b) Y Electronics will cease to disclose Andy's personal data to any third party; and

c) Y Electronics will cease using Andy's contact details for marketing computer and IT products and will instruct its outsourced marketing agent likewise (so that it will cease sending marketing information to Andy).

However, Y Electronics will not be required to inform the third party companies to which it disclosed Andy's contact details, and Andy will have to approach those companies to withdraw consent if he wishes to do.

The withdrawal of consent also does not affect Y Electronics' ability to retain Andy's personal data that it requires for legal or business purposes. For example, Y Electronics may still retain Andy's personal data in its database for the purpose of servicing an ongoing warranty, or records of his purchases that are necessary for audit purposes.

Exceptions to the Consent Obligation

12.55 Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) and enumerates the permitted purposes in the First and Second Schedules to the PDPA. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations.

Legitimate interests exception

12.56 "Legitimate interests" generally refer to any lawful interests of an organisation or other person (including other organisations). Paragraphs 2 to 10 under Part 3 of the First Schedule to the PDPA relate to specific purposes that would generally be considered "legitimate interests", for instance, for evaluative purposes, for any investigation or proceedings, or for recovery or payment of debt owed. Legitimate interests exceptions in paragraphs 2 to 10 under Part 3 of the First Schedule are specific exceptions which organisations can rely on if these are applicable. The general legitimate interests exception ("legitimate interests exception") in paragraph 1 under Part 3 of the First Schedule is a broad exception that can be relied on for any other purposes that meet the definition of "legitimate interests", when other specific exceptions do not apply. To rely on this general exception,

organisations will need to assess the adverse effect and ensure the legitimate interests outweigh any adverse effect.

12.57 As the legitimate interests exception allows the collection, use or disclosure of personal data without consent for a wide range of circumstances and purposes, the onus is on the organisation seeking to rely on this exception to comply with additional safeguards to ensure that the interests of individuals are protected. Organisations must assess that they satisfy the following requirements before relying on the legitimate interests exception:

a) **Identify and articulate the legitimate interests**. Organisations must identify and be able to clearly articulate the situation or purpose that qualifies as a legitimate interest.

b) **Conduct an assessment**. Paragraph 1(2)(a) read with paragraph 1(3) under Part 3 of the First Schedule, provides that an organisation must conduct an assessment before collecting, using or disclosing personal data (as the case may be) to (i) identify any adverse effect that the proposed collection, use or disclosure is likely to have on the individual; and (ii) identify and implement reasonable measures to eliminate, reduce the likelihood of or mitigate the adverse effect on the individual. Where it is assessed that there is likely residual adverse effect to the individual after implementing the measures, organisations are required to conduct a balancing test as part of the assessment to determine that the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect to the individual. Organisations may wish to use the **Assessment Checklist for Legitimate Interests Exception** (at **Annex C**) to conduct the assessment. Please refer to the Personal Data Protection Regulations 2021 and paragraphs 12.64 – 12.69 below for the considerations when conducting the assessment.

c) **Disclose reliance on the legitimate interests exception**. Paragraph 1(2)(b) under Part 3 of the First Schedule provides that organisations relying on the legitimate interests exception to collect, use or disclose personal data without consent must take reasonable steps to provide the individual with reasonable access to information that they are relying on the exception. This may be through any means that is reasonably effective (e.g. disclosure as part of the organisation's public data protection policy).

Identify and articulate the legitimate interests

12.58 In identifying the legitimate interests of collecting, using or disclosing the personal data for a purpose, organisations should be able to articulate the following:

a) ***What the benefits and who the beneficiaries are***: Organisations should identify the benefits arising from the collection, use or disclosure of the personal data, and who the beneficiaries are. The benefits identified should focus primarily on direct benefits of the collection, use or disclosure of the personal data. Examples of benefits include security of business assets and individuals at premises, prevention of fraud and misuse of services, etc. Organisations should also consider whether there could be any negative impact on individuals, or a particular group of individuals should the organisation not be able to collect, use or disclose the personal data without consent for the purpose. Apart from benefits to the organisation, beneficiaries could also include other organisations, the wider public or a segment of the public such as customers, employees, sectors or industries of the economy.

b) ***Whether the benefits are real and present***: In general, the identified benefits should not be purely speculative, and should include both tangible (e.g. increased business efficiency and cost savings) and intangible benefits (e.g. improved customer experience). The presence of related commercial or business interests do not subtract from the public benefits which may be derived, and all the benefits to each identified beneficiary should be considered.

12.59 Organisations cannot rely on the legitimate interests exception to send direct marketing messages. In general, organisations must obtain express consent to send direct marketing messages to individuals. In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or fax, the organisation must comply with the Do Not Call Provisions of the PDPA[13].

Disclose reliance on legitimate interests exception

12.60 Organisations that rely on the legitimate interests exception to collect, use or disclose personal data must make it known to individuals that they are relying on this exception to collect, use and disclose personal data without consent. For example, an organisation could state in its public data protection policy that it is relying on the legitimate interests exception to collect, use or disclose personal data for purposes of security and prevention of misuse of services. To be clear, organisations are not required to make available their assessments of legitimate interests to the public or to individuals as part of disclosing reliance on the exception.

12.61 Organisations must also provide the business contact information of a person who is able to address individuals' queries about the organisations' reliance on the

[13] Refer to PDPC's Advisory Guidelines on the Do Not Call Provisions.

legitimate interests exception. This person may be the Data Protection Officer ("DPO") or someone charged with the responsibility to handle such queries. This is similar to the requirement under the PDPA where an organisation needs to inform an individual of the purpose of the collection, use or disclosure of his personal data when it enters into an employment relationship or appoints the individual to any office; or manages or terminates an employment relationship[14], except that the information relating to the reliance on the legitimate interests exception will have to be provided through channels that are external-facing (e.g. general notification in the company's data protection policy on its publicly-accessible website).

Justify reliance on legitimate interests upon the Commission's request

12.62 Organisations that rely on the legitimate interests exception to collect, use or disclose personal data are to document their assessments and steps taken to mitigate residual risks. Under the Personal Data Protection Regulations 2021, the organisation must retain a copy of its assessment throughout the period that the organisation collects, uses or discloses personal data based on the legitimate interests exception. Upon the Commission's request, organisations are required to provide justification to the Commission on their reliance on the legitimate interests exception, including their assessments of legitimate interests (which includes balancing tests), and other related documents. Given the potential commercial sensitivity of organisations' assessments, the assessments need not be made available to the public or to individuals.

Examples of legitimate interests

12.63 Examples of legitimate interests include the purposes of detecting or preventing illegal activities (e.g. fraud, money laundering) or threats to physical safety and security, IT and network security; preventing misuse of services; and carrying out other necessary corporate due diligence[15]. Subjecting such purposes to consent is not viable as individuals may choose not to give consent or to withdraw any consent earlier given (e.g. individuals who intend to or who had engaged in illegal activities), impeding the organisations' ability to carry out such functions.

---

[14] Section 20(4) and (5) of the PDPA provides that, despite subsection (3), an organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of entering into an employment relationship with the individual or appointing the individual to any office; or managing or terminating the employment relationship with or appointment of the individual, shall inform the individual of (a) that purpose; and (b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure on behalf of the organisation.

[15] This would apply to organisations that intend to conduct further and necessary corporate due diligence on customers, potential customers and business partners in addition to existing statutory requirements. For instance, the collection, use and disclosure of personal data for the consolidation of official watch lists.

Example: Fraud detection and prevention purposes by a company

An insurance company intends to collect, use and disclose personal data about its customers' past insurance claims for fraud detection and prevention.

The insurance company conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data outweigh any adverse effect to the individual. Insurance company states in its data protection policy on its website that it is relying on the legitimate interests exception to collect, use and disclose personal data for fraud detection and prevention purposes.

In this case, the insurance company may rely on the legitimate interests exception to collect, use or disclose personal data for detecting and preventing fraud.

Example: Fraud detection by multiple companies

A healthcare service provider and multiple insurance companies intend to share personal data (i.e. medical records, payment information, patient's health insurance policies, claim records) to detect and prevent healthcare fraud and abuse (e.g. duplicated claims) by creating a fraud detection model.

The companies conduct a joint assessment of legitimate interests, and assess that the benefits of the collection, use and disclosure of personal data outweighs any adverse effect to the individual. These companies also include in their respective data protection policies on their websites that they are relying on the legitimate interests exception to collect, use and disclose personal data for detecting and preventing misuse of services.

The companies may rely on the legitimate interests exception to collect, use and disclose the personal data of their customers to detect and prevent misuse of their services.

Example: Hotels' detection and prevention of misuse of services by guests

Several hotels intend to compile and share a blacklist of hotel skippers (i.e. hotel guests with track record of not fulfilling their payments for use of hotel services) to prevent further misuse of their services. The blacklist would contain the personal data of hotel skippers (i.e. full name, NRIC/passport number, amount owed and details of non-payment) who have two or more occurrences of non-payment for the use of hotel services.

These hotels conduct a joint assessment of legitimate interests, and assess that the benefits of the collection, use and disclosure of the personal data outweigh any adverse effect to the individuals. These hotels also include in their respective data protection policies on their websites that they are relying on legitimate interests exception to collect, use and disclose personal data for detecting and preventing misuse of services.

The hotels may rely on the legitimate interests exception to collect, use and disclose the personal data of customers to detect and prevent misuse of their services.

Example: Bank's network analysis to prevent fraud and financial crime, and perform credit analysis

A bank intends to integrate data across individuals and their associated organisations and businesses to build further profiles about them. The use of personal data allows the bank to identify individuals who may have committed a financial crime or received funds in relation to a crime; and to identify individuals and organisations with credit inter-dependencies to form better assessments of their actual credit standings and sources of funds for repayment.

In addition to comply with the Monetary Authority of Singapore's ("MAS") requirements[16], the bank conducts an assessment of legitimate interests and assesses that the benefits of using the data (i.e. detection and deterrence of flow of illicit funds through Singapore's financial system, understanding prospects' or customers' financial standing) outweigh any likely adverse effect to the individuals (e.g. identification of individuals with potential nefarious intentions, enforcement actions by authorities, and impact on credit facilities to individuals assessed to be of poorer credit standing).

The bank includes in its privacy policy that it is relying on the legitimate interests exception to collect, use and disclose personal data for conducting credit checks, analyses and due diligence checks as required under applicable laws.

In this case, the bank may rely on the legitimate interests exception to collect, use and disclose personal data to prevent fraud and financial crime, and perform credit analysis.

[16] Banks in Singapore are required to ensure their collection, use and disclosure of personal data are in accordance with the MAS requirements to prevent money laundering and countering the finance of terrorism.

Example: Collection and use of personal data on company-issued devices to prevent data loss

As part of its internal security defence and data loss prevention strategy, a technology company intends to install a data loss prevention software on the laptops, desktops and mobile devices which it issues to its employees so that it can effectively detect any unauthorised data leakage, disclosure or loss of its information. The tool collects a variety of personal data about its users (e.g. user log-in details, device information, files, device communications and content).

The technology company conducts an assessment of legitimate interests and assesses that the benefits of the collection of personal data to protect its commercial and proprietary interests outweigh any likely adverse effect on its employees.

The technology company includes in its privacy policy and employee handbook to inform its employees that it is relying on the legitimate interests exception for the collection and use of personal data through the software installed on company-issued devices.

Assessments for relying on deemed consent by notification[17] and legitimate interests exception[18]

12.64 Organisations are required to conduct assessments of any likely adverse effect to the individual when relying on deemed consent by notification or the legitimate interests exception.

12.65 In general, the Commission considers adverse effect to include any physical harm, harassment, serious alarm or distress to the individual. There may be circumstances where individuals may be affected by businesses' decisions resulting from the use of personal data (e.g. differential pricing for customers of differing purchase history or payment track records). To be clear, while the collection, use or disclosure of an individual's personal data could result in differentiated treatment of individuals, not all instances of differential charges (e.g. insurers charging persons with pre-existing health conditions a higher insurance premium) or refusal to provide services (e.g. rejecting loan application from an individual with poor credit rating) will be considered "adverse effect". The Commission generally considers prevailing social norms, including practices that a reasonable person would consider appropriate, when determining whether there is likely adverse effect to the individual.

[17] Refer to section 15A(4)(a) of the PDPA.
[18] Refer to paragraphs 1(2)(a) and (3) under Part 3 of the First Schedule to the PDPA.

12.66 As part of the assessment, organisations are also required to identify and put in place reasonable measures to eliminate, reduce the likelihood of or mitigate any adverse effect to the individual. In determining whether the measures implemented to eliminate or mitigate the likely adverse effects identified are appropriate, the Commission adopts a commercially reasonable standard. Examples of reasonable measures and safeguards include minimising the amount of personal data collected, encrypting or immediate deletion of personal data after use, functional separation, access controls, and other technical or organisational measures that lower the risks of personal data being used in ways that may adversely impact the individual.

12.67 Where it is assessed that there are likely **residual adverse** effects to the individual after implementing the measures, **organisations will not be able to rely on deemed consent by notification** to collect, use or disclose personal data for the purpose. Whereas for the legitimate interests exception, organisations are required to conduct a balancing test as an additional step in the assessment to determine whether the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect on the individual. **Organisations may rely on the legitimate interests exception if the legitimate interests outweigh any likely residual adverse effect** to the individual.

12.68 **Joint assessments** may also be conducted by the disclosing and receiving organisations when relying on deemed consent by notification or legitimate interests exception to collect and disclose the personal data. In such cases, the assessment will factor in the considerations of the organisations involved. Alternatively, the disclosing and receiving organisations may conduct their assessments separately and provide their own justifications for the collection or disclosure of personal data for the identified purposes.

12.69 In determining the likely adverse effect on the individual, the organisation should consider the following:

a) ***The impact of the collection, use or disclosure of the personal data on the individual:*** Organisations are required to assess both the **severity and likelihood** of any adverse effect that may arise from the collection, use or disclosure of personal data. The assessment referred to in these Guidelines requires an assessment of **all reasonably foreseeable risks and adverse effect to the individual** resulting from the intended collection, use or disclosure. In general, the more severe the adverse effect of the collection, use or disclosure to the individual, the more unlikely the benefits of the collection, use or disclosure would outweigh the likely adverse effect. Please refer to paragraph 12.65 on adverse effect.

b) ***The nature and type of personal data and whether the individuals belong to a vulnerable segment of the population:*** In general, the potential adverse effect to individuals will be higher if the personal data is sensitive in nature. Organisations should also consider the individuals to whom the personal data relate, and whether they belong to a vulnerable group such as minors[19], individuals with physical or mental disabilities, or other special needs. The adverse effect may be more severe if the individuals belong to a vulnerable segment of the population.

c) ***The extent of the collection, use or disclosure of personal data and how the personal data will be processed and protected:*** Organisations should consider how extensive the collection, use or disclosure of an individual's personal data will be, and how the personal data will be collected, used or disclosed (e.g. whether collection is one-off or on a continuous basis). Organisations shall ensure that they do not collect, use or disclose more personal data than is reasonably necessary in order to achieve the purpose. For instance, collection of more types of data about an individual is likely to have a higher risk and adverse effect than collection of only specific types of personal data. How the personal data is protected, such as the implementation of access controls to prevent any unauthorised access, use or disclosure, may also affect the likelihood of adverse effect to the individuals.

d) ***Reasonableness[20] of the purpose of collection, use or disclosure of personal data:*** Organisations should ensure that the purpose of the collection, use and disclosure of personal data is proportionate and appropriate in the circumstances. In general, the context should be considered when assessing the reasonableness of purpose. For example, when using or disclosing personal data for a secondary purpose, organisations may wish to consider the primary purpose and how the personal data was collected, and whether it affects the reasonableness of using or disclosing the personal data for the new purpose.

e) ***Whether the predictions or decisions that may arise from the collection, use or disclosure of the personal data are likely to cause physical harm, harassment, serious alarm or distress to the individual***: Where the collection, use or disclosure of personal data is to make predictions or decisions about individuals, organisations should also consider prevailing social norms and practices that a reasonable person would consider appropriate in determining if the decisions are likely to result in unfair

[19] Refer to Chapter 7 of PDPC's Advisory Guidelines on the PDPA for Selected Topics.
[20] Refer to section 18 of the PDPA on Purpose Limitation Obligation.

discrimination, physical harm, harassment, alarm or distress to the individual.

12.70 Please refer to **Annex B** for the Assessment Checklist for Deemed Consent by Notification, and **Annex C** for the Assessment Checklist for Legitimate Interests Exception.

Business improvement exception

12.71 Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule ("business improvement exception") enable organisations to use, without consent, personal data that they had collected in accordance with the Data Protection Provisions of the PDPA, where the use of the personal data falls within the scope of any of the following business improvement purposes[21]:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

12.72 In order to rely on the business improvement exception, organisations will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and

b) The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

12.73 The business improvement exception also applies to the sharing of personal data (i.e. collection and disclosure) between entities belonging to a group of companies[22], without consent, for the following business improvement purposes:

[21] "Relevant purposes" are defined in paragraph 1(2) under Part 5 of the First Schedule to the PDPA.
[22] "Group of companies" refers to related corporations within the meaning of the Companies Act (Cap. 50).