Parliament No:	14
Session No:	1
Volume No:	95
Sitting No:	11
Sitting Date:	2-11-2020
Section Name:	Second Reading Bills
Title:	Personal Data Protection (Amendment) Bill
MPs Speaking:	Mr Shawn Huang Wei Zhong (Jurong),Ms Joan Pereira (Tanjong Pagar),Mr Yip Hon Weng (Yio Chu Kang),The Senior Minister of State for Communications and Information (Dr Janil Puthucheary),Mr Chua Kheng Wee Louis (Sengkang),Mr Sharael Taha (Pasir Ris-Punggol),Mr Desmond Choo,Mr Speaker,Mr Gerald Giam Yean Song,Ms Tin Pei Ling (MacPherson),Mr Gerald Giam Yean Song (Aljunied),The Minister for Communications and Information (Mr S Iswaran),Mr Patrick Tay Teck Guan (Pioneer),Ms Jessica Tan Soon Neo (East Coast),Mr Melvin Yong Yik Chye (Radin Mas),Mr Deputy Speaker,Mr Louis Ng Kok Kwang (Nee Soon)

PERSONAL DATA PROTECTION (AMENDMENT) BILL

Order for Second Reading read.

Mr Speaker: Minister Iswaran.

3.07 pm

The Minister for Communications and Information (Mr S Iswaran): Thank you, Mr Speaker. I beg to move, “That the Bill be now read a Second time”.

Sir, the Personal Data Protection Act, or PDPA, was enacted in 2012. Since then, there have been profound changes in the data landscape, most notably in the sheer variety and volume of data that is being generated and its economic significance. The typology of data is diverse – ranging from personal and machine-generated to meta data – with different risk implications.

The volume of data is growing at an unprecedented rate. Today, Tera/Peta/Zetta bytes of data – you can pick your prefix – are being generated by ubiquitous Internet-of-Things or IoT devices and sensors, our real and virtual world activities, and smart machines in manufacturing and supply chains. The

International Data Corporation estimates that the volume of data that will be created in the next three years will eclipse the total data generated over the past 30 years.

Data is also a key economic asset in the digital economy. Data analytics provides valuable insights that inform decisions, generate efficiencies, enhance products and services, and power innovation. It is a critical resource for emerging technologies like artificial intelligence, which hold much transformative potential.

Our regulatory architecture must evolve and keep pace with these magnitudinal shifts. For example, we have initiated digital economy Agreements to position Singapore as a key node in the global network of digital flows and transactions. The proposed amendments to the PDPA are another step to ensure our legislative and regulatory regime is fit for purpose for a digital economy with a complex data landscape.

Our digital economy must be built on a solid foundation of trust. Consumers must have the confidence that their personal data will be secure and used responsibly, even as they benefit from digital opportunities and data-driven services. Organisations need certainty to harness personal data for legitimate business purposes, with the requisite safeguards and accountability. The proposed amendments to the PDPA seek to strike this balance so as to maximise the potential benefits and minimise the risks of collecting and using personal data.

In drafting the Bill, we have studied the data protection practices in jurisdictions like Australia, Canada, the European Union, Hong Kong and New Zealand. The proposed amendments also incorporate valuable feedback received through four public consultation exercises.

Sir, I will elaborate on the amendments which aim to: first, strengthen consumer trust through organisational accountability; second, ensure effective enforcement; third, enhance consumer autonomy; and fourth, support data use for innovation.

Firstly, to strengthen consumer trust, organisations must undertake responsibility for the personal data in their possession or control. Today, this principle of accountability is implied in sections 11 and 12 of the PDPA. Clause 4 of the Bill inserts a specific reference to accountability at Part III to make the principle explicit and to underscore its centrality.

This shift towards an accountability approach is in line with international trends and best practices in data protection laws. It supports interoperability, allowing multi-national corporations to more easily adapt global best practices in Singapore, and minimises compliance costs for Singapore-based companies which are expanding globally.

To further strengthen organisations' accountability, clause 13 introduces a system for mandatory notification to the Personal Data Protection Commission, or PDPC, when a data breach occurs.

Under this Clause, organisations must notify the PDPC of data breaches that are of significant scale. In addition, organisations must notify both the PDPC and affected individuals when data breaches result, or are likely to result, in significant harm to individuals. This places the onus on organisations to assess the scale and impact of data breaches, ensures they are duly accountable to individuals for the personal

data in their care, and empowers individuals to take timely measures to protect themselves if a data breach occurs.

Sir, the Bill also incorporates the recommendations of the Public Sector Data Security Review Committee in its report of November 2019.

First, clause 3 removes the current exclusion for agents of Government, thereby making clear that all private sector organisations are subject to the PDPA, even when they are acting on behalf of public agencies.

Second, the Bill strengthens individual accountability for the egregious mishandling of data. Clause 22 sets out new offences for (a) disclosure of personal data; (b) use of personal data that results in personal gain for the offender or another person, or harm or loss to another person; and (c) re-identification of anonymised information. Related amendments will also be made to the Public Sector (Governance) Act and the Monetary Authority of Singapore Act to align the public and private sector data regimes.

While the primary responsibility and liability for breaches of the PDPA rest with organisations, these new offences are aimed at individuals who know that their actions are not authorised or who act recklessly. The clause provides for defences to the new offences, such as independent testing of anonymisation deployed in information security systems. Also, these offences should not apply in situations where the conduct is solely in the nature of a private dispute, which should continue to be resolved through civil suits or other forms of dispute resolution.

Sir, let me now move to the second cluster of amendments, which seeks to enhance the flexibility and effectiveness of the PDPC's enforcement.

Clause 23 introduces section 48L, a statutory scheme under which the PDPC may, in lieu of a full investigation, accept written voluntary undertakings from organisations to remedy breaches and prevent their recurrence. For example, such undertakings may be accepted when organisations with effective monitoring and breach management systems notify the PDPC of a data breach, and undertake in writing to implement their breach management plan.

Several jurisdictions, like Australia, Canada and the UK, accept voluntary undertakings as part of their enforcement regimes. The PDPC will exercise this option only if it assesses that it will achieve an outcome similar or superior to a full investigation. For transparency, the undertakings, as well as the PDPC's decisions and considerations for accepting them, will be made public. In the event of non-compliance, the PDPC may issue a direction requiring the organisation to comply with its undertakings, or initiate investigations.

Section 48G of clause 23 empowers the PDPC to establish dispute resolution schemes for the resolution of customer complaints. The PDPC may also direct complainants and organisations to attempt to resolve disputes via mediation, without the need to secure the consent of both parties.

Clause 37 empowers the PDPC to require the attendance of an individual or employee to give statements and produce documents that are relevant to its investigations.

Clause 24 increases the maximum financial penalty for breaches of Parts III to VI, and the new Parts VIA and VIB, to 10% of an organisation's annual turnover in Singapore or $1 million, whichever is higher. This penalty framework is similar to that in other domestic regulation and legislation, including the Competition Act and the Telecommunications Act.

During public consultations, concerns were raised about the higher financial penalties. I would like to assure Members, as well as the broader community, that the PDPC will ensure that financial penalties imposed are proportionate to the severity of the data breach. The Bill also provides for Ministerial discretion to review the effective date for these penalties to commence and we intend for the revised financial penalty cap to take effect no earlier than one year after the Act comes into force.

Sir, I also wish to highlight, at this juncture, that I will be moving a Notice of Amendment during the Committee Stage to address a clerical error in clause 24 of the Bill.

Clause 23 sets out amendments providing for the enforcement of the Do Not Call or DNC provisions under the same civil administrative regime as the data protection provisions. The new Part IXA of clause 22 also prohibits the use of dictionary attacks and address-harvesting software when sending messages to telephone numbers. Under clause 24, the maximum financial penalty that may be imposed on an organisation is 5% of annual turnover in Singapore or $1 million, whichever is higher, and $200,000 for an individual.

The new section 48O under clause 23 of the Bill updates the current right of private action by a person who suffers loss or damage directly as a result of a breach of the data protection provisions. The right of private action will be extended to organisations and public agencies that suffer direct loss or damage arising from contraventions of the new business-to-business obligations in the Bill.

Sir, the third set of amendments confers consumers with greater autonomy over data generated by their use of services and more control over how they receive commercial communications.

Under the PDPA, individuals have the right to access their personal data, and request for corrections to be made or a copy to be provided. Clause 14 extends this right by providing for a new Data Portability Obligation, which will enable individuals to request for a copy of their personal data to be transmitted to another organisation. Data portability is expected to spur competition and benefit consumers by encouraging the development of substitute as well as novel services.

Sir, though data portability has been introduced in practice in jurisdictions like Australia, California and the EU, it is a relatively new concept in Singapore. The PDPC will therefore work closely with all stakeholders for a phased implementation. Regulations will be issued in the coming months on the categories of data that should be portable and other technical and consumer protection details.

Clauses 22 and 41 update both the PDPA and the Spam Control Act to rationalise and harmonise the requirements across all modern digital channels for direct commercial communication with consumers. The options for direct communications have evolved since the enactment of the PDPA's DNC provisions and the Spam Control Act's spam control provisions. For example, instant messaging on mobile devices has become the communication channel of choice for many consumers. With the proposed amendments, organisations can offer consumers a unified experience in managing their

subscription to commercial communications. The Bill also recognises the development of an industry of third party DNC checkers, and delineates the responsibilities and obligations of DNC checkers and the organisations that commission them.

Sir, the final set of amendments aims to provide organisations greater clarity on the use of personal data.

Currently, the PDPA recognises organisations' need to use personal data for legitimate purposes, and accommodates them through exceptions to the consent requirement, or as deemed consent. For all other purposes, organisations have to obtain consent from the individual.

The proposed amendments update, restructure and clarify the lawful purposes recognised as exceptions under the PDPA, and the deemed consent provisions. Let me elaborate how changes to exceptions and deemed consent accommodate modern commercial arrangements and essential purposes such as security, and support business innovation.

Multiple layers of contracting and outsourcing are common in modern commercial arrangements. Clause 6 therefore expands deemed consent to cater for scenarios where personal data is passed from an organisation to successive layers of contractors for the organisation to fulfil the contract with its customer. Crucially, organisations relying on deemed consent for contractual necessity can only collect, use and disclose personal data where it is reasonably necessary to fulfil the contract with the individual.

Clause 31 introduces the First Schedule to the PDPA, which sets out a new exception to consent for these legitimate uses of personal data. To rely on this exception, organisations must conduct an assessment to eliminate or reduce risks associated with the collection, use or disclosure of personal data, and must be satisfied that the overall benefit of doing so outweighs any residual adverse effect on an individual. To ensure transparency, organisations must disclose when they rely on this exception. One of many potential use cases is anomaly detection in payment systems to prevent fraud or money-laundering.

The next set of enhancements supports innovation and introduction of new services.

The new First and Second Schedules introduced in clauses 31 and 32 make clear that organisations may use personal data for business improvement purposes including: operational efficiency and service improvements; developing or enhancing products or services; and knowing the organisations' customers. As a safeguard, this exception can be relied upon only for purposes that a reasonable person may consider appropriate in the circumstances and where the purpose cannot be achieved without the use of the personal data.

Businesses have asked for this exception to also apply to entities within a group as they may consolidate corporate or administrative functions, or concentrate research and development expertise in a single unit that supports the entire group. Recognising this commercial reality, Part 5 of the new First Schedule in clause 31 allows related corporations to collect and disclose personal data among themselves for the same purposes. The Bill provides for additional safeguards for intra-group sharing by

requiring related corporations to be bound by a contract, agreement or binding corporate rules to implement and maintain appropriate safeguards for the personal data.

The current research exception has also been revised in clause 32 to support commercial research and development that is not immediately directed at productisation, in other words, going upstream. This could apply to research institutes carrying out scientific research and development, educational institutes embarking on social sciences research, and organisations conducting market research to identify and understand potential customer segments.

Clause 7 introduces the new section 15A, which expands the consent regime by introducing deemed consent by notification. Under this provision, organisations may notify their customers of the new purpose and provide a reasonable period for them to opt out. Before doing so, organisations must conduct a risk assessment and conclude that the collection, use or disclosure of personal data in this manner will not likely have an adverse effect on the individual.

To illustrate, this would be useful for organisations that wish to use the personal data of existing customers for new purposes. For example, a financial institution may want to use voice data as an alternative means to authenticate and verify its customers. With these amendments, the financial institution can notify its customers of the intended use of their voice data, provide a reasonable opt-out period, and a contact number for customers' queries. It should be noted that the individual may still withdraw his deemed consent any time after the opt-out period has lapsed.

The PDPC will put in place safeguards to ensure that organisations work with anonymised data as much as possible, clearly assess and address any potential adverse effects on individuals, and continue to seek express consent for sending direct marketing messages.

Sir, in summary, the proposed amendments to the PDPA will strengthen consumer trust with greater accountability for the protection of personal data; it will give greater certainty for organisations to use data for legitimate business purposes with the requisite safeguards; and it will ultimately enhance Singapore's status as an important node in the global network of data flows and digital transactions. Sir, I beg to move.

Question proposed.

3.28 pm

Ms Tin Pei Ling (MacPherson): Mr Speaker, Sir, thank you for allowing me to speak on this Bill.

The world is undergoing massive digital transformation. The Fourth Industrial Revolution has perhaps already induced the fifth. Singapore is also set on this path as we strive towards becoming a Smart Nation.

The global digital race is intense. The risk of winner takes all is there and if this happens, where does that leave us. Therefore, there is urgency for us to transform and the urgency for us to transform is also increasing, in large part due to the on-going COVID-19 pandemic. According to a McKinsey study

published in October 2020, companies surveyed across all sectors and regions digitised 20 to 25 times faster during COVID-19.

A consequence of digitalisation is that firms and people become more connected globally. This interconnectedness means access to bigger markets, which can be a boon for our talents and firms.

Singapore is thankfully at the forefront in Asia for having the right conditions to embrace a digital economy and smart nation. For example, in the IMD World Digital Competitiveness 2020 ranking, Singapore came in second, just behind the US.

Against this background, we can understand the explosion of data in Singapore and the importance of data to our digital economy. Data is vital to innovation.

Intuitively, data for innovation and data protection seem to conflict with each other. We need data to create and optimise products, processes and business models. Hence, there must be sufficient room for harnessing and using data. Too much controls leads to high compliance costs and distracts firms from innovating. Start-ups may also find it stifling.

Yet, data protection, specifically personal data, is essential to protecting the privacy and interests of our citizens.

Prior to the introduction of PDPA in 2012, public awareness of personal data protection was generally lower. Anecdotally, we can easily recall instances in which people trustingly and freely share NRIC numbers and other personal information with various parties for various purposes. Consequently, besides receiving unwanted marketing material, they also become vulnerable to scams and crimes.

Having laws and a mechanism to sufficiently protect personal data engenders greater trust. A clearly defined framework and laws that are effectively enforced will build consumers' confidence. One study of GDPR on how data protection regulation affects start-up innovation, published in November 2019, suggests that while the regulation appears to obstruct certain business models and technologies, it also clearly stimulated a certain amount of innovation and market opportunities.

More studies may be needed to study the effects of regulation on innovation. But we can agree that data protection regulation builds trust.

A healthy dose of trust enables meaningful data to be shared and drives innovation. This forms a virtuous cycle. Therefore, a balanced approach to regulation is important. Singapore needs high quality do-good innovations. Facilitating the use of data in a way that does not erode consumer trust will enable Singapore to innovate better and faster, and stay competitive.

Furthermore, firms are no longer confined to Singapore with growing global connections. They can operate out of Singapore and still access markets around the world. With the rise of cross-border e-trade and e-commerce, putting in place the right data laws will enhance our interoperability with global frameworks, thereby making it easier to do business and allow cross-border data flow. The idea of "if it works in Singapore, it works everywhere" will be very helpful in strengthening Singapore's position as a regional and global innovation hub.

Hence, I generally welcome the amendments to the PDPA. A balance in this approach is hard to strike and I do note that four consultations had been conducted to date and I believe that this effort is to precisely to try to strike this balance. But I do have four key concerns and would like to seek the Minister's clarifications.

First, the introduction of data portability and extension of spam controls and DNC provisions to all direct communication platforms would give consumers more control over their own data. But contraventions will now be dealt with as a civil proceeding in Court. I believe that this was originally a criminal proceeding. My concern is that this perceived "step down" will diminish the importance of personal data protection and the severity of breaching the law. Therefore, it risked undermining consumer trust. Can the Minister explain the rationale for this change?

Second, the deemed consent will now be enabled in this amendment. I understand this to be a move to avoid unnecessary inefficiencies in contracts with multiple layers of outsourcing. But I am also concerned, whether this will weaken consumer protection and therefore again, consumer trust. I note the measure that are put in place in Minister's speech earlier, I am just wondering what kind of risk-assessment and disclosure are we talking about. Would the Ministry regularly review whether these mechanisms are sufficient in providing sufficient protection and control to the consumers?

Third, the amendment facilitates the collection, use or disclosure of personal data for a broad range of business purposes such as enhancing goods or services, operational processes, personalised services and research and development. Clearly, sufficient flexibility in harnessing and using data is needed for innovation. But many actions can be categorically explained as addressing one of such purposes. How will the Government prevent abuse in a more upstream manner? Again, I say this because I know that enforcement has been enhanced, even individuals can be liable for breaches, but, I am wondering, whether it can be more upstream to provide enough guidelines to have more controls in place to prevent this in the first place.

I understand that it can be too tedious and time consuming for enterprises to keep applying for Government's approval for every relevant business decision. That would be counter productive to innovation. But, might there be a "whitelist" or "blacklist" that clearly articulates the boundaries, the "dos" and "don’ts", for the firms?

Fourth, finally, will the "relaxation" in the collection, use or disclosure of personal data for commercial innovation purposes in this Amendment be applied to the Government and public service? If so, what measures are in place to ensure consistency and avoid double standards in terms of data protection policy, standards and enforcement? The Government, as a body with regulatory powers and control over significant resources, will have to exercise greater discipline, caution and demonstrate transparency when handling personal data. A better understanding of how the Government handles personal data will no doubt strengthen public trust. Notwithstanding my concerns, I support the Bill.

3.35 pm

Mr Chua Kheng Wee Louis (Sengkang): Mr Speaker, the Personal Data Protection (Amendment) Bill is a much welcome update, eight years after the original Bill was first introduced in 2012. Eight years is a

long time in the digital age. Technology has advanced by leaps and bounds and such technological improvements have also significantly changed our lives.

[Deputy Speaker (Mr Christopher de Souza) in the Chair]

Singapore has one of the highest Internet penetration rates in the world. Eighty-eight percent of the population are Internet users and spend close to seven hours a day on the Internet on average. They 8.9 million mobile connections, approximately 1.5 times more than the country's population. The easy access of the Internet allows people to engage in content sharing, online shopping, access gaming sites and social media platforms amongst others.

The law, too, has to keep up with the times. With increasing usage of such digital platforms comes increasing risk of personal data breaches. Most Singaporeans use their smartphones for social networking or to search for information. And as a result, the number of scammers, impersonators and cyber attacks has jumped nine folds in the last three years with 672 cases in the first 11 months of 2019, with over half the victims in their 20s to 40s. In fact, just a few days ago, personal information from 1.1 million RedMart customers were stolen from Lazada, an e-commerce platform. Personal data such as names, phone numbers, emails and physical mailing addresses were being sold online.

While I appreciate the effort to enhance the legal framework for the collection, use and disclosure of personal data, and to strengthen the accountability of organisations in respect of handling these data, I believe that there is still room for further refinement, namely in strengthening protection against unsolicited communication, clarifications on deemed consent and individuals rights under data portability.

Firstly, protection against unsolicited commercial messages. Mr Speaker, there are multiple safeguards in place within the original PDPA, with the intention to protect data privacy of individuals. One of such safeguards is the Do Not Call Registry when an individual can opt to be excluded for marketing or promotional messages. However, even with such safeguards in place, most Singaporeans still get unsolicited calls and messages from telesales agencies, moneylenders, illegal gambling advertisements and even phishing scam calls claiming to be from SingPost or DHL, asking them to collect the parcel.

Improved controls for unsolicited commercial messages and the section 43, would thus, be welcomed by consumers. A few years ago, I have personally lodged a Police report over persistent and unlicensed moneylending messages, but I was subsequently told by the Investigation Officer that the perpetrators are based overseas and that there is not much that we can do.

I acknowledged that some of these calls and messages are from overseas or even from masked numbers. However, some are actually conducted from local numbers and since 2005, it is compulsory to present customer details to telcos when purchasing both a prepaid and postpaid SIM card. Now, with the revised Bill when organisations have breached the PDPA Act, they could have to pay a penalty of 10% of their annual Singapore turnover or up to S$1 million dollars, whichever figure is higher.

However, I would like to ask, how can we better protect Singaporeans against unsolicited messaging and fraudulent communication from criminal syndicates, especially the elderly who are at risk of such scams. In particular, how does the Commission intend to take action against parties that are not even based in Singapore.

Second is the topic on deemed consent and deemed consent by notification. Mr Speaker, under the section of deemed consent, organisations are allowed to pass information to a third party for the fulfilment of the contract between the person and the organisation. While this makes sense, we should question if there are any mitigating factors to prevent the unwanted spreading of personal particulars or information from the third party organisation to subsequent parties for their benefit. For example, targeted marketing strategies as well as also raising the possible issue of increased risk of the spread of personal information. With personal data held by multiple parties across multiple jurisdictions potentially, the risk of the data leak is much higher and data protection is only as strong as the weakest link.

Furthermore, in the newly added section 15(a), deemed consent by notification, organisations are now able to collect information on the individual as long as the organisation has taken reasonable steps to inform the individual the organisation's intent, purpose to collect, use or disclose the person's data. The organisation itself also has to make sure that this is not likely to have an adverse effect on the individual. Individuals also have the right to opt out or withdraw consent within a reasonable period.

Mr Speaker, this system reduces the power of individuals relative to organisations who have the power to determine if the collection use and disclosure of personal data have any adverse effect on the individuals.

Section 15(a) also gives organisations the freedom to determine whether or not there is any adverse effect on the individual, which may not always be interpreted in the individual's favour. The new provision does serve as an exception to the consent obligation and moves the data protection framework away from express and explicit consent to implicit consent from individuals. For example, online shopping algorithms are designed to identify the type of product a person is interested in and to suggest to the person, items that he or she may like to purchase. If a person for example, has conditions that decreases his overall well-being with these advertisements, for example, having compulsive buying disorder, is that deemed as an adverse effect that should be intervened?

An organisation needs to identify and implement reasonable measures to eliminate or reduce the probability of the adverse effect. What are some of the ways that these can be executed in reality?

Further, what is regarded as a reasonable period for individuals to opt out? Are businesses allowed to determine this or will the commission be providing some guidance on the general timeframe?

Perhaps, we could adopt the practice from the European General Data Protection Regulation or GDPR, where there are specific categories of data in which processing such data is prohibited unless explicit consent is given by the individual. The PDPC could consider something similar by carving out exceptional categories of data where deemed consent by notification, cannot work or requires express consent.

Lastly, on the new Part VIB on data portability. The introduction of the new data portability obligation is a welcome one, where an organisation must at the request of an individual, transmit his or her personal data that is in the organisation's possession or under its control to another organisation in a commonly used machine-readable format. However, while the individual can request for his or her data to be transferred from one organisation to another, individuals themselves do not have the specific right to

receive a copy of such data in a machine-readable format before it is ported over. This may pose issues for individuals that may want to limit or select the data they would like to hand over to the receiving organisation. And this will be unlike Article 20 of the European GDPR, which gives individuals the right to receive the personal data concerning him or her.

I acknowledge that there is an "access request" under section 21 of the current PDPA, where individuals may be able to get a copy of their personal data that is under the possession of the originating organisation. However, it is unclear to what extent this will apply hand-in-hand with the data portability obligation. Further in this digital world, it is often been said that, "the Internet never forgets". Could we perhaps go one step further and that in addition to data portability and access to one's personal data, can the individual be granted the right to request organisations to delete personal data at his or her request? This would then truly give meaning to the phrase under section 26G and that is to provide individuals with greater autonomy and control over their personal data.

Mr Deputy Speaker, to conclude, the updated PDPA is the right step in ensuring the data security of Singaporeans. What has perhaps not been fully addressed is firstly, the ability to enforce such rules to protect against unsolicited messages, particularly from overseas parties; secondly, the power imbalance between organisations and individuals under a deemed consent opt-out regime; and finally, the individual’s rights to his or her data. In this rapidly evolving digital age, it is imperative that we constantly assess and fine-tune the PDPA, in order to maintain the effectiveness of its safeguards.

Mr Deputy Speaker: Ms Joan Pereira.

3.46 pm

Ms Joan Pereira (Tanjong Pagar): Mr Deputy Speaker, Sir, the COVID-19 pandemic has led to the acceleration of digitalisation in almost every aspect of our lives. Hence, it has become even more important for us to ensure that our data protection legislation is keeping pace with advances in information technology.

Recent data breaches, which affected 1.1 million Redmart and 2.8 million Eatigo accounts, highlight once again the dangers lurking in the shadows of Internet space and the importance of cybersecurity and remedial procedures. I understand that users were informed quite quickly and were thus able to take measures to protect themselves, such as changing their passwords.

Different organisations have very different attitudes towards data protection. Therefore, I am very glad that the Bill’s amendments will make it compulsory for all organisations to notify the Personal Data Protection Commission or PDPC and affected individuals of data breaches. This will compel all companies to step up controls or risk heavy financial penalties.

However, I note that notifications are only required where there are significant number of people affected, which had previously been proposed at 500 or more, and where there could be significant harm for affected individuals, such as compromised NRIC and credit card numbers.

I would therefore like to ask the Minister why notifications to PDPC need be made only when the breaches involve a prescribed number of people? I feel that as long as an individual is affected, PDPC

should be informed. I note that the current online reporting form for data breaches is already quite a simple one-page form that takes about eight to 10 minutes to fill up, and hence reporting should not be too onerous for organisations. Of course, any individual acting in a personal or domestic basis will not be caught by these obligations, as such a case is already excluded from the Act.

In addition, the Bill specified that PDPC must be notified within 72 hours and affected persons, without undue delay. This in effect means that there is no timeframe set for notifying individuals. I feel that there should be a clear deadline so that individuals can do the needful to protect themselves. Time is of the essence. The longer it takes to inform them, the greater the potential damage, and the PDPA is not simply a notification regime, but is also an Act that protects individuals and their data. Individuals may also need to take their own steps to change, mask or protect their data, including those on other platforms, especially if the leaks involve their digital identities, which are increasingly interlinked. Sir, in Mandarin.

(*In Mandarin*)*:* [*Please refer to* ***Vernacular Speech***.] In addition, the Bill specified that PDPC must be notified within 72 hours, and affected persons, without undue delay. This in effect, means that there is no timeframe set for notifying individuals. I feel that there should be a clear deadline so that individuals can do the needful to protect themselves. Time is of the essence. The longer it takes to inform them, the greater the potential damage, and the PDPA is not simply a notification regime, but is also an Act that protects individuals and their data. Individuals may also need to take their own steps to change, mask or protect their data, including those on other platforms, especially if the leaks involve their digital identities, which are increasingly interlinked.

(*In English*): I welcome more stringent controls over spam and telemarketing through related amendments to the Spam Control Act or SCA. The SCA will be updated to protect users from unsolicited messages, particularly bulk commercial texts sent to instant messaging accounts, such as WhatsApp and Facebook Messenger. The most common messages make offers of loans, gambling and betting.

My question is how the Ministry would deal with perpetrators from overseas. How can they be caught and what recourse do our people have, besides blocking these numbers as and when they attack? Would the Ministry be able to explore cross-jurisdictional cooperation with countries where these overseas numbers have originated from, so that there is a possibility of either bringing these syndicates to justice or at least to shut them down?

Finally, I urge PDPC to check and conduct selective audits to ensure that all companies that collect consumers' personal data have a tight regime in protecting the data collected. If there are gaps, would PDPC consider providing more resources and experts at a reasonable or low cost to help and guide these companies, since prevention is always better than cure? Sir, I would like to conclude with my support for the Bill.

Mr Deputy Speaker: Mr Shawn Huang.

3.52 pm

Mr Shawn Huang Wei Zhong (Jurong): Mr Deputy Speaker, Sir, the digital landscape of Singapore is constantly evolving. Cross-border data flows and data capitalisation is increasing the importance for

business competitiveness.

The current regime of consent-based data protection faces challenges from the rapid, technological developments. In addition, the recent data breaches suffered by the likes of Lazada, Razer and Eatigo evidenced the need for solid personal data protection laws. Personal data protection laws must offer adequate protection to individuals but still allow businesses to remain agile and competitive. The amendments to the PDPA to shift towards a risk-based accountability approach is practical and in line with modern economy and global data protection laws. These amendments should attend to a basic tenet of protecting the rights of individuals.

I wish to clarify on two points.

Under the Bill, organisations may process personal data without the consent of individuals in circumstances classified as "legitimate interests". This concept may be ambiguous in certain contexts. Without further guidance on the scope of legitimate interests, especially for vulnerable segments such as children be provided. This will ensure that individuals are protected and companies can comply to requirements efficiently and responsibly.

Secondly, the Bill requires organisations to notify PDPC of data breaches that result in or likely to result in significant harm to affected individuals or it is of significant scale. Organisations will also be required to notify affected individuals if the data breach is likely to result in significant harm to them. The concept of significant harm and significant scale may again ne very ambiguous. As such, would further guidance of the concept of significant harm and significant scale be provided. If significant scale constitutes prescribed number, can I clarify on how this number is obtained? I agree with the need to strengthen the accountability of organisations and enabling of meaningful consent as reflected in the Bill. Mr Deputy Speaker, Sir, I support the Bill.

Mr Deputy Speaker: Order. I propose to take a break now. I suspend the Sitting and will take the Chair again at 4.15 pm.

Sitting accordingly suspended

at 3.55 pm until 4.15 pm.

Sitting resumed at 4.15 pm.

[Mr Deputy Speaker in the Chair]

PERSONAL DATA PROTECTION (AMENDMENT) BILL

Debate resumed.

Mr Deputy Speaker: Mr Gerald Giam.

4.15 pm

Mr Gerald Giam Yean Song (Aljunied): Mr Deputy Speaker, before I speak, I would like to declare my interest as a director and shareholder of a technology company which manages and safeguards customers' personal data.

The protection of personal data is a concern of all Singaporeans, particularly when they learn about mass data breaches suffered by public agencies and private companies, both here and abroad.

There is now greater public awareness among members of the public and organisations of the need to safeguard personal data. The public has a right to demand strong protection of their personal data. At the same time, policy-makers have to be aware of the business costs of complying with stringent regulations. It is thus necessary to make periodic amendments to the Personal Data Protection Act or PDPA and the Spam Control Act to bring our data privacy regulations more in line with current realities and global norms.

I will focus on three areas in my speech.

First, ensuring that personal data is protected where it matters to citizens, yet without unnecessarily burdening business with regulations.

Second, aligning the PDPA with the GDPR, the European Union's general data protection regulation to avoid conflating rules.

Third, harmonising the Government's data protection rules with the PDPA to ensure that Government agencies safeguard personal data the same way as it expects private sector companies to do.

Everyone wants their personal data protected from prying eyes and unwanted marketers. No one likes being interrupted by unsolicited phone calls from people they do not know, trying to sell things that they do not want or tricking them into sharing confidential information. They certainly do not want scammers using their NRIC address or credit card numbers to take up unauthorised loans, buy stolen goods or, worst of all, sell their personal data on the dark web.

We had made good progress in personal data protection since the introduction of the PDPA in 2012. However, some things are still slipping through. For example, despite being on the Do Not Call Registry since 2013, I still get phone calls or text messages from individuals offering cheap loans, access to illegal gambling sites or asking me to pick up packages which I never ordered.

More than 46,000 complaints on unsolicited calls and text messages had been made to the Personal Data Protection Commission or PDPC since 2017. I have met residents who were scammed of tens of thousands of dollars by swindlers who persuaded them over the phone to reveal their Internet banking passwords or one-time PINs. Still others had loans in their names taken up with loan sharks because their NRICs were misused. For most Singaporeans, these are the biggest concerns with regard to personal data privacy.

On the other hand, fewer people are concerned about what kind of cookies a website is using to track them and many find cookie notices on websites nowadays more of an irritant than a privacy protecting measure.

There is a debate going on about how to stop big tech companies from hoovering our personal data in order to serve us tailored advertisements. This is a valid concern but not something that keeps the average citizen awake at night. Privacy regulations should therefore give greater focus to the areas of data privacy that matter most to Singaporeans.

I will now move on to discussing the PDPA and GDPR. The general data protection regulation is a wide-ranging personal data protection legislation from the EU which has extraterritorial effect. The GDPR applies not only to European companies but also to Singapore companies that offer goods and services to individuals in the EU, even if those companies do not have an EU presence.

The PDPA covers much of the GDPR but there are many requirements in the GDPR that are more stringent than that of the PDPA. For example, the GDPR provides extra protection for special categories of data, which include data about an individual's race, religion, political opinions and health information. The PDPA does not specifically define what constitutes sensitive personal data although guidance from PDPC suggests that personal data of a sensitive nature should be accorded a higher level of protection as a matter of good practice. The GDPR also sets a more stringent standard for consent, which must be obtained in a clear, open, specific and transparent manner.

Despite its less prescriptive approach compared to the GDPR, the PDPA's model may be preferred by countries whose approach towards privacy is closer to Singapore's than the EU's. However, we should guard against the PDPA acquiring a reputation of providing a GDPR-minus standard of personal data protection. It would be much better if the PDPA were known internationally as a law that strikes the right balance between data protection and business efficiency.

While the PDPA may not be identical to the GDPR, it should not have provisions or interpretations which are in conflict with the GDPR. This way, Singapore businesses, which need to comply with the GDPR will be able to rest easy, knowing that they also comply with the PDPA.

Based on my analysis of the PDPA, I am glad to note that this currently appears to be the case. I hope that this approach will continue through future amendments to the PDPA.

My last point concerns the personal data protection obligations of the Government. Unlike the GDPR, the PDPA specifically exempts the Government from having to comply with it. The Government has explained that this is because it has its own set of data privacy standards, which are set out in the Public Sector Governance Act or PSGA, the Official Secrets Act or OSA, the Banking Act, the Income Tax Act or ITA, the Statistics Act and the Instruction Manual 8 or IM8, among others.

I have worked with the Government both as a civil servant and a government contractor, and I am well aware of the robust rules and practices in place to safeguard personal data. However, complying with a different set of data protection rules from the private sector is problematic for several reasons.

First, the data protection provisions in the various Acts differ in their standard of protection. For example, the maximum fines for violations of the different statutes range from $1,000 to $250,000. This is not surprising since these laws were enacted long before the PDPA and without the specific purpose of general data protection in mind. Having public data controllers governed by a hodge podge of separate legislation is likely to lead to differing standards and gaps in coverage.

Second, the lack of a single set of rules governing privacy leaves individual data owners unclear as to what level of personal data protection they are entitled to. Most individuals concerned about privacy would be more familiar with the protections provided under the PDPA than what is provided for under the PSGA, OSA, ITA, IM8 and others. In fact, the IM8 is not even a public document that ordinary citizens can access.

The Government's exemption from the PDPA could lead to concerns among citizens about how their sensitive data is being used by the Government. For example, many are now worried about how the information collected by SafeEntry and Trace Together will be processed. Others continue to worry about how our security services may be collecting and sharing sensitive information about citizens with little independent oversight.

Third, the Government regulations cover mainly internal checks on the Government Ministries and agencies, and criminal and disciplinary consequences for individual officers. A citizen who has incurred damages as a result of a data breach by a Government agency has little recourse to pursue civil remedies against that agency. The PDPA, on the other hand, grant such recourse against offending organisations. This could be seen as a lower threshold of accountability on the part of the Government should data beaches occur.

Why should public data controllers be treated differently from private data controllers. I believe there is merit in having a universal standard of personal data protection that applies to both private as well as public data controllers. If there is a need to maintain discretion because of national security reasons, these exemptions can be explicitly written into the PDPA.

I hope the Government can eventually harmonise the data protection clauses in the separate legislations and bring them under the umbrella of the PDPA and make the PDPA apply to Government agencies as well.

Mr Deputy Speaker, the overarching goal of data protection legislation is to ensure that personal data is not misused in a way that causes harm to individual. This can be achieved without causing undue inefficiencies in the functioning of businesses or the Government. We need to continue to update the PDPA to keep up with the realities on the ground. The Government should hold itself to the same level of data privacy standards, procedures and accountability it expects of private sector companies. Sir, I support the Bill.

4.27 pm

Ms Jessica Tan Soon Neo (East Coast): Mr Deputy Speaker, I rise in support of the Personal Data Protection (Amendment) Bill.

Sir, with the increasing demand and trend for personalisation of products and services and the pace of digitalisation in many aspects of everyday life and work, sharing personal information is increasingly a requirement for us to be able to gain access to a service, obtain a benefit or even to participate.

Against this backdrop, the Personal Data Protection (Amendment) Bill is timely. This looks to ensuring the protection and responsible use of personal data by organisations. Clear accountability on what data is

collected, used and disclosed digitally or even physically, will help in building consumers' trust. For businesses, having clarity on the use of personal data and the trust of consumers will give them the confidence to use the data to innovate and improve services.

With advancement in technology, the volume of personal data collected and aggregated is vast and growing. With capabilities like data analytics, machine learning and artificial intelligence making sense of the data and using it to gain valuable insights is real. If used appropriately, this can provide benefits but it can also be exploited for not so well-meaning purposes.

To strengthen trust and at the same time derive the value of data, we need to balance and handle the "right to data privacy", "data security" and "the proper use of data to innovate". These objectives may seem at odds.

My speech will focus on trust which I believe is core to achieving the objectives of this Bill. I will speak on two aspects of the proposed amendment which are key to protecting data while appropriately enabling the leverage of data for innovation.

First, the strengthening of organisational accountability. This will enchance the protection for indivduals and is key to building trust with individuals on how their personal data is used.

Second, amendment of section 15 regarding "deemed consent" and changes to the exceptions and the new section 15A "deemed consent by notification" and a reasonable period and manner for the individual to withdraw consent.

Let me touch now on strengthening of organisational accountability.

The amendments proposed in the Bill will make mandatory and will require organisations to report data breaches to the Personal Data Protection Commission or PDPC, if such breaches are likely to result in significant harm or impact to individuals, and/or are of a significant scale. Organisations must also notify affected individuals when a data breach is likely to result in significant harm or impact to them, regardless of the scale of the breach.

Why is this important? Cybercrime statistics show that data breaches continue to rise. And just to cite one example, on SafeatLast Editor's Choice, one of the key cybercrime statistics, that a hacker attack takes place every 39 seconds. So, you can imagine, as I am speaking here, by the time I finish my speech, the number of attacks that have happened. So, notification to individuals is important because it will allow them to take timely mitigating measures but also it is important that there is notification because it allows the national actions, both of the organisations and other organisations impacted to take the necessary actions.

To signal the importance of organisational compliance and the proper handling of personal data, irresponsible organisations will face a higher financial penalty cap of 10% of annual gross turnover in Singapore or $1 million, and if I heard the Minister correctly, whichever is higher. The Bill also includes the introduction of offences for the mishandling by individuals of personal data and fines and imprisonment for a term not exceeding two years or both.

With increased accountability, offences and penalties – while I do agree that it is necessary – there may also be a danger of organisations becoming overly risk averse to protect themselves. This seems a little strange but one would say it is okay for organisations to protect themselves. If they do all the right things, individuals will be protected. It really depends. If the scale is on organisations protecting themselves from being penalised or against enforcement, we may also lose the focus on actually protecting consumer's data privacy and risks. This may also have a negative impact on the desire to use data appropriately to innovate and improve productivity.

The Bill's introduction to require organisations to conduct risk assessments to identify and mitigate the adverse impact on individuals is the right approach because it balances this, because it allows organisations to analyse what is the real risk and really then make that decision of being able to notify and then decide to innovate. I will later touch on this in my speech on the point about "deemed consent" associated with the risk assessments.

These amendments to strengthen accountability of organisations are necessary as they give businesses clear guidelines on how they handle personal data. We must, however, recognise that there will be compliance costs associated. Given the value of personal data and the inherent risks, I think it is important that organisations take the responsibility and it is a necessary cost of doing business. But with the current economic challenges, can the Minister also share if there will be any support given to businesses in managing the increased cost of compliance and also the increased complexity of compliance?

Let me touch on the amendments to section 15 and the point about "deemed consent" and the new section 15A "deemed consent by notification".

As businesses may need to partner, subcontract and outsource services to deliver their contractual obligations to customers, the amendments proposed for section 15 introduces deemed consent by contractual necessity. I think this is important because it does recognise a new business model and facilitates collection, use and disclosure of personal data by organisations with their contractors and partners to enable better understanding of customers for more effective performance and fulfillment of contractual obligations to customers.

But let me now touch on the introduction of the new section 15A relating to deemed consent by notification. What is required of an organisation if it wishes to rely on this new section 15A to obtain deemed consent by notification is that they need to conduct risk assessments to identify and mitigate adverse effects that the collection, use and disclosure of the personal data may have on individuals.

This will allow them to collect and process personal data to use, to improves services as well as productivity research purposes and also for fraud detection and security. All these are good. I do support and agree that there are benefits for consumers when organisations use data to innovate.

I do, however, have questions on how we ensure that deemed consent by contractual necessity and by notification does not lead to unintended and more importantly, uninformed consent?

The requirements outlined in the Bill for notification, the manner and the period for individuals to opt out are fairly broad. I agree that it should not be prescriptive but there must be measures to ensure that

individuals fully understand that they are deemed to have given their consent for the use of their personal data if they do not opt out. And I am glad that the Minister, in his speech did say that the individuals can also withdraw consent even after the opt-out period. I think this is important.

Why am I saying this? Because many of us today, we just tick that box that says "I consent" but not realising that actually, even when you do not do it, it is deemed consent and therefore it is an uninformed consent. What I am asking for is, ensuring that there is informed consent, not necessarily that we take away deemed consent because, at the end of the day, what is important is consumer trust. And if consumers understand that fundamentally, then the protection and the appropriate use of information will be there because organisations will have that confidence to use the data.

Mr Deputy Speaker, I must admit that when I first reviewed the amendments proposed in the Bill, I was concerned with the challenge of how we can achieve the protection of personal data while still allowing the effective use of personal data for innovation because they seem at the opposite of each other.

But having worked through the details of the Bill, and I must admit that there was quite a lot of details on the Bill, I see that it does strive to achieve the difficult balance of protecting consumer personal data and, at the same time, not limit the use of data to innovate and deliver greater benefit. In today's day and age and the role that Singapore plays, I think it is important.

I do want to make a special mention to the team that worked on this because, clearly there was a lot of work put in and a lot of thought given in terms of that balance because when I first started looking at this amendment Bill, I actually had the very opposite feeling about it. But having gone through the details, I think there has been very good thought given to strengthening of accountability but at the same time, not limiting that use of data for innovations while protecting individuals' privacy.

I believe that success will be achieved when individuals trust that their personal data is protected. And this will in turn gives organisations confidence to use and leverage the data for insights to deliver value. Mr Deputy Speaker, I support the Bill.

4.39 pm

Mr Leon Perera (Aljunied): Mr Deputy Speaker, Sir, the PDPA Bill seeks to update the original PDPA Act to strengthen data privacy protections and individual data autonomy, ensure greater accountability on the part of organisations and enhance the power of the PDPC.

I do not oppose the Bill and agree with the comments expressed by my Parliamentary colleagues Mr Gerald Giam and Mr Louis Chua Kheng Wee. I shall focus my speech on just a few areas where I would like to pose technical clarifications and suggestions.

Firstly, Sir, I would like to speak on the mandatory data breach reporting guideline.

I suggest that the we could, in section 26B, provide a clearer and more precise definition of "significant harm" to an individual that would warrant notification. In other words, it would be helpful if the Government could provide a statutory definition or further guidance as to the factors that are to be taken into account in assessing the nature of the "harm" and any relevant thresholds before the PDPC would hold the view that

"significant harm" has been occasioned, so that organisations have clarity in their assessment as to when a data breach will be considered a notifiable data breach. The definition provided in section 26B subsection 2 currently seems rather broad.

Also, on this point, allowing for exemption of organisations by the PDPC from notifying affected individuals of data breaches in the new section 26D is problematic. In this clause, the obligation to notify affected individuals can be waived "subject to any conditions that the [PDPC] thinks fit".

Given that such an overly broad "escape" clause may undermine the legal spirit of the mandatory data breach notification requirement, I would like to ask: what are circumstances in which the Government may activate this clause, and would the Government consider tightening and carefully circumscribing the scope and use of this clause, to reduce any potential for abuse and the perception of arbitrariness?

Secondly, Sir, the amended Bill creates new offences to hold individuals accountable for egregious mishandling of personal data on behalf of an organisation or public agency.

The thrust of the PDPA is to hold businesses responsible such that risk can be treated as a business cost rather than something to be potentially placed on individual "scapegoats" who may have little bargaining power as employees.

With new offences for the unauthorised mishandling of personal data by individuals, including employees, there is the possibility that "scapegoating" may happen. Junior employees with lesser bargaining power may be held liable, while higher ranked employees and the organisation itself may face reduced accountability thereby.

While the amendments spell out possible grounds of defence that the accused individual may take, has the Government given some thought to what additional measures should be put in place to prevent such "scapegoating"?

Thirdly, I would like to speak about what has been referred to, in the context of the GDPR, as the "right to be forgotten".

I would suggest further extending the retention limitation obligations in the PDPA to be aligned with Article 17 of the GDPR, where individuals may interface with an organisation to request the deletion of data and where withdrawal of consent may lead to an obligation to immediately delete personal data. Sir, such an obligation seems to me to be not overly onerous on businesses.

Fourthly, businesses, especially SMEs, sole proprietorships and some not-for-profit organisations, may experience difficulties in adhering to these new, more rigorous regulations.

I would like to ask when this Bill will come into effect and would the Government consider allowing for a transition or grace period? Such a suggestion would be in line with, firstly, the previous 18-month transition period adopted before most of the substantive provisions of the PDPA took effect when it was enacted in 2012; and secondly, the two-year transition or sunrise period which was given when the GDPR was adopted by the European Union in 2016, during which time there was delayed enforcement so that organisations would have time to prepare.

During this transition period, the PDPC could consider providing greater support to SMEs and volunteer organisations in several respects.

Firstly, training of staff to understand the new requirements imposed and guidance to introduce new processes and frameworks in compliance with those requirements.

For instance, in the 2018 SingHealth data breach, the delay of 28 days in the reporting of the incident to senior management could be attributed to lack of staff training and absence of a reporting framework to some extent.

Voluntary organisations, in particular, may benefit from such training as they may lack knowledge of these requirements. For instance, in 2019, Henry Park Primary School Parents' Association was found by the PDPC to have been negligent in failing to make reasonable security arrangements to protect members' personal data and appoint a Data Protection Officer.

Secondly, Sir, the PDPC could, during this transitional period, provide guidance and possibly subsidies for adopting compliant IT systems, to reduce the compliance burden on these organisations while encouraging good data protection practices.

This would be particularly helpful for SMEs and business-to-business or B2B companies in Singapore, as these often store data in an unstructured way, using folders in an ad hoc fashion. As such, if a data breach were to happen, the data review process could be particularly complex, time-consuming and costly for them. Thank you.

Mr Deputy Speaker: Alright. Mr Patrick Tay.

4.45 pm

Mr Patrick Tay Teck Guan (Pioneer): Mr Deputy Speaker, Sir, I declare my interest as a member of the Data Protection Advisory Committee of the Personal Data Protection Commission (PDPC).

I rise in support of this Bill, which seeks to achieve the twin objectives of strengthening consumer confidence that their personal data will be used responsibly; and enabling organisations to confidently harness personal data for innovation which, in turn, would benefit our citizens and Singapore's economy. It has been eight years since the PDPA was enacted in 2012. The objective then was to provide a baseline standard for data protection in the private sector.

This Bill seeks to introduce, inter alia, the concept of organisational accountability, mandatory data breach reporting to the PDPC, new requirements for organisations to conduct risk assessments, a new data portability obligation to enhance consumer autonomy, a higher financial penalty cap, enhanced enforcement of the Do Not Call provisions and new exceptions and definitions of consent to facilitate the use and movement of data by organisations.

Undeniably, there will be some who will question the timing and impact of these proposed amendments. After all, we are only starting to see the effects of the COVID-19 pandemic unravelling and facing a probable imminent global recession. These amendments will necessitate changes in an

organisation’s policies, systems and processes. With organisations already trying to cope with stretched resources and trying to avoid going belly-up, measures, such as stiffer fines for data breaches or making it mandatory for organisations to notify the PDPC, may seem counterproductive. Nevertheless, I support the proposed amendments for the following reasons.

These long-contemplated amendments are vital and tabled none too soon. As we have read in the news, e-commerce and tech companies are looking to expand or invest in Singapore, using Singapore as a launchpad for expansion, not only into the ASEAN region but globally as well. Singapore has hereinafter taken steps to establish and position itself as a data hub. There is, therefore, no better time than the present to refine our data protection regulations as we continue in our race to lead in a data-driven economy.

We must recognise and seize these opportunities to ride the tech wave. Speaking also as the Assistant Secretary-General of NTUC, the creation of job opportunities and the sharpening of Singapore’s innovation capability, without question, would, and can only, be advantageous to our workers in this current economic climate. The refinement of our data protection framework and policies that support the growth of our digital economy is an essential element in our nation's overall blueprint for the future and for continued growth. With our infrastructure and links to the region and the world, we are in a good position to ride the tech wave and to continue tapping and building on our potential and strengths.

Furthermore, data protection laws are still in an early evolutionary stage globally. These proposed amendments seek to bring our data protection laws in greater alignment with the global standard. Indeed, our aspiration is not just to keep up with the data protection regulations like the GDPR. We have more than a fighting chance of becoming one of the leading authorities in data protection in the region and in the world.

At the same time, consumers are increasingly aware and concerned about the way their personal data is being collected, used and shared. They demand for convenience, speed, personalised user experience, flexibility and, at the same time, greater confidence and assurance in the way their personal data is safeguarded and used. I hope this set of changes will let consumers be assured in this respect. This is especially important, in light of the recent compromise of 1.1 million user accounts of RedMart, Lazada's online grocery store and other e-commerce platforms.

Firstly, the framework for the collection, use and disclosure of personal data will be updated to enable consent to be sought when meaningful and necessary. Where consent is not sought, safeguards will be put in place for organisations to be held accountable for their practices. For example, with the introduction of the notification with opt-out option, organisations will be able to obtain meaningful consent from consumers and use this data in new ways. However, organisations must first ascertain that there is no adverse effect on the individual before obtaining consent in this manner.

Even as businesses are given more scope to leverage data, consumers will still have flexibility and the ability to opt out if and when they so choose. Express consent will still be required for organisations to send direct marketing messages and updates to the Spam Control Act and Do Not Call or DNC provisions will allow consumers greater protection from unwanted communications across all direct communication platforms, that is, voice calls, SMSes, instant messaging and emails. At the same time, with the new Data

Portability obligation, consumers no longer need to worry about being locked-in to a single service provider and can easily switch to new services.

For businesses concerned with the increase in the limits of financial penalties, I think there is no cause for alarm, as this is targeted towards irresponsible organisations in the most serious cases. Similarly, the introduction of new offences is only intended for individuals who egregiously mishandle personal data and not where employees are acting within the scope of their employment, or for data professionals, cybersecurity specialists, artificial intelligence engineers or researchers carrying out legitimate activities.

While I am supportive of the amendments to this Bill, I would be grateful if the Minister could address the following concerns.

First, the costs and investment in complying with the new data portability obligation may be significant. Will organisations, especially SMEs, receive any assistance in this regard? Can the Minister share how MCI or PDPC plans to help reduce the compliance burden on organisations?

Second, the proposed amendments seek to remove the exclusion for organisations acting on behalf of public agencies from compliance with the PDPA obligations. Can the Minister elaborate on the impact of this amendment and how organisations, acting as the data intermediaries of public agencies, can be accorded protection in the performance of their tasks? Can such organisations reasonably comply with their obligations under the PDPA, given that public agencies, that, the principal, are not subject to the provisions of the PDPA?

Third, the proposed criminal offences against individuals for the mishandling of personal data have been drafted rather widely. Would the Minister provide some guidance on when and how these provisions would apply?

Sir, clarifications notwithstanding, I stand in support of this Bill.

4.54 pm

Mr Louis Ng Kok Kwang (Nee Soon): Sir, since we passed the Personal Data Protection Act in 2012, the Personal Data Protection Commission has been busy. It has investigated numerous data breaches and received a record-breaking 4,500 complaints last year. Data protection has become only more concerning and this Bill helps address those concerns.

I am heartened by the amendments requiring organisations to inform people who are affected by data breaches and to help people port their data to other services. These changes will help Singaporeans feel a greater sense of control over their data. Many will welcome these enhancements. That said, I have three points of clarification on this Bill.

My first point is on data breaches. The Bill introduces a requirement for organisations to notify the Commission and affected individuals in certain instances where there is a data breach. One instance is when the data breach results in, or is likely to result in, significant harm to an affected individual. I understand the Commission intends to prescribe classes of personal data considered likely to result in significant harm to individuals. Beyond this, can Minister clarify what other circumstances will be

prescribed to help organisations assess whether a data breach may lead to “significant harm” to affected individuals under section 26B?

Further, can Minister clarify what standard the Commission will apply when it reviews an organisation’s assessment on whether a data breach is notifiable? An organisation may decide not to notify affected individuals of a data breach because they assess that there was no significant harm caused and the breach was not of a significant scale. If the Commissioner later disagrees with this assessment and reviews the organisation’s assessment, will the Commissioner do so by holding the organisation to the standard of a reasonable person? Can Minister also clarify whether the Commission will consider a good-faith, systematic assessment by an organisation as a mitigating factor in deciding whether and how much to penalise the organisation for failing to notify the Commission of a data breach?

My second point is on the definition of adverse effect. The Bill now allows organisations to avoid asking for consent in certain cases. In several cases, they have to assess whether their action will have an “adverse effect” on individuals. Under section 15A, organisations have to assess the extent of adverse effect to decide whether deemed consent by notification is sufficient consent. Under section 17, organisations have to weigh such adverse effects against the “legitimate interests” of the organisation or of other people.

Can Minister define what it means to impose an “adverse effect” on an individual and what are some examples of it? Such clarity is important because organisations will likely face practical challenges in identifying every possible adverse effect on an individual, and a wrong assessment may lead to harsher penalties for them.

In line with the Act’s shift to a risk-based accountability approach, I would also suggest applying a standard of reasonableness when determining whether organisations have fulfilled their obligations. In other words, they should be required to assess the “adverse effect” on an individual only to the standard of a reasonable person.

Finally, can Minister also clarify the intended differences between “significant harm” and “adverse effect” on individuals? It will help organisations comply with the new Act.

My third point is about data porting obligation. The Bill empowers individuals to make data porting requests. This means individuals can ask organisations to send their personal information to other organisations. Organisations can say no only under conditions outlined in the new Twelfth Schedule. Will the Commission be releasing guidelines and examples to help organisations understand whether each of the conditions applies to them? The guidelines should especially clarify three conditions.

First, these guidelines should clarify when the data would “reveal confidential commercial information” that could “harm the competitive position of the organisation”. I am sure many companies will be keen to cite this condition if they are asked to transfer data to a competitor.

Second, the guidelines should clarify when the data is “trivial”.

Third, the guidelines should clarify when the data porting request is “frivolous” or “vexatious”.

Data porting is a new concept to many organisations in Singapore. Organisations will benefit from greater clarity on what counts as trivial, frivolous or vexatious.

Sir, notwithstanding these clarifications, I stand in support of the Bill.

4.59 pm

Mr Yip Hon Weng (Yio Chu Kang): Mr Deputy Speaker, Sir, I rise to support the Bill. The Bill is a timely and necessary effort to strengthen personal data management. The pandemic has accelerated the need to go digital. This results in the sharing of personal data with businesses in exchange for their products and services. And unless the data is carefully protected, it will expose many people vulnerable to cybercrimes. According to a July CNBC report, large-scale data breaches have grown in intensity and frequency in 2020. The number of breaches rose by 273% in the first quarter, compared to the same period last year. This is largely attributed to more businesses being conducted online during the COVID period.

I appreciate the move to enhance the Do Not Call provisions. The popularity of instant messaging platforms like Whatsapp, Telegram and WeChat has surpassed that of SMSes. During lockdowns, these are the platforms that residents use to communicate with each other, especially between seniors and their families.

But many of these platforms have been abused to spread fake news, commit fraud and scams. They can even spread malicious links containing malware. We hear of scammers making phone calls supposedly representing MOH during this pandemic. Many seniors, including several from my constituency, have reported falling prey to scams and unsolicited advertisements. Many of these fraudulent messages are from overseas sources. And some phone numbers have been spoofed to conceal the perpetrator's actual number. As such, it is impossible to report them to the authorities, or to block them on your handphone. May I ask how would the Ministry help to safeguard our citizens against these perpetrators? If not, what can be done to safeguard the interests of phone users?

Despite success in the reduction of unsolicited marketing messages from commercial companies, users are at greater risk of more sinister problems. These include scams via robo-calls and text messages from unlicensed moneylenders and online gambling. The frequency of such messages has increased. The culprits prey on the vulnerable. They also exploit the desperation of victims during this challenging period.

I met Mdm K, a young professional, at my Meet the People Session, or MPS, last week, who fell victim to an online scam and was swindled of her $100,000 life-savings. She got a message from an overseas company offering her an investment proposal that promised her 20% annual returns. She did some simple checks on the company. After some brief interactions over email, she decided to wire across the money to the company. She has not heard from the company since. She went to file a police report. If someone like Mdm K can fall for such a scam, other residents like seniors are at an even higher risk.

The Government's amendments for the PDPA and Spam Control Act will only work on legitimate businesses. This case highlights that the Government today has no reach to those entities with criminal

intent and especially those that originate overseas. As such, consumers will need to exercise caution. And this may be an area where technology can provide a solution. Email spam filters is a good example. It works well for emails. We should encourage our entrepreneurs to think of similar solutions for phone and SMS apps.

Mr Deputy Speaker, Sir, the higher compliance required of businesses on data protection also leads to higher business costs. Several businesses are new to e-commerce. Many invested a large sum of money to pivot their businesses. For them, there is still a steep learning curve to scale. They have to now deal with this new enhanced responsibility. Undoubtedly this would be an added burden on their operations and finances. They may then pass on the additional costs to the consumers. Can the Minister share how can Government help them to meet the new requirements without imposing too much on these businesses' finances?

As regulations for companies to gain access and share data for innovation is relaxed, good data collection and protection practices will be increasingly pertinent. Big Data has been mostly lauded for its contribution to innovative product development and improved user experiences. But there are growing privacy concerns. Facebook's Cambridge Analytica data scandal was a wake-up call.

As such, the Government must invest in creating a strong eco-system that protects our data. The efforts must be transparently communicated to consumers to retain their faith in the system. We must be more discerning of the types of information that can be collected and shared, with or without consent. For instance, it is a common marketing practice to entice consumers to sign up for a promotion or a freebie. They provide highly personal information in return. And consumers are required to mark a little box at the end of the form, giving consent to use the data for marketing purposes. It is well and easy to say, if you don't feel comfortable handing over your information, you don't have to. No one is forcing you to sign up. But these marketing techniques leverage a common human weakness. And this is the inclination to act on a good deal. And at that moment, sharing one's personal information may seem of little consequence until a data breach happens. Many Members today have highighted the data breaches at Lazada and Eatigo, affecting millions of accounts. It is therefore critical, as part of measures to enhance data protection, that we do more to prevent the indiscriminate collection of highly personal data.

That said, Mr Deputy Speaker, Sir, I support the use of consumer data to spur innovation. The development of more exciting, relevant products and services will open up new business opportunities and new markets. This also translates into jobs for Singaporeans.

Mr Deputy Speaker, Sir, to quote Bill Gates, "Power comes not from knowledge kept, but from knowledge shared". In conclusion, I believe an enhanced eco-system of data sharing for spurring innovation will give rise to some powerful and exciting developments that are unique to Singapore. I support the Bill.

Mr Deputy Speaker: Mr Sharael Taha.

5.06 pm

Mr Sharael Taha (Pasir Ris-Punggol): Mr Deputy Speaker, Sir, the rapid advancements made in technology over the past decade has drastically changed our digital landscape as well as our economy. The pandemic has also highlighted the critical need for digitalisation at the personal, as well as organisational level. We have done well to keep abreast with this development.

However, if Singapore wants to keep its leading position in the international digital economy, we must recognise the key role that data privacy plays in the digital economy.

Currently, knowingly or unknowingly, personal data is already being shared and traded. When consumers share personal data, there must be robust safeguards to protect their privacy so that we can increase trust and level of participation by one and all in the digital economy.

We must at the same time be mindful that as an innovation hub, businesses and organisations must be able to harness data confidently in their search for creative solutions and ways to improve consumers' experiences, products and services.

In order to enhance the protection of consumer data, we must support increased accountability by organisations and businesses. There was no legal requirement or compulsion to inform the consumer of information breaches. To use the recent Lazada data breach of 1.1 million users and the Eatigo data breach of 2.8 million users as an example, we have a sense of how massive and widespread such breaches can be. Lazada has been forthcoming in this instance and had actively monitored their data security systems, while Eatigo was able to detect the breach after it's users' data was put on sale online.

This should convince us that we cannot leave consumer data security to chance, hoping that businesses and organisations will act in an ethical manner whenever information breaches happen. With the amendments, when there is a breach of significant scale or may cause harm to the individual, there is a framework for these businesses and organisations to assess if both the Commission and the individuals concerned must be informed. This strengthens the confidence of consumers in the organisation's ability to protect their privacy.

Consequently, affected parties can take simple measures like changing their passwords to afford immediate protection to their data. However, we all agree that any data breach is unacceptable and as such, stiff financial penalties is needed to deter poor handling of data security.

Data portability would benefit both consumers and businesses. Ease and security of data portability provides consumer autonomy over their personal data, and plausibly, increase the consumer participation rate in the digital economy. At the same time, it can provide access to data for businesses to better serve their customers' needs or to provide innovative solutions for their clients.

However, how do we prevent companies from exploiting this ease of portability to manipulate customers and shape their behaviour? How can we protect consumers from exploitative and manipulative marketing techniques once businesses get a hold of consumer data? Do less tech-savvy customers, such as our senior citizens and other vulnerable groups understand the implications when they consent to port their data over? At which point does using portable data for highly personalised service becomes exploitation for profit-making purposes, especially if it is used to exploit an individual's pre-existing condition such as compulsive buying disorder? What if a customer just wants part of his data to be

ported? These are important questions we need to answer to assure the public that their privacy is protected.

To illustrate these concerns, take for example a vulnerable consumer giving consent or is perceived to have provided deemed consent to an e-commerce site to port his data. The e-commerce vendor proceeds to use it and may even proliferate the data indiscriminately, and he falls prey to questionable marketing techniques. How do we protect the vulnerable who are less digitally savvy?

I think we can all agree that spam marketing messages in the form of voice calls, text and fax messages are a nuisance and not to mention highly intrusive. Thus, I am supportive of such Do Not Call provisions or DNC under the PDPA. The DNC already prohibits businesses and organisations from sending Instant Messages or IMs, SMS and so on, to Singapore-based telephone numbers which have been registered with the DNC registry.

However, considering that the digital economy is global in nature and is not bounded by the jurisdiction of nation-state borders, how do we enforce these DNC provisions to overseas companies? Are there even ways to minimise the ability of overseas businesses from spamming our consumers? Conversely, how do we ensure that Singapore registered businesses and organisations handle their data ethically when they port them over to overseas vendors and partners? What safeguards do we have to ensure that the data is not proliferated and subsequently manipulated for commercial gains from overseas?

Increasingly, there is the necessity in providing disclosure of personal and even organisational data by a business to its partners or contractors in order to assess and review contractual performance. This may result in multiple layers of outsourcing. Businesses and organisations can then use this disclosed data for their own purposes. However, when businesses and organisations require such data, there should be pre-arranged stipulations such that there is either a time-bound or scope-bound condition in order for the disclosed data to not be traded or sold to other organisations. This would go towards making data disclosure more secure and again, increase participation in the digital economy. It also avoids the situation where disclosed data is knowingly or unknowingly used by other organisations for their own purposes other than that which was agreed upon by the initial contractual obligation.

In addition, if a Singapore-based company then discloses data to its overseas vendors, how do we then ensure that the overseas vendor do not use the data beyond the scope of the original intent, especially when we are then unable to hold them accountable?

In conclusion, with the amendments, we are arguably in a much better off position than we were previously. There is a measure of increased protection for the consumers, as well as more punitive consequences for businesses and organisations who have not taken adequate safety precautions when using data that is made available to them.

To enhance the amendments to the Bill further, I propose considering the following.

One, more must be done to educate the vulnerable so they are aware of what they are consenting to. This would help ensure that all are protected and not unfairly taken advantage of.

Two, guidelines are also to be drawn up to help ensure the ethical use of data. These guidelines should be based on ethical considerations and not on commercial or profit interests of businesses and organisations.

Three, digital literacy programmes for youths should include the awareness of personal data protection, as well as ethical considerations. Our youths are entering a world where the digital landscape is ever evolving. We will have to depend on them to define how data is being used ethically.

Four, potentially, an accreditation system can be used, to give consumers some assurance that their data is secure when dealing with companies that meet, or even surpass, standards, and also to forewarn them to exercise caution when dealing with companies that do not meet these stipulated standards.

And finally, fifth in the absence of the possibility for enforcement, we need to explore ways to protect consumer data from being used or proliferated by foreign companies and businesses.

Mr Deputy Speaker, Sir, may I continue my speech in Malay, please.

(*In Malay*)*:* [*Please refer to* ***Vernacular Speech***.] With this amendment, we are protecting consumer data security in addition to ensuring that businesses and organisations act more responsibly when using data. This amendment will hopefully increase consumer trust and level of participation in the ever-evolving digital economy. There are measures to increase protection for the consumers as well as more punitive consequences for businesses and organisations who have not taken adequate safety precautions when using the data that is made available to them. However, I would like to suggest the following.

First, we must enhance awareness and educate those who are less digitally capable within our community so that they can be aware of what they are consenting to. This will help ensure that they are protected against those who try to take advantage of them.

Second, guidelines must also be drawn up to help ensure ethical use of data by businesses and organisations.

Third, we also need to educate our youths with literacy programmes that include awareness of personal data protection as well as ethical considerations in a digital economy. Our youths are entering a world where the digital landscape is constantly evolving. They must be strengthened with positive values. We have to depend on them to define how data is used ethically in the future.

Finally, we must also have an accreditation system to give assurance to consumers that their data is safe when they transact with companies that meet the standards, as well as forewarn them to exercise caution when dealing with companies that do not meet the stipulated standards.

Given that Singapore is at the forefront of data privacy laws, especially in this region, we need to have a level playing field between Singapore companies and foreign companies. We should not stifle innovation too much but we must do our best to protect consumers from manipulative and exploitative practices. We must give consumers the choice and control over their personal data and how it is used.

As consumers and business owners, we must bear the responsibility and further strengthen our understanding of data usage and data privacy, and we must continue to use data to drive innovation in

order to transform our economy.

(In English): In summary, Mr Deputy Speaker, Sir, given that Singapore is at the forefront on data privacy laws especially in our immediate region, we need a level playing field between Singapore companies and foreign companies. We cannot be overly restrictive but we must still do our utmost to protect our consumers from intrusive, manipulative and exploitative practices. We need to give consumers the choice and control over their personal data and how it is used. With that, Mr Deputy Speaker, Sir, clarifications notwithstanding, I stand in support of the Bill.

5.17 pm

Mr Melvin Yong Yik Chye (Radin Mas): Mr Deputy Speaker, Sir, I stand in support of the Bill, which seeks to strengthen the accountability of organisations when handling and protecting personal data and to provide individuals with greater autonomy over their personal data.

Mr Deputy Speaker, despite the introduction of the PDPA in 2012 some eight years ago, we continue to see worrying lapses and breaches of personal data by commercial entities. Recent examples include: (a) a data breach by Grab, where the details of over 21,000 GrabHitch drivers and passengers were leaked due to an update of the mobile app; (b) a marketing email sent out by electronics retailer, Courts unwittingly exposed the personal data of over 76,000 customers, and (c) even the Central Depository, whose staff had mailed dividend cheques to outdated addresses, putting at risk the personal data of over 200 account holders.

Given the potential severity of these continued breaches, I am supportive of the Bill's proposed increase in financial penalties, from the current cap of $1 million to 10% of the organisation's gross annual turnover. Creating a strict data protection regime and strengthening our enforcement will also be vital in boosting Singapore's position as the region's premier data hub.

However, going back to the data breach by Grab that I mentioned earlier, I note that this was Grab's fourth instance in two years, where the company was in breach of the PDPA, and in this latest case, the company was given a fine of $10,000. Some would see this as a small amount for such a large company. I would like to ask what was the largest penalty that the PDPC had imposed on an organisation for a data breach under the current regime. I would also like to know if the PDPC intends to punish repeat offenders more severely, as repeated offences simply go to show that the organisation has not implemented the necessary safeguards to properly protect personal data, despite previous reported lapses.

Mr Deputy Speaker, I am also supportive of the Bill's proposal to further tighten the rules around telemarketing and unsolicited spam calls and text messages. Many residents have told me that they continue to receive spam calls and text messages related to online gambling and unlicensed moneylending, despite having registered their phone numbers in the Do-Not-Call or DNC registry. This makes them question what was the point of registering their numbers in the DNC registry in the first place. I therefore support the proposed enhancements to the Spam Control Act 2007 and the DNC provisions, which will serve to provide consumers with more protection from unwanted communications across various platforms.

Despite the enhancements, we need to recognise that many spam text messages and calls originate from scammers or unlicensed moneylenders based overseas. I hope that the Ministry could work with our telcos to explore the use of technology to prevent such unsolicited messages, which often contain malware links, as well as spam robo-calls.

In the United States, their mobile and broadband providers have worked with the government to create a new protocol called STIR/SHAKEN, which provides a secure mechanism for service providers to cryptographically sign and verify the Caller ID for calls made over the Internet. This has seemingly helped to combat Caller ID spoofing. Could the Ministry explore implementing similar technology here?

Mr Deputy Speaker, as we debate about the importance of securing the personal data by organisations, the reality is that individuals too have a part to play in ensuring that their personal data is safeguarded. Consumers need to be personal-data-literate and understand what they are consenting to when they tick off the checkboxes under a company's User Agreement. Often, many consumers do not fully read the terms and conditions, as they are written in small font sizes and clauses are often hidden behind many technical jargons. Hence, many simply just check the accept button, not knowing that they would then unwittingly give up their personal data, sometimes in perpetuity, to these commercial entities. We therefore need to educate consumers about personal data literacy, even as the PDPC works to ensure that businesses safeguard data responsibly.

I would also like to urge the PDPC to publish guidelines on how companies should highlight their key User Agreement terms and conditions in a simple and upfront manner, preferably in large font size, and make clear to consumers about the categories of personal data that these companies will collect and how they intend to use them.

Finally, Mr Deputy Speaker, while I am generally supportive of the Bill's proposed amendments, I am, however, concerned about the timing of Bill and its impact to businesses. The proposed amendments to the PDPA are significant and it is likely that many organisations will incur additional costs in adapting to these new regulations. For example, companies will have to undertake an extensive review of their data protection procedures to ensure that they meet the Bill's expanded scope of "deemed consent", as well as ensure that their current systems are able to comply with the new data portability obligation.

Many businesses are already reeling from the impact of COVID-19 and they are worried about the cost of adhering to the revised regime. To alleviate these concerns, will the Ministry consider providing some form of assistance to these organisations, especially our SMEs or consider perhaps a grace period for the new regulations, so that companies have a longer runway to plan for their organisation's compliance to the latest PDPA rules?

Mr Deputy Speaker, the proposed amendments to the PDPA are timely as we seek to transform our economy for the post-COVID-19 future. However, I do think that we need to mete out more deterrent penalties to organisations that continually fail to safeguard the personal data of consumers, as having a stringent data protection policy is important to further strengthen Singapore's position as the region's leading data hub. We also need to focus on educating Singaporeans about personal data literacy, as more organisations seek to collect and monetise our personal data. With that, I support the Bill.

5.25 pm

Mr Desmond Choo (Tampines): Mr Deputy Speaker, Sir, I stand in support of the Bill. Personal data protection is essential for today's increasingly data-driven economy to function effectively. Without adequate safeguards regulating the usage and protection of data, consumers' confidence can be eroded, making it difficult for legitimate companies and entities to operate optimally. Like what the hon Mr Sharael Taha had said, Lazada's recent data breach affecting 1.1 million users or approximately one-fifth the population of Singapore is a timely reminder.

The amendments bring Singapore's data protection regime a step closer to the European Union's General Data Protection Regulation or GDPR. The latter has been internationally regarded as the gold standard for the protection of consumer data.

Notwithstanding the expanded responsibility of organisations under the amendments, I am glad to know that many of the businesses consulted welcome the amendments. This demonstrates their cognisance of the value of a robust data privacy regime, especially with the rise of malicious cyber-actors.

I believe that the amendments have tried to carefully balance the interests of both consumers and businesses. Individuals will have greater control over their data with, for example, the new data portability obligation and the tighter rules on telemarketing with the enhanced DNC provisions. Furthermore, the strengthened penalty regime under the amendments will drive an appropriate investment by companies into data protection and compliance efforts. At the same time, sufficient flexibility is provided through the exceptions to consent provisions to meet commercial needs.

Mr Deputy Speaker, Sir, I seek a few clarifications and will make a few suggestions on the amendments for the Ministry's consideration.

Firstly, I seek clarification on the legitimate interest exception to consent. Per Part 3, section 1(2)(a), the legitimate interest is viewed from an organisation's perspective. This inadvertently encompasses a subjective determination on the part of the organisation in assessing whether their legitimate interests outweigh potential adverse effects on an individual. While section 2 to 10 provides some circumstances whereby the collection, use or disclosure of personal data is necessary, these circumstances may be limited in scope, except for section 2 where the meaning of "evaluative purposes" is seemingly ambiguous. As such, I seek the Ministry's direction to provide guidance on what constitutes "evaluative purposes".

Furthermore, to minimise disputes, perhaps the Ministry may consider looking into prescribing broader, objective guidelines on what constitutes legitimate interests to firstly, ensure greater ease of compliance for organisations who seek to rely on this exception and secondly, enhance consumers' understanding of their rights. Lastly, considering that the collection, usage and disclosure of personal data are central to the business models of data collection and survey companies, I would like to clarify with the Ministry if the availability of this exception should similarly apply to such companies.

My second clarification relates to the new Data Portability Obligation. This is a important advancement in Singapore's data privacy regime, allowing individuals to regain more control over their data. However,

my concern with this obligation lies within its potential impact on businesses costs and operations. Some businesses consulted have cited significant compliance costs, efforts and manpower requirements in meeting these new regulations. This includes tailoring current processes for larger businesses and the construction of new technological structures for smaller businesses. With the global economy experiencing a hard hit from the COVID-19 pandemic, many SMEs are already struggling to stay afloat. In light of this, I have three suggestions to make.

Firstly, could the Ministry consider a transitionary period in relation to the data portability obligation especially for the SMEs? This would help businesses to tide through the COVID-19 crisis and provide an appropriate duration of time to comply with this new obligation.

Secondly, I am concerned about the hardship SMEs and smaller businesses may face in adhering to this obligation. Could the Government support SMEs in setting up basic technological structures to do so? Perhaps the Government can work with unions and trade associations or TACs, for these support platforms to help smaller businesses comply with the new obligations imposed. The unions and TACs can also update businesses, train them, especially SMEs, on the revised amendments. NTUC's Learning Hub currently conducts data-protection related courses and the scope of courses can be expanded to complement the amendments made to the Act.

In addition, section 26H affords consumers the avenue to apply to the Commission to review a porting organisation's failure to transmit the applicable data within a reasonable period of time. Instead of a subjective measure of time, could the Ministry prescribe a stipulated duration of time to fulfil the porting request, with the subjectively determined "reasonable time" only applying in situations where businesses require more than the stipulated time to do so? This would better help businesses and consumers manage their duties and expectations respectively, reducing unmeritorious complaints to the Commission.

My third point of clarification relates to the increased financial penalties under the amendments. The maximum financial penalty that can be meted out is a fine amounting to 10% of the defaulting organisation's annual turnover in Singapore. For comparison, the contravention of Personal Data Laws in Hong Kong attracts a maximum financial penalty of HKD$1 million; in Malaysiam it is RM$300,000 and in the Philippines, it is PHP$5 million.

The worry, which has been similarly reflected during the public consultation, is that the maximum fine that can be imposed might be too large compared to worldwide standards, especially in Asia. Could this disadvantage Singapore as an offshore destination, where MNCs might choose other Asian countries over ours to set up operations? While the penalty imposed on a contravening organisation will vary naturally according to the facts, this might artificially create the impression that the financial penalties under Singapore's data privacy regime are much harsher compared to those of its neighbours. In light of this, can the Ministry reconsider the maximum financial penalty that it is imposing on defaulting organisations to better align with the standards in neighbouring Asian jurisdictions or competing economies?

Lastly, I propose an explicit recognition of the right for individuals to the erasure of their personal data, for the consideration of the Ministry. The right to erasure is recognised in other jurisdictions, such as the

EU's GDPR. Article 17 of the GDPR affords individuals the right to obtain from data controllers the erasure of personal data and the obligation on controllers to erase the concerned data without undue delay under certain circumstances. For example, where the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.

Similarly, under section 25 of the PDPA, the retention limit obligation is imposed on organisations. Under this, organisations shall cease to retain personal data where the purpose for which that data was collected for is no longer served by the retention of personal data and where the retention is no longer necessary for legal or business right.

This obligation seems to complement an individual's right to withdraw consent in section 16. However, while consumers can withdraw consent of the use, collection and disclosure of their data, with organisations thereafter obligated to cease to do so, this does not squarely extend to the right of consumers to direct organisations to erase their data. In furtherance of the amendments' overall objectives, the imposition of this provision assigning an individual the explicit right of erasure is arguably another step ahead to afford greater autonomy to individuals over their personal data. The viability of such a provision is, of course, subject to the further perusal of the Ministry, especially with regard to under what circumstances may such a right be circumscribed or exercised.

Mr Deputy Speaker, Sir, notwithstanding my clarifications and suggestions, I reiterate my support for the Bill. I am confident that by passing the Bill, the House would be taking a big step ahead in priming Singapore in our shift to a data-driven economy.

Mr Deputy Speaker: Senior Minister of State Janil Puthucheary.

5.34 pm

The Senior Minister of State for Communications and Information (Dr Janil Puthucheary): Mr Deputy Speaker, Sir, Mr Gerald Giam has brought up several matters associated with the public sector governance of data and data privacy, data security. I thought I might deal with some of them although they are not directly connected with the Personal Data Protection (Amendment) Bill which we are debating today.

There are some matters of confusion, conflation and, perhaps, a misunderstanding, and I hope I can bring some clarity and understanding to the debate.

The first point I would like to clarify is Mr Giam's assertion that somehow the Government believes that the standards for Government need to be lower than for the private sector. We completely disagree. We believe the standards for the Government should be as high, if not, higher than for the private sector. That is why, several years ago, when there was a Government data security policy in IM8 and there was not something for the private sector, we enacted the PDPA to improve standards for the private sector.

Mr Giam also suggests that, perhaps, we should treat Government and treat businesses the same way, that the same tools and the same behaviours would either be useful or expected in the private realm and the public sector. This is not so. We expect Government to behave as one service, servicing residents, servicing our citizens, servicing our country as one entity. We expect the private sector to

behave as individual entities and there needs to be an appropriate separation and gap in data sharing between private entities.

We have, in Mr Giam's assertions, another confusion. He talked at the beginning of a high compliance burden for public sector officers and then asked later on whether the standards are high enough. The high compliance burden is precisely because the standards are high and, perhaps, more burdensome than for the private sector. Nevertheless, there is internal coherence despite the many different Acts and rules and laws that he cited, which are correct.

Internally, within the Government, the data security and data privacy space is looked after by the Government Data Office, a single point of contact. There is internal coherence, so that we can operate as one Government. Externally, for members of the public that are concerned about their data security, they also have one point of contact – the Government Data Security Contact Centre or GDSCC. That was established and launched publicly on 30 April this year. Members of the public can contact that single point of contact if they are concerned. But if they contact any other arm or organisation within Government, we have our Government working as one through a No Wrong Door policy. And that is enabled precisely because there is sharing of data across Government.

Nevertheless, whoever they contact, they will be referred to the Government Data Office and GovTech to handle the matter.

On the issue of our Government data policy lacking transparency – Mr Giam referred to it; it is IM8 – the Government's personal data policies were published on 30 April this year. It is available on the Smart Nation website and it is there for scrutiny and for examination. And we can debate and discuss this further if he wishes.

Another point of conflation and confusion that I would like to clarify, the monetary fines that are in the PDPA are fines; they are not redress to the individual. They are fines imposed by the regulator on the private sector entity. There is no specific provision for compensation to the individual as a result. The individual would need to pursue legal action if they were looking for compensation.

Mr Giam suggested that there needed to be some corollary of compensation within the public sector for these fines that the PDPA imposes, should there be a data breach. I just want to be clear that the fines are fines from the regulator and if in the private domain, an individual wishes to pursue compensation, they would have to take legal action in order to do so.

For the Government, there is no special provision or exception or protection for the conduct of the Government or Government officers with respect to data; there is no special carve-out there.

So, let me be clear. The PDPA and the PSGA – the IM8 provisions that Mr Giam referred to – are aligned in terms of standards, the expected behaviour of the officers and entities. And they are aligned where there is a single point for people to complain: the PDPC versus the GDSCC. There is an option for individuals to pursue mediation and an option for individuals to pursue action for compensation.

One of the key other points of confusion I want to address is this idea that the PDPA is equivalent to the PSGA or the Public Sector (Governance) Act, when taken together with a whole series of other laws

such as the Official Secrets Act, the Income Tax Act, the Statistics Act. This is not so.

The controls are equivalent between the PDPA and the PSGA. These other laws are then on top of the PSGA, governing and controlling behaviour within specific domains. They also apply to the private sector; for example, the Income Tax Act will apply to certain private sector entities as well. So, the equivalence is between the PSGA and the PDPA.

The key issue is then how do we want Government to behave and how do we want our private sector entities to behave. What we want within Government is for sharing of data to achieve that No Wrong Door, One Government responsiveness to citizens, for policy, for execution and implementation as well as for communications. For that, we need to encourage sharing of data. And because Government has roles that do not exist in the private sector, there are additional controls, because of the additional sensitive data that Government has access to. And hence we take this very, very seriously. How seriously do we take it? We prosecute and I give you three examples.

In April this year, we had a civil servant arrested as a result of leaking COVID-19 case numbers, for accessing a Government COVID-19 database without authorisation to retrieve confidential records and giving that information to a friend. This person was arrested as a result.

Another example also in April. A public servant and her husband arrested for wrongful communication of information, which was about the implementation of home-based learning by schools.

And in December 2017, an HDB officer was fined $2,000 for giving confidential information on HDB resale transaction time and changes to the valuation process to a Straits Times journalist.

We take this very, very seriously and the public sector officers who handle our data, on behalf of our citizens, know that we take this very, very seriously.

The separation of the public and private sector data protection regimes in Singapore remains relevant. It remains necessary for us to keep achieving the outcomes that we want to achieve in terms of good policy, responsiveness to citizens, operating as One Government. It has to be used in a way that drives trust and helps us be effective in maintaining that trust with our citizens.

Nevertheless, we always review these provisions. As we are reviewing the PDPA today, we will regularly review the PSGA as well as other legislation to ensure that they remain relevant and effective in safeguarding personal data for both the public and private sectors.

Mr Deputy Speaker: Mr Gerald Giam, you have a clarification?

5.43 pm

Mr Gerald Giam Yean Song: Thank you, Mr Deputy Speaker. I just want to clarify with the Senior Minister of State that I did not say that the standards for Government should not be higher. In fact, I agree with the Senior Minister of State that the Government standards should be the same or higher than what it expects of the private sector.

In fact, I support the No Wrong Door policy. With regard to data sharing between agencies, I think that is a good thing and it is important for the convenience for our residents. But this provision can also be made within the PDPA, so that Government agencies are allowed to share data between each other. So, why can the myriad of legislation not be brought under the PDPA, so that Singaporeans, public sector officers, will be able to know that there is this harmonised set of data privacy standards that they should all comply with and that they are held to the same standard?

Now, let me first clarify again that I am not saying that currently the Government is operating at a lower standard. Like I said in my speech, in my experience as a civil servant and my experience working as a government vendor in the past, the standards are very high. So, why can these all not be harmonised under one law, just like how they do it in the GDPR for Europe?

Mr Deputy Speaker: Yes, Senior Minister of State Dr Janil, would you like to respond?

Dr Janil Puthucheary: Mr Deputy Speaker, I am glad that Mr Giam agrees largely with us. The issue then is what outcome would he achieve or would we achieve merely by putting it all under one legislation?

I doubt very much there is any confusion among the civil servants about the standards that are expected of them simply because we have two legislative frameworks. The issue is whether or not the outcomes in terms of the number of data breaches, the security that we have in our systems and the trust that our citizens have in our processes would be assisted by his approach, provided he continues to agree that we are effective at maintaining very high standards within the Government. The outcomes demonstrate that we are not doing too badly in our public sector.

The PDPC reports hacks and data breaches. I do not have all the numbers but I was looking at their website. For example, in 2018, in the private sector in Singapore, there were about 13 incidents of exfiltration of data through hacking and in 2019, it was 16 incidents. This is in the private sector. In comparison, in the public sector, we had three in 2018 and zero in 2019.

While hacking is not the only type of breach, we can also have, for example, an accidental loss, that is, inadvertent data breaches. On PDPC's website, in 2018, there were 2,700 instances in the private sector and 4,500 in 2019. I do not have the exact number, but I know it is at least one if not two orders of magnitude lower for the public sector. We do review them and we can happily get those numbers to Mr Gerald Giam and Members of this House. But it demonstrates that our system is not ineffective. People know that we have a robust protection regime as he has repeatedly said, that is, our citizens trust us to do the right thing and we must uphold those standards and have these high expectations of our public sector officers.

We are not alone in this world. There are other jurisdictions in countries, cities and states where they have different legislative frameworks for Government versus the private sector. It is not inherently a weakness. The issue is how you design both of those and whether you make it work for these outcomes. And let me say, categorically, the two are aligned to the same expectations and standards and we will refine them as needed to make sure that that is the case.

However, we believe that we need these two approaches because Government is not a private company nor should it behave as such and you cannot expect a private company to behave like

Government. Mr Gerald Giam goes on about the burdens that he felt as a civil servant. If the private SMEs had to comply with all the regulations that he had to struggle with as a civil servant, they would not be able to do business in quite the same way and perhaps innovation and the ease of customer relations, the ease of coming up with new products would be impeded.

So, there is a difference in behaviour at the entity level and there is a difference of behaviour at an individual level. And so, we have to have the right tools to influence behaviour correctly on behalf of our citizens. That does not mean that we reduce our standards in any way and we have not done so.

Mr Deputy Speaker: Minister S Iswaran.

5.48 pm

Mr S Iswaran: Thank you, Mr Deputy Speaker.

Let me start by thanking all 13 Members who have spoken and for their support for this Bill. To be precise, actually, 11 Members have given explicit support and Mr Leon Perera and Mr Louis Chua, I am assuming, I have their deemed consent since I do not think that there is adverse effect on any individual. I also want to thank them for raising important issues this Bill seeks to address. And I think the comments of Members fall broadly into a few areas about: protecting consumers' personal data, endowing consumers with more control and a greater sense of autonomy and confidence while supporting organisations' legitimate use; and supporting businesses in the use of data for growth and innovation.

I think in the comments that have been made by Members, it is clear that we all appreciate and recognise that there is an inherent tension between these objectives, and the proposed amendments seek to strike a judicious balance between them.

In thinking about these issues and I do propose to address the specific questions raised by Members, it is important that we first recognise that this is a delicate and dynamic balance. It is delicate because if we over-correct in one direction, consumers may not retain their confidence and trust in the system. If we swing the other way, then we shackle our businesses and the very benefits that we seek for our consumers and for our economy will diminish. It is dynamic because technology is changing and the ways data is being generated and being put to use are also changing. And therefore, it is imperative that we find our own balance in the way we regulate the collection and use of data in Singapore.

And there are different jurisdictions with different models. GDPR has been cited by several Members. There is also the APEC CBPR. I do not think any one of these is universally acclaimed because each has its strengths and its weaknesses. And that is why, in this endeavour of moving this legislative amendment, we have sought to understand the different regimes and to ensure that Singapore is able to remain best-in-class and also ensure that we are nimble and remain interoperable, which is key to our positioning as a node in the international flow of data and digital transactions.

And that leads me to the second overall point I want to make, which is we must recognise that whilst legislation and regulation is important, it is not a panacea and neither is it foolproof. And therefore, what it means is whilst we can put in place rules that will govern the data practices and ensure that data is safeguarded to the best of our ability, we cannot eliminate the risk of data breaches.

So, it is important that we recognise that whilst the rules must be formulated and enforced, it must be complemented by good practices and that has to evolve over time so that we understand, as an overall economic system and as a society, our respective responsibilities and roles.

And that brings me to my third overarching point, which is that it is essential that we recognise all of us have a role to play and a responsibility to discharge in maintaining the security and the usability of our data regime and, in a sense, safeguarding the public commons.

So, Government formulates the rules and regulations, enforces, provides guidelines and adapts to changing market situations to ensure that we remain abreast, to the best of our ability, of the developments and ensure that we keep Singapore relevant in the context of a new digital economy.

Businesses must recognise that this is in their self-interest. It is not just about complying with rules or regulations. At the end of the day, in any competitive domain, businesses will be able to differentiate themselves by their data policy and they will be able to signal the quality of the institution by the kind of approaches they take to safeguard their customers' data. So, they must be accountable and responsible, recognising ultimately that it is in their self-interest.

And finally, individuals. I think all of us have the responsibility. Whilst some Members have talked about the so-called power asymmetry, ultimately, I would argue that consumers – individuals like you and me – we are not powerless by any stretch of the imagination. We can choose to decide whom to do business with or whom to give our custom. We can choose to decide what data we want to share. We can choose to decide whether we want to give consent and when we want to withdraw that consent. And, ultimately, we can decide when to sever the relationship if that is what we want.

So, I think we should not lose sight of that aspect as well. Ultimately, the legislation must be seen in that perspective. It is one part of an overall architecture that will ensure a vibrant digital economy, but also one where data is respected, it is safeguarded, but also used for appropriate purposes.

Let me now turn to some of the specific questions that have been raised by Members.

First, on protecting consumers and the data. I think it is important to emphasise PDPA recognises organisations' need to use personal data for legitimate purposes. And today, that is accommodated through exceptions to the consent requirement, or as deemed consent. For all other purposes, organisations have to obtain consent from the individual.

Current exceptions to consent cater for scenarios such as investigations and responding to emergencies. We are updating this list by adding business improvement and legitimate interests and updating the research exception for the benefit of consumers and organisations in the digital economy.

The Bill is also clarifying the deemed consent provision to cover multiple layers of subcontracting when needed to fulfil a contract and to facilitate organisations notifying customers and giving a reasonable period to opt out, before they use data for new purposes. And I would like to reinforce this point and a point that Ms Jessica Tan had also picked up, that ultimately, consumers can opt out at any time and they have the freedom to do so.

I want to assure Mr Desmond Choo that all private sector organisations can rely on these new provisions, regardless of the industry they are in. It is meant to apply uniformly.

And on the whole, the amendments regularise current practices, provide organisations with clarity and confidence to use data, while protecting consumers' interests. As Mr Yip Hon Weng has noted, this will also enhance Singapore's status as an innovation and commercial hub.

Some Members have asked about the safeguards for the new provisions. Stricter process safeguards are prescribed for the general legitimate interests exception and deemed consent by notification, while specific exceptions, such as business improvement and research, are tightly scoped. The safeguards have been designed based on the following principles.

Before relying on the legitimate interests exception, organisations have to conduct a risk assessment and be satisfied that the overall benefit outweighs any residual adverse effect to an individual. And before relying on deemed consent by notification, organisations must conduct a risk assessment to be sure that there is not likely to be any adverse effect on an individual. Individuals may withdraw their consent even after the opt-out period. The PDPC may also require organisations to produce these assessments for its review. Some Members have asked how these provisions might be operationalised. The PDPC has provided guidance on how to conduct risk assessments. It will also issue detailed guidance on the legitimate interests exception and how to identify adverse effect, which generally refers to any physical harm, harassment, serious alarm or distress to an individual.

Exceptions for specific purposes, such as business improvement and research purposes, are tightly scoped. For example, the business improvement exception supports internal use of data within an organisation or a group of companies, with clearly defined limits. And when it comes to sending direct marketing messages, organisations still need to obtain express consent. Mr Sharael Taha enquired about the safeguards for deemed consent by contractual necessity. Essentially, organisations can rely on this provision to share personal data only to the extent necessary to perform their contracts with the individual. So, that is the test.

Mr Desmond Choo asked about the “evaluative purposes". This is actually an existing exception in the PDPA which has now been reclassified under the “legitimate interests exception”.

There has been another set of queries about how we can ensure or have confidence that organisations can be trusted to use personal data in good faith. I think this is an important point. I would start by saying firstly, we must recognise, more importantly, organisations must recognise that it is in their self-interest to safeguard personal data as that would foster consumer trust, strengthen their business reputation, and ultimately, their competitiveness and bottom line.

To support that and to ensure organisations take their obligations to protect data seriously, we are introducing both incentives and penalties – carrots and sticks, if you will. The PDPC will issue new advisory guidelines with examples and illustrations, so that organisations have ample notice of the expected standard of conduct.

As data breaches cannot always be prevented, the PDPC’s enforcement framework reinforces the importance of dealing expeditiously with data breaches to reduce harm, through measures like breach

reporting and statutory undertakings.

Last year, PDPC investigated 185 cases, issued 58 decisions and ordered 39 organisations to pay a total of $1.7 million in financial penalties and that includes the highest financial penalty sums the PDPC imposed in 2019, which were $750,000 and $250,000 on IHiS and SingHealth respctively.

The Bill enhances PDPC's investigation powers and raises the financial penalty cap, to improve the effectiveness of PDPC's enforcement.

We are also creating market incentives, which can motivate organisations to practise high standards of data protection.

I agree fully with Mr Sharael Taha on the value of certification systems and that is why PDPC launched the Data Protection Trust Mark or DPTM in 2019, to make it easier for consumers to recognise organisations with accountable practices and create the demand for good practices along the entire supply and delivery chain. Organisations with the trust mark require their suppliers and contractors to also adhere to the same standards. It has a very beneficial ripple effect. There are signs, based on PDPC's Perception and Awareness Study, that this is having a positive impact on the industry.

For secure exchanges of personal data with overseas entities, transferring organisations must put in place contractual arrangements or binding corporate rules, to ensure that receiving organisations provide a level of protection comparable to PDPA. Apart from contractual transfer mechanisms, the PDPC joined the APEC Cross Border Privacy Rules, or CBPR, and Privacy Rules for Processors systems. These are multilateral certifications which require participating businesses to implement data protection policies consistent with the APEC Privacy Framework.

Consumers also have a crucial role in safeguarding themselves. I think this is a point that I made earlier, and Mr Sharael Taha and Mr Melvin Yong have reinforced that.

That is why on the part of PDPC, it has reached out to almost 70,000 individuals, including youths, through school talks, exhibitions, community roadshows and events. I am also heartened that these efforts have yielded promising results with consumer awareness of the PDPA and PDPC increasing.

Mr Desmond Choo has proposed that a right of erasure be explicitly recognised. I believe Mr Louis Chua was also referring to this. Currently, section 16 of the PDPA provides for individuals to withdraw their consent at any time and the organisation would have to cease the collection, use or disclosure of the personal data unless otherwise required or authorised under any legislation. In addition, the PDPC can also direct an organisation to destroy personal data collected in contravention of the Act. So, we have the provisions. Whilst they are not identical to the right of erasure, I think they give a substantively similar effect.

On unsolicited messages, Mr Melvin Yong asked about our efforts to address spams and scams. In 2019, the PDPC received 2,255 complaints on unsolicited calls and text messages, and has taken action against 427 organisations. These actions range from issuing advisory notices and warnings, to prosecution in Court. The proposed amendments to the PDPA and Spam Control Act establish clear

guardrails for sending unsolicited commercial messages, to safeguard consumer interests while permitting legitimate direct marketing.

Ms Tin Pei Ling and others have asked about the change in enforcement regime for DNC complaints – why we moved towards a civil administrative regime. The answer is that the assessment we had is that this would allow for a more efficacious enforcement. DNC infringements typically stem from commercial motives. Hence, directions and financial penalties are more effective in addressing poor practices by depriving offenders of the financial or commercial gains that they seek. So, it is not a step down. I think it is a more effective way of dealing with this problem.

To Ms Joan Pereira's and Mr Sharael Taha's queries, our response to spam that originates overseas will continue to be multi-pronged, comprising a mix of public education, industry self-regulation and international collaboration.

Scams, on the other hand – the letter makes all the difference; scams versus spams – scams are serious crimes and they are dealt with by the Police. They are enforced under laws like the Moneylenders Act for unlicensed moneylending; and Penal Code, for example, for cheating offences.

For transnational scams, the Police collaborates closely with foreign law enforcement agencies to investigate and, where possible, cripple these syndicates. MCI is part of the Inter-Ministry Committee on Scams formed by MHA to combat scam messages and calls. As many of these scams originate overseas, we have to rely more heavily on technological solutions, as Mr Yip Hon Weng and Mr Melvin Yong have noted. For example, IMDA has required all telcos to implement the "+" prefix for all incoming overseas calls since April this year to help consumers better identify and reject spoof calls. Telcos are also blocking international incoming calls that resemble our Government agency or emergency numbers. So, these are efforts to help consumers discern and avoid being duped.

I would urge consumers to carefully look at the numbers when they receive calls from overseas because I think this is one way. We cannot prevent these calls from coming in but we can put up red flags, and this "+" sign and some of these other measures are for that purpose. We will continue to support the Police in their efforts to tackle scams and other illegal activities.

There have been questions on compliance costs and higher financial penalties.

I think many have asked about what support we are going to give to organisations and clarity for compliance with the new provisions. First, these amendments mark the culmination of a multi-year journey. So, we would like to ask organisations to see this as part of their own investment and effort in building customer trust and commercial reputation. Instead of conducting selective audits for the few as suggested by Ms Joan Pereira, the PDPC will continue to support organisations by providing guidance, training and access to expertise, and recognising accountable organisations, to inculcate good data protection practices as broadly as possible. Essentially, we think a comprehensive upstream approach may be more beneficial.

On guidance, PDPC provides accountability tools and resources, such as guides on implementing data protection management programmes, conducting risk assessments and adopting a data protection-by-design approach when developing IT systems.

On training, PDPC has been building up data protection capabilities through the Data Protection Competency Framework and Training Roadmap. Since its launch in July last year, more than 6,200 people have been trained. Data Protection Officers or DPOs, trained under this framework will be able to implement robust data protection practices as well as support innovation.

On access to expertise, we know and recognise that SMEs may need more help to comply with their data protection obligations. So, we have developed the Data Protection Starter Kit for them and Data Protection-as-a-Service as an affordable alternative for SMEs to outsource some DPO functions. PDPC also makes simple data protection solutions available on its website for free.

We launched the DPTM last year to recognise organisations with good data protection standards. And to-date, 37 organisations have already been recognised.

There are some concerns about the reasonableness of the increased financial penalty cap. Mr Desmond Choo proposed aligning the financial penalty cap with other Asian jurisdictions. The objective here is to ensure that we achieve the requisite deterrent effect on organisations. And that is why the financial penalties have been calibrated in the way that I have described. The proposed maximum financial penalty is comparable with other domestic legislation such as the Telecommunications Act and Competition Act and signals that data protection is of that level of importance in the digital economy.

Some have asked – I think Mr Patrick Tay was one of them – whether in light of the current circumstances we can exercise some flexibility in how these penalties and other elements are phased in. As I mentioned earlier, we intend for the revised financial penalty cap to take effect no earlier than one year after the Act comes into force, and the Minister has the discretion under the Act to review the effective date. So, we will be informed by the overall circumstances because we are conscious of not wanting to unduly burden our companies. The revised penalty cap will apply to breaches that occur after the effective date.

On compliance costs for the Data Portability Obligation, we want to make sure that the approach is balanced and achieves the intended results. So, to address the concerns over the scope of data that can or has to be portable, we have basically intend to help organisations with this new obligation, and introduce the data portability obligation in phases and will issue Regulations and advisory guidelines to provide clarity. This is new for Singapore. So, we want to make sure we do this in a measured way, clear about where we want to go – our destination – but prepared to be flexible in the path.

On Mr Sharael Taha's query on the safeguards for individuals, the regulations will prescribe consumer protection measures like cooling-off periods when porting certain types of data, in case consumers change their minds. To provide additional clarity on scope of implementation, we have also catered for the following:

(a) the scope has been narrowed to only cover individuals with whom the porting organisation has an existing and direct relationship;

(b) data portability will be scoped to user activity and user provided data in electronic form and will apply only to prescribed categories of data; and

(c) organisations are also not required to port data when the burden of porting, including the cost, is unreasonable.

Let me turn to mandatory data breach notification. In the Bill, “significant harm” refers to the impact of a data breach on affected individuals and is used in the context of a data breach notification. I think Mr Leon Perera, Mr Louis Ng and also Mr Shawn Huang had asked about this and I want to tell them that we plan to prescribe in the Regulations, a numerical threshold. This is something that has been developed through consultation and it is a numerical threshold of 500 individuals for what constitutes a data breach of a significant scale. This threshold is based on past enforcement cases and other jurisdictions’ practices as well.

The Regulations will also include categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to individuals, such as identity theft or fraud. One example of such data is full name and confidential financial information.

We will give more guidance through the Regulations but I want to stress – because I think the question was asked how we derived at these numbers. I do not think that there is any rocket science or magic behind it. This is an exercise in judgement, working with the industry and learning from our experience and past practices to arrive at what we think is a reasonable threshold. And I think what will then have to happen is, we see it in practice and learn from experience, and adapt as we go along.

I want to assure Mr Louis Ng that PDPC will take a reasonable approach in exercising its powers proportionately and judiciously. PDPC's decisions are also subject to appeal to the Data Protection Appeal Panel and further appeals can be pursued in the Courts. So, there is recourse but in the first instance, PDPC will exercise due care and proportionality.

Ms Pereira suggested that organisations notify the PDPC of all data breaches and she also advocated setting a fixed timeframe for notifications to individuals. Setting such a threshold for notification is important, but we have to take into account the compliance costs on organisations and also focus the effort on potentially systemic issues. We have not set a fixed timeframe for an organisation’s notification to affected individuals of a data breach because data breach circumstances can be very varied. Our positions have been developed in consultation with the public and benchmarked against jurisdictions like Australia, Canada, the EU and California. I will not rule out anything, but I think in the first instance we want to move forward and see how this works in practice.

There was a question of whether PDPC will exercise its expanded powers appropriately. The new section 48J details a list of factors that the PDPC will consider before imposing financial penalties. To Mr Melvin Yong’s query, this will include whether the organisation had previously failed to comply with the PDPA which can be considered as an aggravating factor.

Mr Patrick Tay has raised a very important question on individuals’ mishandling of personal data: how the new offences would apply for mishandling personal data?

We intend for this to apply only to egregious cases. Employees and service providers who are duly authorised should not have to be concerned. Additionally, we recognise that roles such as teaching and

research may require re-identification of anonymised data and hence we have provided for applicable defences for them in the Act.

We do not intend for these offences to apply in situations where the conduct is solely in the nature of a private dispute. For example, a relationship manager transfers his clients' personal data to his new company with their consent, or a sales agent contacts his clients after commencing new employment. In such cases where the individual reasonably believes that he has the legal right to use or disclose personal data, he has a defence to the new offences. Such private disputes should continue to be resolved through civil suits or other forms of dispute resolution.

To ensure that these actions are not caught, we have provided for defences under clauses 22 and 38.

Ms Jessica Tan can be assured also that we will further set out in Advisory Guidelines the examples on how the new offences would apply so that organisations and workers have clarity and can continue to use data confidently.

Mr Patrick Tay asked about the removal of the exclusion for agents of Government. This makes clear that the PDPA applies to all private sector organisations. Currently, the exclusion of agents of Government has created a situation where the Government can only hold them to account via contracts or laws such as the Official Secrets Act. This gap can undermine security as such agents of Government may handle large and sensitive volumes of personal data.

The removal of the exclusion for agents of Government would provide much-needed clarity and certainty that private sector organisations are subject to the same obligations under the PDPA regime, regardless of the sector their customers are in.

My colleague, Senior Minister of State Janil Puthucheary, has explained in detail our approach towards the data regimes in the public and private sectors, so I do not propose to repeat those, but Ms Tin Pei Ling has asked about whether the two regimes would be aligned.

We will continue to ensure alignment of data protection principles where the policy intent is the same. The amendments further strengthen this by aligning the penalties and scope of offences for individuals' egregious mishandling of personal data across the public and private sectors. In the same vein, the PDPC and the Smart Nation and Digital Government Office or SNDGO are working together to ensure the public sector data protection policies continue to be aligned with the relevant changes to the PDPA.

Deputy Speaker, Sir, I believe I have substantively dealt with the issues that have been raised by Members.

If I may conclude, since the PDPA was enacted eight years ago, we have made significant strides in the extent we use data to make decisions and deliver services. Businesses are employing more sophisticated measures to safeguard personal data. Consumers are also more aware of the importance of data protection.

We need to adapt to the new landscape where digitalisation has shaped our world, bringing new opportunities but also new risks. This Bill is an important step in this direction. It aims to promote strong data governance to enable greater use of data for the benefit of our society and our economy.

What we want is equal emphasis on protection and innovation, so that consumers benefit from data-driven services and solutions, with trust that their data is used responsibly. And businesses use data confidently with proper accountability. And Singapore continues to be an important node in global data flows. Mr Deputy Speaker, Sir, I beg to move.

Question put, and agreed to.

Bill accordingly read a Second time and committed to a Committee of the whole House.

The House immediately resolved itself into a Committee on the Bill. – [Mr S Iswaran].

Bill considered in Committee.

[Deputy Speaker (Mr Christopher de Souza) in the Chair]

Clauses 1 to 23 inclusive ordered to stand part of the Bill.

Clause 24 –

The Chairman: Clause 24. Minister for Communications and Information.

Mr S Iswaran: Mr Chairman, I beg to move the amendment* standing in my name, as indicated in the Order Paper Supplement.

*The amendment read as follows:

In page 54, line 20: to leave out "(6)" and insert "(5A)".

Amendment agreed to.

Clause 24, as amended, ordered to stand part of the Bill.

Clauses 25 to 46 inclusive ordered to stand part of the Bill.

Bill reported with amendment; read a Third time and passed.
