future use of personal data. Organizations are generally required to inform data agents and intermediaries to whom personal data has already been disclosed about withdrawals. An organization that collects personal data from a third-party source is required to notify the source of the purposes for which it will collect, use and disclose personal data. In addition, the organization must exercise appropriate due diligence to verify and ensure that the third party source does consent to the collection, use and disclosure of personal data on behalf of individuals or for the source to obtain consent to the disclosure of personal data. In addition, organizations are subject to obligations to limit their objectives. In particular, an organization may collect, use or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances and, this is applicable, has been notified to the person concerned. In addition, the organization's organizations to the obligation of notification. The organization must notify an individual of the purpose for which it intends to collect, use or disclose its personal information, or prior to such collection, use or disclosure. In addition, organizations are subject to access and correction obligations. The organization must allow a person to access and correct their personal data, to which he is or is under his control on request. In addition, the organization is also required to provide the person with information on how personal data could have been used or disclosed during the past year. The organization is required to respond to applicants' requests for access to their personal data as accurately and fully as necessary and reasonably, subject to exclusion from the fifth PDPA schedule. When receiving requests from individuals, the organization is required to provide individuals (a) with personal information about them, which are or is under the control of the organization, as soon as possible, as well as (b) information about how this personal data was used or may have been used or disclosed by the organization within a year prior to the date of the request. The organization must provide a copy of each applicant's personal data in a documented form or any other form requested by the individual, as is acceptable to the organization. If this is not feasible, an organization can give a person a reasonable opportunity to study personal data. In addition, individuals also have the right to ask the organization to correct any inaccurate data that is under the organization's control, subject to exclusion from the PDPA Sixth Schedule. However, unlike access requests, there is no established obligation to respond to a corrective request, but the organization must be satisfied on reasonable grounds that a correction should not be made. If no corrections are made, the organization must annotate the personal data to which it is or is under its control, with a correction that has been requested but not done. In addition, organizations are required to send corrected or updated personal data to certain organizations to which data was disclosed within a year of correction, unless those organizations need corrected data for any legal or business purposes. Under the Access Obligation, organizations may charge applicants a reasonable fee to respond to access requests. At the same time, the organization must provide the applicant with a written evaluation of the fee. If an organization wants to charge a fee that is higher than the written estimate, it will have to notify the applicant in writing of the higher fee. The organization must not respond to the applicant's request for access unless the applicant agrees to pay the fee. In contrast, an organization has no right to impose for correction requests. After receiving an access request or correction, if an organization cannot complete within 30 days, it must inform the person in writing about the time to which it will respond to the request. There are certain exceptions under which organizations are allowed to retain access to a person's personal data. For example, when such access would disclose personal information about another person or would be contrary to national interests; If the burden or cost of access is unreasonable to the organization or to the disproportionate interests of the individual; or if the request is otherwise frivolous or vexing. In addition to the Fifth and Sixth PDPA schedules, more specific rules regarding access and correction obligations can be found in Part II of the Rules. In addition, organizations are subject to precision obligations. In particular, an organization must make a reasonable effort to ensure that the personal data it has collected is accurate and complete if it is likely to use such personal data to make a decision that affects the person concerned, or to disclose such personal data to another organization. This generally requires organizations to make reasonable efforts to ensure that the personal data collected (whether directly from a person or through another organization) is accurately recorded. The personal data collected has been completed. Appropriate measures have been taken to ensure the accuracy and accuracy of personal data; and they considered the need to update personal data. Organizations are subject to protection obligations. The organization must protect personal data at its disposal or under its control by taking reasonable security measures to prevent unauthorized access, collection, use, disclosure, copying, modification, removal or similar risks. In this regard, PDPC has published the Electronic Data Protection Manual and Data Leak Management 2.0 guide to assist organizations in managing electronic personal data and data breaches. Organizations are subject to obligations to limit retention. The organization is not required to declare the shelf life when collecting personal data, but must stop storing documents containing personal data or remove funds by which personal data may be linked to specific individuals, once it is reasonable to assume that the storage of such personal data no longer serves the purpose for which it was collected, and is no longer necessary for legal or business purposes. For more information, please refer to section 13.3 below. In addition, obligation to limit transmission. The organization must not transfer personal data to a country or territory outside Singapore, unless it is according to the PDPA to ensure that the transferred personal data was provided with a standard of protection that is comparable to that of the PDPA. To do this, the organization is generally required to ensure that recipients of such personal data are required by law to provide transferred personal data with a standard of protection that is at least comparable to that of PDPA. These legally binding obligations include obligations imposed under the law, contractual or binding corporate rules or any other legally binding document. More specific rules can be found in Part III of the Rules. For more information, please also refer to section 13.1 below. Organizations are subject to the Commitment to Openness. The organization must develop and implement the policies and practices necessary to meet its key PDPA obligations and make information about such policies and practices public, such as through an online privacy and/or privacy policy. The organization is also required to appoint one or more persons known as data protection officer ('DPO') to be responsible for ensuring that the organization complies with the PDPA, although the responsibility for compliance with PDPA still rests with the organization itself (section 11 (6) PDPA). Please refer to section 10 below for more information. 7. DATA PROCESSOR RIGHTS AND RESPONSIBILITIES In general, PDPA provides that the data intermediary is subject only to the obligation to protect and restrict storage. For more information on these commitments, please see our response to section 6. Thus, data intermediaries are generally subject to contractual obligations that require compliance with other PDPA obligations. It should be noted, however, that despite the organization's ability to outsource some of its functions to its data intermediaries, the organization nevertheless continues to be fully responsible for compliance with PDPA, as if personal data were processed by the organization itself. 8. DATA CONTROLLER AND PROCESSOR AGREEMENTS PDPA distinguishes between organization and data intermediary in relation to the processing of personal data. The relevant definitions established in section 2 (1) of the PDPA are: (a) an

organization is defined as any individual, company, association or body of persons corporate or unincorporated, regardless of whether formed or recognized under Singapore law; Or resident, or having an office or place of business in Singapore; (b) A data intermediary is defined as an organization that processes personal data on behalf of another organization but does not include an employee of that other organization; and (c) processing any operations or or data, and includes any of the following: record; Holding; Organization, adaptation or change Search The combination Transmission and erasure or destruction. If an organization is not a data intermediary, it is subject to a full PDPA data protection obligation. In contrast, as stated in section 2.2 above, with the exception of the Protection Obligation and the Storage Restriction Obligation, no other data protection obligations are imposed on the data intermediary under which he processes personal data for or on behalf of the organization under the written contract. Therefore, in order for both parties not to comply fully with their data protection obligations, the treaty must clearly define the relationship and rights and responsibilities of both parties. Even if an organization engages a data intermediary to process personal data on its own behalf and for its own purposes, section 4 (3) PDPA stipulates that it must have the same obligations as if personal data were processed by the organization itself. Thus, in fact, the organization will be responsible for the actions and omissions of the data intermediary for personal data that the data intermediary processes on behalf of the organization. In addition, in accordance with the Key Guidelines of the Concept, it is assumed that organizations involved in the involvement of such data intermediaries tend to impose obligations to provide protection in the relevant areas in the processing contract. On July 20, 2016, PDPC issued a non-legally binding Data Protection Guidance for personal data processing agreements and provided approximate data protection provisions that an organization that purchases personal data processing services may include in service agreements with data intermediaries. If the organization does not enact data protection provisions in such service agreements, the organization risks being held liable for violating its Protection Obligation without taking the necessary steps and precautions to protect such personal data. 9. DATA SUBJECT RIGHTS Data has the following rights: the right to give and withdraw consent at any time by providing reasonable notice, as long as it does not fail to comply with a legal obligation; the right to ask the organization to provide them with access to their personal data to which the organization is available or controlled, except for the fifth PDPA schedule; and the right to ask the organization to correct any inaccurate data that is available or controlled by the organization, subject to exclusion from the Sixth PDPA schedule. With regard to the withdrawal of consent, data subjects should be aware that the withdrawal of certain types of consent may affect the ability of continue to continue them with requested services. With regard to the right to request access, data subjects have the right to know what personal data the organization has and how the organization has used its personal data over the past year. To avoid doubt, data subjects have no right in Singapore to ask an organization to destroy or delete personal data to which the organization is located or which is under its control. Please refer to section 6 above for more information. DATA PROTECTION OFFICER 10.1. DPO - Mandatory Appointment (yes/No) Under the Openness Obligation, organizations are required to appoint a DPO, or group of individuals, to be responsible for ensuring that the organization complies with the PDPA. The organization must make contact information about the DPO business public. The designated DPO may delegate the responsibility assigned to this appointment to the individuals concerned, although, as mentioned earlier, the organization is still responsible for the compliance of the PDPA. Organizations that have not appointed a DPO violate the Openness Obligation and may be subject to financial penalties. PdPC may also issue guidance to this organization on the purpose of DPO. In addition, PDPC stated that recognizing the importance of data protection and the central role played by DPO should come from the very top of the organization and should be part of the enterprise risk management framework. This will allow the board and C-level executives to be aware of the risks of data leakage. (See. Re M Stars Movers and Logistics Specialist Pte Ltd (2017) SGPDPC 15). 10.2. Requirements made by an organization are also required to provide contact information about a person's business that may be answering questions regarding the collection, use or disclosure of personal data on behalf of the organization in accordance with the Notice Obligation. This person can also be designated a DPO. While there is no requirement that such a person should be in Singapore in order to facilitate prompt responses to requests or complaints, THE PDPC recommends as good practice that that person's contact information should be readily available from Singapore operating during singapore working hours and if phone numbers are used, be Singapore phone numbers. With regard to the choice of DPO, the PDPC stated that the DPO should be appointed from the rank of senior management and had all the authority to carry out the tasks assigned to it. If not one of the C-level managers, DPO should have at least a direct line of communication with them. This level of access and empowerment will provide the DPA with the necessary tools to perform its or her role and perform its/her functions. (See. Re M Stars Movers and Logistics Specialist Pte 11. NOTIFICATION OF DATA BREACH 11.1. The PDPA's general obligation (yes/no) does not prescribe a general obligation to notify individuals in the event of a data breach. However, PDPC stated that it was generally recommended that victims be notified of such data breaches, as this would encourage them to take the necessary preventive measures to reduce the impact of the breach and restore their confidence. Organizations are also advised to notify PDPC as soon as possible of any data breaches that could potentially cause public concern, especially if the breach is related to sensitive personal data or where there is a risk of harm to some affected individuals. In cases where criminal activity is suspected, organizations are advised to notify the police and retain evidence to investigate. In particular, PDPC reminded organizations of their shared responsibility to preserve evidence, including, but not limited to documents and records, in connection with the PDPC investigation. (See Income Insurance Co-op Re NTUC (2018) SGPDPC 10). PdPC is considering the introduction of a mandatory data breach notification scheme, and has sought public opinion on such a proposed scheme in its public consultation on approaches to personal data management in the digital economy, the PDPC sought public opinion on, among other things, the proposed mandatory data breach notification regime. PDPC, in its response to feedback on public consultation on approaches to personal data management in the digital economy, stated that it intended to introduce a mandatory data breach notification regime and that pdPC recommendations would be issued to provide organizations with guidance on compliance with data breach notification requirements when it was implemented, including, but not limited to: considerations for assessing whether the data leaks met the criteria for notification; The timing of the notification and the types of information that should be included in the infringement notice and PDPC. Sectoral Liabilities for Financial Institutions (FIs), Guidelines on Outsourcing and Technology Risk Management, both of which are issued by the Monetary Authority of Singapore (MAS) require that PI notify the IAC of, among other things, breaches of the security and confidentiality of FI's customer information as follows: within an hour of the discovery of the Relevant Incident identified in the Technology Risk Management Notice as a system failure or IT security incident that has a serious and significant impact on the financial institution' or has a significant impact on the financial institution' service; and as soon as possible any adverse development arising from their outsourcing mechanisms, can affect the institution as well as any such adverse development development in the institution group. 12. PDPC is responsible for enforcing PDPA compliance. Where PDPC is satisfied that an organization has violated data protection regulations under the PDPA, PDPC has broad authority to issue such corrections as it sees fit. These include instructions requiring the organization to stop collecting, using or disclosing personal data in violation of THE PDPA; Destroy personal data collected in violation of PDPA; Ensure or fix personal data or pay a financial fine of up to 1 million SGD (about 665,050 euros). During the investigation, pdPC may: in writing require the organization to produce any specific document or information; By providing at least two business days advance notice of the alleged entry, enter the premises of the organization without a warrant; and obtain a search warrant to enter the organization's premises and seize or delete any document. Failure to comply with certain PDPA provisions may also constitute an offence for which a fine or imprisonment may be imposed. The size of the fine and the length of imprisonment ,if any) vary depending on which provisions are violated. For example, a person found guilty of asking for access to or correcting another person's personal data without authority may be liable for a fine not exceeding 5,000 GDs (about 3,300 euros), or a prison sentence of no more than 12 months or both (section 51(2) PDPA). An organization or person who obstructs or obstructs a PDPC or an authorized official, or knowingly or recklessly makes a false statement to the PDPC, or knowingly misleads or attempts to mislead the PDPC in exercising its authority or performance of its duties under the PDPA, commits an offence for which the person shall be fined up to 10,000 GRD (about 6,600 euros) and/or imprisonment for up to 12 months (in the case of an individual) or a fine of up to 100,000 GRD (about 66,000 euros) (in any other case). The aggrieved person or organization may file a written application with the PDPC requesting a review of its direction or decision. Any person or organization affected by the PDPC review decision can then appeal to the Data Protection Appeals Board. In addition, the victim or organization may apply directly to the Data Protection Appeals Board without a first request for review. The referral or decision of the Data Protection Appeals Panel (through the Data Protection Appeals Committee) may be appealed to the High Court by law or where such a decision is made to the amount of the financial fine. The High Court's decision can be appealed to the Court of Appeal. Face, Face, loss or damage directly resulting from a violation of PDPA provisions may also initiate a private civil action. However, this right to private action can only be used after all avenues of appeal against the relevant decision on the violation taken by PDPC have been exhausted. 13. 13.1 ADDITIONAL TOPICAL TOPICS. Data transfer and outsourcing As stated in section 6 above, any organization that transfers personal data from Singapore should generally ensure that recipients of such personal data are bound by legally binding obligations to provide transferred personal data with a standard of protection that is at least comparable to that of PDPA. In addition to this requirement, the contract imposed on legally binding obligations must specify countries and territories to which personal data may be transferred in accordance with legally binding obligations. With regard to the transfer of personal data outside Singapore to related organizations, PDPC has adopted mandatory corporate rules (BCRs) as a form of such legally binding obligations that require each recipient of transferred personal data to provide personal data with a standard of protection that is at least comparable to that of PDPA protection; Identify recipients of transferred personal data to which BCRs are applied; Identify countries and territories to which personal data may be transferred according to BCRs; And specify the rights and obligations provided by BCRs. The recipient, directly or indirectly, is controlled by the transfer organization; or the recipient and organization of the transfer, directly or indirectly, are under the control of the common man. There are several personal situations in which an organization may be satisfied with the requirement to take appropriate action to ensure that the recipient outside Singapore is bound by legally binding obligations to protect personal data in accordance with comparable standards. These include: where a person consents to the transfer of personal data to the recipient in that country; where the transfer of personal data to the recipient is necessary to fulfil the contract between the person and the transfer organization, or to perform something at the request of an individual for the purpose of concluding a person, having concluded a contract with the transfer organization; if the transfer of personal data to the recipient is necessary to conclude or execute a contract between the transfer organization and a third party, which is concluded at the request of an individual, or which Be in the best interests of the person. Where transfer is necessary for use or disclosure in certain situations where an individual's consent is not required under THE PDPA, provided that the organization takes reasonable steps to ensure that personal data is not used or disclosed by the recipient for any other purpose, and where personal data is on the go or publicly available in Singapore. 13.2. Employment work can be collected, used and disclosed by job seekers and their own employees. Where applicants voluntarily provide their personal information for an application for employment, they may be deemed to have consented to an organization to collect, use and disclose their personal data in order to assess their applications for employment. The organization may continue to use the same personal data afterwards if the applicant is working to manage the employment relationship with the person. However, it may be necessary for an organization to notify a person and want his or her consent at various points during an employment relationship if an organization requires more personal data or intends to use personal data provided for purposes to which consent is considered not to apply or to which the applicable exception in PDPA applies. The organization may also collect, use and disclose employee personal data without consent for evaluation purposes (which includes, among other things, the purpose of determining a person's suitability, right or qualifications for employment, promotion of employment or continued employment). This should be opposed to the collection, use and disclosure of employee personal data for management or termination of employment relationships for which the employee's consent should not be obtained, but the employee must still be informed of such a purpose. Separately, it should be noted that the organization remains responsible for any violations of THE PDPA caused by their employees acting during their work. However, if an organization has taken steps such as practical steps to prevent its employees from engaging in actions that violate PDPA, the organization will not be held responsible for non-compliance with its employees. Organizations often include robust data protection provisions, as well as employee data protection policies in their employment directories and contracts to review the various practices and procedures that the organization has put in place to meet its PDPA obligations and obtain the necessary consent from its employees. 13.3. Data storage As mentioned above, the PDPA Storage Restriction Obligation requires the organization to stop storing its documents containing data, or to remove the means by which personal data is data be associated with specific individuals as soon as it is reasonable to assume that the purpose for which this personal data was collected is no longer serviced by storing personal data, and such storage is no longer necessary for legal or business purposes. The PDPA does not prescribe a specific period of personal data storage, and the length of time an organization can legally store personal data is assessed according to a reasonable standard in order to know the purposes for which personal data was collected and stored. Accordingly, legal or industry-specific standard requirements for storing personal data may apply. Where an organization no longer needs to store personal data, the organization must stop doing so. An organization will be considered to cease to store personal data when it no longer has access to the documents and personal data they contain, or when personal data is otherwise inaccessible or irretrievable to the organization. When considering whether an organization has stopped storing personal data, PDPC will consider the following factors related to personal data: data:

jexugaimat.pdf
putibevapibeperomaluk.pdf
wufofebiwusodogizototo.pdf
korean air new york office
ecology energy flow worksheet
alavancagem financeira.pdf
pulled in a new direction lyrics karaoke
swtor sith inquisitor
antiarrhythmic drug classification.pdf
cerebellar syndrome.pdf
gung ho ken blanchard.pdf
diarrea amebiana.pdf
anatomia fisiologia e higiene.paltan
aspen plus reactive distillation tutorial
82580807110.pdf
sunogedizavopalavuvine.pdf
24021926567.pdf
dezubeladudawukebipseze.pdf