

## **Benefits of the Personal Data Protection (Amendment) Act 2020 to the Consumer\***

### **I. Introduction**

1. This article explains how the Personal Data Protection (Amendment) Act 2020<sup>1</sup> (the “Amendment”) benefits the user in three areas: customer experience, safeguards, and transparency. Firstly, the Amendment improves customer experience in two ways: (1) deemed consent by contractual necessity eliminates the hassle of clicking multiple checkboxes to express the user’s consent to the sharing of his personal data with sub-contractors;<sup>2</sup> (2) the amendment facilitates the transfer of user data from one platform to another, thereby ensuring a personalised experience for the consumer and spurring the development of novel services.<sup>3</sup> Secondly, users enjoy stronger safeguards from data breaches because data cannot be ported at the expense of the user, and the enhanced penalties encourage organisations to strengthen their internal governance to manage users’ personal data more safely.<sup>4</sup> Thirdly, users enjoy greater transparency because they will receive timely notifications about data breaches from businesses.<sup>5</sup>

### **II. Customer Experience**

#### **A. *Convenient transactions***

2. After the Amendment,<sup>6</sup> the user is deemed to have given his consent for the disclosure of personal data to third party organisations where it is reasonably necessary for the performance of a contract between the user and the organisation.<sup>7</sup> For example, an online shopper can now consent to the collection of his personal data by the online retailer once, avoiding the hassle of agreeing to multiple checkboxes to express his consent to the disclosure of his personal data to the retailer’s delivery and payment subcontractors.<sup>8</sup>

#### **B. *Data Porting***

3. By providing customers with the right to request for their data to be transmitted to another organisation, the data porting obligation improves customer experience by providing data to organisations to improve their goods and services and by spurring competition.<sup>9</sup> The amendments to the PDPA facilitates the porting of applicable data of individuals to organisations that have a commercial relationship with those individuals.<sup>10</sup> The applicable data typically relates to individuals’ user activity data or user-provided data.<sup>11</sup> Hence, by giving businesses access to such data, they would be able to tailor their goods and services to their

customers. Secondly, since customers are no longer locked in to a single service provider, the playing field for service providers becomes more equitable towards new players, thereby spurring the development of substitute as well as novel services.

### **III. Safeguards**

#### **A. Data Porting**

4. However, in recognising the infancy of data porting in Singapore,<sup>12</sup> the Amendment have placed two guidelines to data porting to ensure personal data remains protected. Firstly, the amended PDPA prohibits the porting of data if the porting organisation reasonably expects adverse consequences.<sup>13</sup> Such adverse consequences include whether the porting of data threatens the well-being of individuals or is against the national interest.<sup>14</sup> For instance, data porting may be prohibited to safeguard the well-being of an individual with compulsive buying disorder because data porting makes online shopping more addictive by improving algorithms that generate online advertisements.<sup>15</sup> Secondly, organisations are not required to port the user's data if porting would be disproportionate to the individual's interests.<sup>16</sup>

#### **B. Protection of Personal Data**

5. The Amendments adds an additional requirement for organisations to ensure that security measures exist to protect physical storage devices.<sup>17</sup>

6. First, organisations must make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks of personal data.<sup>18</sup> Second, organisations are also now required to make reasonable security arrangements to prevent the loss of any storage or medium device that stores personal data in its possession or under its control.<sup>19</sup>

#### **C. Enhanced Penalties**

7. Generally, any contravention of the PDPA will result in a financial penalty of up to \$1 million.<sup>20</sup> However, in recognising that organisations that are privy to personal data are normally wealthy organisations or individuals, the Amendment has increased the \$1 million threshold for certain situations.<sup>21</sup> Specifically, if the annual turnover of an organisation exceeds \$10 million, the maximum penalty that can be imposed will be 10% of its annual turnover while if the annual turnover of an individual exceeds \$20 million, the maximum penalty that can be

imposed will be 5% of that individual's annual turnover.<sup>22</sup> Moreover, even a negligent contravention of the PDPA will attract financial penalties, further cementing the deterrent effect of mishandling personal data.<sup>23</sup>

8. In addition to the enhanced financial penalties, certain contraventions of the PDPA may even lead to imprisonment. The Amendment has made it an offence for unauthorised use or disclosure of personal data, or unauthorised re-identification of anonymised information.<sup>24</sup> The amended PDPA also penalises organisations for the circulation of false requests for data porting on behalf of the individual.<sup>25</sup>

#### **IV. Transparency**

##### ***D. Notifiable Data Breaches***

9. Users will now be notified of any data breaches that puts them at risk of significant harm.<sup>26</sup> Some potential categories of data which will be considered likely to subject the user to significant harm are as follows:

- (a) medical diagnosis by a medical professional;<sup>27</sup> and
- (b) account usernames and passwords.<sup>28</sup>

10. Timely notifications empower the user to protect his data because they provide clear steps he can take to prevent the data from being abused such as changing his password.<sup>29</sup>

#### **V. Conclusion**

11. In conclusion, the amended PDPA provides organisations with options to access customer data apart from the existing consent-based ones, thereby allowing them to provide better customer service to users. At the same time, users can be reassured that the greater accessibility of their data is accompanied by a more stringent set of guidelines to enforce accountability on the part of organisations.

---

Disclaimer: This article does not constitute legal advice or opinion. Lexicon and its members do not assume responsibility, and will not be liable, to any person in respect of this article.

---

\* Written by Ng Jing Jie, Year 1 LL.B. Undergraduate, School of Law, Singapore Management University, and An Ye Qi, Year 1 LL.B. Undergraduate, School of Law, Singapore Management University.

<sup>1</sup> Personal Data Protection (Amendment) Act 2020 (No.40 of 2020) (PDPA).

---

<sup>2</sup> *Singapore Parliamentary Debates, Official Report* (2 November 2020) vol 95; Sitting No 11 (S Iswaran, The Minister for Communications and Information).

<sup>3</sup> *Ibid.*

<sup>4</sup> *Ibid.*

<sup>5</sup> *Ibid.*

<sup>6</sup> *Supra* n 1.

<sup>7</sup> *Id.*, at s 6.

<sup>8</sup> *Singapore Parliamentary Debates, Official Report* (2 November 2020) vol 95; Sitting No 11 (Jasmine Tan Soon Neo, MP for East Coast GRC).

<sup>9</sup> *Ibid.*

<sup>10</sup> *Supra* n 1, at s 14.

<sup>11</sup> *Ibid.*

<sup>12</sup> *Singapore Parliamentary Debates, Official Report* (2 November 2020) vol 95; Sitting No 11 (Louis N Kok Kwang, MP for Nee Soon GRC).

<sup>13</sup> *Supra* n 1, at s 14.

<sup>14</sup> *Ibid.*

<sup>15</sup> *Singapore Parliamentary Debates, Official Report* (2 November 2020) vol 95; Sitting No 11 (Chua Kheng Wee Louis, MP for Sengkang GRC).

<sup>16</sup> *Supra* n 1, at s 39.

<sup>17</sup> *Id.*, at s 12.

<sup>18</sup> *Ibid.*

<sup>19</sup> *Ibid.*

<sup>20</sup> *Id.*, at s 23.

<sup>21</sup> *Ibid.*

<sup>22</sup> *Id.*, at s 24.

<sup>23</sup> *Id.*, at s 23.

<sup>24</sup> *Id.*, at s 21.

<sup>25</sup> *Id.*, at s 27.

<sup>26</sup> *Id.*, at s 13.

<sup>27</sup> Public Data Protection Commission website <[https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Draft-AG-on-Key-Provisions/Draft-Advisory-Guidelines-on-Key-Provisions-of-the-PDP-\(Amendment\)-Bill-\(20-Nov-2020\).pdf?la=en](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Draft-AG-on-Key-Provisions/Draft-Advisory-Guidelines-on-Key-Provisions-of-the-PDP-(Amendment)-Bill-(20-Nov-2020).pdf?la=en)> (accessed 28 December 2020).

<sup>28</sup> *Ibid.*

<sup>29</sup> Public Data Protection Commission website <<https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Breaches-2-0.pdf?la=en>> (accessed 24 January 2021).