Centre for Information Policy Leadership
Hunton & Williams LLP

30 ST MARY AXE
LONDON, EC3A 8EP
TEL +44 (0)20 7220 5700
FAX +44 (0)20 7220 5772

2200 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20037
TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

5 May 2015

Comments of the Centre for Information Policy Leadership

Brazil's draft law (the "draft") "On the processing of personal data to protect the personality and dignity of natural persons"

The Centre for Information Policy Leadership (the "Centre") appreciates the opportunity to provide comments on Brazil's draft law "On the processing of personal data to protect the personality and dignity of natural persons". The Centre is a global privacy and security think tank in the law firm of Hunton & Williams, established over 12 years ago. It is supported by approximately 35 member companies that are leaders in key sectors of the global economy. The Centre provides thought leadership and expertise on global privacy and security policy issues, working with privacy officers, regulators and external experts to develop best practices to ensure effective privacy protection and information management in the modern information age. For more information, please see the Centre's website at http://www.informationpolicycentre.com/. Nothing in this comment should be construed as representing the views of any individual Centre member or of the law firm of Hunton & Williams LLP.

I. General Statement

The Centre commends the drafters of the proposed law for having developed a draft that addresses a wide array of key protections that must be included in any privacy law. The draft represents a good starting point to further develop a law that ultimately will maximise privacy protections for individuals, facilitate beneficial and innovative uses of data in an ever-changing technological and business environment and ensure Brazil's economic competitiveness in this environment.

We support the drafters' recognition of some of the modern data privacy concepts and best practices. In particular, we endorse the concept of a single, national data protection authority ("competent authority"), the ability to take personal data outside the scope of the law through de-identification and anonymisation, the recognition of the importance of enabling cross-border data flows to and from Brazil with a wide array of instruments and the inclusion of the concept of "good practices" that can be developed by organizations to implement the requirements of the law and demonstrate compliance.

On the other hand, we believe that the draft would benefit from certain clarifications and modifications in some areas. These include the area of jurisdiction, the distinction between controllers and processors, the purpose specifications and the concept of "compatibility", the

nature of consent and the exceptions and additional alternatives to consent, and the options of cross-border transfer mechanisms.

We hope that our recommendations below will assist the drafters in finalizing the proposal in a way that fully realizes its promise. In that connection, we commend the drafters for initiating a comprehensive consultation process on the proposed bill and would suggest that a second round of consultations might be appropriate on a revised draft before presenting the final bill from the executive branch to the legislative branch. By its nature, this bill is broad in scope and will impact every area of commercial and government activity, as it covers processing of personal data of all individuals, whether it is in their roles as citizens, employees, consumers, customers, businesses or other. Therefore, it is essential that there is a broad consultation and solicitation of views as well as impact assessments from all stakeholders – the public and private sectors, large and small organizations including start-ups, and all sectors of industry and society.

II. Specific Comments

1. Jurisdiction and Controller/Processor Distinction

Article 2:

This Law applies to any processing operations performed through totally or partially automated means, by a natural person or by a legal person under public or private law, regardless of the country where they are located and the country where the database is located, provided that:

I - The processing operation is performed within the national territory; or

II - The personal data subject to processing have been collected within the national territory.

§ 1 Personal data are regarded as collected in the national territory if their data subject was located in the national territory at the time of collection.

. . .

Article 6

Personal data processing activities shall comply with the following general principles:
. . .

Centre comments: The jurisdictional scope of the draft appears to be overly broad as drafted and thus differs from what is customary in other data privacy laws globally. In some places, it also fails to clearly distinguish between data controllers and data processors (even though they are treated separately in the definitions, Article 5 VIII and IX, as well as in later chapters, including Chapter II, Articles 7, 10 and 11; Chapter III, Article 17 and 19; and Chapter V, Article 30). Both the overly broad jurisdiction and the failure to clearly distinguish between controller and processor responsibilities in all contexts may create unintended consequences and result in interpretations of the law that cause commercial disadvantage to the Brazilian IT service industry without any countervailing benefits to privacy protections.

Controller/processor distinction. The draft law generally appears to recognize that data controllers are the entities that collect and use data about individuals for various purposes, make all decisions regarding data processing and may engage third-party data processors to perform various processing functions on their behalf. Thus, it appears that the draft recognizes that controllers are the entities that should be responsible for complying with data privacy law as the third-party processors only act on their behalf and are merely implementing any legal requirements pursuant to the controller's instructions and contract. While this division of responsibility appears to be recognized in several portions of the draft law, including the definitions, this distinction is not consistently reflected in other portions of the text, most notably in Chapter I, Article 2 defining the scope of the law, and Article 6 concerning the principles of data processing. Both provisions appear to be written as though they apply equally to both controllers and processors. This may create uncertainty and conflicting obligations for both controllers and processors in Brazil. We suggest that the distinction between controllers and processers be clarified throughout the law.

Jurisdictional scope. With respect to the jurisdictional scope of the draft law, foreign data controllers should not be subject to Brazilian privacy law when they are using Brazilian processors to process non-Brazilian data in Brazil. Imposing Brazilian privacy law on foreign controllers would create significant impediments for the Brazilian IT service industry as well as other processors in Brazil that provide services to global clients.

Also, data processors located in Brazil should not be subject to Brazilian privacy law other than via contract (if they are processing on behalf of Brazilian controllers). Indeed, if they are processing non-Brazilian data on behalf of foreign controllers subject to foreign requirements, such processors would not be able to comply with both the foreign controllers' privacy obligations and any conflicting Brazilian requirements.

In sum, in our view, the privacy law's jurisdiction over controllers should extend only to those controllers established in Brazil or to controllers that are located outside of Brazil but who are directing their services to Brazilian residents and purposefully collecting personal data of Brazilian residents (though in that case, it may be difficult to enforce the law if the entity has no presence in Brazil).

Accordingly, Articles 2 and 6 might be amended as follows:

Article 2

This Law ***imposes obligations on*** ~~*applies to any processing operations*~~ ***controllers with respect to processing operations*** *performed through totally or partially automated means* ***directed at individuals residing in Brazil*** ~~*by themselves or by a natural person or by a legal person under public or private law*~~*, regardless of the country* ***in which the controllers*** ~~*they*~~ *are located and the country where the* ***processing takes place*** ~~*database is located*~~*, provided that*~~:~~
I - ~~*The processing operation is performed within the national territory; or*~~
~~*II –*~~ ~~*T*~~*the personal data subject to processing have been* ***purposefully*** *collected* ***from or about individuals*** *within the national territory.*

*§ 1 Personal data are regarded as collected **from or about individuals** in the national territory if their data subject was located in the national territory at the time of collection.*

II. With respect to the good practice requirements of Art. 48 and 49 this law also applies to processors with processing operations within the national territory.

Article 6

***Controllers are responsible to ensure that** personal data processing activities shall comply with the following general principles:*

2. Anonymous Data

Article 5 (Definitions):

IV - anonymous data: data pertaining to a data subject that cannot be identified by the controller for the processing or by any other person, taking into account the means that can be reasonably used to identify said data subject;

Centre comments: This definition appears to have no *explicit* application or consequence in the draft. However, by implication and coupled with the definitions of "personal data" and "processing" in Article 5 I and II, anonymous data is not subject to this law and we commend the exception of anonymous data from this law. We also appreciate the inclusion in the draft of a reasonability component and note that while there may be circumstances creating theoretical risks of re-identification, in many cases, such theoretical risks are remote and the privacy of Brazilians is better served by incentivizing organizations to de-identify personal data. However, we recommend that the purpose of this provision be made explicit by clearly stating that the de-identification and anonymisation of personal data take such data outside the scope of this law. For example, anonymous data should be explicitly excluded from the definition of "personal data" in Article 5 I.

3. Principles, Purpose Specification and "Compatibility"

Article 6

Personal data processing activities shall comply with the following general principles:

I - Principle of purpose, by which the processing must be performed for legitimate, specific, and explicit purposes that are known to the data subject;

II - Principle of suitability, by which the processing must be compatible with the purposes sought and with the data subject's legitimate expectations, according to the context of the processing;

Centre comments: With respect to the first principle, we would suggest expanding the scope of "known to the data subject" to include what is reasonably expected by the data subject given the context of the processing.

We also support the second principle to the extent it provides that processing would be allowed so long as it can occur and co-exist without conflict with the original purpose or the data subject's expectations (*i.e.,* is "compatible" with the original purpose and expectations). This is exactly the case with many additional and new beneficial uses of data where such uses are not yet known or knowable at the time of collection but where these new uses do not undermine and can co-exist with the original purposes.

For example, many applications of big data and analytics provide tangible benefits to individuals and society as a whole, such as by enabling more targeted medical research, providing better health care, enabling more efficient use of public services and funds and preventing fraud.

- Big data and analytics have been transforming the health care sector by correlating patient data from a wide range of sources and uncovering patterns that can, for example, identify individuals most likely to use emergency services. When Dr. Jeffrey Brenner collected records of 600,000 hospital visits in Camden, NJ, he was not sure what he would uncover. He built a map linking hospital claims to patients' addresses and to his surprise just 1 percent of patients accounted for 30 percent of hospital bills. These patients were making particularly frequent hospital visits, imposing significant costs on the health care system. Providing more effective, efficient care to these types of patients is a challenge facing the health care system around the world. However, by using the power of data in this particular case, caseworkers were able to identify specific patients and make proactive home visits to encourage these high-risk patients to stay on their medication. This resulted in a dramatic reduction in hospital bills in that region.

- The New York Police Department (NYPD) has been increasingly using big data technology to fight crime. The NYPD's Domain Awareness System, created in 2012, contains everything from arrest records, gun permits and outstanding warrants to the text of 911 calls in real time. This has enabled police officers to access vital information before responding to a crime. The system has been so efficient that the NYPD has been developing an app for tablets and phones so that officers can access that information on the go.

- Big data has been used to catch fraudulent tax returns. A report from the US Treasury inspector general for tax administration estimated that fraudulent tax refunds resulting from identity theft totaled about US $3.6 billion for the 2011 tax filing season. That number is down by US $1.6 billion from the previous year due to the use of big data tools to better detect these fraudulent tax returns. These tools scan several databases of public information to find suspicious returns.

To enable economic growth, new products and services and other public benefits based on data-driven innovation, it is important that the legal regime be sufficiently flexible to allow for new purposes and uses of data, while also protecting the privacy rights of individuals.

However, to ensure correct interpretation of what constitutes a compatible purpose, it would be desirable to include some further guidance on the factors that controllers should take into account when determining if a subsequent purpose is compatible or not. This is the approach adopted in

Europe by the Article 29 Working Party[1] in its April 2014 opinion on purpose limitation (Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203), as well as in the discussions in the European Council on the proposed EU Data Protection Regulation. For example, according to the Article 29 Working Party, the test for "incompatibility" includes an assessment of both the negative and positive impacts of the proposed further processing on the data subject, whereby the more negative or uncertain the impact becomes, the less likely it is that the processing will be deemed "compatible."

Finally, where the relevant test determines "incompatibility," there should, nevertheless, be the ability to process data where there is a "legitimate interest" to do so. (*See* discussion of the "legitimate interest" ground for processing in Section 4 regarding "consent," below.)

Thus, we would make the following recommendations with respect to principles I and II:

Personal data processing activities shall comply with the following general principles:

I - Principle of purpose, by which the processing must be performed for legitimate, specific, and explicit purposes that are known to, ***or reasonably expected by,*** *the data subject,* ***taking into account the context of the processing****;*

II - Principle of suitability, by which the processing must be compatible with the purposes sought and with the data subject's legitimate expectations, according to the context of the processing;

In deciding if a subsequent processing is compatible with the original purposes sought, the controller shall take into account
a) any link between the original purposes sought and purposes of intended further processing;
b) the context in which data have been collected and processed;
c) the nature of the personal data;
d) any impact of further processing on the data subject, including the likelihood and severity of harm to data subjects; and
e) the existence of appropriate safeguards.

Where the purpose of further processing is not compatible with the original purposes sought and with the data subject's legitimate expectations, according to the context of the processing, the further processing must be in accordance with Chapter II, Section I on consent and exceptions to consent. Further processing for incompatible purposes on grounds of legitimate interests of the controller or a third party shall be lawful if these interests override the interests of the data subject.

[1] The Article 29 Working Party comprises the heads of all EU data protection authorities. Among other things, this group provides written interpretations and opinions concerning the principles and requirements contained in the current EU Data Protection Directive, including several that are relevant to the Centre's comments herein, such as the concepts of purpose limitations, legitimate interest, accountability and the concept of "Binding Corporate Rules." More information about the Article 29 Working Party is available at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

4. Consent

Article 7

Personal data processing is only allowed when free, express, specific, and informed consent is given by their data subject, except in the case described in art. 11.
. . .

Article 11

Consent is exempt in the case of unrestricted public access data, or whenever processing is necessary to:

Centre comments: While consent is an important basis for data processing, not all data processing can or should be based on consent. In particular, over-reliance on consent may result in consumer fatigue, apathy and loss of ability to distinguish between data collection or processing posing significant privacy risks from those activities that do not. Some contexts require alternatives to consent that are not yet included in the exceptions provided for in the draft law. Moreover, not all consent should have to be express so long as it is free, specific and informed.

In some contexts, controllers should be able to process data based on other criteria, such as where they have a "legitimate interest" in processing. "Legitimate interest" is one of the bases for processing under the EU Data Protection Directive and the proposed EU Data Protection Regulation. It allows a controller to process data if it is necessary for a legitimate interest of the controller or a third party that is not outweighed by the fundamental rights or freedoms of the data subject. According to the Article 29 Working Party's April 2014 opinion on "legitimate interest" (Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN, WP 217), the analysis of whether the legitimate interest basis can be met involves a contextual, case-specific benefits/risk analysis weighing the interest of the controller against the potential harms to the data subject. (*See also* the discussion of risk assessments and privacy risk management in Section 7 regarding "Good Practices" below.)

The legitimate interest ground for processing is important especially in the context of the increasing digitalization of business processes and society and in connection with the Internet of Things and big data analytics, where express and specific consent cannot always be obtained as a practical matter. In such cases, other legitimate grounds for processing must exist in order to facilitate responsible and accountable data uses that are beneficial to individuals and society and that enable legitimate business practices and innovation, while avoiding harms and respecting individuals' privacy. A rigid application of a consent requirement when it would be impractical or inappropriate to obtain valid consent would result in illusory, uninformed and meaningless consents and undermine effective privacy protections. Thus, to ensure that data privacy rules remain technology neutral and can be applied contextually in the future, it is necessary to provide for additional and more flexible grounds for processing, such as legitimate interest (in addition to the other exceptions to consent provided in the draft).

Also, organizations have the right and an increasing need to protect their data, intellectual property, IT systems and networks and other assets against fraudulent uses or cybersecurity attacks. Such protective measures often require the processing of personal data of individuals, including those who may be engaged in fraudulent activity or cybersecurity attacks. Obtaining consent in those circumstances would defeat the purpose of processing. We believe these examples of processing should also be based on a "legitimate interest" exception.

Other examples of processing based on legitimate interest include the use of data by organizations to market their own products and services, as well as usual business uses of data within an organization to improve their products and services and to enable collaboration and sharing of information within the organization for these purposes.

Consent should also not be required when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. This exception is also included in the EU Data Protection Directive and would be in line with the Brazilian Law of Access to Information (Lei No. 12.527 of November 18, 2011), which excludes the need for consent in several instances, including "for the protection of the overriding public and general interest" (Article 31, V). An exception in the case of public interest is important for tax authorities to be able to collect and process an individual's tax return to determine and confirm the amount of tax to be paid. Another example is a professional medical association that is responsible for carrying out disciplinary procedures against members in the case of medical fraud and abuse. These are all public interest cases where an individual, such as the doctor who committed fraud, would not consent to the inclusion of their personal information into a database if given the option. Cases like the above are beneficial to society and should be recognized under Brazilian law.

Finally, requiring consent to be "express" in all cases also suggests that "opt-out" would not be an option. However, in some contexts, opt-out may be a more appropriate option. Thus, it would be good to allow more flexibility in the definition of consent and not specify the type of consent required.

In sum, from a policy perspective, over-reliance on consent does not actually protect individuals. Experience shows that most individuals do not read or understand lengthy and complicated privacy policies and notices. As a result, they are not an effective basis for individual choice and control and, indeed, any "consent" based on such notices is illusory. The requirement in Europe to obtain express consent for the use of cookies and other tracking technology on individuals' hard drives is an example. It has led into an avalanche of meaningless cookie notices on European websites that users, instead of actually reading, simply click on to make them disappear. Clearly, the consent process is not working in this context.

Thus, we recommend the following change and additions to the exceptions to consent in Article 7 and 11:

Art. 7 – Personal data processing is only allowed when free, ~~express~~, specific and informed consent is given by their data subject, except in the case described in art. 11.

Art. 11 - Consent is exempt in the case of unrestricted public access data, or whenever processing is necessary to:
. . .

VIII – process data consistent with a legitimate interest of the controller, or a third party, providing such interests are not outweighed by any harms or negative impact on the data subject.

IX – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

5. Cross-border Transfers

Article 28

International transfer of personal data is only allowed for countries that provide a level of protection for personal data that is equivalent to the level established in this Law, with no prejudice to the following exceptions:
. . .
III - When the competent body authorises the transfer under the terms of the regulations;

Article 30 – *(regarding authorisation in Art. 28 Section III)*

The authorisation mentioned in section III of the main clause of art. 28 shall be granted when the controller for the processing provides sufficient guarantees of compliance with the general principles of protection of the data subject's rights, presented in contractual clauses approved for a specific transfer, in standard contractual clauses, or in global corporate standards, under the terms of the regulations.

§ 1 The competent body may establish standard contractual clauses, which shall comply with the general principles of protection of the data subject's data and rights, ensuring the joint liability of the transferor and the transferee, regardless of fault.

§ 2 Any controllers and processors that are part of the same economic group or multinational conglomerate may submit global corporate rules for approval by the competent body, which shall be mandatory for all the companies in the group or conglomerate with no need for specific authorisations, subject to compliance with the general principles of protection and the data subject's rights.

Centre comments: The Centre welcomes the draft law's approach to cross-border data transfers to the extent it provides for a spectrum of mechanisms that can be used to legitimize transfers of personal data to countries that do not have similar levels of data protection.

We welcome the incorporation of the widely accepted concepts of "standard contractual clauses" and "global corporate standards" or "global corporate rules" (known in Europe as "Binding

Corporate Rules" or "BCR"[2]). These concepts are good starting points for positioning Brazil for data transfers with Europe and other countries that recognize these European cross-border transfer mechanisms. However, standard contractual clauses and binding corporate rules have their limitations – the former can result in undue complexity and the latter are limited to transfers within a corporate group and lack scalability. Therefore, while we encourage Brazil to include these options as legitimate mechanisms for international data transfers, we also encourage Brazil to work with experts experienced in these mechanisms, including the Centre, to improve on these mechanisms, to make them more practical and scalable for widespread use by companies of all sizes.

Moreover, given that modern data flows and economic activity are truly global in nature, it is important to include in the menu of choices additional cross-border transfer mechanisms that mirror those that are available in other jurisdictions and regions and that extend beyond intra-company transfers. Thus, we would encourage inclusion of additional mechanisms such as privacy marks and seals and other organizational codes of conduct that are certified by appropriate third parties or a competent authority.

One such example is the APEC Cross-Border Privacy Rules system developed by the Asia-Pacific Economic Cooperation (APEC) forum. The APEC Cross-Border Privacy Rules for controllers (CBPR) and the APEC Privacy Rules for Processors (PRP) are enforceable codes of conduct for intra- and inter-company cross-border data transfers by companies that have been reviewed and certified for participation in the CBPR system by an approved third-party certification organization known as an "Accountability Agent." Enforcement of the CBPR is provided by participating APEC data protection and privacy authorities that have joined the APEC Cross-Border Privacy Enforcement Arrangement (CPEA).[3]

We emphasize that data transfer mechanisms should allow for transfers not only within a global corporate group that has implemented and approved its global corporate rules, but also between unaffiliated companies, as is the case with the APEC CBPR today and is likely to become the case with BCR in Europe under the proposed EU Data Protection Regulation.

With respect to the requirement in the current draft that the "competent body" authorise these global corporate standards, we encourage that this requirement be modified to recognize the authorisations of such corporate rules by foreign competent bodies, both with respect to the

[2] The EU Binding Corporate Rules (including controller rules and processor rules) are legally enforceable internal rules within a corporate family for the processing of personal data that, upon formal data protection authority approval, are a recognized cross-border transfer mechanism under the current EU Data Protection Directive.

[3] The CBPR for controllers track and implement the nine high-level APEC privacy principles. The CBPR were finalized in 2011 and are currently in their initial implementation phase. All 21 APEC member economies endorsed the CBPR and expressed their intent to join the system and to recognize the CBPR in their countries. To join the system, an APEC country must have at least one privacy authority that can enforce the CBPR and one "Accountability Agent" that can certify organizations. The current participants are the US, Mexico, Japan and Canada, and other APEC countries will soon follow. Three Latin American countries (Chile, Peru and Mexico) are APEC members and eligible to join the CBPR system. In February 2015 APEC endorsed a corollary set of cross-border privacy rules for processors, the APEC Privacy Recognition for Processors (PRP). For more information about the CBPR system, please see www.cbprs.org.

global corporate standards and any code-of-conduct system or cross-border privacy rules system similar to the APEC CBPR. Requiring organizations to seek approval or authorisation for their corporate rules from multiple authorities and multiple jurisdictions would result in significant inefficiencies, would undermine the usability and effectiveness of such cross-border transfer mechanisms and may preclude effective scalability for SMEs. This is evidenced by the European experience with BCR, which has resulted in the possibility to now seek authorisation from one "lead" authority in Europe in a process of mutual recognition. It is also why the APEC CBPR require certification under the CBPR in only the one APEC country in which the company or group of companies is headquartered.

Indeed, an effort is underway between APEC and the EU's Article 29 Working Party to explore ways to streamline the CBPR/BCR certification and approval processes where companies seek "dual certification" under both systems. Thus, the Centre recommends that any Brazilian counterparts to these mechanisms be designed so that they become "interoperable" with other similar cross-border transfer schemes, to ensure that companies that have certified or received approval under a non-Brazilian scheme can be deemed authorised in Brazil to the extent the requirements overlap and *vice versa*.

Furthermore, given the ever-increasing need for cross-border transfers of data, to avoid overwhelming any future Brazilian data protection authority, the draft should include a provision that allows for the use of pre-authorised standard contractual clauses both for transfers to controllers and transfers to processors (similar to those in the EU).

Finally, aside from data transfers that are subject to authorisation by the data protection authority in Art. 28 and those that are subject to consent in Art. 29, there should be a provision to allow for transfers of personal data in cases similar to the exceptions to consent in Art. 11 of the draft. Thus, transfers of data to third countries should be allowed under the same exceptions that exist with respect to consent for processing of data within Brazil. This is consistent with other privacy laws that also contain restrictions on cross-border data transfers.

Accordingly, we recommend the following amendments to the following articles:

Article 28

International transfer of personal data is only allowed for countries that provide a level of protection for personal data that is equivalent to the level established in this Law, with no prejudice to the following exceptions:

. . .

VI. – (new provision) When the transfer takes place under one of the conditions for which no consent is necessary under Article 11.

Article 30 – (regarding Authorisation in Art. 28 Section III)

The authorisation mentioned in section III of the main clause of art. 28 shall be granted

when the controller for the processing provides sufficient guarantees of compliance with the general principles of protection of the data subject's rights, presented in contractual clauses approved for a specific transfer, in standard contractual clauses, or in global corporate standards, under the terms of the regulations.

§ 1 The competent body may establish standard contractual clauses ***for controller to controller transfers and controller to processor transfers****, which shall comply with the general principles of protection of the data subject's data and rights, ensuring the joint liability of the transferor and the transferee, regardless of fault.* ***The use of standard contractual clauses will not be subject to individual authorisation mentioned in section III of the main clause of art. 28.***

§ 2 Any controllers and processors, or groups of controllers and processors, ~~that are part of the same economic group or multinational conglomerate~~ may submit ***enforceable*** *global corporate rules for approval by the competent body* ***or global corporate rules that have been approved by a foreign competent body, or may submit evidence of participation in a recognized enforceable cross-border code of conduct or privacy seal or mark,*** *~~which shall be mandatory for all the companies~~ ~~in the group or conglomerate~~ with no need for specific authorisations* ***to the extent these instruments comply*** *~~subject to compliance~~ with the general principles of protection and the data subject's rights.*

6. Data Transferred to Brazil and Consent

Article 32

In the event of an international data transfer from a foreign country to the national territory, processing in Brazil is only allowed when the operations performed in the foreign country have complied with its standards for obtaining consent.

Centre comments: Many jurisdictions (if not most) either do not require consent or provide for alternative bases or exceptions to consent for data use (*e.g.,* legitimate interest in the EU, or exceptions to consent in Singapore). Thus, any requirement that data transferred to Brazil for processing is subject to Brazilian consent requirements in the foreign jurisdiction will exclude data from most jurisdictions and will significantly undermine the ability of Brazilian companies to process foreign data. Indeed, this provision would preclude foreign controllers from using Brazilian processors located in Brazil and thus undermine the growing IT services industry in Brazil. We recommend that this requirement be removed.

7. Good Practices

Article 48

The parties responsible for personal data processing, individually or by means of associations, may formulate good practice rules establishing conditions for organisation, operational system, procedures, security regulations, technical standards, specific obligations for the various parties involved in the processing, training actions, or internal oversight

mechanisms, in compliance with the provisions in this Law and in complementary data protection statutes.

Sole paragraph. Good practice rules, made publicly available and update [sic], may be recognised and disseminated by the competent body.

Centre comments: The Centre welcomes this provision, which seems to accept the modern concepts of organizational accountability (corporate privacy programs) and organizational or industry codes of conduct. However, we recommend five areas in which the concept of "good practices" could be clarified and elaborated upon.

First, to ensure consistency globally, this provision might clarify that these "good practice rules" would encompass the full range of essential elements of "organizational accountability" as they are increasingly recognized in other international guidance on accountability and discussed in the work of the Centre. This would include internal oversight and verification, risk assessment, internal policies and procedures, training, internal enforcement and complaint handling. For more information on the essential elements and types of accountability *see* http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Data_Governance_Paper_2011.pdf.

Second, we recommend that any provision on good practices explicitly emphasize privacy risk management as an integral part of organizational accountability and as a necessary tool for effectively implementing and calibrating applicable legal requirements based on context and the actual privacy risks at hand.

Indeed, risk assessment mechanisms that are capable of assessing the risks *and* benefits to individuals of proposed data processing are increasingly important in the modern information age, not only in the context of big data, the Internet of Things and data processing on grounds other than consent, such as on grounds of "legitimate interest" and for purposes of determining the "compatibility" of additional new uses of data (*see* Sections 3 and 4 above), but also in connection with virtually all data processing. The key benefits of a risk management approach to data processing include the following:

- Privacy risk assessments help organizations determine whether and how to proceed with proposed information uses based on a better understanding of the actual or potential risks and harms they may cause to individuals. Specifically, understanding the likelihood and potential severity of harms to individuals that may result from proposed information uses in specific contexts allows organizations to devise appropriate and more targeted mitigations and controls and also facilitates weighing countervailing benefits of the proposed use against any residual risk of harms after mitigations have been implemented, before making any decision with respect to such use.

- Privacy risk assessments place the burden of privacy protection on the organization and are especially useful in situations where individual control and consent would be impossible or burdensome due to the absence of direct interaction with the individual or the complexity of the involved information processing, as is increasingly the case.

- Privacy risk assessments also reduce inefficient deployment of organizational resources by allowing organizations to prioritize their privacy controls according to the likelihood and severity of harm associated with a proposed data use. Such prioritization is likely to contribute to the overall effectiveness of privacy protections.

Thus, to become a truly effective privacy law in light of the demands of the modern information age, the proposed law should be sensitive to the fact that different types of data and different types of uses may present different levels of risk and thus require nuanced "risk-based" compliance responses. Accordingly, privacy risk assessment and privacy risk management should be integrated more prominently into the proposed law in appropriate places, including but not limited to the section on "good practices." For more information on the role of risk management in the context of privacy protections and good practice frameworks, please refer to two Centre white papers on the topic: "A Risk-based Approach to Privacy: Improving Effectiveness in Practice", available at http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/A_Risk-based_Approach_to_Privacy_Improving_Effectiveness_in_Practice.pdf and "The Role of Risk Management in Data Protection", available at http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF.

Third, the provision should also establish the incentives and advantages for companies to formulate or participate in such good practice rules. For example, companies that participate in such rules and are able to demonstrate good faith efforts of compliance in an enforcement proceeding might receive lower penalties in the event of a violation, which may be accounted for in Chapter VIII regarding "Administrative Penalties".

Fourth, the provision should clarify that these "good practice rules" could also serve as recognized cross-border transfer mechanisms, as described above in Section 5 on cross-border data transfers.

Fifth, it should be made explicit that the good practices rules apply to both controllers and processors, as both would benefit from implementing proactive privacy and security management programs.

By way of one specific textual amendment to incorporate a risk-based approach to compliance, we recommend the following text:

New Article ___:

In establishing good practice rules, controller and processor shall take into account the nature, scope and purpose of processing and the data, as well as the likelihood and severity of risks of harms to individuals.

8. Timeframe for Adoption

Article 52

This Law shall come into force within 120 (one hundred and twenty) days from its publication date.

Centre comments: We urge you to significantly extend this timeframe to enable companies to come into compliance with the new law. A reasonable timeframe would be at least one year.

9. Competent Authority

Centre comments: The draft law's many provisions cannot be implemented without the "competent authority" referenced throughout, yet the draft law does not address the creation of this authority. The experience with other data privacy laws and oversight around the world demonstrates that for this law to be effective, a single independent data protection and privacy enforcement authority ("competent authority") is essential and should be created simultaneously with the draft law. To ensure consistency in interpretation and enforcement of the law, it is important that there be a single national competent authority rather than multiple competent authorities.[4]

National data protection supervisory authorities and privacy enforcement authorities play an important role in oversight, application, interpretation, education and enforcement concerning national data privacy law. Much more so than courts, they have the necessary expertise to interpret privacy law with the nuance and flexibility appropriate to the circumstances. They also have an important role to play as ombudsmen in resolving complaints from individuals. Finally and significantly, they are indispensable to ensure a more harmonized and consistent approach to data privacy regulation and enforcement across borders. National data protection and privacy enforcement authorities work closely with each other through regional and international organizations such as the International Conference of Data Protection and Privacy Commissioners,[5] the Asia Pacific Privacy Authorities (APPA),[6] the Ibero-American Data Protection Network (RIPD), the APEC Cross-border Privacy Enforcement Arrangement (CPEA)[7] and the Global Privacy Enforcement Network (GPEN).[8] It is vitally important that Brazil be represented in these organizations through a national privacy authority.

---

[4] Most data protection laws provide for a single data protection authority. Even Japan, which provided for the various Ministries to oversee and enforce the application of Japan's data protection law in each of their respective areas of responsibility, is revising its law to provide for a single data protection authority. *See Outline of the System Reform Concerning the Utilization of Personal Data,* Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters), June 24, 2014, available at http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/07/English-Translation-of-Japanese-Government-Proposal-on-Privacy.pdf.

[5] http://icdppc.org/

[6] http://www.appaforum.org/

[7] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

[8] https://www.privacyenforcement.net/

III. Conclusion

Thank you for considering our comments and recommendations. If you have any questions or require further information, please contact Bojana Bellamy, President, Centre for Information Policy Leadership (bbellamy@hunton.com) or Markus Heyder, VP and Senior Policy Counselor, Centre for Information Policy Leadership (mheyder@hunton.com).