



June 30, 2023

## **BSA COMMENTS ON THE PERSONAL INFORMATION PROTECTION ACT DRAFT ENFORCEMENT DECREE**

### **Submitted Electronically to the Personal Information Protection Commission (PIPC)**

BSA | The Software Alliance (**BSA**)<sup>1</sup> welcomes the opportunity to provide our comments on the Draft Enforcement Decree to the recently amended Personal Information Protection Act (**Draft Decree** and **PIPA** respectively).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software.

BSA has followed the development of the PIPA closely and participated in many related consultations.<sup>2</sup> We note that the Draft Decree provides further details to the PIPA amendments, including how they would be implemented. We appreciate the PIPC's efforts in this regard and provide further recommendations for PIPC's consideration.

### **Exempt “outsources” from consumer-facing obligations**

**Neither the Draft Decree nor the amended PIPA have clearly recognized the distinct roles played by data controllers and processors, which are referred to as “personal information controller” and “outsourcer” respectively in the PIPA. We recommend that PIPC, either through the Draft Decree or future amendments to the PIPA, recognize the distinct roles of data controllers and data processors – defined as “personal information controllers” and “outsources” respectively in the PIPA – and ensure that consumer-facing obligations do not apply to “outsources”.**

The distinction between companies that decide when and how to collect and use data about individuals (i.e., data controllers) and companies that only process data on behalf of other companies

---

<sup>1</sup> BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

<sup>2</sup> See: BSA Submission on Draft Presidential Decree Implementing Personal Data Protection Law Amendments, May 2020, <https://www.bsa.org/policy-filings/korea-bsa-submission-on-draft-presidential-decree-implementing-personal-data-protection-law-amendments>; BSA Submission on Draft Partial Amendments to the PIPA, Feb 2021, <https://www.bsa.org/policy-filings/korea-draft-partial-amendments-to-the-personal-information-protection-act>; BSA Submission on Proposed Revisions to the PIPA, Nov 2021, <https://www.bsa.org/policy-filings/korea-bsa-submission-on-proposed-revisions-to-personal-information-protection-act>.

(i.e., data processors) is an important one because both data controllers and data processors have important, but distinct roles in protecting personal information. For that reason, personal data protection laws worldwide reflect a global consensus that clearly distinguishes between the two types of entities and assigns each type of entity responsibilities that reflect their different roles in safeguarding personal data. Data protection laws that have adopted this approach include the European Union's General Data Protection Regulation (**GDPR**),<sup>3</sup> California's Consumer Privacy Act (**CCPA**),<sup>4</sup> Japan's Act on the Protection of Personal Information (**APPI**),<sup>5</sup> and Singapore's Personal Data Protection Act (**PDPA**).<sup>6</sup>

**The amended PIPA does not adequately distinguish, and oftentimes conflates, the roles and responsibilities of the data controller and processor. Notably, Article 26(8) of the amended PIPA establishes that many of the consumer-facing obligations that apply to the “personal information controller” will apply to the “outsourcer” as well.<sup>7</sup> Accordingly, we urge the PIPC to make clear that these consumer-facing obligations do not apply to “outsourcers”.**

These obligations belong on data controllers because such companies often have a direct relationship with individual data subjects and decide when and why to collect what kind of consumers' data. In contrast, data processors generally do not have direct relationships with individual data subjects. Instead, they process data on behalf of a data controller, usually pursuant to a contractual relationship and in line with the data controller's instructions. In this role, data processors may not be privy to the nature of the data they are processing or the purposes for which such processing is being conducted — because those purposes are determined by the data controller. Moreover, data processors may be contractually *prohibited* from accessing data they store or otherwise process for a controller or from processing that data for purposes other than those directed by the controller. Placing consumer-facing obligations on data processors may inadvertently undermine consumer privacy since it may require data processors to access data they would otherwise not, and to analyze and identify individuals to whom they must reach out to satisfy their legal requirements. This can create a host of privacy and security issues, particularly to the extent that data processors could be required to provide data to individuals they do not know and whose identity they may be unable to rightfully authenticate. The obligation to interact with those individuals should instead fall on data controllers to ensure these important rights and obligations are not exercised in a manner that inadvertently undermines PIPA's privacy protections.

**BSA notes that the Draft Decree would only provide further details on how the provisions in the amended PIPA would be implemented. However, when the PIPA may be further amended, we recommend amending Article 26(8) to exclude “outsourcers” from the following sets of obligations:**

- **The consumer-facing obligations in Articles 15 to 25(2), 27 and 28, which impose obligations based on the purpose for which data is processed. As noted above, data processors may not be privy to the nature of the data they are processing or the purposes for which such processing is being conducted — because those purposes are determined by the data controller.**

---

<sup>3</sup> European Union General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

<sup>4</sup> California Consumer Privacy Act of 2018, [http://leginfo.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](http://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5).

<sup>5</sup> Amended Act on the Protection of Personal Information (English), [https://www.ppc.go.jp/files/pdf/Act\\_on\\_the\\_Protection\\_of\\_Personal\\_Information.pdf](https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf).

<sup>6</sup> Personal Data Protection Act 2012, <https://sso.agc.gov.sg/Act/PDPA2012>.

<sup>7</sup> These include obligations to: obtain consent from data subject to process their data (Article 22, 22(2)), notify the data subject in case of transferring data due to business transfer (Article 27), obtain consent from the data subject in case of cross-border transfer and to respond to data's subject's request to stop the cross-border transfer (Article 28(8), 28(9)), notify the data subject in case of a data breach (Article 34), respond to a request made by data subjects to transfer its data (Article 35(2)), respond to consumer rights request, including requests made by data subject to delete its data (Article 36), requests to stop the processing of its data (Article 37), and requests made by the data subject to explain the automated decision-making process (Article 37(2)).

- The obligations subject to a privacy impact assessment under Article 33 and to notify data subjects of a breach under Article 34.
- The consumer rights articulated in Articles 35-38. As noted above, data controllers are best positioned to interact with individual data subjects while data processors are unlikely to know those data subjects and may lack information needed to authenticate their identity.

In addition, we note that the PIPC published a revised Personal Information Processing Consignment Guide in December 2020 (Guide),<sup>8</sup> which provided further information on the operation of Article 26, among other issues. We recommend that PIPC update the Guide to reflect the different roles of “personal information controllers” and “outsourcers”. In this regard, we have also enclosed BSA’s position paper on the distinction between data controllers and processors for your reference.<sup>9</sup>

While the PIPA’s consumer-facing obligations are critical for effectively protecting personal information and upholding privacy, we urge the PIPC to ensure these obligations are not inappropriately applied to entities that have very different roles in handling consumers’ data. Instead, these consent-based obligations and consumer rights requests should apply to data controllers, whereas data processors should be accountable for handling data securely in line with a controller’s instructions. Distinguishing the two roles will strengthen privacy and data security.

## Facilitating Cross-Border Data Transfers

BSA appreciates that the PIPA amendments have established additional legal bases for the overseas transfer of personal information. Notably, under Article 28-8 of the amended PIPA, cross-border transfers of personal information without consent are permitted if the overseas recipient to whom the data is transferred has obtained a data protection certification by the PIPC OR if the overseas recipient is a country recognised by the PIPC as having an appropriate level of personal data protection. To implement this obligation, Article 29-12 of the Draft Decree sets out that a “Specialized Committee for Overseas Transfer of Personal Information” (**Committee**) will review policies for the overseas transfer of personal information.

**BSA recommends that the Committee be allowed under the Draft Decree to recommend the use of other third-party certification processes and data transfer mechanisms, such as intra-corporate binding rules, international trustmarks and regional certifications, which can help create more flexibility in supporting cross-border data transfers.** These mechanisms are incorporated in other global data protection frameworks to promote cross-border data flows, including the Global and APEC Cross Border Privacy Rules (**CBPR**) of which Korea is a participant, the European Union’s General Data Protection Regulation (**GDPR**), and Japan’s Act on the Protection of Personal Information. For example, the Draft Decree could allow the Committee to recommend the use of the Global CBPR certification as a certification that would allow the transfer of personal information across borders without the need to obtain consent from the data subject.

Enabling personal information controllers to use different mechanisms to transfer personal information across international borders affords businesses the flexibility to determine the mechanisms that will be most optimal and relevant for them. In contrast, requiring multiple certifications or certifications that are market-specific will create significant burdens for both Korean and non-Korean businesses delivering global services.

<sup>8</sup> Personal Information Processing Consignment Guide, Revised Dec 2020, <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7040#LINK>

<sup>9</sup> Controllers and Processors: A Longstanding Distinction in Privacy, Oct 2022, <https://www.bsa.org/files/policy-filings/10122022controllerprodinction.pdf> and enclosed.

Relatedly, BSA notes that the PIPA amendments grant the PIPC authority to order a suspension of the transfer of personal information (**suspension order**) if: (i) such transfer takes place or is expected to take place in a manner that violates the PIPA; or (ii) the recipient, country or international organisation receiving the personal data does not provide adequate protection vis-à-vis what is required under the PIPA.

BSA appreciates that the Draft Decree has set out the factors that PIPC should consider before issuing a suspension order.<sup>10</sup> These factors set out clear guidelines for when such a power can be invoked. However, while the suspension order may be effective in preventing *future* transfers of personal information when there is a PIPA violation, it is difficult to see how it would work in respect of an *ongoing* transfer, given the speed of data transfers. **BSA would be grateful for further details on how the suspension of an *ongoing* transfer would work in practice.**

## Designating Domestic Agents

Article 32-3 of the Draft Decree sets out the scope of entities which are required to designate a Domestic Agent.<sup>11</sup>

BSA appreciates that the requirement to designate a domestic agent is not overly expansive and takes into consideration the total revenue generated and the amount of data handled by companies. A domestic agent, which will take on the duties of a privacy officer, as well as other notification and reporting duties, will assist businesses in maintaining compliance with their data protection obligations. Given that businesses vary in size, complexity and volume of personal data processing, they should be permitted to appoint their DPOs based on their suitability and their organizational structure. **To that end, we recommend that the PIPC continue to avoid implementing overly prescriptive thresholds for companies to appoint domestic agents, such as minimum qualification requirements, or specific certifications mandated by the PIPC.**

## Conclusion

We hope that our comments will assist with the implementation of the PIPA amendments. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,



Tham Shen Hong  
Manager, Policy – APAC

---

<sup>10</sup> Factors include the type and size of personal information transferred, the seriousness of the violation, and whether the suspension would benefit the data subject. Before issuing an order to suspend, the PIPC is also required to consult the Specialized Committee.

<sup>11</sup> Namely, any online service provider without an address or business office in Korea and: a) whose total revenue for the previous business year is a trillion won or more; b) who stores and manages personal information of one million domestic data subjects or more on average per day during the three months period immediately preceding the end of the previous year; or c) who has been requested by PIPC to submit relevant items, documents or materials for having caused, or suspected for causing, a violation of the PIPA.



## Controllers and Processors: A Longstanding Distinction in Privacy

Modern privacy laws have coalesced around core principles that underpin early privacy frameworks. For example, leading data protection laws globally incorporate principles of notice, access, and correction. They also identify appropriate obligations for organizations in fulfilling these rights, making important distinctions between companies that decide how and why to process personal data, which act as controllers of that data, and companies that process the data on behalf of others, which act as processors of such data. Privacy and data protection laws worldwide also assign different obligations to these different types of entities, reflecting their different roles in handling consumers' personal data.

The concepts of controllers and processors have existed for more than forty years. These roles are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework, and ISO 27701.

### The History of Controllers and Processors

#### 1980: OECD PRIVACY GUIDELINES

The OECD Privacy Guidelines launched the modern wave of privacy laws, building on earlier efforts including a 1973 report by the US Department of Health, Education and Welfare that examined privacy challenges posed by computerized data processing and recommended a set of fair information practice principles.<sup>1</sup>

The OECD Guidelines, adopted in 1980, define a "**data controller**" as the entity "competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf."<sup>2</sup>

Comments to the 1980 Guidelines recognize "[t]he term 'data controller' is of vital importance" because it defines the entity "legally competent to decide about the contents and use of data."<sup>3</sup>

#### 1981: COUNCIL OF EUROPE CONVENTION 108

The Council of Europe in 1981 opened for signature the first legally binding international instrument in the data protection field. Convention 108 defined a "**controller of the file**" as the person "competent . . . to decide" the purpose of automated files, as well as "which categories of personal data should be stored and which operations should be applied to them."<sup>4</sup>

#### 1995: EU DATA PROTECTION DIRECTIVE

The 1995 EU Data Protection Directive, which previously formed the basis of privacy laws in EU member countries, separately defined both controllers and processors.<sup>5</sup> **Controllers** were defined as the natural or legal person that "determines the purposes and means of the processing of personal data," while **processors** were defined as a natural or legal person "which processes personal data on behalf of the controller."

## 2005: APEC PRIVACY FRAMEWORK

The APEC Privacy Framework builds on the OECD Privacy Guidelines and provides guidance on protecting privacy, security, and the flow of data for economies in the APEC region. It was endorsed by APEC in 2005 and updated in 2015. The Framework defines a **controller** as an organization that “controls the collection, holding, processing, use, disclosure, or transfer of personal information,” including those instructing others to handle data on their behalf. It does not apply to entities processing data as instructed by another organization.<sup>6</sup>

## 2011: APEC CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

All 21 APEC economies endorsed the Cross-Border Privacy Rules (CBPR) System in 2011, creating a government-backed voluntary system designed to implement the APEC Privacy Framework.<sup>7</sup> The CBPR system is limited to **data controllers**. In 2015, APEC created a separate Privacy Recognition for Processors (“PRP”) System to help controllers identify qualified and accountable **processors**.<sup>8</sup>

## 2016: EU GENERAL DATA PROTECTION REGULATION

The EU General Data Protection Regulation replaced the 1995 Directive, maintaining the definition of **controller** as the entity that “determines the purposes and means” of processing personal data, and the definition of **processor** as the entity that “processes personal data on behalf of the controller.”<sup>9</sup> It was adopted in 2016 and took effect in 2018.

## 2018: COUNCIL OF EUROPE MODERNIZED CONVENTION 108

Convention 108 was modernized in 2018, revising the definition of **controller** and adding a definition of processor. A controller is the entity with “decision-making power with respect to data processing.”<sup>10</sup> A **processor** “processes personal data on behalf of the controller.”<sup>11</sup>

## 2019: ISO 27701

The International Organization for Standardization published ISO 27701 in 2019, creating the first international standard for privacy information management. ISO 27701 allocates obligations to implement privacy controls based on whether organizations are controllers or processors. It recognizes that a **controller** determines “the purposes and means of processing”<sup>12</sup> while **processors** should ensure that personal data processed on behalf of a customer is “only processed for the purposes expressed in the documented instructions of the customer.”<sup>13</sup>

## 2023: US STATE PRIVACY LAWS

In the United States, five new state consumer privacy laws will take effect in 2023, in California, Colorado, Connecticut, Utah, and Virginia. All five laws distinguish between **controllers** or businesses that determine the purpose and means of processing, and **processors** or service providers that handle personal information on behalf of the controller or business.









According to a March 2021 report, **more than 84%** of countries responding to an OECD questionnaire define “data controller” in their privacy legislation.<sup>14</sup>



## Controllers and Processors: A Distinction Adopted Around the World

Privacy laws worldwide draw from longstanding privacy frameworks, recognizing the distinction between controllers and processors and assigning different responsibilities to these different entities based on their different roles in processing personal data. The chart below identifies some of the countries with national privacy or data protection laws that reflect the roles of controllers and processors.

|  <b>JURISDICTION</b> |  <b>CONTROLLER</b>  |  <b>PROCESSOR</b>  |
|---|--|---|
| <b>Brazil</b> <sup>15</sup>   | <b>Controller:</b> A “natural person or legal entity . . . in charge of making the decisions regarding the processing of personal data.”   | <b>Processor:</b> A “natural person or legal entity . . . that processes personal data in the name of the controller.”  |
| <b>Cayman Islands</b> <sup>16</sup>   | <b>Data Controller:</b> A “person who, alone or jointly with others <i>determines the purposes, conditions and manner</i> in which any personal data are, or are to be, processed . . . .”   | <b>Data Processor:</b> Any person “who processes personal data <i>on behalf of</i> a data controller but, for the avoidance of doubt, does not include an employee of the data controller.”         |
| <b>European Union</b> <sup>17</sup>   | <b>Controller:</b> A natural or legal person that “alone, or jointly with others, <i>determines the purposes and means of processing</i> personal data. . . .”   | <b>Processor:</b> A natural or legal person that “processes personal data <i>on behalf of</i> the controller.”  |
| <b>Faroe Islands</b> <sup>18</sup>  | <b>Controller:</b> A natural or legal person that “alone or jointly with others, <i>determines the purposes and means of the processing of</i> personal data.”   | <b>Processor:</b> A natural or legal person that “processes personal data <i>on behalf of</i> the controller.”  |
| <b>Hong Kong</b> <sup>19</sup>  | <b>Data User:</b> A person who “either alone or jointly or in common with other persons, <i>controls the collection, holding, processing or use of the data.</i> ”   | <b>Data Processor:</b> A “person who:<br>(a) Processes personal data <i>on behalf of</i> another person; and<br>(b) <i>Does not process the data for any of the person’s own purposes.</i> ”        |
| <b>Kosovo</b> <sup>20</sup>   | <b>Data Controller:</b> A natural or legal person that “alone or jointly with others, <i>determines purposes and means of personal data processing.</i> ”  | <b>Data Processor:</b> A natural or legal person that “processes personal data for and <i>on behalf of</i> the data controller.”  |
| <b>Malaysia</b> <sup>21</sup>   | <b>Data User:</b> A person “who either alone or jointly or in common with other persons processes any personal data or <i>has control over or authorizes</i> the processing of any personal data, but <i>does not include a data processor.</i> ”  | <b>Data Processor:</b> A person “who processes the personal data solely <i>on behalf of</i> the data user, and <i>does not process the personal data for any of his own purposes.</i> ”             |
| <b>Mexico</b> <sup>22</sup>   | <b>Data Controller:</b> An individual or private legal entity “ <i>that decides on the processing of</i> personal data.”   | <b>Data Processor:</b> The individual or legal entity that “alone or jointly with others, processes personal data <i>on behalf of</i> the data controller.”   |
| <b>Philippines</b> <sup>23</sup>  | <b>Personal Information Controller:</b> A person or organization “ <i>who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes a person or organization who performs such functions as instructed by another person or organization.</i> ” | <b>Personal Information Processor:</b> A natural or juridical person “to whom a personal information controller may <i>outsource</i> the processing of personal data pertaining to a data subject.” |
| <b>Qatar</b> <sup>24</sup>  | <b>Controller:</b> A natural or legal person “who, whether acting individually or jointly with others, <i>determines how Personal Data may be processed and determines the purpose(s) of any such processing.</i> . . . .”   | <b>Processor:</b> A natural or legal person “who processes Personal Data for the Controller.”   |
| <b>Singapore</b> <sup>25</sup>  | <b>Organisation:</b> Any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore or (b) resident, or having an office or a place of business, in Singapore.  | <b>Data Intermediary:</b> An organisation “which processes personal data <i>on behalf of another organisation</i> but does not include an employee of that other organisation.”                     |

|  <b>JURISDICTION</b> |  <b>CONTROLLER</b>   |  <b>PROCESSOR</b>  |
|---|---|---|
| <b>South Africa</b> <sup>26</sup>   | <b>Responsible Party:</b> A public or private body or any other person that “alone or in conjunction with others, determines the purpose of and means for processing personal information.” | <b>Operator:</b> A person who “processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party.”                            |
| <b>Thailand</b> <sup>27</sup>   | <b>Data Controller:</b> A person or juristic person “having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data.”                      | <b>Data Processor:</b> A person or juristic person who “operates in relation to the collection, use, or disclosure of Personal Data pursuant to the orders given by or on behalf of the Data Controller.” |
| <b>Turkey</b> <sup>28</sup>   | <b>Data Controller:</b> A natural or legal person “who determines the purposes and means of processing personal data.”  | <b>Data Processor:</b> A natural or legal person “who processes personal data on behalf of the data controller upon its authorization.”   |
| <b>Ukraine</b> <sup>29</sup>  | <b>Personal Data Owner:</b> A natural or legal person who “determines the purpose of personal data processing, the composition of this data and the procedures for its processing.”         | <b>Personal Data Manager:</b> A natural or legal person who is “granted the right by the personal data owner or by law to process this data on behalf of the owner.”                                      |
| <b>United Kingdom</b> <sup>30</sup>   | <b>Controller:</b> A natural or legal person that “alone or jointly with others, determines the purposes and means of the processing of personal data.”                                     | <b>Processor:</b> A natural or legal person that “processes personal data on behalf of the controller.”   |

## Endnotes

- <sup>1</sup> Dept. of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens (1973), <https://aspe.hhs.gov/reports/records-computers-rights-citizens>.
- <sup>2</sup> OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, § 1(a) (1980), <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>.
- <sup>3</sup> *Id.* at Explanatory Memorandum, § IIB, para. 40.
- <sup>4</sup> Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, art. 2(d), Jan. 28, 1981, ETS No. 108, <https://rm.coe.int/1680078b37>.
- <sup>5</sup> Directive 95/46/EC, art. 2(d)-(e), <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML>.
- <sup>6</sup> APEC, APEC Privacy Framework (2015), § II.10, <https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf>.
- <sup>7</sup> See APEC, 2011 Leaders' Declaration, [https://www.apec.org/meeting-papers/leaders-declarations/2011/2011\\_aelm](https://www.apec.org/meeting-papers/leaders-declarations/2011/2011_aelm); <http://cbprs.org/privacy-in-apec-region/>.
- <sup>8</sup> See APEC Privacy Recognition for Processors (“PRP”) Purpose and Background, <https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf>.
- <sup>9</sup> EU General Data Protection Regulation, art. 4(7)-(8), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.
- <sup>10</sup> Council of Europe, Modernised Convention for the Protection of Individuals With Regard to the Processing of Personal Data, art. 2(d), May 17-18, 2018, ETS No. 108, [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf).
- <sup>11</sup> *Id.* at art. 2(f).
- <sup>12</sup> Int'l Org. for Standardization, International Standard ISO/IEC 27701 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines 1, 4-5, 29-55 (2019).
- <sup>13</sup> *Id.* at 43.
- <sup>14</sup> OECD, Report on the Recommendation of the Council Concerning Guidelines Governing Protection of Privacy and Transborder Flows of Personal Data, 16 (2021), <https://www.oecd.org/sti/ieconomy/privacy.htm>.
- <sup>15</sup> Law No. 13,709, Aug. 14, 2018, art. 5 VI-VII (as amended by Law No. 13,853, July 8, 2019, Official Journal of the Union [D.O.U.] July 9, 2019), [https://iapp.org/media/pdf/resource\\_center/Brazilian\\_General\\_Data\\_Protection\\_Law.pdf](https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf).
- <sup>16</sup> Data Protection Act (2021), § 2, [https://ombudsman.ky/images/pdf/laws\\_regs/Data\\_Protection\\_Act\\_2021\\_Rev.pdf](https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf).
- <sup>17</sup> EU General Data Protection Regulation, art. 4, 2016 O.J. (L 119), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3A%3A2016%3A119%3ATOC>.
- <sup>18</sup> Act on the Protection of Personal Data No. 80 (2020), §§ 6(6)-(7), <https://dat.cdn.f0/media/opcxh1q/act-on-the-protection-of-personal-data-data-protection-act-act-no-80-on-the-7-june-2020.pdf?s=LA6lqXBchs1Ryn1Kp9h3KSPuFog>.
- <sup>19</sup> Personal Data (Privacy) Ordinance, (1996) Cap. 486, § 2(1), <https://www.elegislation.gov.hk/hk/cap486>. See [https://www.pcpd.org.hk/english/data\\_privacy\\_law/ordinance\\_at\\_a\\_Glance/ordinance.html](https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html).
- <sup>20</sup> Law No. 06/L-082 on Protection of Personal Data (2019), art. 3, §§ 1.11, 1.14, [https://www.dataguidance.com/sites/default/files/law\\_no\\_06\\_l-082\\_on\\_protection\\_of\\_personal\\_data\\_0.pdf](https://www.dataguidance.com/sites/default/files/law_no_06_l-082_on_protection_of_personal_data_0.pdf).
- <sup>21</sup> Act 709 Personal Data Protection Act 2010, § 4, <https://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf>.
- <sup>22</sup> Federal Law on Protection of Personal Data Held by Private Parties, art. 3, XIV & IX, Official Gazette July 5, 2010, <https://www.dataguidance.com/legal-research/federal-law-protection-personal-data-held>.
- <sup>23</sup> Data Privacy Act of 2012, Rep. Act No. 10173, §§ 3(h)-(i) (Aug. 15, 2012), <https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/#:~:text=11.,transparency%2C%20legitimate%20purpose%20and%20proportionality>.
- <sup>24</sup> Law No. 13 of 2016 Personal Data Privacy Protection, art. 1, [https://www.dataguidance.com/sites/default/files/law\\_no\\_13\\_of\\_2016\\_on\\_protecting\\_personal\\_data\\_privacy\\_-\\_english.pdf](https://www.dataguidance.com/sites/default/files/law_no_13_of_2016_on_protecting_personal_data_privacy_-_english.pdf).
- <sup>25</sup> Personal Data Protection Act 2012, as amended, § 2(1), <https://sso.agc.gov.sg/Act/PDPA2012>.
- <sup>26</sup> Protection of Personal Information Act, 2013, Act 4 of 2013, Chap. 1, <https://popia.co.za/>.
- <sup>27</sup> Personal Data Protection Act, B.E. 2562 (2019), § 6, <https://cyrilla.org/es/entity/si9175g71u?page=1>.
- <sup>28</sup> Law on Protection of Personal Data No. 6698 (2016), art. 3(g), 3(i), <https://www.kvkk.gov.tr/icerik/6649/Personal-Data-Protection-Law>.
- <sup>29</sup> Law of Ukraine on Personal Data Protection (2010) (as amended), art. 2, 4(4), <https://zakon.rada.gov.ua/laws/show/en/2297-17#Text>.
- <sup>30</sup> UK General Data Protection Regulation 2016 (as amended), c. 1, art. 4(7)-(8), <https://www.legislation.gov.uk/eur/2016/679>. See also UK Information Commissioner's Office, Who Does the UK GDPR Apply To?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/>.