30 January 2018

Comments by the Centre for Information Policy Leadership

on the Indian Ministry of Electronics and Information Technology's

White Paper of the Committee of Experts on a Data Protection Framework for India

The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to submit brief comments to the "White Paper of the Committee of Experts on a Data Protection Framework for India" (the "White Paper").

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 59 member companies that are leaders in key sectors of the global economy. CIPL is based in London, Washington D.C. and Brussels. (The White Paper cites to some of CIPL's earlier work on "accountability.") CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see 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 of Hunton & Williams.

The White Paper is exemplary in its thoroughness and clarity. It identifies and articulates the most important challenges and issues associated with effectively protecting privacy while also enabling the modern digital economy and beneficial uses of personal data. Due to the short deadline and multiple conflicting obligations and commitments during the comment period, our comments are brief, touch only on a few select issues and rely mainly on submitting earlier CIPL white papers, public comments to other consultations and articles that directly address or are relevant to the questions posed in the White Paper. However, we look forward to future opportunities to provide additional information and comments and to more extensively engage in India's process to develop an effective and modern data protection law.

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

Comments on Part II
Scope and Exemptions

1. Cross-Border Flow of Data

Cross-border data flows are essential to the modern digital economy. A large portion of CIPL's work has been focused on the question of how to ensure free and accountable data flows across borders. The preferred model for accomplishing this in our view is the "accountability" model, pursuant to which organizations would be responsible and accountable for ensuring that personal data they collect and transfer to third parties and countries remains protected at the same level as it was under the laws that applied at the point of collection. This is essentially the model of Canada and the United States. In countries that include data transfer restrictions in their data protection laws, it is important to include cross-border transfer mechanisms enabling cross-border transfers despite such restrictions and to ensure that these mechanisms mirror and/or are able to work with the same or similar mechanisms in other jurisdictions. Such cross-border transfer mechanisms include, EU Binding Corporate Rules (BCR), APEC Cross-Border Privacy Rules (CBPR), APEC Privacy Recognition for Processors (PRP), Standard Contractual Clauses (SCC), the EU-US Privacy Shield, other certifications and codes of conduct and similar schemes. Key to developing effective cross-border transfer mechanisms is that they are "interoperable" with other such mechanisms globally. This is important to avoid the inefficiencies, costs and other negative consequences of duplicative or even conflicting cross-border transfer schemes and to provide global businesses with global data transfer solutions.

Please see the following relevant CIPL white papers and consultations for a more detailed discussion of these issues:

- Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, CIPL, 25 September 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf.

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's Working Documents Setting Up Tables for Binding Corporate Rules and Processor Binding Corporate Rules, 17 January 2018: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_bcr_working_documents_wp256_and_wp257_.pdf

- CIPL Response to the Consultation by the Irish Data Protection Commissioner on the Topics of Transparency and International Data Transfers under the GDPR, 13 October 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_irish_dpc_consultation_on_transparency_and_international_data_transfers_under_the_gdpr.pdf

- CIPL Response to the Consultation by the Commission Nationale De L'Informatique et des Libertés on the Topics of Transparency and International Data Transfers under the GDPR, 19 October, 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_cnil_consultation_on_transparency_and_international_data_transfers_under_the_gdpr.pdf

- CIPL Discussion Paper on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, 12 April 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf

- CIPL Discussion Points on Brazil Proposed Data Protection Legislation 5276/2016 – Ministry Bill, 1 June 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_discussion_points_on_brazil_ministry_bill_5_april_2017__1_june_2017_.pdf

2. Data Localisation

Data localisation requirements generally work at cross-purposes with the global free flow of data (which is of utmost importance to the modern digital economy and societal advancement). In addition, localisation requirements typically do not effectively advance their specific stated or unstated goals, such as increasing data security, promoting domestic industry, lowering cost for domestic business, and creating local jobs. For an insightful discussion of this topic, please see:

- Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity, US Chamber of Commerce and Hunton & Williams, 2014: https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf

Note also that the Asia-Pacific Economic Cooperation forum (APEC) recently amended the APEC Privacy Framework to explicitly discourage and limit restrictions on cross-border data flows of personal information. See APEC Privacy Framework, 2015, Part IV. B.iv, paragraphs 69 and 70, page 31 (and Part IV.B.iii, paragraph 65, page 30): https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf

Comments on Part III
Grounds of Processing, Obligation on Entities and Individual Rights

1. Consent

The role of consent in the modern digital environment has been one of CIPL's principal areas of concern. Given the increasing complexity and sheer volume of personal data processing, obtaining valid and informed consent is becoming increasingly challenging, not least

because of the problem of consent fatigue. CIPL believes that consent has an important role to play in circumstances where it can be effective, i.e., where individuals can be effectively informed about their choices and are able to make a choice. Where that is not possible or practicable, as is increasingly the case in many contexts, other legal bases that provide effective protections for the individual must be made available and relied upon. These include the important "legitimate interest" legal basis that is found in the EU Data Protection Directive and also in the EU General Data Protection Regulation (GDPR). (We have submitted separate comments on "legitimate interest" further down in this consultation). Also, other concepts, mechanisms and protections must be employed to protect individuals from harm resulting from data processing, especially where consent is not available. These include the concepts of organizational accountability, risk-assessments, privacy by design, proper oversight and training of relevant employees, among others. CIPL has previously addressed the issue of consent in detail in a number of relevant papers, public consultations and articles, including the following:

- CIPL Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, May 19, 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

- CIPL's comments to the WP29's Proposed Guidelines on Consent, 29 January 2018: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf

- Bellamy and Heyder, CIPL, Empowering Individuals Beyond Consent, 2 July 2015: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/empowering_individuals_beyond_consent.pdf

2. Notice

The issue of notice, and more broadly "transparency", has been a key focus of CIPL's work. Notice and transparency are not just important prerequisites for obtaining valid and informed consent, they underlie all aspects of an effective digital economy that depends on trust by individuals as well as by regulators. As the information-based economy becomes more and more complex and data processing and sharing become ubiquitous, providing effective "transparency" with respect to such processing is becoming increasingly difficult but also increasingly important. Thus, any modern information law must account for this challenge and must enable a sensible approach to providing information to individuals that is both user-friendly as well as sufficiently comprehensive to provide individuals with the information they need. One important goal of transparency must be to help individuals understand the value exchange between them and the organizations and the benefits of data processing. Another goal is to demonstrate to individuals that organizations are taking necessary steps to mitigate and protect them against potential risks that may be associated

with the data processing. Combined, these goals will advance consumer trust in the digital economy. CIPL has previously prepared the following materials on this topic:

- CIPL Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, May 19, 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

- CIPL/Telefonica, Reframing Data Transparency, 30 June 2016: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/reframing_data_transparency.pdf

- CIPL's comments to the WP29's Proposed Guidelines on Transparency, 29 January 2018: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_transparency-c.pdf

- CIPL Response to the Consultation by the Irish Data Protection Commissioner on the Topics of Transparency and International Data Transfers under the GDPR, 13 October 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_irish_dpc_consultation_on_transparency_and_international_data_transfers_under_the_gdpr.pdf

- CIPL Response to the Consultation by the Commission Nationale De L'Informatique et des Libertés on the Topics of Transparency and International Data Transfers under the GDPR, 19 October, 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_cnil_consultation_on_transparency_and_international_data_transfers_under_the_gdpr.pdf

- Heyder, CIPL, Transparency and the Future of Driverless Privacy, 20 November 2015: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/transparency_and_the_future_of_driverless_privacy.pdf

3. Other Grounds of Processing

Including grounds for processing other than consent is essential in the modern information age. Given the increasing complexity and sheer volume of personal data processing, obtaining valid and informed consent is becoming increasingly challenging, not least because of the problem of consent fatigue. CIPL believes that while consent has an important role to play in circumstances where it can be effective, i.e., where individuals can be effectively informed about their choices and are able to make a choice, where that is not possible or practicable, as is increasingly the case in many contexts, other legal bases that

provide effective protections for the individual must be made available and relied upon. These include the important "legitimate interest" legal basis that is found in the EU Data Protection Directive and also in the EU General Data Protection Regulation (GDPR). CIPL has written extensively about the importance of the legitimate interest legal ground. CIPL has also more generally written about the risk-based approach to privacy as well as risks assessments and "data protection impact assessments", which are an essential component of the legitimate interest ground for processing. Finally, the risk-based approach and the proper use of risk assessments and data protection impact assessments must be seen in the larger context of organisational accountability, of which they are an essential component. CIPL has written extensively on organizational accountability (indeed the White Paper cites to some of CIPL's accountability materials, see footnotes 670 and 673):

- CIPL Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, (see also APPENDIX II "CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data" – Part I: Summary of categories and examples of legitimate interest processing and Part II: Specific case studies [of legitimate interest]), May 19, 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

- CIPL white paper "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", 21 December 2016: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", 19 May 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf

- CIPL white paper "A Risk-based Approach to Privacy: Improving Effectiveness in Practice", 19 June 2014: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf

- CIPL white paper "The Role of Risk Management in Data Protection", 23 November 2014: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf

- CIPL white paper "Protecting Privacy in a World of Big Data, Paper 2 — The Role of Risk Management", 16 February 2016: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf

- CIPL white paper "Protecting Privacy in a World of Big Data, Paper 1 — The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society", 21 October 2015: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

4. Purpose Specification and Use Limitation

Purpose specification and use limitation must be applied in a way that is consistent with the modern information economy (e.g. big data, the IoT, AI and machine learning) where beneficial uses of data may not always be known at the point of collection and may be inappropriately eliminated by these concepts. Data protection rules should not unnecessarily prevent beneficial uses of data for societal and scientific progress or for the benefit of individuals where appropriate mechanisms are available to protect individuals from harmful processing. Such protections may include the full range of elements comprising "organisational accountability", including privacy by design, risk assessments and effective mitigations (such as anonymisation), oversight and training, and consumer redress and complaint mechanisms. A more flexible approach that relates the permissibility and means of processing data for previously unknown and unknowable purposes to the specific risks and the mitigations against it would more effectively balance privacy with innovation, growth and societal progress. CIPL has written extensively on how "organizational accountability" can be used to broaden the permissible uses of personal data without sacrificing personal data protection.

- CIPL white paper "Protecting Privacy in a World of Big Data, Paper 1 — The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society", 21 October 2015: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

- Heyder, CIPL, "Tackling the Risks of Big data", IAPP Perspectives 24 September 2014: https://iapp.org/news/a/tackling-the-risks-of-big-data/

5. Individual Participation Rights

CIPL has addressed the issue of **algorithmic transparency** in two of its recent papers, addressing some of the challenges associated with this issue. In addition, CIPL has recently

initiated a new work stream specifically on accountable machine learning and AI, with the goal of producing at least two white papers on the subject in the coming months, which we hope to share with global stakeholders:

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Automated Individual Decision-Making and Profiling", 2017, 1 December 2017, pp. 16-17: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf

- CIPL Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, 19 May 2017, pp. 8-9: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

6. Individual Participation Rights

To the extent India decides to include a **right to data portability**, it should be kept in mind that this is a new right raising significant practical, technical, legal and policy challenges. CIPL has recently addressed several data portability issues in response to the EU's Article 29 Working Party proposed guidelines on data portability:

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability", 15 February 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf

Automated decision making will be central to virtually all data processing in the digital age. As such, great care should be taken in devising and implementing rules in relation to automated decisions affecting individuals. Overly restrictive rules that broadly preclude such decisions and/or that require human intervention under too many circumstances, are likely to significantly stifle modern data processing and undermine its key benefits. Indeed, a right to human intervention and review of automated decisions must be limited to cases in which the decisions have a legal effect or similarly significant effect and "similarly" and "significant" must be interpreted narrowly to only impact cases where the decisions are capable of a truly profound impact on the individual's life. CIPL has recently addressed these issues in response to the EU's Article 29 Working Party proposed guidelines on automated decision making and profiling:

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Automated Individual Decision-Making and Profiling", 1 December 2017:

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf

Comments on Part IV
Regulation and Enforcement

1. Enforcement Models

Self-regulatory and/or co-regulatory models of enforcement can play a significant role in improving privacy protections for individuals. For example, by providing specific data protection requirements consistent with the governing data protection law, they promote compliance by participating businesses and promote more efficient oversight, consumer redress and complaint handling and enforcement. Moreover, insofar as they rely on third-party certification bodies or "Accountability Agents" (as the APEC CBPR system calls them) to review, certify, provide consumer redress mechanisms and front-line enforcement of such schemes, they significantly augment the capabilities and reach of data protection authorities (DPAs) who have limited resources for such hands-on and day-to-day oversight activities. They enable data protection authorities to step in and provide backstop enforcement of these schemes only in the most serious cases involving the most egregious violations, thereby freeing up valuable DPA time and resources for other priorities and widening the general scope and reach of data protection. CIPL has done extensive work on these issues and promoted these self- or co-regulatory models over the years. Here are two recent white papers and an article addressing key aspects of this issue:

- CIPL Discussion Paper on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, 12 April 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf

- Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, CIPL, 25 September 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf

- Bellamy, The Rise of Accountability from Policy to Practice and Into the Cloud, IAPP Privacy Perspectives, 10 December 2014: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_rise_of_accountability_from_policy_to_practice_and_into_the_cloud.pdf

2. Accountability

CIPL has been instrumental in developing the concept of "accountability" and socializing it globally. In fact, the White Paper cites to one of our earlier papers on the topic. See footnotes 670 and 673. Accountability must be at the core of all modern data protection frameworks. Organisations' information management and data protection programs implementing the elements of organizational accountability (including, risk assessment, policies and procedures, privacy by design, transparency, training and awareness, monitoring and verification, response, complaint handling and enforcement, and leadership and oversight) will not only ensure maximal compliance with applicable data protection laws, but also generate the public trust necessary for the effective use of personal data for a wide range of beneficial purposes. In addition to the CIPL materials you have already reviewed, we refer you to the following additional and more recent writings on this topic:

- CIPL white paper "Protecting Privacy in a World of Big Data, Paper 1 — The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society", 21 October 2015: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

- Bellamy, CIPL, "The Rise of Accountability from Policy to Practice and Into the Cloud", IAPP Perspectives, 10 December 2014: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_rise_of_accountability_from_policy_to_practice_and_into_the_cloud.pdf

3. Codes of Practice

As discussed above under Question 1.4.1 under Part IV, Chapter 1, codes of practice as well as certifications can play an important role in a modern data protection regime. The following two CIPL papers discuss the role of such mechanisms both as compliance or accountability mechanisms and as cross-border transfer mechanism:

- CIPL Discussion Paper on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, 12 April 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf

- Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, CIPL, 25 September 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf

4. Personal Data Breach Notification

Data breach notification requirements can be an important accountability tool. However, care should be given that any such requirements, including reporting time-lines, are based on appropriate risk or harm thresholds and take into account the various steps an organization may have to take to investigate the breach before being in a position to notify individuals or a regulator. CIPL strongly urges India to consult the US experience with its data breach notification regimes, as well as relevant industry stakeholders in developing sensible and workable data breach notification requirements. CIPL has recently commented on the EU Article 29 Data Protection Working Party's proposed data breach notification guidelines, addressing some of these issues:

- Comments by the Centre for Information Policy Leadership On the Article 29 Working Party's "Guidelines on personal data breach notification under Regulation 2016/679", 1 December 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_breach_notification.pdf

5. Additional Obligations on Data Controllers

Data Protection Impact Assessment

An effective modern data protection law must apply a risk-based approach. In essence, this means that organisations must assess the risks to individuals of their data processing activities and implement appropriate mitigations for these risks. Risk assessments enable the identification of high-risk activities and the prioritizing of effective mitigation measures for these high-risk activities. They also allow a proper identification and weighing of the expected benefits of the processing activity at hand and a balancing of the respective interests of relevant stakeholders — the business, individuals, and society. Data Protection Impact Assessments (DPIAs) essentially are such a risk assessment. Under the EU General Data Protection Regulation (GDPR), DPIAs are a type of risk assessment specifically for "high risk" processing activities. CIPL has pursued a separate work stream on the risk-based approach to privacy, risk assessment and DPIAs and has published several papers on the topic and commented on the GDPR's risk assessment provisions:

- CIPL white paper "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", 21 December 2016: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", 19 May 2017:

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf

- CIPL white paper "A Risk-based Approach to Privacy: Improving Effectiveness in Practice", 19 June 2014: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf

- CIPL white paper "The Role of Risk Management in Data Protection", 23 November 2014: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf

- CIPL white paper "Protecting Privacy in a World of Big Data, Paper 2 -- The Role of Risk Management", 16 February 2016: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf

- Heyder, CIPL, "Tackling the Risks of Big data", IAPP Perspectives 24 September 2014: https://iapp.org/news/a/tackling-the-risks-of-big-data/

Data Protection Officer

A data protection officer, chief privacy officer or otherwise titled person responsible for an organizations data protection and privacy program is a crucial component of data protection. CIPL has written extensively on the role, responsibilities and necessary qualifications of the data protection officer. We refer you to the following CIPL papers on the topic:

- CIPL white paper "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation", 17 November 2016: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf

- Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Officers (DPOs)" 24 January 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipls_comments_on_wp29_dpo_guidance_24_january_2017.pdf

- CIPL, "The Role and Function of a Data Protection Officer in the European Commission's Proposed General Data Protection Regulation," (2013): https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_fu

nction_of_dpo_in_the_eu_commissions_proposed_general_data_protection_regulation__discussion_paper_.pdf

- CIPL, "The Role and Function of a Data Protection Officer in Practice and in the European Commission's Proposed General Data Protection Regulation: Report on DPO Survey Results," (2015): https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_a_dpo_in_practice_report_on_survey_results.pdf

6. Data Protection Authority

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.

However, given the size of the country and the many responsibilities of such an authority, it is crucial to also develop mechanisms and processes that augment the capabilities and reach of this centralized authority. These include as data protection codes of conduct and certification schemes run by third-party certification organizations or "Accountability Agents" that have operational responsibility for these mechanisms, including the review and certification process, providing consumer redress mechanisms and front-line enforcement of such schemes (but are subject to oversight and enforcement by the DPA in appropriate cases) (See discussion above on "enforcement models").

CIPL has written extensively on these issues, focusing in particular on specific recommendations on how to maximize the effectiveness of DPAs through results- and risk-based prioritization of their many responsibilities and constructive engagement with industry. Please review the following discussion paper and public consultation paper:

- CIPL discussion paper "Regulating for Results, Strategies and Priorities for Leadership and Engagement, 10 October 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement__2_.pdf

- Centre for Information Policy Leadership Response to the Public Consultation on the Brazilian Strategy for Digital Transformation, 25 August 2017: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_-_public_consultation_on_the_brazilian_strategy_for_digital_transformation__english_.pdf