Centre for Information Policy Leadership
Hunton & Williams LLP

25 August 2017

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE
PUBLIC CONSULTATION ON THE BRAZILIAN STRATEGY FOR DIGITAL TRANSFORMATION

The Centre for Information Policy Leadership at Hunton & Williams LLP (CIPL)[1] welcomes this opportunity to respond to the Brazilian Ministry of Science, Technology, Innovation and Communications (MCTIC) on its initiative to develop the Brazilian Strategy for Digital Transformation (the "Strategy"). While the Strategy deals with several themes, CIPL's response primarily concerns the aspect of confidence in the digital environment. CIPL believes that having a single national and independent data protection authority (DPA) is critical to a safe and reliable digital environment. Designating such a national authority responsible for the protection of personal data ensures effective privacy protections for individuals, responsible and accountable uses of personal information by organizations, the promotion of best practices with respect to the use of personal information, effective engagement with global DPAs on privacy policy and enforcement cooperation matters, and is essential for enabling the modern data economy and innovation.

1. Designation and Purpose of a Central Data Protection Authority

Confidence in the digital environment can be promoted through the designation of a central and independent DPA. It is important that there be a single national competent authority rather than multiple competent authorities for several reasons. The experience with other data privacy laws and oversight around the world demonstrates that a centralised authority ensures:

- Consistency in the interpretation and enforcement of data protection law;
- Uniform guidance, education efforts and advice on data protection matters;
- Consistent enforcement procedures;
- Uniform standards and best practices for organisations;
- Avoidance of forum shopping by consumers who submit complaints or by organisations facing sanctions for non-compliance, unfair or deceptive practices or other unacceptable behaviour.

[1] CIPL is a privacy and data protection think tank in the law firm Hunton & Williams LLP and is financially supported by the law firm and 54 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. For more information, please see the CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm Hunton & Williams.

- Harmonisation of data protection across borders with other nations;

- One point of contact with regional and international organisations such as the International Conference of Data Protection and Privacy Commissioners (ICDPPC), the Ibero-American Data Protection Network (RPID), the Asia Pacific Privacy Authorities (APPA), the APEC Cross-border Privacy Enforcement Arrangement (CPEA), the Global Privacy Enforcement Network (GPEN) and others;

- One point of contact for international DPAs for cross-border enforcement matters; and

- One national agenda (which takes into account the view of all relevant stakeholders) for the development of data privacy law and practices unhindered by multiple competing agendas by several authorities.

A central "expert" authority will represent Brazil on data protection issues with one voice both domestically and internationally. Its mission will be to stay up to date on the development of technology, relevant business practices and privacy concerns and to implement measures that can practically and effectively address the issues while ensuring the advancement of technological innovation and the growth of the digital market. On the international scale, the central authority will speak for Brazil on global data protection policy issues and work and cooperate with foreign counterpart data protection authorities on cross-border privacy enforcement matters. Multiple authorities, however well-intentioned, cannot achieve such goals. Designating a single competent authority will ensure strong leadership, flexibility and most importantly confidence for Brazil's digital environment. Moreover, this central authority should be functionally and operationally independent from the government, particularly with respect to its investigations, enforcement decisions, leadership and staffing matters, as such independence is a relevant criterion for membership and effective participation in certain global DPA organizations, such as the ICDPPC.

2. Ensuring that the Central DPA is Effective

Confidence in the digital environment can be enhanced by the designation of a single competent DPA provided that the DPA is given a clear role which it can perform effectively. Maximising DPA effectiveness is a complex task. Their functions are numerous, expectations are high and resources likely are limited. DPAs cannot do everything and therefore they must be able to make difficult but essential choices about strategies and priorities. DPAs must also adopt modern and strategic approaches to regulation that achieve best outcomes for individuals, society and regulated organisations. This involves responsively engaging with and supporting businesses which are seeking to handle personal information well, while also dealing firmly with those who are not trying. CIPL defines this approach as a results-based approach. The foundations of a results-based approach can be summarized by the following high-level principles:

- Regulating for results requires an independent DPA to have the mandate to be strategic, effective, co-ordinated and transparent;

- A DPA should be able to produce cost effective outcomes which protect individuals in practice, promote responsible data use and facilitate prosperity and innovation;

- A DPA should give top priority to securing protection for individuals;

- A DPA should transparently spell out the outcomes it is seeking and the priorities and approaches it will adopt to achieve those outcomes;

- A DPA should be able to collaborate and co-ordinate policy and enforcement priorities and approaches with foreign counterpart DPAs to improve consistency in a global data economy as much as possible.

- A DPA should treat regulated organisations in a consistent manner – adopting similar approaches across and within sectors;

- A DPA should adopt a risk-based approach to all its activities, basing policy and enforcement priorities on conduct that creates the most harm to individuals or to democratic and social values;

- An approach of constructive engagement with industry with the emphasis on leadership, information, advice, dialogue and support should be adopted rather than excessively relying on deterrence and punishment;

- A DPA should foster open and constructive relationships with businesses handling personal information, based on honest dialogue and mutual co-operation, but without blurred responsibilities;

- Regulated organisations should be assessed in particular by reference to demonstrable good faith and due diligence in their efforts to comply;

- Organisations trying to behave responsibly should be encouraged to identify themselves, for example, by transparently demonstrating their accountability, their privacy and risk management programmes, the influence of their DPOs and their use of seal or certification programmes, codes of conduct, Binding Corporate Rules (BCR), APEC Cross-Border Privacy Rules (CBPR) and other accountability frameworks.

- Punitive sanctions should be mainly targeted on non-compliant activity that is deliberate, wilful, seriously negligent, repeated or particularly serious;

- Complaints should be tightly managed as they can distract from more strategic DPA activity and can be very resource intensive. There should be no requirement to investigate each and every complaint but rather a DPA should be able to choose which

cases to investigate carefully while also taking into account that complaints are a valuable source of intelligence.

3. Potential Challenges for a National Authority for Data Protection

There typically are particular challenges associated with the designation of a national authority for data protection that are important to consider and address. These include provision of adequate DPA resources and overcoming regulatee scepticism while finding the appropriate level and modes of constructive engagement with the regulated entities, among others.

- **Provision of adequate DPA resources**: In order to carry out their tasks effectively, DPAs must be adequately resourced. The most recent comparative survey of DPA budgets was carried out as a census by the ICDPPC in 2017[2]. For 26 EU countries[3] that provided data, the total budget for these authorities in 2016 was €205,703,574 for a total population for that year of 507,471,970.[4] This would suggest, across these 26 countries as a whole, that the budget per citizen was less than €0.41. This is very meagre funding and demonstrates the limited resources available to each DPA. We understand however that some substantial budget increases are being implemented in EU states or are under active consideration. To ensure the effectiveness of its DPA and in turn promote confidence in the digital environment, Brazil will need to ensure that it provides adequate financial resources and take its DPA into account when forming the country's annual budget. Some DPAs already receive income from chargeable services such as auditing, training and publications. DPAs should, at all costs, avoid trying to fund themselves by imposing non-compliance fines on those they regulate. Any such attempt will be highly controversial and open to ethical, political and legal challenge. A possible source of income may be to charge a modest fee each year to all organisations processing personal data (in reality probably all businesses and public bodies). . Considering Brazil's size and number of regulated businesses, a fee of just 75 Brazilian Real would generate millions in Revenue to assist the DPA to carry out their functions effectively. A well-resourced DPA provides confidence to the public that their data privacy rights are being protected by an organisation that has the means to do so.

- **Regulatee Scepticism**: As Brazil does not currently have a national data protection authority, there may be some resistance in working with the DPA by those whom the authority would regulate. Although engagement with regulated organisations is essential and should be promoted as it constitutes one aspect of the effective DPA, some regulated organisations may be inclined to keep their distance from a DPA

[2] The census data is available upon request from the International Conference of Data Protection and Privacy Commissioners Secretariat, https://icdppc.org/the-conference-and-executive-committee/icdppc-census/.
[3] Figures were not available for Austria or Croatia and the figure for Germany is lower than the actual value as only 7 out of 16 Länder provided data.
[4] Population figures for the 26 relevant EU countries were sourced from the World Bank on 27 July 2017, http://data.worldbank.org/indicator/SP.POP.TOTL.

because of fear of receiving penalties for past misconduct, having documents or practices disclosed to the DPA during consultations and then used against them in an enforcement matter, or fear of veto for a planned innovation. To avoid this risk, it is up to the DPA to establish mutual trust with the regulated organisations and promote an environment of support and collaboration. Doing so will generate confidence in the digital environment for organisations.

Conclusion

We hope the above provides useful insight into how Brazil can promote confidence in the digital environment and how to adapt their strategy on digital transformation going forward. The present comment represents a brief summary of a discussion paper entitled "Regulating for Results in the Digital World: Strategies and Priorities for Leadership and Engagement", which CIPL will be releasing at the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong in September 2017. We will submit this paper to you when it is published as a follow-on to this comment for further elaboration on our points above. We would also be delighted to discuss any aspect of our thinking which may specifically assist the Brazilian initiative.

If you would like to discuss any of these issues further or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.