

BUILDING BRIDGES TO FOSTER SUSTAINABLE DATA FLOWS AMONGST THE BRICS COUNTRIES

Walter Britto Gaspar and Luca Belli

Abstract

This concluding chapter focuses on the possibilities of BRICS countries' cooperation regarding the personal data flows, trying to understand which types of mechanisms would be more suitable to foster sustainable transborder data exchanges, to foster digital trade and cooperation while guaranteeing that data subjects rights are respected, and cybersecurity is fully enforced. The elements of convergences and divergences in the BRICS frameworks regulating data transfers reveal idiosyncrasies of each country's jurisdiction and approach to personal data regulation. Even where the rules converge amongst BRICS countries, it is interesting to observe the small differences that exist, which point to the juridical specificities of each system and the often-heterogeneous manners for implementing similar normative prescriptions through regulatory techniques. This chapter provide an overview of the main regulatory strategies adopted by the BRICS countries to frame international data transfers, comparing these approaches to subsequently identify what could be the most promising path for cooperation in data governance. Lastly, we dare proposing some concrete guidance regarding how such cooperation could be enacted by the BRICS grouping, leveraging the existing venues to enhance their digital cooperation.

CONTENTS

1. Fostering sustainable data flows in the BRICS countries, towards a global framework for data governance	1
1.1. Introduction	1
1.2. A shared data protection skeleton.....	3
1.3. Innovative BRICS Data Protection Practices	6
1.3.1. Brazil and the LGPD implementation: the National Council of Data Protection and Privacy and the influence of the consumer protection framework.....	6
1.3.2. Freely Shareable Personal Data, Opt-out, and Data Localization in Russia	8
1.3.3. The Indian Data Empowerment and Protection Architecture	10
1.3.4. China's facilitative regulation, institutional coordination, data security approach and the normative innovation of the Personal Information Protection Law (PIPL).....	13
1.3.5. The South African framework: POPIA's scope and the nature of the DPA and of the DPO	16
1.4. Governmental access to personal data in the BRICS	17
1.5. Data Protection in the new BRICS: Egypt, Ethiopia, Indonesia, Saudi Arabia, the United Arab Emirates, and Iran.....	21
1.5.1. Egypt.....	21
1.5.2. Ethiopia.....	22
1.5.3. Indonesia	23
1.5.4. Saudi Arabia.....	24
1.5.5. United Arab Emirates	25
1.5.6. Iran	26
1.6. Transborder data transfers in the BRICS	26
1.6.1. Consent and adequacy decisions	27
1.6.2. A BRICS-led approach to international data transfers rules	29
1.7. A principle-based approach for data governance cooperation in the BRICS and Beyond .	32
1.8. From shared Model Contractual Clauses to a BRICS-led data governance framework.....	36
1.9. Conclusions	38
1.10. Annex: model contractual clauses for the transfer of personal data from controller to controller/processor in the BRICS countries.....	41

1. FOSTERING SUSTAINABLE DATA FLOWS IN THE BRICS COUNTRIES, TOWARDS A GLOBAL FRAMEWORK FOR DATA GOVERNANCE

1.1. Introduction

This book has explored a wide range of issues regarding the emerging data architectures of the BRICS members. Each of these countries have built or considerably restructured its national data protection framework over the past five years, taking inspiration from similar models and engaging in several types of legal transplants, but introducing also important elements of innovation. Particularly, we can highlight that Russia and South Africa, having been the first two BRICS countries to legislate on the matter, have drawn strong inspiration from the “classic” European model, while Brazil, China and India can be seen as latecomers, thus having had the time to introduce more original and novel elements in their systems¹.

China and India, particularly, have introduced the highest level of innovation in their regulatory models, which are amongst the most recent and the most original in the realm of data protection laws, as we will discuss in the forthcoming sections. Possible hypotheses for their willingness to develop an original model are intrinsic characteristics of these two countries, besides the specific traditions and characteristics of their legal systems. For instance, their size might exempt these countries from being guided out from external pressures and demands regarding their data protection choices, thus allowing them to enjoy greater leeway to craft their regulations more independently. Hence, the main preoccupations of China and India may be meeting their internal demands and adopting their own pace, rather than regulating to keep pace with Europe. Social and political circumstances are also to be considered, such as the greater flexibility with which state actors can move and the greater coordination they enjoy, including regarding the implementation of data protection legislation.

This concluding chapter focuses on the possibilities of BRICS countries’ cooperation, to foster convergence and legal interoperability regarding the regulation of personal data flows. It builds on the previous chapters’ descriptions and analysis of BRICS data protection frameworks to highlight converging and diverging points, as well as innovative normative developments in BRICS jurisdictions. This is showcased in the image of a shared data protection skeleton on top of which BRICS countries can build efforts of legal interoperability, with particular focus on fostering sustainable transborder data exchanges, digital trade and cooperation while guaranteeing that data subjects’ rights are respected, and information security is fully enforced.

As it emerged along the chapters of this volume, besides convergences and space for cooperation, there are also significant gaps and divergences between the data governance models adopted by these countries. The upcoming sections will first highlight some key points of convergence that give rise to a shared data protection skeleton that can support legal interoperability ambitions of the grouping. Subsequently we will stress what are the most innovative elements of the BRICS frameworks and to what extent they diverge. We will also stress that BRICS countries foresee large exceptions for governmental access to personal data, an element that should be considered carefully when crafting strategies aimed at enhancing legal interoperability. Moreover, as we will discuss, the entrance of new

¹ Luca Belli, ‘New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a Post-Western Model of Data Governance’ (2022) 18 *Indian Journal of Law and Technology* 1
<<https://www.ijlt.in/journal/new-data-architectures-in-brazil%2C-china%2C-and-india%3A-from-copycats-to-innovators%2C-towards-a-post-western-model-of-data-governance>> accessed 7 March 2023.

countries in the BRICS grouping adds a new layer of complexity as a larger number of national idiosyncrasies needs to be considered. The careful consideration of these elements is particularly relevant to avoid that existing divergences hinder the BRICS ambitions of developing “a global framework for data governance, including cross-border data flows, to [...] ensure the interoperability of data regulatory frameworks at all levels.”²

Importantly, as we have anticipated in the introductory chapter of this volume, the promotion of legal interoperability in data governance can be seen as a form of collective exercise of data sovereignty,³ through the joint definition of shared regulatory strategies which can promote secure international data flows, while respecting national legislation. Data sovereignty is a concept that can be defined as “the capacity to understand how and why (personal) data are processed and by whom, develop data processing capabilities, and effectively regulate data processing, thus retaining self-determination and control.”⁴ In this perspective, the elaboration of shared data governance arrangements, particularly as regards data transfers, aims at allowing multiple parties - spanning from the BRICS members to potentially all UN members - to agree upon common solutions, enhancing transparency, accountability and security of data processing, thus constructing a multilateral approach to data sovereignty. In fact, the establishment of shared data governance mechanisms is instrumental to extend the reach of data subjects’ rights, and increase legal certainty for data controllers as well as for regulators, while promoting cooperation as regards research, development, and trade.

As we will argue in this chapter, there are multiple paths to foster legal interoperability. These span from the adoption of binding international agreements, negotiated at the international level, which can establish shared data protection standards and facilitate institutional cooperation; to the adoption of mutual adequacy decisions by national regulatory authorities, recognising the respective frameworks of the BRICS members as equally protective; or the use of standard contractual clauses, that can be approved by regulators and incorporated in contracts to bind contractual parties to the respect of shared data governance requirements; or the mutual recognition of binding corporate rules that multinational companies generally include in their internal policies to frame data governance.

These options are not mutually exclusive and can be combined. However, the former two strategies mentioned above are considerably more complex due to their bureaucratic nature, while the latter two may be much easier to implement as they rely on contractual tools, thus making them inherently more agile and easier to adopt. Aware of the existing heterogeneities and similarities amongst BRICS data protection frameworks, this chapter will provide some concrete suggestions of potential paths to be pursued to promote legal interoperability, after having discussed the main convergences and divergences of the BRICS data protection regimes.

Notably, in the final part of this chapter, we adopt a proactive approach, distilling a set of shared principles that can be seen as the conceptual basis of both BRICS and global data governance frameworks and will emphasize that model contractual clauses are likely the most palatable and realistic option to foster a shared BRICS data governance solution. In this perspective, the final Annex to this chapter will provide a concrete proposal of Model Contractual Clauses for Data Transfers in the BRICS Countries, explaining how such clauses may look like. Importantly, the BRICS countries should

² BRICS. Kazan Declaration “Strengthening Multilateralism For Just Global Development And Security”. XVI BRICS Summit. Kazan, Russia. (23 October 2024). Paragraph 71. <https://dirco.gov.za/xvi-brics-summit-kazan-declaration-strengthening-multilateralism-for-just-global-development-and-security-kazan-russian-federation-23-october-2024/>

³ See Belli, Gaspar and Singh (2024), *supra* n (91).

⁴ *Idem*.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

be seen as a laboratory for data governance. Indeed, given their heterogeneity, we can argue that the approaches that can work at the BRICS level may be likely scaled up at the global level.

1.2. A shared data protection skeleton

Based on our analysis, we can identify a non-exhaustive but telling list of policy elements around which BRICS data protection frameworks are converging.⁵ Due to the relatively recent development of the BRICS data protection framework, decision makers in these countries have enjoyed the privilege of constructing their legal frameworks based on existing best practices and, as we will highlight, also to find creative solutions for problems that other legislators have not been able to tackle properly.

A patent example of convergence is the definition of personal data in itself, which all BRICS consider as the information related to an identified or identifiable natural person, although, interestingly, the South African framework extends the protection further, encompassing data related to legal persons also, as we will discuss in the next section.⁶ A similar approach also underpins the definitions of sensitive data, data subject and data controller, although the terminology utilised may slightly vary.⁷

The core principles upon which the data protection architecture is erected are also commonly shared. The principles included in BRICS frameworks may be found in virtually all data protection regulations and allow identifying a globally applicable principle-core that is usually common beyond BRICS, at least as regards the first four principles. The BRICS data protection principles⁸ include consent, purpose limitation, fair and lawful processing, necessity, data minimisation, and accountability. Furthermore, BRICS legislators have included a similar spectrum of rights although with different flavours.⁹ All BRICS frameworks embrace provisions establishing the individual rights of access to data, correction of incomplete, inaccurate, or outdated data, elimination of personal data processed with the consent of the data subject, and revocation of consent.

BRICS data protection frameworks also present a very comparable set of obligations for data controllers and processors.¹⁰ Interestingly, the data controller concept has different contours in the five frameworks. The South African framework uses the term “responsible party” rather than “controller”. The new Chinese Personal Information Law refers to a “personal information handler”, meaning “organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods” (art. 73.1). This would be roughly synonymous with the Brazilian and Russian (or EU) data controller, while the PIPL’s “entrusted party” (art. 21) would reflect the data processor acting according to the controller’s instructions.¹¹

Meanwhile, the Indian Digital Personal Data Protection Act uses the concept of “data fiduciary”, which the Justice Srikrishna Committee claimed to be a conscious decision to depart from the narrative of a “controller” and “subject”, thus stressing the duty of care that underpins the relationship between a principal and a fiduciary.¹² The core obligations for data controllers in the BRICS include abiding to data

⁵ See Belli, L. *Data Protection in the BRICS Countries: Enhanced Cooperation and Convergence towards Legal Interoperability*. In *New Media Journal*. Chinese Academy of Cyberspace Studies. (2021).

⁶ See CyberBRICS Project ‘BRICS Data Protection Map’ (CyberBRICS Project 2021) Policy Question 7 <<https://cyberbrics.info/data-protection-across-brics-countries/>> accessed 8 October 2021

⁷ See *ibid*, “Definitions”

⁸ *ibid*, Policy Question 9

⁹ *ibid*, Policy Question 13

¹⁰ *ibid*, Policy Question 14

¹¹ See (n 51)

¹² See Rishab Bailey and Trishee Goyal, ‘Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019’ (*The Leap Blog*, 13th January

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

protection principles, obtaining free and informed consent in order to process data, duly communicating information on the data processing, and ensuring the security of all personal data under their responsibility.

The normative elements enshrined in the Indian Act demonstrate concrete potential to adopt innovative approaches that can inspire both BRICS countries and other countries globally. Perhaps, the most relevant example is the trend to move the Bill itself from an approach focused purely on legislation to one aimed at leveraging Digital Public Infrastructures, such as “accessible, transparent and interoperable platforms” (art 2.g) as technical tools of data regulation for consent management purposes.

Importantly, all BRICS countries have considered the essential role of international data transfers for the (digital) economy. All BRICS allow for international data transfers, whenever foreign third parties are deemed as providing an acceptable level of protection, but some of them have explicit data localization provisions (Russia and China) or specific data localization regimes (India). Hence, we can note both a convergence and divergence regarding key international issues such as data localization and transfer restrictions. India is a particularly interesting case, prescribing both localization of specific types of personal data, such as financial, payment and insurance data¹³, but simultaneously allowing unrestricted transfers of personal data as a general rule (art. 16). The Brazilian and South African frameworks include no requirement to store any types of personal data within national jurisdictions but define requirements for data transfers to be legal. Russia was the first country to enshrine a data localization obligation in its national framework, since 2015.

The same applies to China where, the PIPL prescribes that all personal data must be stored within the country, unless the Cyberspace Administration of China (CAC) determines differently. The Indian approach has evolved considerably from the draft Personal Data Protection Bill 2021, which proposed to require that every data fiduciary ensure that at least one serving copy of personal data to which the framework applies had to be stored on a service or in a data centre located in the country, to the much more liberal approach enshrined in the DPDP Act. Indeed, the current general rule is no restriction, but exceptions can be defined with specific regulation, as it happens for the Indian banking and insurance sectors.

In case of international data transfers, the evaluation of a sufficient level of protection is performed through quite heterogeneous mechanisms, spanning from the adoption of adequacy decisions on foreign legal frameworks, as foreseen in the GDPR, or specific administrative authorisations to transfer data for national service providers, or yet the use of corporate rules or binding agreements admitted by national authorities.¹⁴ Given the large number of criteria and the variety of mechanisms that BRICS countries adopt to regulate international data transfers, and considering how crucial this issue is to facilitate BRICS digital cooperation, especially regarding intra-BRICS free flows of information, we will explore it in the concluding chapter of this book, so that the reader will be able to fully appreciate its relevance after having delved into the data protection system of each specific BRICS country.

2020) <<https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html>> accessed 8 October 2021

¹³ Notably, section 94 of the Indian Companies Act 2013, read with sections 88 and 92 of the Companies Accounts Rules 2014, mandates to store financial information at the registered office of the company. In 2018, the Reserve Bank of India ordered all payment system providers to store information relating to payment systems in servers located under India’s territorial control, according to a circular titled “Storage of Payment System Data.” Section 3(9) of the Insurance Regulatory and Development Authority of India’s Maintenance of Insurance Records Regulation, 2015 requires covered organisations to store insurance data within India.

¹⁴ See (n 49) Policy Question 22

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

Importantly, all data protection frameworks in BRICS countries have an extraterritorial reach, except for South African law, which only applies when either the responsible party is domiciled in the country or is using means in South Africa, but does not extend to foreign entities providing services, goods, or collecting data about South African nationals from abroad. Perhaps surprisingly, all BRICS data protection laws apply also to the government. However, a lot of exceptions exist, such as the Brazilian law exemption of any activity related to national security, national defence or criminal enquiry to the application of the law, or the Indian Digital Data Protection Act 2023 highly criticized clauses attributing sweeping powers to the federal government to exempt any governmental agency from the scope of the law.

As for situations where social and cultural traits have a broader importance, major differences between BRICS data protection frameworks may be observed. Such is the case, for example, of the measures protecting children's data. Brazil has chosen a system akin to the European one, considering children as any person under twelve years old. The most recent version of India's Bill differs, considering all persons under 18 years old as unable to express consent legally. In this particular matter, the Cyberspace Administration of China (CAC) released in 2019, prior to China's data protection law, a data privacy regulation related to children, the "Provisions on Cyber Protection of Personal Information of Children", which is sometimes compared to COPPA (the US Children Online Privacy Protection Act), requiring paternal consent for children under 14.

Finally, all BRICS countries seem to envisage a benefit in having a specific authority overseeing the implementation of the law, although the way they design their national authorities differs considerably and may be seen as a reflex of their legal and institutional frameworks. In 2020, Brazil has established a new Data Protection Authority (DPA), the National Data Protection Authority (ANPD), complemented by a very innovative multistakeholder body acting as a Privacy and Data Protection Council (CNPD). Recently, the ANPD became an independent body, after the promulgation of a decree¹⁵ by the Federal Government later confirmed by Brazilian Parliament, but the ANPD is not fully independent as its budget is still defined - rather discretionarily - by the Ministry of Justice.

In Russia, data protection is overseen by the Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor), while in China the responsible body is the Cyberspace Administration of China (CAC). Importantly, both the Russian and Chinese regulators are not independent bodies but are incorporated as parts of the respective federal governments. Besides data protection, both organs have extremely large remits, encompassing several attributions that, in other countries, are typically attributed to different regulators, such as cybersecurity, content regulation, or telecommunications regulation. Importantly, their lack of independence has been criticized and identified by scholars and observers alike as one of the core reasons why the Russian and Chinese frameworks cannot be deemed as providing protections that are substantially equivalent to data protection systems where the regulators' independence is guaranteed.¹⁶

However, one must acknowledge that, despite being criticisable for the lack of independency, the Russian and Chinese model of super-regulators present a clear advantage of having a unique authority for digital matters to which new departments can be added to deal with emerging challenges regulated by new laws, such as artificial intelligence or platform governance, with no need to establish new ad hoc regulators. Indeed, as shown by the South African and Brazilian experience, the need to establish

¹⁵ See (n) 58.

¹⁶ See for instance Jan Czarnocki et al. Government access to data in third countries. Study prepared by Milieu under Contract No EDPS/2019/02-13 for the benefit of the European Data Protection Board (EDPB). (2019).

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

a new regulator, rather than expand an existing super regulator, is frequently one of the most visible vulnerabilities of a new regulatory systems, whose effectiveness ends up being considerably jeopardized by political gridlock regarding the funding, staff, independence and many other administrative details which may lead to enormous delays and dysfunctional regulatory systems not taken seriously by the regulated.

Lastly, the Indian Digital Personal Data Protection Act 2023 provides for the establishment of the Data Protection Board of India, although this regulatory body has not been established at the time of this writing. Lastly, South Africa was the only BRICS country to have a genuinely independent Information Regulator, subject only to the Constitution and to the law and accountable to the National Assembly. However, it is worth mentioning that it took exactly ten years since the approval of POPIA for the regulatory system to start being effective and such an enormous delay has inevitably undermined the credibility of the regulator.

1.3. Innovative BRICS Data Protection Practices

While BRICS countries are taking relevant inspiration from existing frameworks to develop their own national data protection regimes, it is essential to acknowledge that they are also introducing considerable innovations. In this section we offer a selection of the most innovative features of the BRICS data protection frameworks. While these elements have only been introduced recently, they should be considered carefully as they offer some interesting and innovative approaches that are likely to be replicated by other countries in the future.

1.3.1. Brazil and the LGPD implementation: the National Council of Data Protection and Privacy and the influence of the consumer protection framework

The Brazilian data protection framework¹⁷, even if only very recently enacted and still lacking several steps to be fully implemented, clearly presents some very particular characteristics. Importantly, such features mainly stem from typical experiences and practices present in other fields of the country's legal system.

The framing and drafting of the LGPD took at least 8 years since its first official draft was released¹⁸ till its enactment. In fact, this first official draft is the development from unofficial drafts produced during the series of debates in a Mercosur (the economic area bounding together Argentina, Brazil, Paraguay and Uruguay) working group on electronic commerce which, since 2004, evaluated a proposal made by Argentina of a data protection model law for the economic area.¹⁹ As Brazil did not have such a law nor a bill, some drafts began to circulate within federal government's boundaries at that time²⁰, which developed into a draft bill submitted to public consultation in 2010 by the Brazilian Ministry of Justice²¹.

This first draft resembled, in its structure and fundamental concepts, the data protection framework in Convention 108 of the Council of Europe and Directive 95/46/CE of the European Union. At the same

¹⁷ Parts of this section are based on Belli L. and Doneda D. (2022) *supra*, n (2).

¹⁸ A record of the original draft submitted to public consultation as well as the contributions received are available at <<http://www.doneda.net/2020/03/08/consultas-publicas-protecao-de-dados/>>.

¹⁹ Mercosur, 'XII Reunión ordinaria del subgrupo de trabajo n°13 – Comércio Eletrónico' (15 June 2004) <https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf> accessed 8 October 2021

²⁰ For a description of the development of Brazilian General Data Protection Law since its first drafts, see Danilo Doneda, 'Panorama histórico da proteção de dados pessoais' in Laura Schertel Mendes, Danilo Doneda, Ingo Sarlet and Otávio Rodrigues Jr., *Tratado de Proteção de Dados Pessoais* (Forense 2020) 3-20. The original draft law is available at <<http://culturadigital.br/dadospessoais/>>.

²¹ This consultation is still available at <<http://pensando.mj.gov.br/dadospessoais2011/>> (April 2021)

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

time, it presented some typical traits of the Brazilian law system, such as the explicit reference to Brazilian consumer law pillars and to the Public Civil Action law. The final text of the LGPD, even if based on this initial draft, changed enormously, due to the relevant number of contributions received in the public consultations organized by the Brazilian Ministry of Justice, and the intense legislative process, from 2016 to 2018, which included a series of public hearings, consultations and calls for suggestions and meetings with stakeholders.

The result of such participatory process was the engagement of several actors in this discussion but also the introduction of Brazilian legal system views and instruments into the texts as a way of absorbing the views of the various stakeholders. Moreover, as we will highlight, the participatory multistakeholder process, which led to the elaboration of the Law, has been baked into the governance system designed by the law. The final text of what later became LGPD is the result of an intense debate among diverse sectors of Brazilian society which not merely legitimized data protection tools and concepts transplanted from foreign legislations, but rather shaped them in a way they could best fit Brazilian legal tradition, introducing regulatory and participatory structures which became key characteristics of the Brazilian data protection framework in comparison with international standards.

These remarks on the LGPD's formative process are brought into consideration to give context on some specific characteristics of LGPD which we identified as innovative practices. This context is also different than the one found in other non-European countries, which typically debated their own data protection bills for a shorter time and, typically, considered the need to include into their legal system the rules that could facilitate international data transfers, thus fostering digital trade with Europe.

In Brazil, the pressure to shape domestic legislation to better accommodate international data flows has never been one of the major guiding forces for the elaboration of a data protection framework. In fact, one of the few elements of external pressure was the commitment of the federal government to join the OECD as a member country²², which would require the integration of several OECD Recommendations in the Brazilian legal system, including the establishment of a data protection framework. Nevertheless, this urge was important to motivate some of the federal government bodies, which were traditionally silent if not sceptical about LGPD, to endorse the proposal.

Such multistakeholder endorsement from the Brazilian private sector, academia and civil society, together with the consensus reached in the National Congress, played a relevant role to facilitate the LGPD's approval and enactment. Considering this background, it is not surprising that the resulting law would reflect (i) the presence of a multistakeholder consultative council as an auxiliary body to the Brazilian Data Protection Authority, and (ii) strong connection to the Brazilian consumer protection framework, noticeable in both procedural and substantial material aspects of the LGPD.

LGPD created as its Data Protection Authority the National Data Protection Authority (ANPD or "*Autoridade Nacional de Proteção de Dados*"), together with a consultative multistakeholder body, the National Data Protection and Privacy Council ("*Conselho Nacional de Proteção de Dados e Privacidade*"). The Council has strictly consultative functions and does not make decisions, nor has any supervision or administrative tasks. Its competences are listed in article 58-B of LGPD and include providing ANPD with suggestions, proposals and support for its actions and, particularly, for the development of the National Data Protection Policy; drafting annual reports on the actions performed by ANPD; drafting studies and promoting debates and public hearings and, generally, promoting data protection knowledge and culture among Brazilian people.

The Council presents a multistakeholder composition: out of its 23 members, 5 are appointed by the Federal Government, 1 by the Federal Senate, 1 by the House of Representatives, 1 by the National

²² OECD's Guidelines on the protection of privacy and transborder dataflows of personal data was a pivotal document on the development of international data protection standards when it came out in 1980 and maintains its importance. Compliance with these guidelines is one of the requirements if Brazil is eventually to join OECD as a member country. See 'Personal Data Protection at the OECD' (OECD, 2021)

<<https://www.oecd.org/general/data-protection.htm>> accessed 8 October 2021

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

Justice Council, 1 by the Public Ministry National Council, 1 by the Brazilian Internet Steering Committee, 3 chosen amongst representatives of non-governmental organizations, 3 from science and technology institutions, 3 from national confederations from the productive sector, 2 from the private sector and 2 from unions and worker organizations. The nomination process for each counsellor is defined by the institutions themselves. The stakeholder groups mentioned generically will have the possibility to suggest candidates and the board of directors of ANPD will choose the most adequate representatives of each group, and subsequently submit those names to the Presidency of Republic, which will have a final say on the list and nominate the counsellors.

The presence of a sound multistakeholder element in the Council pays tribute to, at least, two driving factors. First, the noticeable multistakeholder experience of the Brazilian Internet governance ecosystem, where CGI.br – the Brazilian Internet Steering Committee (“*Comitê Gestor da Internet*”) – has played a pivotal role in the development of the Internet in the country since its early days, frequently characterized as a “multistakeholder model” that became a global benchmark.

The second factor was the concrete dialogue between several sectors by the time LGPD was yet a Bill and was being debated in National Congress. The resonance among diverse stakeholders gave birth even to a coalition of institutions, enterprises, and organizations from several areas to support the approval and enactment of LGPD, and one of the side products of these discussions was indeed the need to create a governance structure in the Brazilian data protection framework to accommodate and give a voice to these stakeholders in the process of implementation of data protection.

It is important however, to stress that while the Brazilian framework may be seen as a hallmark of multistakeholder participation in policy suggestion, it is much less performing as regards policy implementation.

1.3.2. Freely Shareable Personal Data, Opt-out, and Data Localization in Russia

In Russia, personal data protection is regulated by Federal Law No. 152-FZ, which was adopted in 2006 and subsequently amended in December 2017 and in December 2020.²³ As emphasized above, the Russian data protection framework is implemented by Roskomnadzor, a super regulator with particularly large competence and powers, which has been frequently criticized for its lack of independence, being administratively subordinated to the Russian Ministry for Media and ICTs. The latest amendments to the Russian framework entered in force partly in March 2021 and partly in July 2021. As discussed by Zanfir-Fortuna and Iminova²⁴, these amendments aim at tackling four areas.

First, the amended provisions introduce a new category of personal data that can be freely shared and are defined as “personal data allowed by the data subject to be disseminated.” Second, the Russian legislation now includes rules allowing personal data to become freely sharable with an unlimited number of persons. To do so, the law establishes the obligation to collect specific, affirmative, and separately collected consent from the data subject. The rationale behind the creation of this new category of personal data resembles the one behind GDPR Article 9(2)(e), a largely underappreciated norm²⁵, which allows the processing of sensitive data when “processing relates to personal data which are manifestly made public by the data subject.”

²³ See Russian Federal Law No. 519-FZ of 30 December 2020 ‘On Amendments to the Federal Law ‘On Personal Data’ <<http://publication.pravo.gov.ru/Document/View/0001202012300044>> accessed 8 October 2021

²⁴ Gabriela Zanfir-Fortuna and Regina Iminova, ‘Russia: New Law Requires Express Consent For Making Personal Data Available To The Public And For Any Subsequent Dissemination’ (CyberBRICS Project, 2 March 2021) <<https://cyberbrics.info/russia-new-law-requires-express-consent-for-making-personal-data-available-to-the-public-and-for-any-subsequent-dissemination/>> accessed 8 October 2021

²⁵ For a rare analysis of this norm, see Edward S. Dove and Jiahong Chen, ‘What does it mean for a data subject to make their personal data ‘manifestly public’? An analysis of GDPR Article 9(2)(e)’ [2021] 11(2) *International Data Privacy Law* <<https://academic.oup.com/idpl/article/11/2/107/6146670>> accessed 8 October 2021

According to the amended Russian data protection framework, personal data allowed by the data subject to be disseminated can only be processed when an organisation or individual processing them can prove that the data subject expressed consent according to the modalities specified by the law. Third, the law introduces the possibility for Roskomnadzor – the Russian of Communications, Information Technologies, and Mass Communications Regulator – to create a centralized database of all the expressions of consent regarding the unlimited dissemination of personal data. Lastly, the law establishes a new absolute right to opt out of the dissemination of personal data, which can be exercised “at any time.”

Conspicuously, consent is the only legal basis for the processing and dissemination of “freely” shareable personal data. Such data is defined by a new paragraph 1.1, in Article 3 of the Law, as “personal data to which an unlimited number of persons have access to, and which is provided by the data subject by giving specific consent for the dissemination of such data, in accordance with the conditions in the Personal Data Law.” According to the new Art 10.1, personal data can be freely shared only after the obtention of specific, express, unambiguous, and separate consent. Under Law 152-FZ, the natural or legal person that determines the purposes of personal data processing, the composition of personal data to be processed, and the operations performed with personal data is defined as the “data operator.”²⁶ Article 10.1(1) creates a new obligation for the operator to obtain the data subjects’ separate, specific and express consent to be able to disseminate personal data, on top of the regular consent to process data.

Silence or inaction cannot configure the consent needed for free dissemination of data and the data subject must also enjoy the possibility to choose specific categories of personal data that can be freely disseminated. Furthermore, any operator, be it the first one collecting the freely shareable data or anyone else processing freely shareable personal data bears the onus to “provide evidence of the legality of subsequent dissemination or other processing”, under Article 10.1(2).

The establishment of the aforementioned obligation has also led the Russian legislator to introduce the possibility for Roskomnadzor to create a centralized consent management system to collect all the expressions of consent. Indeed, according to Article 10.1(6), consent to turn personal data into freely shareable data can be collected by the operator or via a dedicated “information system” which may be envisaged as a digital public infrastructure established by Roskomnadzor.²⁷ This system may resemble the Data Empowerment and Protection Architecture implemented by India and discussed in the next section.

Another innovative practice introduced by the recent amendments of the Russian law is the new absolute right to opt-out of dissemination of freely shareable personal data. Indeed, Article 12.1(12) prescribes that the free dissemination of personal data can be halted at any time, on request from an individual. Such right to opt out from dissemination can be exercised to withdraw the previously expressed consent, by specifically identifying the personal data to which the request refers, and the diffusion of which should be terminated. Interestingly, the opt-out request can also be used as a tool to stop the dissemination of data about which consent has not been lawfully collected. In this latter case, the data subject can address the request either to the operator that is illegally disseminating the personal data or to a Court of law.

The timeframe for stopping the dissemination will depend on the modalities of the request. In the case of lawful collection of consent, Article 10.1(13) establishes that sharing must terminate as soon as the request is received. In the case of illegal sharing, Article 10.1(14) prescribes that sharing will need to stop within three business days from the reception of the request or within a different timeframe established by a Court order.

²⁶ This term refers to both roles of controller and processor, which are split in other BRICS frameworks such as the Brazilian LGPD or the South African POPIA. See CyberBRICS Project (n 10)

²⁷ The provisions dedicated to the establishment of this system are scheduled to enter in force in July 2021. At the time of this writing, Roskomnadzor has not yet published the technical specifications outlining the functioning of this consent management system.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

Lastly, it is important to mention that, although Russian “data localization” policies are not particularly recent, Russia can be considered a “trailblazer” in this peculiar field, as the normative provisions it adopted as early as September 2015, have inspired many other countries²⁸, including BRICS neighbours, such as China and India. Particularly, Article 18 of the Federal Law No. 152-FZ enshrines the obligation of the operator to ensure the localization within Russian servers of the processing activities related to all personal data collected from Russian citizens.

Data localization came into force on 1st September 2015 and includes the possibility of blocking the operator’s online resources, whenever personal data of Russian citizens are processed in violation of localization requirements. Clearly, the recent Russian invasion of Ukraine and the consequent Western sanctions have exacerbated the already ongoing tendency towards data localization and “Internet sovereignty” which is deemed by Russia as top priority of national security, justifying the implementation of a wide array of restrictive measures.²⁹

To illustrate this tendency, several scholars have highlighted the relevant number of initiatives that Russia has introduced, over the past years, with the aim to expand control over data flows and regulate Internet users’ behaviour, for instance blocking access to a large number of content labelled as “extremist information,” while also building considerable cyber-defence capabilities.³⁰ As such, data localization has become one of the fundamental tussles – although not the only one – of the Russian strategy for the assertion of digital sovereignty, based on a blend of data-related policies and “infrastructure-embedded control.”³¹ It is important to recognise that this Russian blend of digital sovereignty is increasingly inspiring governments and legislators globally.³²

1.3.3. The Indian Data Empowerment and Protection Architecture

In July 2015, the Government of India launched the Digital India³³ program, an ambitious plan aimed at fostering the digital transformation of the country. While Digital India has very strong connectivity and eGovernment components, another key component, which is based on the establishment of a Digital Public Infrastructure, is a set of APIs³⁴ commonly referred to as the “India Stack”³⁵ that is particularly relevant to explain the evolutions that the Indian data protection framework undertook since the inception of Digital India.

Indeed, the India Stack is deemed by the Indian Government as instrumental to achieve the Digital India vision, consisting in a substantial digital transformation fostering inclusive growth in highly strategic areas, such as digital products and services, automated manufacturing, thus unleashing job opportunities.³⁶

²⁸ For up-to-date details on how widespread the adoption of data localisation norms is, see Cory N., and Dascoli L. *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. Information Technology & Innovation Foundation. (2021).

²⁹ See Shcherbovich, A. Data protection and cybersecurity legislation of the Russian Federation in the context of the “sovereignization” of the internet in Russia. In Belli, L. (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer. (2021) p. 67-131. https://link.springer.com/chapter/10.1007/978-3-030-56405-6_3
Daucé, F. and Musiani F. (Eds.) *Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet*. Vol. 26. N. 5 (May 2021). <https://firstmonday.org/ojs/index.php/fm/issue/view/693>

³⁰ Idem.

³¹ See Daucé and Musiani (2021) cit. supra.

³² See Cory and Dascoli (2021) cit. supra.

³³ Digital India, available at <<https://www.digitalindia.gov.in/>> accessed 8 October 2021

³⁴ An API, or application programming interface, is a piece of software that allows different software applications to interact and exchange data, according to the specifications established by the API.

³⁵ See <<https://www.indiastack.org/>>.

³⁶ Importantly, such vision is not exempted from critique, notably considering that India Stack has been essentially designed by iSpirt (the Indian Software Products Industry Round Table), a think tank for the Indian software products industry which has been criticised for its close ties with both government and large corporations, raising concerns related to conflict of interests, transparency and accountability. See <https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf>

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

While the expansion of connectivity is instrumental to support the abovementioned vision, two elements of the India Stack are key for our analysis: Aadhaar and DEPA.

Aadhaar means “foundation” in Hindi and is the national digital identity system that, as of 2021, has been extended to more than 94% of the Indian population, making it “one of the most successful rollouts of any tech product anywhere.”³⁷ As noted by Kak, Parsheera and Kotwal, Aadhaar’s ability to uniquely identify individuals based on their biometric/demographic information has led the Indian government to make “mandatory, the use of Aadhaar numbers for various welfare schemes like the transfer of direct cash benefits under public distribution of food grains, employment guarantee benefits, midday meals in schools, subsidies, etc.” While Aadhaar can be made mandatory for government benefits and welfare, it continues to be extensively used on a “voluntary basis” as an ID proof for all these other purposes.

Due to the Aadhaar potential for privacy abuses, the constitutionality of the program was challenged before the Indian Supreme Court. As discussed in this volume’s chapter dedicated to India, with the landmark Puttaswamy case³⁸, the Supreme Court seized the occasion to pronounce the existence of a fundamental right to privacy in India, which can only be limited through fair, just, and reasonable procedures, clearly foreseen by the law. At the same time, the Court’s decision opened the path to the elaboration of the first draft of the Indian Data Protection Bill, which later became the Digital Personal Data Protection Act, 2023.

One of the most compelling features of the Indian approach to data governance is the use of digital public infrastructures (DPIs) as techno-regulatory tools, embedding normative values in technical architectures. In August 2020, the Indian government’s policy think tank Niti Aayog issued a draft paper aimed at fostering discussion on a new Data Empowerment and Protection Architecture (DEPA) framework.³⁹ The paper builds upon previous development of the “electronic consent framework”, which was adopted in 2017,⁴⁰ as well on the existing implementations of the concept through the account aggregators framework, already adopted by the Indian financial sector.⁴¹ DEPA is presented as a “secure consent-based data sharing framework to accelerate financial inclusion.”

While the Indian concept of consent managers may recall already existing Personal Data Stores (PDSs) or Personal Information Management System (PIMSs) such as CitizenMe and Solid, it is important to stress that previous PDS and PIMS examples are relatively niche initiatives.⁴² The Indian experiment of electronic consent management frameworks within the DEPA, is the first nationwide initiative stemming from the Indian digital transformation “India Stack” plan and has become a new hallmark of the Indian data architecture.

Through the establishment of DEPA, Niti Aayog aims at creating “an evolvable regulatory, institutional, and technology design for secure data sharing” that can “empower individuals with control over their

³⁷ Aaryaman Vir and Rahul Sanghi, 'The Internet Country: How India created a digital blueprint for the economies of the future' (Tigerfeathers, 14th January 2021) <<https://tigerfeathers.substack.com/p/the-internet-country>> accessed 13 October 2021

³⁸ For an analysis of the case, see Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' [2017] 11 *IndraStra Global* <<https://nbn-resolving.org/urn:nbn:de:0168-ssor-54766-2>> accessed 13 October 2021

³⁹ See Niti Aayog, *Data Empowerment And Protection Architecture: Draft for Discussion* (2020) <https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf> accessed 13 October 2021

⁴⁰ See iSPIRT, 'Electronic Consent Framework' (ProductNation, 5 May 2019) <<https://pn.ispirit.in/tag/electronic-consent-framework/>> accessed 13 October 2021

⁴¹ See George Mathew, 'Account Aggregators: New framework to access, share financial data' (The Indian Express, September 8 2021) <<https://indianexpress.com/article/explained/account-aggregators-new-framework-to-access-share-financial-data-7490966/>> accessed 13 October 2021

⁴² See Abiteboul, S. André, B., Kaplan, D. Managing your digital life with a Personal information management system. *Communications of the ACM, Association for Computing Machinery*, 2015, 58 (5), pp.32-35; Brochot, G. et al. “Personal Data” Stores, Cambridge Judge Business School. (2015).

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

personal data.”⁴³ The elaboration of DEPA is particularly relevant, as it has been conceived to create a software architecture, based on shared public protocols, allowing all Indians to regulate, and somehow “customize”, the flow of personal information that third parties may collect and process.

In practice, DEPA act as a system of digital consent management. The system will be based on the development of technical specifications to allow individuals to give consent to processing of personal data, defined by Ministry of Electronics and Information Technology⁴⁴, and the introduction of “consent managers” that will act as a new category of intermediaries. Such DEPA framework has already been adopted in the financial sector, through the Account Aggregator system, established by the Reserve bank of India. This latter system is grounded on the specification of technical standards and the establishment of a category of regulated intermediaries, named “account aggregators,” which act as consent managers within the financial sector.⁴⁵

In this perspective, the goal of the DEPA consent managers is to facilitate the flow of personal data from information providers to the users of the information, based on the consent of the individual. Thus, consent managers are supposed to act as data fiduciaries, which enable a data principal to gain, withdraw, review, and manage his consent through an accessible, transparent, and interoperable platform. They are not supposed to exploit personal data, but rather to be “data blind” and merely serve as a “conduit for encrypted data flows.”⁴⁶

Importantly, DEPA is also presented by Niti Aayog as the final layer of the India Stack, aimed at providing secure digital data sharing through consent. To understand DEPA, is indeed necessary to take a step back and remind that DEPA is a key “layer” of the India Stack, which aims at allowing all interested stakeholders – be them public bodies, businesses, start-ups, or non- profits – to use the Indian public digital infrastructure to deliver services.

However, one common concern with the DEPA model is that it could lead to the over-simplification of consent. Indeed, the “consent manager” proposed under DEPA has the potential to become an element for both enhancement or reduction of data control from the individual, depending on how the DEPA structure is designed and its degree of synergy with the implementation of the Digital Personal Data Protection Act by the Data Protection Board of India that, at the moment of this writing has not been established yet. As emphasized by Reddy et al., one must keep in mind that the primary objective of the DEPA framework shall be to grant individual control over personal data through the establishment of a secure and well-functioning protocol to share data across institutions, ultimately leading to individual empowerment and well-being.

Lastly, it is important to note that the Indian legislator seems to have taken inspiration from their Chinese neighbours, as regards the need to couple its normative framework with a didactic approach, introducing “illustrations” aimed at exemplifying concepts that might be new for Indian stakeholder. This is indeed a very useful technique explored by the Chinese legislator by annexing examples to the regulatory standards, such as the Personal Information Security Specification, which proves to be extremely useful to facilitate compliance.

⁴³ See Niti Aayog (n 88) 26-27

⁴⁴ See Ministry of Electronics and Information Technology, *Electronic Consent Framework - Technology Specifications Version 1.1* (2016) <<http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf>> accessed 13 October 2021

⁴⁵ See Reserve Bank of India, ‘Account Aggregator Ecosystem API Specifications’ (8 November 2019) <<https://api.rebit.org.in/>> accessed 14 October 2021

⁴⁶ See Niti Aayog (n 88) 15

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

1.3.4. China's facilitative regulation, institutional coordination, data security approach and the normative innovation of the Personal Information Protection Law (PIPL)

China's approach has been innovative in terms of facilitative regulation, institutional coordination, relevance of cybersecurity, and normative updates. One of the most relevant features of the Chinese approach is its understanding of regulation as a technique that does not solely yield restrictive outcomes.⁴⁷ Indeed, regulation can also aim at generating facilitative effects, thereby expanding the operational latitude of regulated firms. Both facilitative and restrictive regulations encompass the formal and informal rules, practices, and norms designed to respectively broaden and constrain the freedom of action of regulated entities.

Facilitative regulations can significantly enhance the operational capabilities of regulated entities. For instance, governments may offer tax credits or grants to companies investing in research and development, thereby fostering innovation and technological advancement. In this perspective, China's administrations compete among each other to offer the best conditions for start-ups and enterprises to develop their (digital) products and services.⁴⁸ Conversely, most data protection frameworks are based on restrictive regulations, imposing obligations and prohibiting certain types of data processing operations rather than incentivising the desired ones through incentives.

As noted by Belli, in 2015, China adopted a set of ambitious policy and investment strategies including the "Internet Plus" and "Made in China 2025" which focused on facilitating digital transformation through the expansion of Internet connectivity, the IoT and its enablers, followed by a National Plan for Artificial Intelligence Development and the AI Governance Principles, to reap the benefits of connectivity and datafication.⁴⁹ These plans complemented the adopted legal documents, such as the Cybersecurity Law, the Personal Information Security Specification, the E-Commerce Law, and PIPL with facilitative regulation instruments, promoting the development of domestic industries.⁵⁰ In this perspective China's focused industrial policy on key sectors where the government has strongly backed domestic players including via huge public investments and facilitating the export of Chinese digital products and services.⁵¹

Moreover, having realised the complexity of digitisation processes and of the regulation of data processing, starting from 2014 China has redesigned its cyber-related institutions to facilitate the elaboration and implementation of policies regarding information governance and cybersecurity. In this perspective, China established a new Cybersecurity and Informatization (CI) "*xitong*", created the new Cyberspace Administration of China (CAC) as a new cyber regulator, and organized the new Central Commission for Cybersecurity and Informatization (CCCI)⁵². A *xitong* is a peculiar Chinese

47 Ma, A. (2024). *China as a double-bind regulatory state: How internet regulators' predicament produces Regulatees' autonomy*. Palgrave Macmillan.

48 Idem.

49 Belli L. *New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance*. *Indian Journal of Law and Technology*. (2022)

50 *Made in China 2025: Global ambitions Built on local protections*, 2017, US Chamber of Commerce, https://www.uschamber.com/assets/archived/images/final_made_in_china_2025_report_full.pdf

51 *Cross-border data flows and development: For whom the data flow*, Digital Economy Report 2021, United Nations Conference on Trade and Development, UNCTAD/DER/2021.

52 See Creemers, R. *China's Cyber Governance Institutions*. Leiden Asia Centre. (2021).

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

administrative structure,⁵³ aimed at providing a dedicated “policy system”, involving all the public sector stakeholders affected by a specific policy area.

The goal of the *xitong* is to deal with the complexity of a multi-layer administration in a gigantic state, thus being able to coordinate and regulate efficiently specific sectors. This systemic approach should be studied and considered carefully as it can facilitate enormously stakeholder communication, cooperation and coordination, well beyond the policy suggestion, promoted by the Brazilian multistakeholder approach. Interestingly, Brazil also adopts a similar type of administrative configuration, also called system, in some policy areas such as the National Consumer Protection System and the Brazilian Military Cyberdefence System⁵⁴.

Furthermore, China has openly stated its willingness to leverage data governance to assert sovereignty on cyberspace, exerting control, and protecting from foreign threats its national digital assets, while developing solid cybersecurity. It is important to emphasize that the expansion and control over digital infrastructures as well as the use of technology to maintain social stability and detect potential threats are high priorities for the Chinese government and have historically been considered as complementary dimensions and pursued jointly. The high relevance of these goals and their interdependence have been tellingly highlighted by President Xi Jinping himself, stressing that “cybersecurity and informatisation are two wings of one bird, two wheels of one cart, we must uniformly plan, uniformly deploy, uniformly move forward, and uniformly implement matters.”⁵⁵

The strong cybersecurity component is indeed a key feature of the Chinese data architecture, emphasised since the 2012 decision of the National People’s Congress to consider data protection and information security as necessary extensions of public order and national security.⁵⁶ In this perspective, the Cybersecurity Law prescribes that the State is responsible for establishing and improving a system of cybersecurity standards,⁵⁷ including rules for a “graded protection of cybersecurity.”⁵⁸

⁵³ See Barnett, D. *Cadres, bureaucracy, and political power in communist China*. Columbia University Press. (1967).

⁵⁴ National Consumer Protection System (Sistema Nacional de Defesa do Consumidor – SNDC) <https://www.consumidor.gov.br/pages/conteudo/publico/6> ; Ordinance No 3.781/GM-MD. (17 November 2020). Military Cyber Defense System (SMDC) <https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860>

⁵⁵ See Creemers, R. Central Leading Group for Internet Security and Informatization Established. (1 March 2014). China Copyright and Media. <https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/>

⁵⁶ *Ibid*; Wang, Z. ‘Systematic government access to private-sector data in China’ (2012) 2(4) *International Data Privacy Law* 220 221-224.

⁵⁷ Art. 15 Cybersecurity Law of China.

⁵⁸ Article 21 Cybersecurity Law of China. The “graded protection of cybersecurity” refers to the Multi-Level Protection Scheme (MLPS), a concept which can be dated back to administrative rules from 1994 and 2007, and turned into a statutory obligation with the Cybersecurity Law’s Article 21, and reinforced by the 2022 Data Security Law’s Article 27 (“...in data processing by making use of the internet or any other information networks, the abovementioned data security obligations shall be fulfilled on the basis of the **classified protection system for cyber security**.”). According to the MLPS scheme, information systems need to be graded on a range from 1 to 5, and network operators must apply the cybersecurity measures according to the system’s grade. PricewaterhouseCoopers, ‘Cyber Security Law – Addressing the Compliance Complexities’ (PwC, 30 November 2022), <https://www.pwc.de/en/international-markets/german-business-groups/china-business-group/cyber-security-law-addressing-the-compliance-complexities.html>. Furthermore, in May 2019, three national standards

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

Building on the bases set by the Cybersecurity Law, the Personal Information Security Specification of 2018 established that it is obligatory to “disclose the scope, purpose, and rules for processing personal information in a clear and comprehensible manner and accept external oversight.”⁵⁹ The elaboration of the Specification was considered as necessary to fill many normative gaps, providing guidance on how to improve data subject awareness, corporate compliance, national oversight, and business good practices, setting new guidelines for personal data processing.

It is also important to stress that, despite the non-binding status of specifications in the Chinese legal system, the Personal Information Security Specification must be seen as a cornerstone of the Chinese data architecture. Indeed, the Specification plays an essential role translating normative elements easily understandable for lawyers into technical commands easily understandable for developers, thus critically supplementing legislation with technical standards that can be easily updated. In this perspective, shortly after the adoption of the Specification, the Chinese National Information Security Standardisation Technical Committee, a key standard-setting body typically referred to as “TC260”,⁶⁰ started to update the specification to amend several requirements for personal information controllers to make them clearer and more easily implementable. On 6 March 2020, TC260 and the State Administration for Market Regulation issued the 2020 amended version (GB/T 35273-2020), which took effect on 1 October 2020.

The Specification provides guidance on the i) scope, ii) normative references, iii) terms and definitions iv) basic principles of personal information security, v) personal information collection, vi) personal information retention, vii) use of personal information, viii) rights of personal information subjects, ix) entrusted processing, sharing, transfer, and public disclosure of personal information, x) handling of personal information security incident, xi) and personal information security management requirements for organizations.

Critically, the Specification adopts a remarkably didactic approach⁶¹, offering detailed instructions and concrete examples – especially in its appendix – illustrating how to comply with normative provisions. Notably, the Specification Annexes provide examples of what is to be considered personal information (annex A); a guide on how to identify sensitive personal information (Annex B); methods to safeguard independent choice of personal information subject (Annex C); and a model explaining how to draft a Personal information protection policy (Annex D).⁶² This approach is a particularly relevant feature of the Chinese systems, which understands the difficulty of complying with a new and highly technical law, regulating a matter with which much of the population is highly unfamiliar, and cannot be successful without explicit guidance.

Lastly one of PIPL’s major innovations consist in going beyond existing standards including some last-generation norms yet to be considered in other major data protection legislations, such as the

were issued by Chinese regulators: Information Security Technology - Baseline for Cybersecurity Classification Protection (GB/T 22239-2019), known as the “MLPS 2.0 Baseline”, Information Security Technology - Technical Requirements of Security Design for Cybersecurity Classification Protection (GB/T 25070-2019); and Information Security Technology - Evaluation Requirements for Cybersecurity Classification Protection (GB/T 28448-2019). Together, they provide detailed and technical and administrative requirements on how to implement the MLPS. Li, B. ‘China: MLPS 2.0 - Baseline Requirements and Practical Takeaways for Businesses’ (*DataGuidance*, 22 August 2022), <https://www.dataguidance.com/opinion/china-mlps-20-baseline-requirements-and-practical>.

⁵⁹ Personal Information Security Specification, 2018, art. 4e.

⁶⁰ See <https://www.tc260.org.cn/>

⁶¹ See Belli, Chang and Chen (2023) n (53).

⁶² Personal Information Security Specification, 2020, Annex A, B, C, D.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

provision on its article 58 that commands big platform internet services to establish an independent supervision board with external members. This is a relevant accountability measure which can have very positive effects and is not found in any other data protection framework. The same article 58 also mentions the obligation of internet platforms to release reports on their data processing activities and to accept what is described as “society's supervision”.

PIPL, in fact, provides for a set of provisions which are entirely new to data protection frameworks, such as the ban on automated decision-making for price discrimination (Article 24) or the provisions for handling people's data of deceased individuals (Article 49). This latter type of provisions usually depends not only on data protection standards but on other aspects of a country's legal system regarding the protection of personality and family law, among others, but, in PIPL, this issue has been regulated by the data protection framework. It is important to stress this element of innovation as it is already deploying an international influence, as it is visible in article 14 of the Indian Digital Personal Data Protection Act, 2023, which regulates data protection in the event of death, clearly taking inspiration from its Asian neighbour.

1.3.5. The South African framework: POPIA's scope and the nature of the DPA and of the DPO

POPIA is a data protection law of the Republic of South Africa, established in November 2013 to bring transparency and accountability on entities processing personal data, aiming at providing individuals with control over their personal information. POPIA applies to any organization processing personal data within South Africa and to foreign organizations processing personal information in the country. However, the territorial scope defined by Section 3 of POPIA can be seen as narrower than the GDPR or LGPD, as the South African law only applies when the responsible party (*i.e.* the controller) is either domiciled in South Africa or is “using means” in South Africa, hence avoiding the more overarching reference to the offering of goods or services, or monitoring of individuals from abroad.

While its most distinguishing features are not unique in the world, they deserve to be mentioned as they make the South African framework unique within the BRICS context and may serve as useful experiences to be studied by other (BRICS). First, POPIA applies not only to personal data relating to living individuals, but also to personal data relating to existing legal persons, such as companies and non-profits. Second, POPIA establishes the Information Regulator as the independent data protection authority within the South African jurisdiction, but also empowering the body to monitor and enforce compliance with the Promotion of Access to Information Act, 2000 (PAIA Act 2 of 2000). In this sense, the data protection officer has a broader function than the one usually attributed by other frameworks. For this reason, the DPO is defined by POPIA and PAIA as an “information officer”, which plays an instrumental role to fulfil obligations related to both the protection of personal data and the due regulation of access to records held by public or private entities.

One of the main peculiarities of POPIA is that its Section 1 considers as a “data subject” the individual or the “juristic person” to whom personal information relate. In the same spirit, personal information is any information relating to an identifiable, living, natural person, and where it is applicable an identifiable, existing “juristic person.” In the South African legal framework, there are two categories of legal subjects: natural persons and juristic persons (which are usually defined as “legal persons” in other frameworks). All human beings are considered as natural persons and legal subjects. Juristic persons are certain types of associations of natural persons, such as companies or non-profits. Hence, a major peculiarity of POPIA is that it includes juristic persons under its scope of application.

All responsible parties must appoint an Information Officer (IO). If no appointment is made, the head of the organization (for example, the Chief Executive Officer or Managing Director) is automatically considered as the organisation's IO. Importantly, the details of each organization's IO must be registered

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

with the Information Regulator of South Africa or InfoReg (the national DPA), which has established a dedicated online portal to facilitate this task.⁶³ IOs are also allowed to delegate their duties to deputy information officers.

Lastly, an important procedural element is the appointment of the Board of InfoReg, as it is both a testament to the highly democratic and open tradition that South Africa has endeavoured to bake into all governance processes since the Mandela era and a good practice that other countries could very easily copy. To identify members of the InfoReg, with appropriate qualifications and a sufficient degree of diversity – at least one member must have experience as a practising advocate or attorney, or a professor of law at a university, while the remaining members must be appointed on account of any other qualifications, expertise and experience relating to the objectives of the regulator – the South African Parliament issues an open Call for Applications or Nominations.⁶⁴

1.4. Governmental access to personal data in the BRICS

After having highlighted some of the main elements of innovation in the BRICS framework this section will discuss how the countries regulate governmental access to personal data. Indeed, conditions surrounding governmental access and processing of personal data in the BRICS countries may prove a crucial point of tension regarding legal interoperability of data protection systems.

The following table summarises the treatment given to government processing of such data in the Brazilian, Russian, Indian, Chinese and South African data protection laws, while the frameworks of the newly added members of the grouping – i.e. Egypt, Ethiopia, Indonesia, Iran, Saudi Arabia, and the UEA – will be analysed in the following section. The table showcases different approaches – some more detailed, others less so – toward the matter. However, it is important to emphasise that data protection legislation alone does not provide a full picture of the data protection architecture in this regard, since there are areas of government use of personal data, such as police investigations and intelligence activities, which may not be covered by personal data protection laws or that may be further specified in other laws, as demonstrated in following.

Table 1.1 - Government processing of personal data in BRICS countries

Country	Definition of processing agents include State agents	Specific legal basis for State processing	Specific requirements for data processing by the State	Special exceptions for data processing by the State	Shared use between Public and Private agents
Brazil (law n. 13,709 / 18)	Art. 5, VI and VII, include natural or legal persons governed by "public or private law".	Art. 7, III and 11, II, b contain specific legal bases for processing by the Public Administration.	Chapter IV (art. 23 to 32) contains specifications regarding processing of personal data by Public Authorities.	Art. 4 exempts data processing for public safety, national defense, state security or activities of investigation and prosecution of criminal offenses from the LGPD's provisions.	Art. 26 regulates the shared use of personal data between public entities and private entities for the execution of public policies, requiring transparency and adherence to data protection principles.

⁶³ Online Portal – Registration of Information Officers, available at <<https://www.justice.gov.za/inforeg/portal.html>> accessed 14 October 2021

⁶⁴ The most recent Call is available at <<https://www.parliament.gov.za/press-releases/media-statement-justice-and-correctional-services-committee-calls-nominations-information-regulator>> accessed 14 October 2021

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Russia (Federal Law n. 152-FZ)	Art. 1 expressly mentions various governmental bodies. Art. 3 (2) defines operator to include "a state authority, municipal authority".	Art. 6 (4) contains a legal basis for data processing necessary to the execution of various executive powers by state authorities.	Art. 13 covers data processing in the context of state or municipal information systems.	
India	The definition of Data Fiduciary and Processor mention "any person", without specific mention of State actors.	Art. 7 (b) and (c) contain specific authorisations for state processing of data for the State to provide certain services to the Data Principal or to perform instrumentalities or functions or, finally, in the interest of the country's sovereignty and integrity.	Art. 17 exempts government from application of the law when processing is necessary "in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order".	Section 19 of the Personal Data Protection Bill allows the State to share personal data with private entities for the provision of services or benefits, subject to safeguards.
China (PIPL)	Personal data processors are not defined in specific terms to include or exclude State actors.	There is no specific legal basis, although broader bases such as Art. 13 (3) or (7) may include state authorities in specific situations. There is, however, a specific section (3) of Chapter II dedicated to information processing by State Organs.	Art. 36 establishes a data localization obligation for personal data, as well as a specific security assessment of these data processing activities. Art. 37 extends Section 3's rules (art. 33 to 37) to organisations administering public affairs via authorization by law or regulation.	
South Africa (POPIA)	The concept of "responsible party" explicitly includes "public or private" bodies.		There is no legal basis per se. However, there is an exclusion for processing by a public body in limited cases, meaning the law does not apply in the hypotheses of art. 6 (c).	

Source: Authors' own elaboration.

Chinese data protection law does not provide much specification of government access and processing of personal data. Data processors are generally defined to arguably include government actors. Legal bases do not include a specific hypothesis for government use, although some could be used by government actors to access and process personal data in specific situations. The most specific terms in this regard are given in section 3 (articles 33 to 37), concerning "Special provisions on the processing of personal information by state organs". Of note are article 36, which establishes a data localization requirement when data is processed by state organs, and article 37, which extends that section's provisions to organizations managing public affairs by force of law or regulation.

Although the treatment of government access to personal data in the PIPL is limited, there is a wider legal context that affects this matter. The Chinese framework on criminal investigations, the Cybersecurity Law, the National Security Law, the National Intelligence Law and the Counter-Espionage Law are some of the main normative documents influencing the status of government access to personal data in China. In general, the authors highlight shortcomings in these laws that may lead to undue or arbitrary government access to personal data, due to use of undefined or broadly defined legal terms and processes. That is to say, the lack of a definition of, for example, “strict formalities” in the Counter-espionage Law article 12 may lead to access to personal data under insufficient restrictions. Similarly, the use of terms like “public security” and “societal interests” in these laws are broad and grant extensive leeway for data access. This problem is compounded by insufficient independent oversight mechanisms and pathways to the realization of data subjects’ rights, especially in face of security, intelligence or criminal investigation activities⁶⁵.

Regarding Russia, although there are specific provisions related to personal data processing by State authorities in the Federal Data Protection Law, there remains broad powers with minimal oversight, particularly under the Yarovaya Law (Federal Law of March 6, 2006 No. 35-Fz on counterterrorism) and the Data Localization Law (Federal Law No. 242-FZ), as well as the Data Protection Act (Federal Law No. 149-FZ). As noticed in the Chinese scenario, these laws can be used to enable extensive state access to personal data, especially for purposes related to national security and anti-terrorism, with few constraints and limited transparency. Russia’s personal data law framework technically acknowledges privacy rights, but enforcement is inconsistent. Notably, the Federal Security Service (FSB), the Russian government’s internal security and counterintelligence agency, has wide-ranging authority to access stored data without subject notification. The absence of independent oversight mechanisms is particularly concerning, as this leaves individuals with limited avenues for challenging or even being aware of government data access.

India’s Digital Personal Data Protection Act of 2023 contains equally general language that leaves leeway for ample governmental access and processing of personal data. This is especially evident in its section 17. Section 17 (1) creates exceptions to the application of Chapters II (obligations of data fiduciary) and III (rights and duties of data principal), as well as section 16 (restrictions of international transfers) for law enforcement, criminal investigations and judicial activities. Section 17 (2) creates an ample exception to the Act when personal data is processed by State actors when:

17 (2) The provisions of this Act shall not apply in respect of the processing of personal data — (a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and (b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.

These jurisdictions share the issue of containing overly broad permissions or insufficiently defined safeguards to government access and processing of personal data, especially in activities related to security and intelligence. Brazil’s LGPD, on the other hand, contains a chapter solely dedicated to

⁶⁵ Jan Czarnocki and others, ‘Government Access to Data in Third Countries’ (European Data Protection Board 2021) EDPS/2019/02-13.

personal data and processing by public authorities, besides containing specific legal bases for execution of public policies requiring personal and special category personal data processing. That chapter's contents provide specification on the conditions under which processing by public authorities may take place, such as the connection of the stated purpose to public interest objectives, transparency and accountability duties, indication of a Data Protection Officer, and the exceptional cases where data may be transferred to private entities from those public authorities.

However, article 4 of LGPD also contains a set of broad exceptions for public security, national defence, state security, and activities for the investigation and prosecution of criminal offenses. These cases should be regulated in a specific law, but such law does not exist yet, which leaves a significant legal gap in control over government access to personal data in crucial hypotheses. The LGPD principles still apply, as well as the existing safeguards in laws such as Law No. 9,296/1996 (Interception of Communications), Law No. 12,850/2013 (Organized Crime Law), Law No. 13,344/2016 (Human Trafficking Law), and Law No. 12,965/2014 (Marco Civil da Internet), where applicable, such as the need for judicial authorization for accessing personal data and judicial oversight of such activities.

Finally, South Africa is a similar case to Brazil, as POPIA creates an exception for use of personal data by a public body (section 6 c):

- (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

Government access and processing of personal data in these cases is regulated by other norms, such as the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), the National Strategic Intelligence Act and the Cybercrimes Act. All these have faced criticism before for overly broad language and a lack of safeguards, such as “notification to the subject of surveillance, independent judicial authorization, protection for journalists and practicing lawyers, and proper management of intercepted information”⁶⁶, issues that have led the country's Constitutional Court to declare RICA unconstitutional⁶⁷ and to attempts to reform it to better protect privacy⁶⁸.

In summary, a crucial tension point in government access to personal data are those cases where public security, national defence and intelligence activities are involved. China, Russia and South Africa showcase issues in existing regulation of these activities, with overly broad language which leaves space for abuses. Brazil is lacking in terms of specific regulation of government access to personal data in these exceptional cases, however it does provide specific guidance in other situations and has pre-

⁶⁶ Anja Hofmeyr, 'An End to Secret State Surveillance under RICA' (*Cliffe Dekker Hofmeyr*, 16 February 2021) <<https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/Dispute/Dispute-Resolution-Alert-16-February-2021-An-end-to-secret-state-surveillance-under-RICA.html>> accessed 8 November 2024.

⁶⁷ *ibid*.

⁶⁸ Admire Moyo, 'Good Attempt but RICA Bill Still Flawed, Say Legal Experts' (*ITWeb*, 15 November 2023) <<https://www.itweb.co.za/article/good-attempt-but-rica-bill-still-flawed-say-legal-experts/P3gQ2qGAPRG7nRD1>> accessed 8 November 2024.

existing laws that provide some safeguards regarding privacy in the course of those state activities that are accepted in the general data protection law.

1.5. Data Protection in the new BRICS: Egypt, Ethiopia, Indonesia, Saudi Arabia, the United Arab Emirates, and Iran

As we have pointed out in the introductory chapter of this volume, the BRICS grouping has recently expanded including four new members: Egypt, Ethiopia, the United Arab Emirates and Iran. The first three have all approved general data protection laws in the past two years. In July 2020, Egypt adopted its Resolution No. 151 of 2020 on the Protection of Personal Data; in 2021, the United Arab Emirates adopted the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, which entered into force in January 2022; and in July 2024, Ethiopia enacted the Personal Data Protection Proclamation No. 1321/2024. Only Iran is still in the process of elaborating its framework upon the Draft Protection of Personal Data Law, proposed by the Ministry of Communications and Information Technology and announced in 2018.

Given the very recent entry of these countries in the BRICS grouping as well as their relatively reduced experience with data governance, the new BRICS members' framework have not been analyzed in detail, but some key features of their data protection laws are explored in this section. Notably, we highlight the existing set of principles, data subject rights, data security obligations, and data transfer mechanisms embedded in their respective legislations, as these elements might be particularly relevant regarding the new BRICS quest to develop "a global framework for data governance, including cross-border data flows, to [...] ensure the interoperability of data regulatory frameworks at all levels."⁶⁹

1.5.1. Egypt

Egypt's Personal Data Protection Law, No. 151 of 2020 was published in the Official Gazette on July 15, 2020, and came into effect on October 14, 2020. Its introduction was motivated by the increasing reliance on digital technologies and the need to safeguard citizens' personal data amidst rising concerns about privacy violations and data misuse. The law mandates that personal data be collected for specific, legitimate purposes that are clearly communicated to the data subject. Article 3 also states that the data must be accurate, valid, and secured, processed legally and within the scope of its collection purposes. Retention of personal data should not exceed the necessary duration for its intended purpose. The law also requires data controllers to ensure the confidentiality and security of personal data, preventing unlawful access, breach, damage, alteration, or manipulation through illegal procedures, per Article 4.⁷⁰

Article 2 grants Egyptian citizens several rights under this law, including the right to know, review, access, and obtain their personal data; to withdraw prior consent for the retention or processing of their personal data; to rectify, edit, erase, add, or update their personal data; to limit the scope of data processing; to be informed of any personal data breach affecting their data; and to object to the processing of their personal data or its results if it conflicts with their principal rights and freedoms.

⁶⁹ BRICS. Kazan Declaration (2024). Paragraph 71.

⁷⁰ See Baker and McKenzie. Egypt: Government issues new data protection law. (28 Sept 2020).

<https://insightplus.bakermckenzie.com/bm/data-technology/egypt-and-united-arab-emirates-egypt-issues-new-data-protection-law>

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

As regards data security obligations, Article 7 mandates that data controllers must report personal data breaches to the Data Protection Centre within 72 hours. Breaches related to national security must be reported immediately. Controllers also need to inform the data subject within three business days, detailing the steps taken. A Data Protection Officer (DPO) must be appointed to oversee data protection compliance (Article 8).

Transferring personal data to a foreign country is prohibited unless the destination guarantees equal or higher protection levels, and a license or permit is obtained (Article 14). Indeed, Article 14 of the Law mandates that any company wishing to transfer personal data outside of Egypt must first obtain a license from the Regulator. Moreover, such transfers are permitted solely to countries that provide a level of protection for personal data equivalent to that established by Egyptian law. Article 15 outlines several exceptions to the restrictions imposed by Article 14, all of which are contingent upon the prior acquisition of explicit consent from the data subject. Conditions for transfer include the conformity of the data's nature or purpose, legitimate interest in the data by controllers, processors, or subjects, and a data protection level abroad that is not below Egypt's standard (Article 16).

To enforce the provisions of this law, the Egyptian government established the Personal Data Protection Centre (PDPC) as the independent regulatory authority responsible for overseeing compliance. Article 19 delineates an extensive array of duties and competencies assigned to the Regulator. Notably, it is tasked with the responsibility of issuing licenses to companies for the processing of data and for facilitating cross-border data transfers. The PDPC is tasked with issuing licenses for data processing activities and ensuring adherence to the law's requirements. It has the authority to impose administrative penalties for non-compliance, including fines and operational restrictions.

Despite the establishment of this regulatory body, the law has faced criticism regarding its implementation and potential shortcomings. Critics argue that the law lacks clarity in certain provisions, particularly concerning the rights of individuals and the obligations of data controllers. Additionally, some stakeholders worry that the law may not adequately protect against state surveillance practices, given Egypt's historical context of stringent governmental control over personal freedoms.

1.5.2. Ethiopia

Ethiopia's Personal Data Protection Proclamation No. 1321/2024 stipulates that data collection and processing should be limited to specific purposes explained to users, ensuring legitimacy and transparency (Article 6). Users must be informed about how their data is handled (Article 12).

Ethiopian citizens have rights to be informed about data processing activities (Article 24); access their personal data (Article 25); correct or erase data under certain circumstances (Articles 27 & 28); restrict processing (Article 30); object to processing for specific reasons (Article 29); and receive their data in a transferable format (Article 32).

The Proclamation on Personal Data Protection was enacted in May 2022 as part of broader reforms aimed at modernising the country's legal framework in line with international standards. This law emerged from a growing recognition of the need to protect personal information amid rapid digital transformation and increased internet penetration in Ethiopia. The Proclamation seeks to establish clear guidelines for data processing activities while safeguarding individual privacy rights. Its approval marked a significant step forward in addressing concerns about data privacy in a country where such regulations were previously lacking. However, the Ethiopian government later decided to designate

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

the Ethiopian Communications Authority (ECA) as the data protection regulator, raising significant concerns regarding impartiality and accountability of the organ.⁷¹

Critics argue that entrusting a government agency with such a critical role undermines the effectiveness of data protection measures, as the ECA is inherently susceptible to governmental influence, which may compromise its ability to operate independently and objectively. Furthermore, the ECA's oversight capabilities are questioned in light of its existing responsibilities to oversee the telecoms sector, leading to fears that it may prioritize governmental interests over personal data protection.

The proclamation mandates the implementation of measures like encryption and data transfer restrictions, providing safeguards against unauthorized access, disclosure, or data loss (Article 17). Personal data cannot be transferred to countries lacking adequate data protection standards unless certain conditions are met (Article 18). These conditions include: adequate protection abroad; data subject's informed consent; necessity of the transfer according to the Proclamation standards, which include execution of a contract; and transfer of personal data collected from a public register (Article 20).

1.5.3. Indonesia

Through the enactment of Law No. 27 of 2022, Indonesia's Personal Data Protection Law (PDP Law) enables Indonesia to closely align with international standards of data privacy, modelled on the European Union's General Data Protection Regulation. Following the enactment of the PDP Law, data controllers and processors were given a two-year transition period to conform, which ended on 17 October 2024. Before the PDP Law, Indonesia did not have a comprehensive law on personal data protection, instead separate legislations which were either sector, matter or nature specific that regulated general aspects of privacy and personal data protection.

Under Article 20 of the PDP Law, for data processing to be lawful an organisation must either obtain express consent from the data subjects to process their data for specific purposes, or be fulfilling contractual obligations, protecting key interest of the data subjects, serving public interests, complying with legal requirements, or have a legitimate interest. The Indonesian Data Protection Authority is formally tasked with the functions of policy specification, supervision and enforcement of the PDP law, including dispute resolution, as defined by Articles 58-61 of the legislation. However, the Authority has not been established yet, at the time of this writing, and the Ministry of Communication and Informatics (MOCI) is temporarily fulfilling the abovementioned responsibilities, ensuring compliance, supervising the implementation of data protections, coordinating cross-border data transfers, overseeing notifications of data breaches and enforcing sanctions for non-compliance.

The PDP Law outlines key principles that govern the collection and processing of personal data in order to address their country-specific concerns whilst aligning Indonesia's data protection standards with international standards, thus improving the safety and trust of digital interactions within Indonesia. These principles include lawfulness and transparency (Article 27), purpose limitation (Article 28), data minimisation (Article 27), accuracy (Article 29), and integrity and confidentiality (Article 36). Data subjects are also afforded several rights, including the right to be informed (Article 5), right to access (Article 7), right to erasure (Article 8), right to rectification (Article 6), right to restrict processing (Article

⁷¹ Ashenafi Endale. Critics fear Comms Authority personal data dominion, impartiality in legislative wrangle. (13 January 2024) <https://thereporterethiopia.com/38279/>

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

11), right to object to processing (Article 8), right to data portability (Article 13), right to withdraw consent (Article 9), right to sue and receive compensation (Article 12), and the right to object to automated decision-making (Article 10).

The law requires certain organisations to appoint a Data Protection Officer (DPO) per Article 53, a role crucial in ensuring data protection regulation compliance. An organisation is required to appoint a DPO if processing personal data is part of their core activities or if an organisation handles large quantities of sensitive personal data. A failure to appoint a DPO where required can lead to administrative sanctions such as a written warning, fine or temporary suspension of data processing activities.

Although the PDP Law does not provide any specific technical measures or standards, Article 35 specifies general measures to data controllers as they are obligated to protect and ensure the security of the personal data that they process. These obligations include the setting out and implementation of operational technical measures in order to protect personal data from any disruption whilst being processed which is contrary to law and regulation provisions, and to determine the appropriate level of security necessary for the personal data by taking into account the nature of the data and risks. Importantly, when data breaches occur, the data controller and data processor must notify the affected data subjects and the Indonesian DPA within 72 hours and include the personal data involved, when and how the breach occurred and any measures taken to mitigate harm, per Article 46.

Lastly, article 56 of the PDP Law sets data transfer conditions in order to ensure that cross-border personal data transfers from Indonesia meet clear data protection standards. The recipient country must have a level of personal data protection that is equivalent to or exceeds that which is provided under the PDP Law. The yet-to-be-established Indonesian Data Protection Authority will be the entity responsible to perform such assessment. If this level of adequate protection is not met, the data exporter must ensure that binding, adequate safeguards, such as standard contractual clauses (SCCs) are in place. If neither adequacy of protection nor appropriate safeguards are in place, prior consent is required from the data subject, per Article 56(4).

1.5.4. Saudi Arabia

The Kingdom of Saudi Arabia's Personal Data Protection Law (PDPL) was issued 16 September 2021 and then amended 27 March 2023. It is based on a similar set of key principles that we find in most BRICS countries, set by Article 11, including lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. According to Article 5(1) PDPL, the primary legal basis for the processing of personal data is consent from the data subject. However, the PDPL also provides circumstances where consent is not required for the processing of personal data, such as compliance with a legal obligation or is necessary for the fulfilment of a contract (Article 6.2), and for the purpose of legitimate interest (Article 6.4).

Data controllers are obligated to comply with the PDPL, including the restriction on the use of personal (Article 14) and sensitive data (Article 35), and to enforce security measures (Article 19) and manage data breaches (Article 20). Furthermore the PDPL mentions in Article 30(4)(c) the need for data controllers to register with the 'Competent Authority', the Saudi Authority for Data and Artificial Intelligence (SDAIA). Article 30(2) states that data controllers must also appoint a data protection officer in certain cases such as when the data controller is a public entity who processes personal data

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

on a large scale, when large scale personal data processing is a primary activity or when processing sensitive data is a core activity of the data controller.

Article 4 of the PDPL also affords individuals data subject rights in order to empower their citizens and increase their level of control over their personal data. These rights include the right to be informed (Article 4.1), a right to access their personal data (Article 4.2), a right to request correction if their personal data is inaccurate, incomplete or out of date (Article 4.4), a right to request erasure (Article 4.5), a right to withdraw consent (Article 5.2), and a right to request provision of personal data in a readable and clear form (Article 4.3). Whilst these rights provide a level of control to individuals, their enforcement relies upon the performance of the newly created SDAIA.

Lastly, data transfer are specifically regulated by Article 29 of the PDPL. Organisations willing to transfer Saudi personal data must ensure the receiving country has an adequate level of personal data protection, per Article 29(2)(b). If the protection level falls below the PDPL standards, additional safeguards is necessary. These safeguards may include standard contractual clauses (SCCs) or binding corporate rules (BCRs). Furthermore, the Law sets additional requirements for the transfer of sensitive data, including the implementation of appropriate security measures to protect the personal data when at rest and in transit, notifying the data subject about the transfer and providing them with information regarding the data protection laws of the recipient country, and obtaining a written agreement from the receiving organisation which outlines the security measures that will be utilised to protect the data. Importantly, the Article 1(11) of law provides an explicit definition of sensitive data, which include but are not limited to: biometric data, data on sexual orientation, ethnic origin, religious beliefs, children's data, criminal records, political opinions, and health data.

1.5.5. United Arab Emirates

The United Arab Emirates' Federal Decree-Law No. 45 of 2021 prescribes lawfulness, fairness, transparency, purpose limitation, data minimization, data quality, retention, and security. Additional provisions may be detailed in the Executive Regulations (Article 5). The Federal Decree-Law was enacted in September 2021 as part of a broader vision to enhance privacy protections as a strategic step to foster legal certainty within a rapidly evolving digital landscape. This law reflects a commitment from UAE authorities to align local regulations with global standards, such as GDPR and OECD Guidelines, while promoting innovation and economic growth through digital transformation initiatives.⁷²

According to the new framework, UAE citizens have rights to access their data; transfer their data; object to data processing; rectify and erase their data; have their data processed without consent in specific cases (e.g., public interest, health protection, contractual performance) (Article 4). The law also requires the implementation of technical and organisational measures to maintain high data security standards, such as encryption and pseudonymization. Measures must ensure the availability and testing of the effectiveness of implemented security protocols (Article 20). A DPO with sufficient skills and knowledge in data protection must be appointed (Article 10).

The enforcement of this law is managed by an independent regulator known as the UAE Data Office, which operates under the Ministry of Digital Economy. This office is tasked with overseeing compliance

⁷² See the official website of the United Arab Emirates, dedicated to data protection issues <https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws>

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

with data protection regulations, providing guidance to organizations on best practices, and handling complaints from individuals regarding potential violations of their data rights. The UAE Data Office has been empowered to issue fines for non-compliance and ensure that organizations adhere to established standards for data processing and protection.

Lastly, data transfers are restricted to approved countries or specific situations (e.g., contractual necessity, public interest). There is no mechanism to use contracts to safeguard data transfers to unapproved countries, according to Articles 22 and 23 of the decree-law.

Despite these advancements, critics have raised concerns about certain aspects of the UAE's data protection regime. Some argue that while the law establishes important principles for personal data handling, it lacks robust mechanisms for accountability and transparency, particularly regarding government access to personal information. Additionally, there are worries about how effectively individual rights will be enforced in practice.

1.5.6. Iran

As mentioned previously, Iran has not enacted yet a comprehensive data protection framework, although the Ministry of Communications and Information Technology proposed a Draft Protection of Personal Data Law in 2018.⁷³ Importantly, the draft has been criticized for being “poorly conceived and inconsistent with the international legal obligations of Iran to adequately protect the privacy rights of its citizens” including by failing to clearly define the key data protection principles that typically represent the conceptual basis of each data protection framework.⁷⁴ Furthermore, the draft also includes broad definitions of “security” exceptions in Article 12, which has been criticized for allowing data processing under vague circumstances related to national security.⁷⁵

Oversight of the implementation of this law is to be managed by a yet-to-be-created Data Protection Commission, as proposed in Article 13. This commission would be tasked with ensuring compliance with the law and protecting individuals' rights concerning their personal data. However, concerns have been raised regarding the composition of this commission, as it may include members associated with security agencies. This raises questions about the effectiveness and impartiality of oversight in a context where governmental surveillance is common.

As regards regulating personal data transfers, it is important to note that Article 38 of the draft law sets data localization requirements limiting “foreign-based processing.” Indeed, the article would prescribe that Iranian citizens’ personal data “can only be stored in the data centres located in the sovereign realm of the Islamic Republic of Iran or the foreign-based data centres approved by the relevant authorities.”

1.6. Transborder data transfers in the BRICS

Normative mechanisms regulating international data transfers and including some forms of data localization present some converging paths among BRICS countries while each country has established unique mechanisms to regulate them, with varying degrees of flexibility.

⁷³ Mohammad Mustafa Mohiqi. Personal Data Protection in the Iranian Legal System. *Journal of Politics and Law*; Vol. 16, No. 3. (2023). <https://doi.org/10.5539/jpl.v16n3p10>

⁷⁴ See Article 19. Iran: Personal Data Protection and Safeguarding Draft Act. (June 2019).

<https://www.article19.org/wp-content/uploads/2019/06/Legal-Analysis-of-Draft-Data-Protection-Act.pdf>

⁷⁵ *Idem*.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

The elements of convergence and divergence in the BRICS frameworks regulating data transfers reveal idiosyncrasies of each country's jurisdiction and approach to personal data regulation. Even where the rules converge amongst BRICS countries, it is interesting to observe the small differences that exist, which point to the juridical specificities of each system and the often-heterogeneous manners for implementing similar normative prescriptions through regulatory techniques.

The following sections provide an overview of the main regulatory strategies adopted by the BRICS countries to frame international data transfers, comparing these approaches to subsequently identify what could be the most promising path for cooperation in data governance. Lastly, the concluding section of this chapter dares proposing some concrete guidance regarding how such cooperation could be enacted by the BRICS grouping, leveraging the existing venues to enhance their digital cooperation.

1.6.1. Consent and adequacy decisions

One resounding element of convergence is represented by data transfers based on the data subject's consent. This legal basis allows data processing in all jurisdictions. It comes surrounded by adjectives that give specific requirements for its validity, such as "full knowledge, and in a voluntary and explicit statement" (China's PIPL, art. 14); "free, specific, informed, unconditional and unambiguous with a clear affirmative action" (Indian DPDP Act 2023, section 6) "voluntary, specific and informed" (RSA's POPIA, art. 1); and "free, informed and unequivocal" (Brazilian LGPD, art. 5). The Russian 2015 Data Localization Law has also required data operators to process personal data of Russian citizens within Russia as a "primary" jurisdiction for the database, although data can be transferred abroad when complying with additional requirements.

Interestingly, in the DPDP Act, the general standard adopted by the law is based on non-restriction of data transfers, unless the Indian Government defines specific limits, such as the Reserve Bank of India's Directive 2017-18/153, whose paragraph 2(i) mandates data localization for payment system providers, that are required to store payment data within India.

Hence, in all BRICS jurisdictions, consent is one of the possible legal bases for data processing in general, which becomes particularly useful in case of data transfers. However, the qualification of consent with varying strict conditions aims at making sure that it truly represents the will of the data subject, while also maintaining more leverage in the regulators' capability to restrict transfers if needed.

In the case of international data transfers, consent is a possible legal basis in all BRICS jurisdictions, except for a significant difference in the case of China. Indeed, due to the specific structure of PIPL's article 13, consent cannot be deemed as an independent legal basis allowing data transfers, but rather as a prerequisite of almost any international data transfer, which must also observe the requirements set forth in art. 38.

In other words, except under one of the six non-consent cases in article 13 of the PIPL, it is a necessary legal basis for data transfers outside of Chinese borders. Additionally, these transfers must either pass a security assessment by a state agency, undergo a personal information protection certification as regulated by a state cybersecurity and informatization department, or implement standard contractual clauses, recently adopted by China⁷⁶. This creates a unique structure enabling the control of data

⁷⁶ CAC and China, 'Standard Contractual Measures for the Transmission of Personal Information [Automatic Translation]' (*Cyberspace Administration of China*, 24 February 2023) <http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm> accessed 20 June 2023.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

transfers, whereby the state maintains important regulatory prerogatives regarding cybersecurity and data protection matters, being able to define under what conditions transfers are allowed. This approach aligns with the Chinese data architecture's close ties "with data sovereignty, national security and increasingly personal data protection to maintain the 'legal, secure and free flows' of transborder data"⁷⁷.

Given the existence of consent as a shared legal ground for personal data processing, with some specific caveats, it is important to emphasise that the design of contractual tools based on the joint application of consent as a lawful ground for processing and the adoption of model contractual clauses as a facilitator of international data transfers may be one of the most promising strategies to foster intra-BRICS data flows. This option will be explored in further details in the following sections, to understand the extent to which it might be feasible and under what conditions.

Another increasingly widespread regulatory basis for the international transfer of personal data is the use of the so-called "adequacy decisions"⁷⁸ issued either by the national data protection regulator or a government branch, recognising the substantially equal level of data protection in third countries and, therefore, allowing data transfers. Being the first BRICS country to have adopted a data protection framework, Russia offers an interesting example of the use of adequacy decisions, as it automatically extends such recognition to all signatories of the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, more commonly known as "Convention 108" and signed by Russia in 2006⁷⁹. Furthermore, Roskomnadzor, the Russian ICT regulator, has also formally deemed as adequate numerous non-European countries, such as Argentina (which received adequacy also from the European Union) and several African countries that the European Commission has never considered as adequate, such as Angola, Benin, Gabon, Mali, Morocco, South Africa, and Tunisia.⁸⁰

Importantly, the majority of BRICS countries' data protection frameworks, except for South Africa and India, contain provisions allowing international data transfers in accordance with specific international engagements. China and Brazil share a commonality regarding this hypothesis. Both countries allow international data transfers in compliance with treaties concerning judicial or law enforcement cooperation, with an additional mention of "intelligence" activities that justify personal data transfers in the case of Brazil.

This latter point seems particularly puzzling in the case of Brazil, since the Brazilian LGPD excludes from its scope data processing for law enforcement purposes, thus creating a remarkably wide grey area allowing the transfer of data but exempting law enforcement from abiding to the general data protection framework.

Indeed, Brazil allows data transfer under the more general "international agreements" category in article 33, VI – "where the transfer results in a commitment undertaken under an international

⁷⁷ Yik-Chan Chin and Jingwu Zhao, 'Governing Cross-Border Data Flows: International Trade Agreements and Their Limits' (2022) 11 *Laws* 63, 6 <<https://www.mdpi.com/2075-471X/11/4/63>> accessed 4 July 2023.

⁷⁸ Adequacy evaluations, according to which a national regulator determines if a foreign jurisdiction's data protection law meets the national standards, have become widespread in many countries while being based on highly diverse criteria. According to a recent study, besides the European Union, sixty-five countries have already established adequacy reviews of foreign jurisdictions to ascertain if international transfers of personal data may be allowed to cross their borders. See Chander, Anupam and Schwartz, Paul M., *Privacy and/or Trade* (February 18, 2022). 90 *University Chicago Law Review* 49 (2023).

⁷⁹ Council of Europe, 'Chart of Signatures and Ratifications of Treaty 181' (*Treaty Office - CoE*) <<https://www.coe.int/en/web/conventions/full-list>> accessed 20 June 2023.

⁸⁰ See *Ibid.* p. 75.

cooperation agreement”. It must be acknowledged that the wording of this provision creates remarkable confusion, since, if taken at face value, it seems to enact conditional legality of a current data transfer. A less unclear formulation could have suggested the legality of transfers resulting *from* a commitment, rather than *in* a commitment. This obscure provision may lead to multiple interpretations. It could be that the legislator intended to allow for the preparatory measures for an international agreement, or that the data transfers following an international agreement are allowed. The exact sense and the solution to this legal conundrum remain open to the Data Protection Authority’s guidance.

Lastly, the new BRICS countries present a similar set of options. Apart from the above-mentioned embryonic Iranian framework, which seems to propose a general data localization mandate, all the other newcomers in the BRICS grouping allow data transfers to countries deemed as adequate by the national regulators, or under other specific conditions. Article 15 of the Egyptian law allows transfers when a license has been obtained from the DPA and where the level of protection is not less than that provided under the Law. However, the Law does not specify the criteria to be followed to ascertain which national regimes can be deemed as adequate unlike other data protection laws. As such, the DPA will need to define the criteria for adequacy and licenses for cross border transfers in future policies and regulations.

The Ethiopian Proclamation presents a more ample menu of options allowing data transfers when the data controller or processor must provide evidence that the receiving jurisdiction has an appropriate level of protection for personal data, as outlined in Article 18 of the Proclamation; when the data subject has given explicit consent for the transfer after being informed about the potential risks involved; when the data transfer is necessary according to the provisions of the Proclamation (Article 20), such as contractual obligations or legal compliance; and when personal data is originally collected from a public register intended to provide information to the public (Article 21).

Lastly, the UAE framework allows data transfers through signing agreements with foreign institutions and companies to comply with the UAE personal data protection law, and where either consent is provided, or the transfer is contractually necessary.

1.6.2. A BRICS-led approach to international data transfers rules

A BRICS-led approach to international data transfers could be seen in two perspectives. On the one hand, it could act as a framework facilitating data flows amongst BRICS members and partners, providing an alternative to established international data governance frameworks, such as the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, better known as Convention 108, or the African Union Convention on Cyber Security and Personal Data Protection, better known as Malabo Convention. In this perspective, the aim of the possible shared solutions would be to foster legal interoperability amongst leading emerging economies.

On the other hand, a BRICS-led approach may be particularly interesting as a prototype of what could be scaled up as a global framework for data governance, promoted by the “locomotive forces of the Global South.”⁸¹ These options are not mutually exclusive and, on the contrary, they are complementary. In both cases, besides fulfilling the commitments of the Kazan Declaration, setting the bases for the elaboration of a global framework for data governance, a BRICS enhanced cooperation

81 Belli, L. BRICS: The New Digital Locomotives. Beijing Review. (11 July 2022).
<https://www.bjreview.com/Opinion/Voice/202207/t20220711_800300500.html>

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

on these matters would contribute directly to the implementation and expansion of the 2021 BRICS Framework for Ensuring Consumer Protection in e-Commerce.⁸²

This consideration is particularly relevant as talks around a multilateral framework for e-commerce, which would include aspects of cybersecurity and personal data protection, have been ongoing under the World Trade Organization's Joint Initiative on E-Commerce, which delivered a "stabilized text" after five years of negotiations"⁸³. WTO efforts might prove useful to identify elements of consensus, but they might have limited effectiveness, per se, due to the current WTO paralysis. Given the recent adoption of a UN Convention against Cybercrime proposed and brokered under the relevant influence of BRICS countries, it would be interesting to utilize the BRICS as a laboratory to test the elaboration of the data governance framework to be discussed at the UN level. In this perspective a BRICS-led initiative could be built to complement and expand the UN Proposed Normative Foundations for International Data Governance: Goals and Principles⁸⁴, with the aim of providing concrete proposals to support international data governance.

Moreover, as mentioned in the introduction of this volume, since the 2021 BRICS Summit, resulting in the New Delhi Declaration, BRICS leaders have not only established a formal mechanism for enhanced cooperation in e-commerce but they have also expressed the intention to "[...] advance practical intra-BRICS cooperation in [cybersecurity] including through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring Security in the Use of ICTs and the activities of the BRICS Working Group on Security in the use of ICTs, and underscore[d] also the importance of establishing legal frameworks of cooperation among BRICS States on this matter and acknowledge[d] the work towards consideration and elaboration of proposals, including on a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries."⁸⁵

In this perspective, one of the reasons of the BRICS grouping's unusual character is that despite their highly heterogeneous nature, all countries have relevant interests in increasing both cybersecurity and trade, by leveraging data processing fostering their data sovereignty.⁸⁶ As noted by Burri, all these international developments reveal the "intensified contestation between free data flows as an essential element of the data-driven economy and the protection of privacy as a sovereign right of states to safeguard their citizens"⁸⁷. As such, they are ongoing processes that will determine sovereign states' policy choices – such as the ability to enact data localization legislation, to adopt policies directed at concepts such as "data sovereignty" and to promote policies directed at promoting digital development and bridging existing divides⁸⁸.

82 BRICS. BRICS Framework for Ensuring Consumer Protection in e-Commerce. (2021) <https://brics2023.gov.za/wp-content/uploads/2023/07/Framework-for-ensuring-consumer-protection-in-e-commerce-2021.pdf>

⁸³ WTO. Joint Statement Initiative on E-commerce. INF/ECOM/87. (26 July 2024). https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

⁸⁴ UN Chief Executives Board for Coordination. Proposed Normative Foundations for International Data Governance: Goals and Principles. United Nations system contribution to the advancement of international data governance. CEB/2024/2/Add.1. (8 November 2024). <https://unsceb.org/proposed-normative-foundations-international-data-governance-goals-and-principles>

⁸⁵ See *supra* n (701).

⁸⁶ Belli, Gaspar and Singh (2024) *supra*.










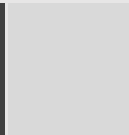
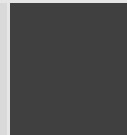



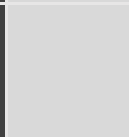

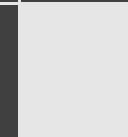


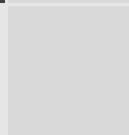



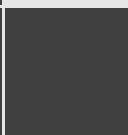
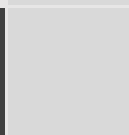
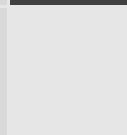
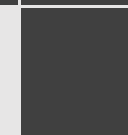
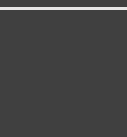
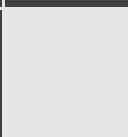
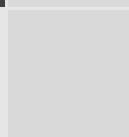
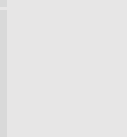
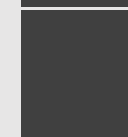
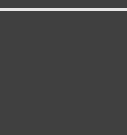

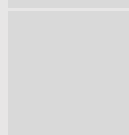

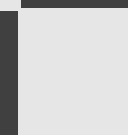
⁸⁷ Burri (n 784) 152.

⁸⁸ Chin and Zhao (n 773).

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

Data transfers are at the core of digital transformation efforts and, depending on how they are regulated, they can undermine or strengthen digital sovereignty.⁸⁹ The following table provides a schematic overview of the data transfer requirements defined by the BRICS countries in their respective frameworks.

Table 1.2 - BRICS international personal data transfer rules

Rule / Country	Norm absent in this jurisdiction =  Norm present in this jurisdiction = 				
	Brazil	Russia	India ⁹⁰	China	South Africa
Adequacy decision or adequate protection in destination country's law					
With consent from the data subject					
When related to international agreements					
Contract clauses (standard clauses or negotiated clauses)					
For the execution of a contract or its preliminary acts					
Global corporate norms					
Certificates and codes of conduct					

⁸⁹ Belli, Gaspar and Singh (2024) *supra*.

⁹⁰ India's Digital Personal Data Protection Act (DPDP Act) 2023 determines in section 17 that the government may restrict cross-border flows, but does not set localisation obligations or predetermined cross-border flow rules or restrictions. There are, however, sectoral regulations that prescribe data localisation for specific categories of data, and have been maintained by the Act, such as the Reserve Bank of India's localisation requirements. See Burman, 'Understanding India's New Data Protection Law' (*Carnegie Endowment for International Peace*, 3 October 2023) <<https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en>> accessed 7 November 2024.

Protection of life and health				
Authorization by the data protection authority				
To a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action				
Passing a security assessment organized by the State cybersecurity and informatization department				
When the transfer is necessary for the execution of public policy or legal attribution of the public service				
For the protection of values provided for in federal laws				
In the interest of the data subject				
To comply with a legal or regulatory obligation				
To exercise rights in a judicial, administrative or arbitration procedure				
Data localisation				
Source: the authors, based on Belli and Doneda 2022; CyberBRICS Project 2020. A detailed table can be found at: https://is.gd/uwapus .				

1.7. A principle-based approach for data governance cooperation in the BRICS and Beyond

Data Protection Authorities of the BRICS countries are called to play a fundamental role in the regulation of data transfers and digital trade, ultimately having the power to facilitate or limit legal interoperability among the BRICS members and beyond. In this respect, it seems important to emphasize that continuous interactions and cooperation between DPAs would be essential to reach common understandings of, for example, what are the basic data protection principles to which all

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

data processing activities shall abide and the minimum procedural and substantive protections for data subjects. The definition of such elements at the BRICS level, especially as regards a shared principle base, should be seen as a highly instrumental step towards the definition of a developing “a global framework for data governance, including cross-border data flows, to [...] ensure the interoperability of data regulatory frameworks at all levels.”⁹¹ Indeed, the agreement of a shared set of BRICS principles for data governance could help crystallize a consensus position upon which global efforts could be built.

Furthermore, the BRICS countries’ definition of pre-determined legal pathways of ensuring compliance across jurisdictions, as well as what certification schemes, contractual clauses, or binding corporate rules, can be mutually accepted. This scenario could be reached by formal and informal means, via formal intergovernmental cooperation projects involving DPAs as well as through dedicated research initiatives fostering shared analysis of common problems, such as the data governance-related activities promoted by the CyberBRICS project. As suggested by Belli and Doneda⁹² the ideal and most sophisticated type of cooperation could even take the form of “a general ‘BRICS Data Protection Framework’ or a more specific ‘BRICS Data Transfers Framework’ or ‘BRICS Data Security Framework’”. However, it is important to stress that, to date, no official coordination mechanism for BRICS Data Protection Authorities has been established and, typically, this type of effort requires considerable diplomatic preparatory work that may take several years to achieve even very timid results.

In this perspective, we believe that the first step should be the establishment of a BRICS Working Group on Data Governance, facilitating information exchange and involving the regulators, ideally, creating a calendar of regular meetings of the BRICS Data Protection Authorities. Such initiative could be moulded on the best practices defined by the BRICS Working Group on the Security of ICTs and the BRICS E-commerce Working Group. Indeed, a BRICS Working Group on Data Governance would play an instrumental role to promote digital cooperation, stimulating the joint analysis of a variety of data-related issues of mutual concern, including automated processing of personal data and artificial intelligence regulation, while also preparing the terrain for the construction of a BRICS data governance framework.

While the establishment of a joint working group facilitating discussion could be relatively easy, it is important to acknowledge that the elaboration of an intra-BRICS data governance framework may be a much more ambitious and arduous task as it would require overcoming apparent incompatibilities and grey areas. Such incompatibilities include overbroad norms (e.g., the Russian mention of allowing transfers for the protection of the Constitution, national defence and state security), differing legal requirements or definitions (e.g., the Chinese general consent rules and the Chinese and Russian data localisation models) and very heterogeneous organisational structures (mainly, the matter of the independence of DPAs in each country’s administrative structure). This list may become even longer when considering the idiosyncrasies of the new BRICS countries, as illustrated in the previous section.

Such framework, however, should be seen as the final goal providing the necessary legal certainty for the flourishing of an open, secure and mutually beneficial digital environment, based on shared rules facilitating digital trade and services among BRICS countries, guaranteeing equivalent protections to

⁹¹ BRICS. Kazan Declaration "Strengthening Multilateralism For Just Global Development And Security". XVI BRICS Summit. Kazan, Russia. (23 October 2024). Paragraph 71. <https://dirco.gov.za/xvi-brics-summit-kazan-declaration-strengthening-multilateralism-for-just-global-development-and-security-kazan-russian-federation-23-october-2024/>

⁹² ‘Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence’ [2022] *International Data Privacy Law* ipac019, 43 <<https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipac019/6809023>> accessed 20 December 2022.

data subjects. Furthermore, such framework may be reached incrementally, starting by the definition of a less ambitious yet equally important set of shared data governance principles, upon which future agreements might be built. These principles not would only safeguard individual rights but also promote interoperability, enhance data security, and consider developmental aspects. This essay identifies key data governance principles grounded in existing norms.

Importantly, such principles can be already distilled from the comparison of the BRICS frameworks exposed in this volume and their agreement at the BRICS level could represent a positive step forward in the achievement of the goals recently set by the UN Global Digital Compact with regard to data governance at the international level, advancing “responsible, equitable and interoperable data governance approaches” with particular emphasis on data privacy and security and cross-border data flows.⁹³ In this spirit, the analysis conducted along this book illustrate that BRICS countries could already agree on a shared set of principles that can be distilled from their frameworks.

Below we propose a set of normative and operational principles that could be agreed upon by BRICS countries in order to enhance their cooperation on data governance.

Normative principles:

- Informational self-determination. This well-established data protection principle underpins the right and capacity to decide when and to whom (personal) data is disclosed, and the extent to which data can be processed. In its individual dimension, corresponding to the right of a natural person to control and determine what others can do with data that refers to them. Its collective dimension is the sentence of data sovereignty, corresponding to the sovereign right to promote the use and regulation of data in the national interest.
- Lawfulness and good faith. This principle applies to data processing at both national and international level, emphasizing that the processing of personal data must adhere to legal standards, being conducted in good faith by all actors involved in the processing, and only when an explicitly identified legal ground allows data processing. The principle is instrumental to ensure that individuals and regulatory authorities are informed about how their data will be used, guaranteeing that any kind of processing involving more than one entity at domestic or international level, will abide to agreed standards.
- Rights-based approach. A rights-based approach considers that data protection plays an essential role to foster the full spectrum of human rights and policy frameworks need to uphold individuals' rights of access, rectification, deletion, limitation of processing, portability and opposition.
- Informed consent. When processing of personal data relies on consent as a legal ground, consent must be a free, informed and unequivocal expression of the data subject's agreement to the processing of his/her personal data for a specific purpose.
- Purpose specification. Data processing should be limited to specific, legitimate purposes that are clearly defined at the time of collection. This principle mitigates the risks of misuse by ensuring that data is not used in ways that are incompatible with its original purpose.
- Transparency. This principle mandates that information regarding the processing of personal data, including about which entities are involved in such processing and how, is communicated to the individual to which the data refers to, in a clear, precise and easily accessible manner.

⁹³ The Global Digital Compact was adopted by world leader on 22 September 2024 at the Summit of the Future in New York. See United Nations Global Digital Compact A/79/L.2 https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf

- **Accountability.** This principle is highly complementary to legality and good faith as clear accountability mechanisms to ensure compliance with data governance norms. Accountability typically includes a clear definition of roles and responsibilities as regards data processing, keeping track of all data processing activities, conducting regular audits, and providing remedies for individuals whose rights have been violated.
- **Data security.** The data security principle mandates the implementation of appropriate technical and organizational safeguards against unauthorized access, loss, or damage to personal data. Effective security measures must be implemented from the conception until the implementation phase of the data processing to protect individual rights, preserve data confidentiality, integrity and availability, thus enhancing cybersecurity as a whole and, in turn, public trust in digital systems.
- **Necessity and proportionality.** This principle involves collecting only the data necessary for the specified purposes, thereby reducing the risk of exposure and misuse. The principle can be also referred to as “data minimisation.”
- **Data quality and accuracy.** According to this principle, processed data should be accurate and, where necessary, updated to fulfil the specified purposes. Hence, the parties responsible for processing data shall take reasonable steps to keep data up-to-date and eliminate incorrect data, particularly when decisions affecting individuals are made based on this information.
- **Non-discriminatory processing.** Processing of personal data cannot be carried out for unlawful or abusive discriminatory purposes.

Operational principles

- **Effective oversight and remedies.** This principle requires the establishment of well-resourced regulatory bodies capable of enforcing data protection laws and promoting a culture of compliance. Hence, regulators must ensure that individuals are fully informed about their data rights and have accessible mechanisms to seek redress, while data processors are held accountable for their practices.
- **Interoperability.** To facilitate cooperation in data processing at both national and international level, technical and legal interoperability is essential. This principle mandates the adoption of shared and compatible technical and normative standards that enable seamless cross-border data flows while maintaining high levels of information security and trust.
- **Secure and Legal Data Transfers.** This principle aims at ensuring that data subjects' rights are safeguarded and data-related obligations are respected, even when data are transferred internationally, thus preventing unauthorized access and misuse of personal data during cross-border transfers.
- **Privacy by design.** This principle mandates a proactive approach that integrates data protection principles into the development and operation of technologies, systems, and business practices. This principle ensures that privacy is considered at every stage of the data lifecycle, minimizing risks and enhancing the protection of personal data by default
- **Promotion of Privacy Enhancing Technologies (PETs).** PETs play a remarkably important role providing software and hardware solutions aimed at strengthening data protection. PETs can be developed in the form of Digital Public Infrastructures (DPIs) by leveraging digital systems built on open, secure and interoperable technologies to facilitate safe and trusted exchange of data, based on user consent management.
- **Facilitative regulation.** Facilitative regulation is based on the dedication of financial resources in the form of investments, tax exemptions, and grants to promote research, development and innovation that promote data processing in alignment with data protection principles. This

principle encourages the funding and adoption of innovative solutions that enhance data security, privacy, and compliance, so that technological advancements contribute positively to data governance frameworks.

The abovementioned principles are interdependent and serve as a foundation for building trust in digital ecosystems crucial for economic growth and social development, being instrumental to foster a cohesive approach to data governance at the BRICS and global level. However, the next section will argue that it is important to consider how BRICS countries are already regulating cross-border data flows, to be able to increment BRICS cooperation towards the definition of shared mechanisms, beyond, the identification of shared principles.

1.8. From shared Model Contractual Clauses to a BRICS-led data governance framework

The previous sections have highlighted the existence of common ground amongst the BRICS regarding the importance of consent as a shared legal basis allowing international data transfers as well as the relevant role played by data regulators in all the members of the grouping. Importantly, all BRICS except for Russia also deem as legal all data transfers occurring in accordance with model contractual clauses. While Russia does not recognize explicitly this option, the fact that transfers are allowed by the country in case of execution of a contract provides some room for potential use of model contractual clauses also in this country. Indeed, while such model contractual clauses would not be automatically recognized by the Russian system as a legal basis for data transfers per se, their inclusion in contractual agreements explicitly accepted by the data subject could reach the desired outcome. In this perspective, the use of BRICS model contractual clauses becomes a practical and pragmatic option for all the members of the grouping.

In terms of the actual language adopted in model contractual clauses, there are already existing references that might be indicative of a shared path in BRICS countries. Relevant references in this sense already exist, such as the Council of Europe Model Contractual Clauses for the Transfer of Personal Data, the ASEAN's Model Contractual Clauses, the Ibero-American Data Protection Network's, Model International Transfer of Personal Data Agreement, as well as China's Personal Information Export Standard Contract and Measures on the Standard Contract. These documents aim at providing adequate language to ensure that personal data are transferred with a corresponding level of protection in contracting parties' jurisdictions. They all draw inspiration from the EU's standard contractual clauses, but contain⁹⁴.

As indicated by Matheson and Roberts et al.⁹⁵, some topics of particular interest, due to representing relative convergence or divergence in these existing instruments, include:

- Subsequent processing of personal data after transfer, including government access requests and subcontracting of processing;
- Models differentiated according to the types of actors involved, i.e., controller-to-controller contracts, controller-to-processor contracts etc.;
- Pre- and post-transfer due diligence, audit and record-keeping obligations, including in reference to processing activities and purposes and their respective subsequent alterations;
- Choice of law and forum;

⁹⁴ Linklaters, 'Comparison. EU and China's Standard Contracts for Cross-Border Data Transfers'; Alex Roberts, Roger Li and Tiantian Ke, 'China's Standard Contract for Cross-Border Data Transfers Released: Key Implications and Comparison against the EU SCCs' (*Linklaters*, 7 March 2023) <<https://www.linklaters.com/en/insights/blogs/digilinks/2023/march/chinas-standard-contract-for-cross-border-data-transfers-released>> accessed 20 June 2023; Lee Matheson, 'Not-so-Standard Clauses. Examining Three Regional Contractual Frameworks for International Data Transfers' (Future of Privacy Forum 2023).

⁹⁵ Matheson (n 789); Roberts, Li and Ke (n 789).

- Transferring sensitive personal data and data related to automated decision-making.

These subjects are crucial to ensuring correct processing of personal data in international data flows, as well as legal certainty in face of contracting parties and the various legal systems involved. A BRICS-oriented project of legal interoperability based on model contract clauses would have to address these issues as a unified front, allowing for a facilitated exchange of data rooted in information security, national sovereignty, informational self-determination and protection of user rights. In this perspective, the Annex to this chapter offers a concrete blueprint that BRICS countries could follow to face these issues. Indeed, we believe that the proposed Model Contractual Clauses could be readily utilised to ensure an appropriate level of protection for the transfer of personal data within BRICS members.

As demonstrated in this volume, although most BRICS countries are at the beginning of their data protection journeys, they have made significant strides in this area, setting up their data architectures, and even proving their willingness to be creative rather than merely engaging in legal transplants. Further coordination in this area could prove beneficial and provide a pathway to the development of a “post-western model of data governance”⁹⁶ shaping rules governing international flows with a Global South perspective. A first step towards such vision could be the definition of BRICS model contractual clauses, regulating data transfers through an agile and more easily updatable tool that could be adopted by all current and future club members, with no need for a remarkably complex - if possible, at all - alignment of multiple adequacy measures or burdensome and highly unlikely international law instruments.

Importantly, the BRICS alignment towards shared data protection mechanisms has the potential to be particularly beneficial, reducing transaction costs, deflating barriers to cross-border trade, and fostering similar levels of protection of individual rights. The convergence towards increasingly legally interoperable frameworks is already happening due to a phenomenon of transnational diffusion,⁹⁷ grounded on a process of adoption and reproduction of rules, procedures and good practices that are deemed as reliable and efficient. On top of such phenomenon, BRICS countries are demonstrating their willingness and capacity to be innovators and offer important contributions to the creation of a new generation of data protection policy and technology tools. The definition of BRICS model contractual clauses, or even, perhaps one day, a BRICS-led international treaty on data governance or a more institutionalized mutual adequacy system may considerably boost digital trade and digital cooperation of the bloc, as long as data transfers are regulated in a way that enable electronic commerce and services while ensuring that national sovereignty is fully respected.

Given the BRICS appetite for artificial intelligence, Internet of Things (IoT), Smart Cities, fintech, and a variety of data-hungry technologies, and given the already relevant degree of compatibility of the existing BRICS data protection frameworks, this policy area should be considered a suitable testbed to further cooperation enhancement. In this sense, it is important to stress the BRICS leaders’ approval of the revised Terms of Reference of the BRICS Working Group on Security in the Use of Information and Communication Technologies (WGSICT), which plays a key role as regards BRICS digital policy coordination and cooperation, the BRICS Roadmap of Practical Cooperation on Ensuring Security in the

⁹⁶ Luca Belli, ‘New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a Post-Western Model of Data Governance’, *Indian Journal of Law and Technology* 18, no. 2 (2022): 1–58

⁹⁷ For a more detailed discussion on how juridical systems be interoperable, see Belli and Zingales, n (31).

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

Use of ICTs, and the recent establishment of the BRICS Framework for Ensuring Consumer Protection in e-Commerce.⁹⁸

In this context the BRICS leaders have explicitly reaffirmed “the importance of establishing legal frameworks of cooperation among BRICS member States on ensuring security in the use of ICTs and acknowledge the work of the WGSICT towards consideration and elaboration of proposals on this matter.”⁹⁹ Moreover, the 2021 BRICS Framework for Ensuring Consumer Protection in e-Commerce explicitly recognizes that “[a]dequate safeguards and measures are needed to ensure privacy and security of the consumers [and resolves] to enhance cooperation through the BRICS E-commerce Working Group”¹⁰⁰ thus elevating data protection to an explicit cooperation item in the BRICS digital policy agenda.

Considering the high level of compatibility of existing data protection frameworks in the BRICS and the ongoing tendency towards enhanced cooperation on digital matters, it would be interesting to see the WGSICT and the E-Commerce Working Group putting forward concrete proposals on a BRICS data cooperation framework, perhaps starting by proposing BRICS model contractual clauses for international data transfers. Both the WGSIC and E-Commerce Working Group enjoy a unique position as well as an explicit mandate to elaborate proposals in this sense, thus becoming a key vector of legal interoperability within the BRICS.

Such proposals would also allow to concretely implement a BRICS STI Architecture, offering a unique opportunity to test a cooperation mechanism that is explicitly aimed at improving the coordination of BRICS initiatives on science, technology, and innovation.

1.9. Conclusions

BRICS countries have demonstrated that, while they remain a very heterogeneous grouping, they can achieve impressive results, when coordinating joint concrete actions, spanning from the establishment of an entirely new global financial institution such as the New Development Bank, to the proposal and brokering of a new treaty, such as the UN Convention against Cybercrime. Despite their obvious diversity as countries, the BRICS perspectives over personal data protection align on many fronts, and their frameworks are already presenting a considerable level of compatibility, even in the absence of a formal international agreement.

Moreover, the BRICS have a relevant advantage of being a small club that continues to share an ample range of interests, although the recent expansion has brought considerable new complexity into the BRICS family. Enhancing intra-BRICS cooperation on digital matters, generally, and data governance, particularly, is not only possible, but it should be seen as strategic choice aimed at regulating international data flows in a secure and trustworthy fashion.

There is an increasing yearning for enhanced cooperation on digital governance amongst BRICS countries, as especially highlighted by the 2021, 2022, 2023 and 2024 BRICS Summit Declarations, as well a renewed political impetus, bringing willingness to expand the grouping and utilize it as a leading force for the Global South. Such cooperation may have a variable geometry, considering that some countries have a stronger ideological alignment than others, especially regarding the IBSA countries, the China-Russia duo, and the new middle eastern BRICS partners. However, considering that many

⁹⁸ See BRICS ‘Declaration of the 11th BRICS Summit’ (Brasília 2019) para 19 <<https://eng.brics-russia2020.ru/images/00/68/006895.pdf>> accessed 14 October 2023.

⁹⁹ See <https://is.gd/fuyito>.

¹⁰⁰ BRICS. Framework for Ensuring Consumer Protection in e-Commerce. (2021). <https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-44.pdf>

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) *Personal Data Architectures in the BRICS Countries*. Oxford University Press. (2025)

data protection policy elements are already remarkably compatible and converging, the enhancement of BRICS' legal interoperability looks not only feasible, but also achievable.

In their 2024 Declaration, BRICS leaders have made explicit their appetite for the development of "a global framework for data governance" and, as we argued in the introduction of this volume, BRICS policies are starting to be seen as models influencing other countries, especially in the Global Majority. The development of convergent and legally interoperable data protection frameworks should be uppermost in the list of their policy priorities as it is one of the few regulatory fields that is simultaneously key in protecting individuals, providing juridical certainty to businesses, fostering international trade, and enhancing cybersecurity.

Growing cooperation and legal interoperability amongst BRICS countries regarding digital policy is not only possible, it is already happening, and is explicitly advocated by BRICS leaders themselves. The degree of policy convergence now depends on how much BRICS will manage to synchronize their political priorities and, critically, how much they will decide to dare in the implementation of the tools that are at their disposal. The shared principles identified in the previous section and the Model Contractual Clauses included in the Annex offer a useful path to follow to enhance cooperation on data governance issues.

Indeed, as clearly demonstrated by the Kazan declaration, BRICS are interested in seizing the opportunity to further enhance their cooperation, as the increased convergence and compatibility of their data protection frameworks may be beneficial for both individuals and businesses in the grouping. To do so, multiple venues are available and should be explored. The BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs¹⁰¹ could offer a suitable framework for cooperation and implementation of the recent BRICS commitments to enhance intra-BRICS cooperation on digital policies and data governance, and to leverage the BRICS Science, Technology, and Innovation (STI) Architecture, which aims at enabling and evaluating BRICS initiatives in the STI field.

The BRICS Framework for Ensuring Consumer Protection in e-Commerce, could offer an interesting venue for experimentation of new proposals, and exchange of good practices through the BRICS E-commerce Working Group. Ideally, a new dedicated BRICS Working Group on Data Governance should be created to foster better coordination and exchange of information on the issue and, ultimately, facilitate the elaboration of BRICS Model Contractual Clauses – which can be based on the clauses we offer as annex of this chapter – and, if necessary, a more ambitious BRICS Data Governance Framework.

As discussed along this volume, the BRICS countries have many differences but also relevant incentives to deepen their cooperation and alignment, even more so considering their renewed impetus and recent expansion. The policy experimentation with the goal of establishing a new BRICS-led data governance regime should be considered seriously, beyond mere academic exercises, as it has the potential to set the basis for a new post-western model of data governance. Only history will be able to tell if the BRICS grouping will be able to play a major role in the development of a global data governance approach. Meanwhile, this volume offers a humble contribution to support a better understanding of where BRICS countries start from, which directions they may pursue, and which goals they may reach in their journey towards the construction of their personal data architectures, and how such architectures may contribute to their aspiration to shape global frameworks for data governance.

¹⁰¹ The Roadmap was proposed at the 8th BRICS Summit in Goa, India, and adopted at the 9th BRICS Summit in Xiamen, China. See <https://brics2021.gov.in/BRICSDocuments/2017/Xiamen-Declaration-2017.pdf>.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1.10. Annex: model contractual clauses for the transfer of personal data from controller to controller/processor in the BRICS countries

NOTE: These Model Contractual Clauses (hereinafter “the Clauses”) aim to ensure an appropriate level of protection for the transfer of personal data to countries that are BRICS members

PART I – GENERAL CLAUSES

Clause 1. Purpose and scope

1.1. The aim of these Clauses is to ensure compliance with the requirements for the Transfer(s) of Personal data to BRICS members. In this regard, these Clauses, together with their Annexes which form an integral part thereof provide an appropriate level of protection for the transfer of Personal data involved in the Transfer.

1.2. These Clauses shall apply to the Transfer(s) of Personal data as described in Annex 1.

1.3. The purpose(s) of the Transfer(s) of Personal data is described in Annex 1.

1.4. These MCC will apply, unless a more protective model or Data Protection law is available in the country of origin or the country of destination.

Clause 2. Definitions

As used in these Clauses, the following terms starting with a capital letter shall have the following specific meanings:

Applicable law: rules for the protection of Personal data applicable in the jurisdiction of the Data exporter.

Biometric data: data resulting from a specific technical processing of Personal data concerning the physical, biological or physiological characteristics of an individual, which allows the unique identification or authentication of the individual when it is precisely used to uniquely identify the data subject.

BRICS: bloc of countries formed by Brazil, Russia, India, China and South Africa, and all members formally included in the grouping.

Controller: the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making powers with respect to the Processing.

Data breach: any accidental or unauthorized access to, destruction, loss, use, modification or disclosure of Personal data due to a violation of the principle of data security.

Data exporter: the Controller, located in a country that is a Member of BRICS that transfers Personal data to a Data importer.

Data importer: the Controller to which the Data exporter transfers Personal data and that is located in a country that is a member of BRICS.

Genetic data: all Personal data relating to the genetic characteristics of an individual that have been either inherited or acquired during early prenatal development, as they result from an analysis of a

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

biological sample from the individual concerned including chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

MCC: These Model Contractual clauses.

Onward transfer: the transfer of Personal data by the Data importer to another Controller or Processor located in the same or in another jurisdiction.

Party (or Parties): the Data importer and/or Data exporter signatories to these Clauses.

Personal data: any information relating to an identified or identifiable individual (hereinafter "Data subject"), whatever his/her nationality or residence.

Processing: any operation or set of operations performed on Personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, processing means an operation or set of operations performed upon Personal data within a structured set of such data which are accessible or retrievable according to specific criteria.

Processor: a natural or legal person, public authority, service, agency or any other body that processes Personal data on behalf and under the instructions of the Controller.

Sensitive data: (i) genetic data, (ii) Personal data relating to offenses, criminal proceedings and convictions, or related security measures; (iii) Biometric data processed for the purpose of uniquely identifying a person; or (iv) Personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

Supervisory authority/ies: one or more authorities responsible for ensuring compliance with the provisions of the Applicable law.

Third party beneficiary: the Data subject whose Personal data have been transferred under these Clauses.

Third Party: a natural or legal person, public authority, service, agency or any other body that is not a Party to these Clauses but to which the Personal data is onward transferred by the Data importer, located in the same or in a different jurisdiction as the Data importer.

Transfer: the disclosure or making available of Personal data to a recipient subject to the jurisdiction of a country that is a member of the BRICS.

Clause 3. Amendment of the MCC

3.1. These Clauses set out appropriate safeguards, including, obligations for Controllers, enforceable Data subject rights and effective legal remedies, provided they are not modified, except to add or update information in the Annexes or to choose an option where it is provided for by the specific Clause. This does not prevent the Parties from including these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses, or the Applicable law.

3.2. These Clauses are without prejudice to obligations to which the Data exporter is subject by virtue of the Applicable law.

Clause 4. Interpretation and relation with other agreements

4.1 These Clauses shall be read and interpreted in the light of the provisions of the Applicable law.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

4.2 These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the Applicable law. If the meaning of the Clauses is unclear or there is more than one meaning, the meaning which most closely aligns with the Applicable law will apply.

4.3 In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail. The exception to this is where the conflicting terms of the related agreements provide greater protection for Data subjects, in which case those terms shall prevail over these Clauses.

Clause 5. Execution of the Clauses and Notices

5.1 These Clauses may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all counterparts together shall constitute a single agreement. Once each Party has received a counterpart signed by the other Party (or a digital copy of that signed counterpart), those counterparts will together constitute one and the same instrument and each of which will be, and will be deemed to be, an original.

5.2 Each Party warrants that it has full corporate power and has been duly authorized by all necessary corporate action on its part, to enter into, execute, deliver and perform its obligations under these Clauses.

5.3 All notices and requests under these Clauses by a Party to another Party shall be in writing and shall be served by regular mail, or by electronic mail to the key contact indicated on the First Page, or to such different addresses as may be communicated by the Party by written notice to the other Party. If the notice or request is sent by electronic mail, it will be deemed to have been delivered at the time the electronic mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounce back is received.

Clause 6. Accession clause

6.1 An entity that is not a Party to these Clauses may, with the agreement of the other Parties, accede to these Clauses at any time, either as a Data exporter or as a Data importer, by completing and signing Annex 2 and, if required, updating the description of the transfer in Annex 1.

6.2 Once it has completed and signed Annex 1.2, the acceding entity shall become a Party to these Clauses and shall have the rights and obligations of a Data exporter or Data importer in accordance with its designation in Annex 1.2.

6.3 The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 7. Third party beneficiaries

The Parties agree and acknowledge that any Data subject whose Personal data were transferred under these Clauses shall be entitled to invoke the safeguards and guarantees set out in Section II and III of these Clauses as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject with respect to its Personal data.

SECTION II – DATA PROTECTION SAFEGUARDS: RIGHTS AND OBLIGATIONS OF THE PARTIES

Clause 8. Due diligence and cooperation

8.1 The Data exporter warrants that it has used reasonable efforts to determine that the Data importer is able, in particular, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.2 The Data exporter shall cooperate with and provide reasonable assistance to the Data importer, if that is necessary to enable the Data importer to comply with its obligations set out in this Section.

Clause 9. Purpose limitation

The Data importer shall process the Personal data only for the specific purpose(s) of the Transfer, as set out in Annex 1.1. It may also process the Personal data:

- (a) when this is necessary to preserve the vital interests of the Data subject;
- (b) for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings in a particular case.

Clause 10. Transparency of processing

10.1 In order to enable Data subjects to exercise their rights effectively pursuant to these Clauses, the Data importer shall proactively inform them, free of charge, either directly or through the Data exporter of:

- (a) its identity and the contact details;
- (b) the legal basis and the purpose(s) of the intended Processing;
- (c) the purposes and categories of Personal data processed;
- (d) the Recipients or categories of Recipients of the Personal data, if any;
- (e) the means of exercising the rights set out in these Clauses;
- (f) any necessary additional information in order to ensure fair and transparent Processing of the Personal data such as the retention period, the logic underlying the Processing (in particular in case of the use of algorithms for automated decision making, including profiling) or information on Onward transfers (including the grounds therefor and the measures taken in order to guarantee an appropriate level of protection); and (g) the right to obtain a copy of these Clauses.

10.2. Paragraph 1 shall not apply where the Data subject already has the relevant information.

10.3 Where the Personal data are not collected from the Data subjects, the Data importer shall not be required to provide such information to the Data subject or to the Data exporter where the processing is expressly prescribed by law, or this proves to be impossible or involves disproportionate efforts. In the latter case, the Data importer shall, to the extent possible, make the information publicly available.

Clause 11. Accuracy and data minimisation

11.1 Each Party shall ensure that the Personal data is accurate and, where necessary, kept up to date. The Data importer shall take every reasonable step to ensure that Personal data that is inaccurate, having regard to the purpose(s) of Processing, is erased or rectified without delay.

11.2 If the Data importer is informed by the Data exporter of corrections made by the Data exporter to the Personal data, the Data importer shall promptly implement those corrections.

11.3 The Data importer shall ensure that the Personal data is adequate, relevant and not excessive in relation to the purpose(s) of Processing.

Clause 12. Limited retention period

The Parties agree that the Data importer shall retain the Personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical and organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

Clause 13. Data security

13.1 The Data importer and, during transmission, also the Data exporter shall implement appropriate security measures, both of a technical and organizational nature, for each Processing, in particular to protect against the risk of Data breaches. In adopting such measures, they shall take into account, in particular, the nature of the Processing, the nature and volume of the Personal data processed, the degree of vulnerability of the technical architecture used for the Processing, the state of the art and the cost of implementation. The measures should be commensurate with the seriousness and probability of the potential risks. The Parties shall consider having recourse to security techniques such as encryption or pseudonymisation, including during transmission, where the purpose(s) of Processing can be achieved in that manner.

13.2 The Parties have agreed on the technical and organisational measures set out in Annex 1.3. The Data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security and shall update them where this is no longer the case.

13.3 If there is a substantial change in the security measures implemented and described in Annex 1.3, the Parties shall update the Annex.

13.4 In the event of a Data breach concerning Personal data processed by the Data importer under these Clauses, the Data importer shall take appropriate measures to address the Data breach, including measures to mitigate its possible adverse effects.

13.5 The Data importer shall notify – without undue delay and, where feasible, not later than 72 hours after having become aware of the Data breach – at least the Data exporter, who shall notify the competent Supervisory authority in case the Data breach may seriously interfere with the rights and fundamental freedoms of the Data subjects.

13.6 In addition, the Data importer shall notify, either directly or through the Data exporter without undue delay, the Data subjects concerned by the Data breach, where it is likely to result in a high risk to their rights and freedoms. Such notification is not required if appropriate technical and organizational measures have been applied to the Personal data affected that render it unintelligible to any person not authorized to access it, if the Data importer has taken subsequent measures which ensure that the high risk is no longer likely to materialize, or if it would involve disproportionate efforts (in which case the Data importer shall instead make a public communication or take a similar measure whereby the Data subjects are informed in an equally effective manner).

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

13.7 In both cases, the notification shall include adequate and meaningful information on, notably, the nature of the Data breach, the contact points where more information can be obtained and possible measures that Data subjects could take to address the Data breach, including measures to mitigate its possible adverse effects.

13.8 Where not all the relevant information related to the Data breach is available, notification may take place “in stages”, with more information to be provided as soon as it becomes available.

Clause 14. Sensitive Data

Where the Transfer involves Special categories of data, the Data importer shall apply additional safeguards that guard against and are adapted to the risks that the Processing of such data may present for the interests, rights and fundamental freedoms of the Data subject, notably the risk of discrimination.

Clause 15. Onward transfers

15.1 The Data importer shall not onward transfer the Personal data to a Third party unless:

- a) the law of the Third party’s jurisdiction, including its international commitments under applicable international treaties or other agreements, ensures an appropriate level of protection or,
- b) the Third party enters into a legally binding and enforceable instrument with the Data importer ensuring the same level of data protection as under these Clauses, and the Data importer provides a copy of the instrument to the Data exporter or,
- c) the Onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings in a particular case or,
- d) the Onward transfer is necessary in a specific case in order to protect the vital interests of the Data subject or of another natural person; or,
- e) where none of the other conditions apply, the Data importer has obtained the explicit consent of the Data subject for the specific Onward transfer, after having informed him/her of its purpose(s), the identity of the Third party and the possible risks of such transfer to him/her due to the lack of an appropriate level of data protection. In this case, the Data importer shall inform the Data exporter of the Onward transfer based on consent and, at the request of the latter, shall transmit to it a copy of the information provided to the Data subject.

15.2 Any Onward transfer is subject to compliance by the Data importer with all the other safeguards under these Clauses, in particular as regards purpose limitation.

Clause 16. Processing under the authority of the Data importer

16.1. The Data importer shall ensure that any person acting under its authority, including a Processor, processes the data only on its instructions and in compliance with these Clauses.

16.2 The Data importer remains fully liable to the Data exporter, the competent Supervisory authority/ies and Data subjects for its obligations under these Clauses where it has subcontracted the processing to its Processors or authorized an employee or other person to process the data under its authority.

Clause 17. Documentation for compliance purposes

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

17.1 Each Party shall be able to demonstrate compliance with its obligations under these Clauses. To this end, it shall keep appropriate documentation of the Processing activities carried out under its responsibility.

17.2 Each Party shall make such documentation available to the competent Supervisory authority/ies on request.

17.3 The Data importer guarantees that it has carefully considered the impact the intended Processing might have on the rights and fundamental freedoms of Data subjects prior to the commencement of such Processing, according to the circumstances of the specific Transfer, and has taken the necessary and appropriate technical and organizational measures to comply with these Clauses, and to demonstrate such compliance to the competent Supervisory authority/ies.

Clause 18. Rights of Data subjects

18.1 Without undue delay, and at the latest within one month of the receipt of the enquiry or request, the Data importer, if necessary, with the assistance of the Data exporter, shall deal with any enquiries and requests it receives from a Data subject related to the Processing of his/her Personal data, including Onward transfers, and the exercise of his/her rights under these Clauses. That period may be extended by up to two further months where necessary, taking into account the complexity and number of enquiries and requests. The Data importer shall inform the Data subject of any such extension as soon as possible, and no later than five days before the end of the maximum period indicated in the first sentence, together with the reasons for the delay.

18.2 The Data importer shall inform Data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point competent to receive enquiries, deal with requests (including on the exercise of individual rights) and handle complaints.

18.3 The Data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of Data subject rights. Any information provided to the Data subject shall be in an intelligible and easily accessible form, using clear and plain language that should be understood by a lay person.

18.4 Data subjects shall have the following rights against the Data importer:

- a) not to be subject to a decision significantly affecting them based solely on the automated processing of their Personal data without having the right to challenge such a decision, to put forward their point of view and arguments, and obtain a human review, unless the automated decision is authorized by law which provides for suitable measures to safeguard the interests, rights and fundamental freedoms of the Data subject;
- b) to obtain, on request, at reasonable intervals and without excessive delay, confirmation of the Processing of Personal data relating to them, the communication in an intelligible form of the data processed, and all available information on their origin, on the retention period as well as any other information that the Data importer is required to provide in order to ensure the transparency of Processing in accordance with Clause 10.1;
- c) to obtain, on request, information on the reasoning underlying the Processing where the results of such Processing are applied to them;
- d) to object at any time, on grounds relating to their situation, to the Processing of Personal data concerning them, unless the Data importer demonstrates legitimate grounds for the Processing which override their interests, rights and fundamental freedoms;

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

e) to obtain, on request without excessive delay, rectification of their Personal data that is incorrect or out of date, or erasure if their Personal data are being, or have been, processed contrary to these Clauses;

f) to obtain a copy of these Clauses, provided that the Data importer may redact any information contained in the Annexes of these Clauses that it or, following consultation, the Data exporter has reasonably identified as a trade secret or other confidential information. Parties should, in such cases of redaction, provide a meaningful summary of the Clause so that the Data subject should be able to understand their content and exercise their rights.

g) to be provided with information on a contact person under the control of the Data importer, whose responsibility is to ensure compliance with letters (a) to (f) of this Clause. Data subjects shall be free to turn to the contact person at any time and at no cost in relation to the Data processing, including Onward transfers, and where applicable, to obtain assistance in exercising their rights.

18.5 The exercise of these rights shall be free of charge.

18.6 The Data importer may restrict or refuse the exercise of those rights if such restriction or refusal is provided for by its domestic law, such restriction or refusal respects the essence of fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a) the protection of national security, defense, public safety, public order or public policy; important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offenses and the execution of criminal penalties, and other essential objectives of general public interest;

b) the protection of the Data subject or the rights and fundamental freedoms of others, notably freedom of expression;

c) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the interests, rights and fundamental freedoms of Data subjects.

Clause 19. Redress for the Data subject

19.1 Where the Data subject invokes a Third-party beneficiary right pursuant to Clause 7, the Data importer shall accept the decision of the Data subject to lodge a complaint with the competent Supervisory authority/ies pursuant to Clause 21, and/or to refer the dispute to the competent courts pursuant to Clause 26.

Clause 20. Liability of the Parties

20.1 Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

20.2 Each Party shall be liable to the Data subject, and the Data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the Data subject by breaching these Clauses. This is without prejudice to the liability of the Data exporter or the Data importer under the Applicable law or the law applicable to the Data importer.

20.3 Where more than one Party is responsible for any damage caused to the Data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the Data subject is entitled to bring an action in court against any of these Parties.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

20.4 The Parties agree that, if one Party is held liable under the previous paragraph, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to the other Party's/Parties' responsibility for the damage.

20.5 The Controller remains responsible for the Processing where it engages a Processor to act on its behalf. The Parties may not invoke the conduct of a Processor or sub-Processor to avoid their own liability.

Clause 21. Supervisory authority

21.1 The Supervisory authority/ies with responsibility for ensuring compliance by the Data exporter with the Applicable law as regards the Transfer shall act as competent Supervisory authority/ies.

21.2 The Data importer agrees to submit itself to the jurisdiction of and cooperate with the competent Supervisory authority in any procedures aimed at ensuring compliance with these Clauses, and to abide by its decision. In particular, the Data importer agrees to respond to enquiries, submit to review or audits, and comply with the measures adopted by the Supervisory authority, including remedial and compensatory measures. It shall provide the Supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 22. Local laws and practices affecting compliance with the Clauses

22.1 The Parties warrant that they have no reason to believe that the laws and practices in the country of destination applicable to the Processing by the Data importer, including any requirements to disclose Personal data or measures authorising access by public authorities, prevent the Data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of human rights and fundamental freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in International Human Rights law, are not in contradiction with these Clauses.

22.2: The Parties declare that in providing the warranty pursuant to previous paragraph, they have taken due account in particular of the following elements:

- a) the specific circumstances of the Transfer;
- b) the laws (including case-law) and practices in the country of destination relevant in the specific circumstances of the Transfer;
- c) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses.

22.3 The Data importer warrants that, in carrying out the assessment pursuant to paragraph 22.2, it has made its best efforts to provide the Data exporter with relevant information and agrees that it will continue to cooperate with the Data exporter in ensuring compliance with these Clauses.

22.4 The Parties shall document the assessment pursuant to paragraph 22.2 and make it available to the competent Supervisory authority on request.

Clause 23. Obligations of the Data importer in case of access by public authorities

23.1 Notification

- a) In so far domestic law of Data importer allows, the Data importer shall notify the Data exporter and, where possible the Data subject promptly or use its best efforts to do so if it is compelled to preserve, grant access, make available or disclose Personal data transferred from the Data exporter to a Third party including to a public authority.
- b) If the Data importer is prohibited from notifying the Data exporter and/or the Data subject, then in so far domestic law allows it agrees to use its best efforts to obtain a waiver of the prohibition with a view to communicating as much information as possible. The Data importer agrees to document its efforts in order to be able to demonstrate them to the Data exporter, on request.
- c) Where permissible under the laws of the country of destination, the Data importer agrees to provide the Data exporter, on request, with as much relevant information as possible on any requests for disclosure it has received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d) The Data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent Supervisory authority on request.
- e) Paragraph (a), (b) and (d) is without prejudice to the obligation of the Data importer pursuant to Clause 22.5 and Clause 24 to inform the Data exporter promptly where it is unable to comply with these Clauses.

23.2. Review of legality and data minimisation

- a) The Data importer shall review the legality of any request for disclosure, in particular whether it is within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data importer shall, under the same conditions and in line with its domestic legislation pursue possibilities of appeal. Pending the determination of any challenge (including on appeal, as relevant) the Data importer shall, to the extent available under domestic legislation, seek interim measures to suspend the effects of the request. These requirements are without prejudice to the obligations of the Data importer under Clause 22.5 and Clause 24.1.
- b) The Data importer shall document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, shall make the relevant documentation available to the Data exporter. It shall also make it available to the competent Supervisory authority on request.
- c) When responding to a request for disclosure, the Data importer shall, having complied with the duty in 23.2, and confirm the lawfulness of the request provide, only the information which is necessary to respond to the request, in accordance with the domestic legislation.

SECTION IV – FINAL PROVISIONS

Clause 24. Non-compliance with the Clauses and termination

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

24.1 Each Party shall promptly inform the other Party/ies if it is unable to comply with these Clauses, for whatever reason.

24.2 In the event that the Data exporter has clear information that the Data importer is in breach of these Clauses or unable to comply with these Clauses, the Data exporter shall suspend the transfer of Personal data to the Data importer under these Clauses until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 22.6.

24.3 The Data exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal data under these Clauses, where:

- a) the Data exporter has suspended the Transfer of Personal data to the Data importer pursuant to paragraph 24.2 and compliance with the Clauses is not restored within a reasonable time and in any event within one month of suspension;
- b) the Data importer is in substantial or persistent breach of these Clauses; or
- c) the Data importer fails to comply with a binding decision of a competent court or a competent Supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent Supervisory authority of such non-compliance. Where the contract involves more than two Parties, the Data exporter may exercise this right to termination only with respect to the non-compliant Party, unless the Parties have agreed otherwise.

24.4 Personal data that has been transferred prior to the termination of the contract pursuant to paragraph 24.3 shall at the choice of the Data exporter immediately be returned to the Data exporter or deleted in its entirety. The same shall apply to any copies of the data. The Data importer shall certify the deletion of the data to the Data exporter. Until the data is deleted or returned, the Data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data importer that prohibit the return or deletion of the transferred Personal data, the Data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law. The Data exporter should be notified of the relevant local law and the required retention period. Only the minimum amount of Personal data should be retained to comply with domestic law.

Clause 25. Governing law

These Clauses shall be governed by the law of the country of the Data exporter.

Clause 26. Choice of forum and jurisdiction

26.1 Any dispute arising from these Clauses shall be resolved by the courts of [_____].

26.2 Data subjects may also bring legal proceedings against the Data exporter and/or Data importer before the courts of the country in which they have their habitual residence.

26.3 The Parties agree to submit themselves to the jurisdiction of such courts.

Clause 27. Arbitration clause

Option 1: WIPO Rules

Any dispute, controversy or claim arising under, out of or relating to this contract and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect,

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

interpretation, performance, breach or termination, as well as non-contractual claims, shall be submitted to mediation in accordance with the WIPO Mediation Rules. The place of mediation shall be [specify place]. The language to be used in the mediation shall be [specify language].

If, and to the extent that, any such dispute, controversy or claim has not been settled pursuant to the mediation within [60][90] days of the commencement of the mediation, it shall, upon the filing of a Request for Arbitration by either party, be referred to and finally determined by arbitration in accordance with the WIPO [Expedited] Arbitration Rules. Alternatively, if, before the expiration of the said period of [60][90] days, either party fails to participate or to continue to participate in the mediation, the dispute, controversy or claim shall, upon the filing of a Request for Arbitration by the other party, be referred to and finally determined by arbitration in accordance with the WIPO [Expedited] Arbitration Rules. [The arbitral tribunal shall consist of [a sole arbitrator][three arbitrators].]* The place of arbitration shall be [specify place]. The language to be used in the arbitral proceedings shall be [specify language]. The dispute, controversy or claim referred to arbitration shall be decided in accordance with the law of [specify jurisdiction]. (* The WIPO Expedited Arbitration Rules provide that the arbitral tribunal shall consist of a sole arbitrator.)

Option 2: ICC Rules

If the Parties are unable to resolve any difference they may have, the dispute shall be finally settled under the Rules of Arbitration (hereinafter, the “Rules”) of the International Chamber of Commerce (“ICC”) by three arbitrators designated by the Parties. Each Party shall designate one arbitrator. The third arbitrator shall be designated by the two arbitrators designated by the Parties. If either Party fails to designate an arbitrator within thirty days after the filing of the dispute with the ICC, such arbitrator shall be appointed in the manner prescribed by the Rules. An arbitration proceeding hereunder shall be conducted in [City, Country], and shall be conducted in [specify language]. The decision or award of the arbitrators shall be in writing and is final and binding on both Parties.

By the signatures of their authorized representatives below, the Data exporter and the Data importer agree to be bound by these MCC.

Data exporter name:

Main address:

Key contact:

Data importer information:

Main address:

Key contact:

Signed for and on behalf of the Data exporter Signed:

Date of signature [MM/DD/YEAR] Full name:

Job title:

Signed for and on behalf of the Data importer Signed:

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Date of signature [MM/DD/YEAR] Full name:

Job title:

Annex 1.1

Information about the transfers

[NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate annexes for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one set of annexes. However, where necessary to ensure sufficient clarity, separate sets of annexes should be used].

Description of the transfer:

- The categories of Data subjects whose data are transferred;
- The categories of Personal data transferred;
- The Special categories of data transferred (where applicable) and the restrictions or safeguards applied, which take full account of the nature of the data and the risks involved, such as, for example, strict purpose limitation, lawful basis for the processing (ex: explicit consent of the Data subject) access restrictions (including access only for staff who have received specific training), restrictions regarding further disclosure, retention of records of data sharing, restrictions on Onward transfers, specific organizational or technical security measures (ex: data encryption, pseudonymisation) or additional security measures;
- The frequency of data transfers (e.g. whether data are transferred once or continuously);
- The nature of the Processing;
- The purpose(s) of the data Transfer and further processing;
- The period for which the Personal data will be stored or, where this is not possible, the criteria for determining this period;

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Annex 1.2

Signature form

[Term: Start date [MM/DD/YEAR] – End date [MM/DD/YEAR]]

Data exporter information Full legal name:

Trading name (if different):

Main address (if a company registered address):

Official registration number (if any):

Key contact (full name, job title, contact details including email):

Data importer information Full legal name:

Trading name (if different):

Main address (if a company registered address):

Official registration number (if any):

Key contact (full name, job title, contact details including email):

By the signatures of their authorised representatives below, the parties agree to be bound by these Model Contractual Clauses (hereinafter “the Clauses”).

Signed for and on behalf of the Data exporter Signed:

Date of signature [MM/DD/YEAR] Full name:

Job title:

Signed for and on behalf of the Data importer Signed:

Date of signature [MM/DD/YEAR] Full name:

Job title:

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Annex 1.3

Security measures

This annex has to be completed and updated by the Data importer. The technical and organizational measures must be described in specific (and not generic) terms. It must be clearly indicated which measures apply to each transfer/set of transfers.

Examples of possible measures:

Measures of pseudonymisation and encryption of Personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services

Measures for ensuring the ability to restore the availability and access to Personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing

Measures for user identification and authorisation

Measures for the protection of Personal data during transmission

Measures for the protection of Personal data during storage

Measures for ensuring physical security of locations at which Personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure