EVALUATING PERSONAL DATA TRANSFER MECHANISMS TO INTERNATIONAL ORGANISATIONS UNDER THE MALABO CONVENTION: A CORE REGULATORY APPROACH

By

2857573

Submitted in partial fulfilment of the requirements for the degree of Master of Laws by Coursework and Research Report at the University of Witwatersrand, Johannesburg

Date: 27 February 2025

DECLARATION

I, **2857573,** declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Laws in the field of Information Technology and Communications Law at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in any other university.

I have submitted my final Research Report through Turnitin and have attached the report to my submission.

Word count: **10,487**

2857573

27 February 2025

ABSTRACT

The African Union Convention on Cyber Security and Personal Data Protection (hereinafter the Malabo Convention) was strategically intended to establish a harmonised regional framework on data protection and cybersecurity issues. Its approach is anchored on the reliance on State obligation to establish national frameworks that develop the required standards elaborated in the Convention. However, the lack of detail in its enforcement structure has resulted in minimal motivation and slow adoption of the Convention by African Countries. Instead, many African countries are focused on adopting legislation similar to the GDPR that is elaborate in structure. This is notwithstanding the far-reaching effects on collaborative limitations, particularly in responding to data transfer issues that do not respond to prescriptive provisions dictating specific mechanisms like Standard Contractual Clauses and adequacy decisions. This paper analyses this problem by observing the regulatory limitations when prescribing adequacy requirements of personal data transfer to international organisations. This paper analyses the weaknesses of the GDPR's personal data transfer mechanisms to IOs compared to that of the Malabo Convention, considering their regulatory structures. This paper highlights the concerns of adopting regulations with structures that lack dynamism in responding to data protection challenges and how we can resolve these concerns by re-thinking command and control regulations in support of core regulations.

TABLE OF CONTENTS

I. INTRODUCTION

a. Problem Statement

In today's interconnected world, data has become increasingly integral to societal activity,[1] ranging from commerce to governance.[2] With this shift, data protection law is arguably becoming an all-encompassing framework.[3] But, its comprehensive nature still remains questionable as its regulatory framework often falls short in addressing data transfer issues that transcend national borders and organisational structures. One emerging issue is the incompatibility of data protection legislation that limits trans-border data transfer. This is reflected through problems such as the regulation of personal data transfer to International Organisations (IOs) such as United Nations High Commissioner for Refugees (UNHCR), International Committee of the Red Cross (ICRC) and, World Health Organization (WHO) that enjoy immunity status outside the confines of jurisdictional boundaries.[4] The regulatory challenge lies in navigating the privilege and immunity status within data protection frameworks and the competing parallel data protection frameworks adopted by IOs through global soft law instruments.[5] This is the immunity question.

This immunity, based on the principle of functional necessity, makes it challenging for national courts to hold them accountable for data breaches or privacy violations, even when they operate in regions with strict data laws like the European Union's GDPR.[6] This creates a significant regulatory gap concerning accountability and the protection of individual rights. In Africa, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) aims to create a regional framework for data protection. However, its effectiveness in solving this immunity question is limited due to a lack of ratification and underdeveloped enforcement mechanisms. The core of this issue is that existing treaties on IO immunities, such as the 1946 Convention on the Privileges and Immunities of the United Nations[7], are too general. They do not

[1] Orla Lynskey 'Complete and Effective Data Protection' (2023) 76 *Current Legal Problems* 1 at 297.
[2] UNCTAD 'Data protection regulations and international data flows: Implications for trade and development' available at https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf, accessed on 26 May 2024.
[3] Orla Lynskey op cit note 1 at 297.
[4] Ibid.
[5] Ibid.
[6] Inji Mammadli 'International Organisations and Accountability for Human Rights Abuses: Obstacles caused by Jurisdictional Immunity' (2023) 66 *Baku State University Law Review* 9 at 67.
[7] Convention on the Privileges and Immunities of the United Nations (adopted 13 February 1946, entered into force 17 September 1946) 1 UNTS 15.

provide clear guidance on how domestic data protection laws should apply to IOs,[8] leaving a significant conflict between the need for data protection and the legal immunity of these organisations.

This research report also argues that reaching a consensus on an interoperable data protection framework cannot mean identical or even harmonised laws when seeking to effectively navigate jurisdictional and regulatory challenges faced by entities such as IOs.[9] Instead, an interoperable framework should be focused on a pragmatic approach that facilitates cooperation between fragmented approaches to privacy and data protection across various levels.[10] The focus will be on analysing a practical arrangement that addresses trans-border enforcement challenges, particularly pertaining to the transfer of personal data to IOs. In this research report, I shall argue that concerning data protection issues, there is an overreliance by states on a command-and-control regulatory structure, which tends to be unresponsive and confined to compliance with a strict set of rules.This approach is founded primarily on three elements of regulation: standard setting, surveillance, and behavioural oversight,[11] which continues to challenge the flexibility of the command-and-control structures.

b. The Malabo Convention as an African regional framework for data protection

The African Union Convention on Cyber Security and Personal Data Protection (2014) is a regional binding treaty for African Union Member States adopted on 27 June 2014.[12] Currently, 55 African Union Member States have ratified the framework.[13] The historical development dates back to 2 February 2010 when the Addis Ababa declaration was made by the head of states of African Union recognising the importance of regulating and harmonising ICT due to its reaching impact on development in Africa.[14] Its focus on cybersecurity and data protection is founded on respect rights of citizens, as enshrined in both domestic law and international human rights

[8] Johan G. Lammers 'Immunity of International Organisations' Immunity of International Organisations: *The Work of the International Law Commission* ed (2015) 82

[9] Robinson L. K. Kizawa and E. Ronchi op cit note 4 at 11.

[10] Ibid.

[11] Ibid.

[12] African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) adopted on June 27, 2014, by the twenty third Ordinary Session of the African Union Assembly, EX.CL/846(XXV).

[13]Status list of the Malabo Convention available at 29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf accessed on 24 February 2025.

[14] African Union, *Addis Ababa Declaration on Information and Communication Technologies in Africa: Challenges and Prospects for Development* (adopted 2 February 2010) Assembly/AU/Dec.1(XIV).

conventions and treaties.[15] The Malabo Convention reflects a deliberate effort to be agile, with intention of accommodating changing technological landscape and the diverse interests of its members. It constitutes three chapters focused on electronic transactions, personal data protection, and promoting cyber security and combating cybercrime.[16] While the Convention covers a wide range of topics, this research report focuses specifically on chapter two, which deals with personal data protection. Of particular interest are Article 8 and Article 14(6), as they are key to establishing data transfer frameworks compatible with divergent interests of member states.

The Malabo Convention shares many structural similarities with Eurocentric data protection regimes like the GDPR, including principles for data subjects' rights and obligations for data controllers. However, it differs as it requires Member States to develop national legal frameworks with territorial application limited to each member states and provides leeway for member states to adopt exceptions under national frameworks.[17] For instance, Article 14(6) on data transfer. While it provides for adequacy standard, it does not state the requirements leaving the details to be defined by each national data protection authority.[18] Therefore, this non-prescriptive approach forms the basis of this research report analysis on whether the Malabo Convention offers a good starting point. This paper will explore whether it can serve as a model for developing flexible, common approach to personal data transfer, especially to entities like IOs that might not be subject to the stringent requirements under regional and national laws.

c. Purpose of the Research

This research report shall analyse whether despite the Malabo Conventions slow uptake and underdeveloped enforcement structures, it provides a sufficiently robust yet flexible framework to regulate personal data transfers to IOs, and whether complementing it with core regulatory mechanisms such as memoranda of understanding can enhance its implementation value.

[15] Ibid 20.
[16] Ibid.
[17] Lukman Adebisi & Hlengiwe Dube, 'Data Privacy Law in Africa: Emerging Perspectives' *The African world view on privacy* ed (2024) 63-64
[18] Ibid.

d. Research Questions and Methodology

The main research questions are:

1. To what extent does the Malabo Convention provide a legal basis for reconciling IO immunities with state obligations in data protection?
2. How does the Malabo framework compare with the GDPR's adequacy regime in addressing transfers to IOs?
3. Can core regulation (e.g. MOUs, bilateral agreements) serve as a viable complement to Malabo's obligations in practice?

e. Methodology

The study is overall, a desktop-based enquiry of the relevant primary and secondary legal sources. This method was used to analyse the concepts of command and control and core regulation within regional data protection frameworks and examine the gaps in regulating transfer of personal data to IOs. It relied on a comparative analysis of international and foreign law instruments, namely the GDPR and the Malabo Convention, towards determining an appropriate regulatory structure.

f. Overview of Remaining Chapters

To begin with, Chapter II of this research report analyses the appropriateness of the Malabo Convention as a regional framework for balancing the issue of immunity for IOs and regulating transfer of personal data to IOs. In Chapter III, I address the inadequacies of existing trans-border data transfer mechanisms through a comparative analysis of the GDPR and the Malabo Convention and their effect on achieving an interoperable data transfer framework. This analysis shall identify the gaps in existing mechanisms when addressing the complexities of transborder data transfer and the adjustments needed to make them efficient. Thereafter, Chapter IV reflects on a practical framework for harmonising divergent approaches when regulating personal data transfer mechanisms to IOs. Chapter IV shall highlight why the core regulatory approach is an appropriate means to realising safe personal data transfer to IOs. The Chapter shall conclude as a call to action for states to intensify discussions on core regulatory approaches and the need to adopt data transfer mechanisms that promote agile and interoperable frameworks.

II. THE IMMUNITY QUESTION IN THE TRANSFER OF PERSONAL DATA TO IOS

a. Introduction

The immunity question arising from the transmission of personal data to IOs calls for a discussion on the interaction of international law and national law.[19] Specific attention is brought to the relationship between national and regional frameworks on one end and the specific data protection frameworks of IOs on the other end.[20] This has led scholars such as Marelli to question whether a harmonious coexistence can be achieved through overlapping frameworks.[21] In his view, a pragmatic approach achieves the harmony between respecting personal data protection and acknowledging the mandate of IOs under international law.[22] Nevertheless, some scholars find the question of immunity taxing due to the varying and sometimes conflicting approaches at the domestic and international levels.[23]

Focusing on the Malabo Convention, this chapter discusses whether there is a harmonious interaction amongst the overlapping data protection frameworks while appreciating the divergent approaches to the immunity question. This will begin with a discussion on how regional frameworks, such as the Malabo Convention, address immunity issues before exploring whether there is a co-existence between the various domestic, territorial, and international frameworks. It has been consistently highlighted that data privacy is an international issue which requires equivalent standards of data protection in all countries.[24] Therefore, this chapter argues that there is an equivalent standard of protection demonstrated by the data protection principles in the various overlapping frameworks that warrant a harmonious interaction. Part of this shared standard is reflected in IOs' specific frameworks and compliance systems. However, this co-existence is better achieved when IOs limit their privileges and immunities for purposes of fulfilling their mandate

[19] Massimo Marelli 'The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders' (2023) 50 *Computer Law & Security Review* at 1.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Tom Ruys, Nicolas Angelet and Luca Ferro *The Cambridge Handbook of Immunities and International Law* ed (2019) i-ii.
[24] van der Merwe 'Data Privacy Law' (ed) *Information Communications and Technology Law* 3 ed (2021) 372.

attributed to them by the international community.[25] This international community includes State Parties, obligating IOs to act in good faith and give due consideration to their domestic legislation.

b. Monist v Dualist approach to the immunity question under the Malabo Convention

In international diplomacy, the effects of state sovereignty on the adoption of international law is a key issue.[26] Particularly, the legal developments in the Malabo Convention on emerging issues such as transfer of personal data to IOs is largely dependent on the reception of international law into national legal framework of AU Member States.[27] When looking at the immunity question under the Malabo Convention, it must be borne in mind that regional entities such as the AU lack the sovereignty to directly incorporate international law into regional frameworks.[28] Therefore, international law questions such as legal immunities of IOs require an examination of the adoption of international law into domestic law.[29] Often, this relationship is observed through the monist *versus* dualist debate.

Monist states directly adopt international law into domestic law[30] but in the event of a conflict, international law takes precedence.[31] Contrastingly, dualist states treat international law as a distinct and separate legal system[32] that only becomes applicable through domestication in statute or legislative process.[33] However, the complication that arises is that even at the national level, there are pluralist forms of both monism and dualism.[34] Therefore, it remains imperative that the question of immunity is addressed by national frameworks.

---

[25] Christopher Kuner and Massimo Marelli 'Basic Principles of Data Protection' *Handbook on Data Protection in Humanitarian Action* (2017) 27.
[26] van der Merwe 'Data Privacy Law' (ed) *Information Communications and Technology Law* 3 ed (2021).
[27] Michelle Barnard 'Legal Reception in the AU against the Backdrop of the Monist/Dualist Dichotomy' (2015) 48 *Comparative and International Law Journal of Southern Africa* 1 at 144.
[28] Ibid 145.
[29] Ibid.
[30] Wilfred Mutubwa 'Monism or Dualism: The Dilemma in The Application of International Agreements Under the South African Constitution' (2019) 3 *Journalofcmsd* 1 at 27.
[31] Itumeleng Shale 'Historical perspective on the place of international human rights treaties in the legal system of Lesotho: Moving beyond the monist-dualist dichotomy' (2019) 19 *African Human Rights Law Journal* 1 at 197.
[32] Ibid.
[33] Wilfred Mutubwa op cit note 24 at 27.
[34]Madelaine Chiam 'Monism and Dualism in International Law' available at https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0168.xml, accessed on 26 May 2024.

Retaining the immunity question under national frameworks ensures that the institutional sovereignty of the African Union (AU) is limited. As a result, State Parties Obligation[35] by default becomes the biggest implementation value of the Malabo Convention because it contextualises and limits the approach to regulating personal data transfer to IOs within the realm of State Parties. From this viewpoint, the Malabo Convention is seen to create a convergence of immunity rules by promoting the compatibility of certain fundamental rights under international human rights,[36] such as the right to privacy, which entails data protection. This convergence is orchestrated under the Malabo Convention through the accountability approach by obligating State Parties[37] to set up national data protection laws that satisfy the required standards detailed in the Convention.[38] Therefore, it can be argued that the Malabo Convention does not aim to create a harmonised data protection framework in Africa through prescriptive legislation but through binding international principles.

This accountability approach by the Malabo Convention fosters the open progress of globally applicable data protection standards, which are key to boosting the confidence of IOs in collaborating with the regulatory ecosystem.[39] This ensures enhanced global data flow that goes beyond mere legal revisions and into evolved privacy standards.[40] By embracing new privacy paradigms as reflected in the Malabo Convention, legislators are assured of the prioritisation of simple, flexible, and less bureaucratic frameworks that focus on meeting core objectives while ensuring compatibility across diverse global data protection systems.[41] It is through this accountability approach that I argue that the Malabo Convention makes the question of immunity a direct one for State Parties. However, the evolved privacy paradigm does not emanate from jurisdictional limitations. Instead, it is the flexibility from the Malabo Convention that facilitates states to achieve compatibility between immunity rules and data protection frameworks. This

[35] Article 8(1) of Malabo. State Parties Obligation means the commitment to establish a legal framework aimed at the protection of physical data.
[36] Rosanne Van Alebeek *The Immunity of States and Their Officials in International Criminal Law and International Human Rights Lawed* (2008*)*.
[37] Article 1 of Malabo. State Parties means Member State(s) which has ratified the present Convention.
[38] ALT Advisory 'THE MALABO ROADMAP: Approaches to promote data protection and data governance in Africa' available at https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf, accessed on 26 May 2024.
[39]Internet Society 'The Future of Privacy' available at https://www.internetsociety.org/wp-content/uploads/2017/09/future-privacy-20100914.pdf, accessed on 26 May 2024.
[40] Ibid.
[41] Ibid.

flexibility further provides a baseline for interoperability through harmonised data protection principles. It is on this basis that I find that the Malabo Convention is one step ahead in recognising that the future of privacy is convergence through horizontal, flexible, and neutral frameworks.[42]The Malabo Convention advances regulatory clarity by promoting common foundations for State Parties' regulatory frameworks.[43] This approach reduces ad hoc proposals that complicate compliance and promotes the international agenda of creating convergence with other immunity rules.

c. Compatibility of the Malabo Convention with Immunity Rules

The convergence[44] on regulating immunity is not only seen at the regional and domestic level but also the global level. Unlike most regional instruments that transfer the immunity question to the national level, the immunity question at the international scene shifts accountability from States to IOs that enjoy immunity from jurisdictions where they operate.[45] For this reason, it has been argued that the first line of safeguarding of personal data lies with the IOs.[46] To promote this compatibility, IOs have sought to create their own data privacy frameworks and policies[47] such as the United Nations Personal Data Protection and Privacy Principles, the International Organization Data Protection Manual, the Policy on the Protection of Personal Data of Persons of Concern to United Nations High Commissioner for Refugees (UNHCR) and International Committee of the Red Cross Rules (ICRC) on Personal Data Protection, among others.[48] At the minimum, these data protection frameworks share similar core principles with national frameworks for personal data processing.[49] This convergence creates an overlap of the data

[42] Antonio Muñoz Marcos 'The future of privacy is convergence' available at https://www.telefonica.com/en/communication-room/blog/the-future-of-privacy-is-convergence/ , accessed on 26 May 2024.
[43] Ibid.
[44] See p.11.
[45] Christopher Kuner and Massimo Marelli 'Creating International Frameworks for Data Protection: The ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action' available at https://www.ejiltalk.org/creating-international-frameworks-for-data-protection-the-icrcbrussels-privacy-hub-handbook-on-data-protection-in-humanitarian-action/ accessed on 26 May 2024.
[46] Ibid.
[47] Christopher Kuner 'International Organizations and the EU General Data Protection Regulation' (2019) 16 *International Organizations Law Review* at 158.
[48] Christopher Kuner 'The GDPR and International Organizations' (2020) 114 *American Journal of International Law* at 16.
[49] Alexander Beck and Christopher Kuner 'Data Protection in International Organizations and the New UNHCR Data Protection Policy: Light at the End of the Tunnel?' available at https://www.ejiltalk.org/data-protection-in-international-organizations-and-the-new-unhcr-data-protection-policy-light-at-the-end-of-the-tunnel/, accessed on 26 May 2024.

protection norms across national, regional, and international frameworks, thereby equipping these principles with inherent normative authority.[50]

The influence of these principles is evident in their integration into data protection codes as independent guidelines and are regularly referenced as justifications for the processing of personal data.[51] This overlap in the national, regional, and IOs data protection frameworks creates the need for an accountability framework that checks each of the three frameworks.[52] Often, this accountability requirement is reflected through a practicable framework that recognises the core principles stipulated as absolute. Still, the difference lies in their elaboration within international and national frameworks.[53] It is these differences in approach that make 'adequacy' requirements for personal data transfer incompatible. Therefore, for the immunity question to be correctly dealt with, there is a need for a convergence on the interoperability of data transfer mechanisms as opposed to adequacy requirements to transfer personal data. Regional frameworks such as the Malabo Convention provide the ideal legal environment to foster interoperable frameworks due to its prescriptive limitation on international law while fostering accountability through recognised principles and practical frameworks.

d. Finding the balance between immunity entitlements and data protection

While the Malabo framework offers a good regulatory landscape to foster accountability, its overriding objective should not be a prioritisation of data protection goals at the expense of the immunity question. Instead, the practical frameworks should endeavour to maintain an appropriate balance that is essential to realising the individual's data privacy rights while respecting the jurisdictional immunities of IOs. This jurisdictional immunity is necessary for IOs to act independently when carrying out their mission.[54] Most importantly, because IOs operate in various member states and their mandates surround humanitarian action and peacekeeping operations that affect lives in the international community as a whole, it is paramount that they are protected from

[50] Lee A. Bygrave 'Core Principles of Data Privacy Law' *Data Privacy Law: An International Perspective* ed (2014) 145.
[51] Ibid.
[52] Christopher Kuner op cit note 38 at 158.
[53] Lee A. Bygrave op cit note 41 at 145.
[54] David P. Stewart & Ingrid Wuerth 'The Jurisdictional Immunities of International Organisations: Recent Developments and the Challenges of the Future' in Paul B. Stephan & Sarah A. Cleveland (ed) *The Restatement and Beyond: The past, present and future of U.S. Foreign Relations Law* (2020) 411-432.

becoming subjects of national law interests.[55] As it stands, IOs face numerous challenges, such as their lack of capacity to fund their mandates, forcing them to rely on member states contributions.[56] As a result, IOs are exposed to threats of default payments that cripple their operations should they ignore member state interests.[57] Furthermore, states already have sweeping exemptions such as national security interests within their data protection frameworks which allows them to perform their national functions. Therefore, it would only be impartial to safeguard the immunity status of IOs. Opening up existing data protection frameworks to accommodate different stakeholders' mandates and not just national interests, widens the accountability channels of regulating data exclusivity.

To effectively achieve the harmonious co-existence of regional, national, and IOs data protection frameworks, the issue of conflict of laws must be addressed. Legal frameworks, by design, confer jurisdiction to sovereigns, yet this jurisdiction is not universal; it is contextual and refers to different specialist areas of law.[58] Therefore, conflicts arise when different sovereigns attempt to state the law that is deemed to be the jurisdiction of another sovereign. This is particularly the issue with IOs data protection frameworks and national data protection frameworks. It is challenging to achieve data sovereignty or determine the competent lawful authority due to the different contexts in which IOs and States operate their jurisdiction. To resolve this conflict, it is paramount that the Malabo Convention be interpreted as a global law and not international law. As interestingly observed by Hornle, international law is related to global law, but it is not synonymous to it.[59] The scholar finds that international law addresses the relationship between States and universal obligations concerning statehood.[60] While global law can be understood to be a remedy to a regulatory issue, an instrument of addressing global problems, with its norms forming the core of all legal systems, thereby facilitating universal application.[61] One form of global lawmaking is cooperation between governments, with cooperation efforts occurring

[55] Edward Okeke 'The tension between the Jurisdictional Immunity of International Organisations and the Right of Access to Courts' in Peter Quayle (ed) *The Role of International Administrative Law at International Organisations* (2020) 25-53.
[56] Kgothatso Shai et. Al 'A critical analysis of the difficulties faced by international organisations within the context of the role of the United Nations (2019) 7 *APSDPR* 1.
[57] Ibid.
[58] Julia Hornle 'Heads in the Clouds: The clash between Territorial Sovereignty, Jurisdiction, and the Territorial Detachment of the Internet' in Julia (ed) *Internet Jurisdiction Law and Practice* (2021) 4-32.
[59] Ibid.
[60] Ibid.
[61] Ibid.

in neutral areas such as the regional level. Aligning with Hornle's perspective, I find that the Malabo Convention promotes a harmonious co-existence of IOs and Member States by limiting its dictate on jurisdiction but facilitating global law-making through cooperation using shared data protection standards. Additionally, it offers flexible requirements that can respond to emerging regulatory challenges. This provides an avenue to develop cooperation mechanisms through shared standards while navigating the dilemma of conflict of laws.

e. Conclusion

This chapter has highlighted the need for a conceptual shift in the interpretation of the Malabo Convention as an international law framework to a global law instrument. This widens its reach beyond traditional state actors to include global state actors such as IOs. Furthermore, it narrows the gaps that emerge from the applicability of the traditional scope of international law and paves way for practical steps required for IOs to align with a global framework and strengthen global enforcement.

On this basis, the next chapter addresses the need for existing approaches to cross-border data transfer to evolve to a higher but flexible 'adequacy' requirement that focuses on Member States as opposed to Third Countries or IOs. This ensures that the data protection paradigm evolves to an interoperable framework focused on achieving consensus rather than compatibility.

III. EXISTING APPROACHES TO TRANS-BORDER DATA TRANSFER

a. Introduction

The ubiquitous nature of personal data has seen the review of data protection legislation in attempts to facilitate safe trans-border personal data transfer.[62] In response to this imperative, many countries are grappling with legislating effective trans-border data transfer regulatory standards. While certain countries such as the United States, Canada, and Mexico have less stringent restrictions on such transfers opting for an accountability approach, other countries are opting for material restrictions.[63] For countries opting to impose material restrictions, they have often adopted the European Union (EU)framework enshrined in the GDPR, which often sets a higher 'adequacy' standard for the transfer of personal data to jurisdictions lacking substantially similar safeguards.[64] However, the complex and rigid compliance strategies have led to conflicting data transfer requirements under national and international laws. This is particularly notable with regard to personal data transfer to IOs.

The question is whether the compliance priorities under the existing data transfer mechanisms should be on compatibility or convergence, particularly in responding to conflicting immunity rules applicable to IOs. Currently, the governance of trans-border data flow has broadly been categorised into unilateral, bilateral, and multilateral approaches, all with different transfer instruments.[65] Bilateral approaches mainly focus on building consensus through judicial cooperation, regulatory cooperation, and memoranda of understanding; while multilateral approaches focus on international collaboration through international agreements. Due to the influential adoption of unilateral approaches, this chapter, for the most part, focuses on this approach and its inadequacies in governing transfer of personal data to IOs.

b. Unilateral approaches

Unilateral approaches emphasize the transfer of personal data using mechanisms that impose certain conditions.[66] These mechanisms include the use of adequacy decisions, standard

[62] The *White Paper on Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy* (published by the Centre for Information Policy Leadership of 25 September 2017 updated 7 July 2017).
[63] Ibid.
[64] Ibid.
[65] United Nations 'G20 Members' Regulations of Cross-Border Data Flows (2023) available at https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf, accessed on 27 May 2024.
[66] Casalini F., J. López González and T. Nemoto 'Mapping commonalities in regulatory approaches to cross-border data transfers' (2021) *OECD Trade Policy Papers*, No. 248.

contractual clauses, binding corporate frameworks, data transfer arrangements needing government authorisation, data localisation requirements and consent from data subjects.[67] Through these instruments, conditions on the sharing of personal data are imposed either through 'open safeguards' or 'pre-authorised safeguards.'[68] Of the existing conditions of transfer, the EU model focused on adequacy requirements remains influential in regulating trans-border data protection.[69] The adequacy requirement adopts a three-part assessment that requires any third country or IO to initiate the transfer of personal data to demonstrate respect for human rights, the existence of a specialised regulatory entity, and the adoption of international agreements or multilateral agreements on the protection of personal data.[70]

However, this adequacy approach has been criticised for its incompatibility with the status, privileges, and immunities of IOs.[71] This is due to the sovereignty of the EU under Article 45(2) of the GDPR in providing adequacy assessments on what constitutes adequate levels of protection.[72] It is this institutional sovereignty that Marelli argues would interfere with the independence of IOs as opposed to the lack of compatibility on core data protection to be considered in the adequacy assessment.[73] Therefore, what Marelli finds is that had the adequacy assessments have been excluded from the jurisdiction of the European Commission, it would have been possible to regulate IOs using the GDPR, but this remains a distant reality.[74] This incompatibility has also been acknowledged by the European Commission in its practical guidance on the use of New Standard Contractual Clauses, where it has proposed the use of unique mechanisms.[75] This has seen scholars attempt to discover unique mechanisms in the EU framework through the necessity test under Article 49(1)(d) of the GDPR.[76] However, I find that

[67] United Nations 'G20 Members' Regulations of Cross-Border Data Flows (2023) available at https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf, accessed on 27 May 2024.
[68] Casalini F., J. López González and T. Nemoto op cit note 50 at 12.
[69] Xi Yang 'Regulatory Approaches of Cross-border Data Flow in the Big Data Era: China's Choice' (2021) 1848 *Journal of Physics*: *Conference Series* at 1-9.
[70] Ibid.
[71] Massimo Marelli op cit note 5 at 27.
[72] Bjørn Aslak Juliussen, Elisavet Kozyri, Dag Johansen and Jon Petter Rui 'The third country problem under the GDPR: enhancing protection of data transfers with technology' (2023) 13 *International Data Privacy Law 3* at 225-243.
[73] Massimo Marelli op cit note 5 at 24-29.
[74] Ibid.
[75] European Commission, 'The New Standard Contractual Clauses—Questions and Answers Overview' at ad14 available at https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf, accessed 27 May 2024.
[76] Ioannis Ntouvas 'Exporting personal data to EU-based international organizations under the GDPR' (2019) 9 *International Data Privacy Law* 4 at 281.

though the public interest test offers independence to IOs, it does not promote neutrality in the determination of what constitutes public interest. Therefore, even the accountability framework under the derogations approach, fails to account for the independent status of IOs.[77]

It is likely that the accountability framework will remain Eurocentric, as seen in the case of *Maximillian Schrems v Data Protection Commissioner (Schrems*)[78]. While in *Schrems I*[79], we see that the Court of Justice of the European Union (CJEU) clarified that the standard of "essentially equivalent" does not mean an identical level of protection, in *Schrems II*[80], we see the (CJEU) invalidate the EU-U.S Privacy Shield.[81] The Privacy Shield is invalidated based on the differences in the laws of the U.S. and E.U in articulating the necessity and proportionality test to the standard required by EU adequacy requirements.[82] From the *Schrems II* case, not only do we see an "identical requirement" but also that the limitation requirement under Article 49(1)(d) is still subject to an adequacy assessment[83] by the European Commission. Therefore, conflicts arising from the independence of IOs and the dominance of the European Commission are unlikely to be evaded without independence from the control or influence of a single, dominant regulatory body, such as the European Commission.

c. Transborder data transfer approaches in Africa

Similar to the European Union, Africa's regulation of trans-border data flows is fragmented with different approaches. For instance, Kenya's Data Protection Act[84] provides for appropriate safeguards, while South Africa's Protection of Personal Information Act[85] provides for adequate legal protection requirement, and Nigeria provides for data localisation requirements. Despite the diversity of approaches, it has been pointed out that some African states look to regional instruments such as the Malabo Convention to remedy any defect in their national legislation and

[77] See Article 49(1) of the GDPR.
[78] CJEU, Grand Chamber, *Maximilian Schrems v Data Protection Commissioner* Case C- 362/14 OF 6 October 2015.
[79] Ibid.
[80] CJEU, Grand Chamber, *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems* Case C-311/18 of 16 July 2020
[81] EU-U.S Privacy Shield, IP/16/216 .
[82] European Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework available at https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf para 185 accessed on 27 May 2024.
[83] Massimo Marelli op cit note 5 at 24-29.
[84] Kenya's Data Protection Act Cap. 411C.
[85] Protection of Personal Information Act (POPIA) Act 4 of 2013.

ensure Country's compliance with international instruments.[86] However, this reliance, as Babalola has argued, is restricted by the duplication of the GDPR template despite many African countries having incompatible enforcement mechanisms.[87] The lack of regional institutionalisation of unilateral approaches such as adequacy requirements hinder the desired effect of the GDPR.[88] However, I find that the biggest barrier lies not in the lack of regional institutionalisation but in the duplication of the GDPR in most national data protection frameworks. A purposive reading of the transfer mechanisms under the GDPR shows that there is need to embrace an accountability approach that accommodates unique adequate mechanisms to provide timely responses to emerging issues such data transfer to IOs.

The layout of the Malabo Convention under Article 14 in regard to data transfer mechanisms provides such an accountability approach focused on data subject obligation, controller and processor accountability and state and regulatory oversight. Unlike the GDPR, which sets out rules and instruments for safe data transfer, the Malabo Convention lacks such specificity. Instead, the requirements for transfer of personal data protection under the Malabo Convention can be classified into two main categories: derogations for specific situations,[89] and State adequacy requirements. The lack of specific adequate requirements under Article 14 of the Malabo Convention provides an avenue for advancing compatibility between data protection requirements and the independent status of IOs. Specifically, Article 14(2) provides for public interest as a specific condition for data processing on four main grounds. First, it provides that processing shall not be prohibited where data is made manifestly public by the data subject.[90] Article 14 demonstrates an inherent three-tiered accountability approach. It begins by placing an obligation on the data subject to safeguard their legitimate expectation of privacy. This first tier endorses a reasonableness criterion to determine wrongful intrusion or invasion based on the subjective expectation that is objectively viewed.[91] As a result, the Malabo Convention moves away from the fixation on personal information approach to an accountability approach based on reasonableness.

[86] Olumide Babalola 'Transborder flow of personal data (TDF) in Africa: Stocktaking the ills and gains of a divergently regulated business mechanism' (2024) 52 *Computer Law & Security Review* at 4.
[87] Ibid.
[88] Ibid.
[89] GDPR
[90] Malabo Convention.
[91] J Neethling 'The protection of the right to privacy against fixation of private facts: notes' (2004) 121 *SALJ* 3 at 519.

Additionally, processing can take place under the Malabo Convention where there is a public interest on three grounds: preferably for historical, statistical, or scientific purposes, where it is necessary for the performance of a task in the interest of the public or where it is necessary for compliance with a legal or regulatory obligation to which the controller is subject.[92] The second tier of accountability rests on the data controller, who has a public interest that is necessary. Unlike Article 49(1)(d) of the GDPR, which does not provide for what is legitimate and proportionate, the Malabo Convention stipulates an accountability framework. It prefers public interest to be for specific purposes such as historical, statical and scientific purposes without making it mandatory. In the alternative, the public interest is also legitimate and proportionate where there is the necessity to perform a task or compliance with a legal and regulatory obligation. The defined parameters of the necessity test are compatible with the status of IOs, as it focuses mainly on mandate as a legitimate and proportionate aim of transferring personal data.

Lastly, the Malabo Convention under Article 14(6) extends the accountability approach to State Parties. While transfers under Article 45 of the GDPR are based on an adequacy decision determined by the European Commission and the requirement of an adequate level of protection is placed on third countries and IOs, the same is not replicated under the Malabo Convention. Contrastingly, Article 14(6)(b) shifts the obligation to the State Parties to determine adequacy requirements by giving the national protection authority of a State Party the mandate to issue any authorisation regarding the processing of data.[93] This accountability approach provides flexibility to State Parties to converge unilateral and bilateral approaches to personal data transfer mechanisms. It further provides an opening for the use of unique mechanisms proposed by the European Commission when considering safe requirements for the transfer of personal data that are compatible with the immunity status of IOs. Through this approach, State Parties can take advantage of fostering cooperation by engaging in diplomatic negotiations with IOs while committing to frameworks that strengthen the protection of personal data.

d. Conclusion

This chapter has highlighted the regulatory approaches that are utilised by states to effect trans-border data transfer. The core problem lies in the regulatory gap created by the fragmented and

[92] Supra note 13.
[93] Supra note 13.

often incompatible approaches to data protection, compounded by flexible yet underdeveloped frameworks. This makes it difficult to hold IOs accountable for data breaches especially because compliance priorities often lean toward compatibility rather than convergence. The aim of international discussion on regulation should be to foster trust and cooperation by finding a common ground.[94] This entails shifting focus from compatibility to convergence by identifying commonalities in the various data transfer instruments, convergence of the core principles and data protection frameworks, and complementarity of the various instruments.[95] The next chapter highlights an appropriate framework for viewing these commonalities to promote complementarity of the various data transfer approaches.

[94] OECD Trading Policy 'Mapping commonalities in regulatory approaches to cross-border data transfer' (2021) available at https://issuu.com/oecd.publishing/docs/mapping_commonalities_in_regulatory_approaches_to_ accessed on 27 May 2024.
[95] Ibid.

IV. DATA FREE FLOW WITH TRUST AS A PRACTICAL FRAMEWORK FOR HARMONISATION THROUGH COMMONALITIES

a. Introduction

In chapter two, I delved into the immunity question and the conflict of laws issue, highlighting the complexity of balancing these concerns with the demands of data protection laws.[96] It is this conflict that makes it difficult to streamline national, regional, and international frameworks.[97] This problem is exacerbated as seen in chapter three by the stringent adequacy requirements that focus on compatibility rather than complementarity of data transfer approaches. Due to the varying standards of adequacy, cross-harmonisation of data transfer frameworks is the wrong solution particularly in achieving a balance.[98] Currently, focus is shifting towards reconciling perception to provide a basis for negotiations.[99] This shift has prompted the need to address two interconnected issues: the misconception that harmonisation through identical uniformity achieves consensus, and, second, the importance of transitioning from the prescriptive approach to a more collaborative approach. Achieving consensus in perception requires flexible adequacy requirements for data transfer, as seen in the Malabo Convention, as well as a standard practical framework for interpreting common standards utilised in the various cooperative mechanisms. This chapter proposes Data Free Flow with Trust (DFFT) as one appropriate approach to achieving interoperability between IOs data protection frameworks and national data protection frameworks.

b. From divergence to convergence: the journey of data protection law

From my discussion in Chapter 2 and Chapter 3, I find that the Malabo Convention is better understood as an instrument to promote cooperation rather than a strict enforcement mechanism. The flexible enforcement structures allow for flexible cooperative efforts to negotiate enforcement of the shared data protection principles. This generalised approach in setting the fundamental principles as the core foundation of regulation is meditative of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"), which were strategic and intended to reflect the conflicting views of different States while refraining from

[96] See chapter 2 subsection c.
[97] OECD Trading Policy op cit note at 80.
[98] Christian Pauletto 'Options towards a global standard for the protection of individuals with regard to the processing of personal data' (2021) 40 *Computer Law & Security Review* at 14-17.
[99] World Economic Forum 'Every country has its own digital laws. How can we get data flowing freely between them?' available at https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/, accessed on 27 May 2024.

imposing a regulatory approach on international data flows.[100] States are currently witnessing a rising quest for such flexible frameworks as the tide is gradually shifting to bilateral and multilateral agreements. Not only are the shared privacy principles forming a mutual backstop for convergence in the various bilateral and multilateral instruments, but each agreement is evolving these principles into a unique framework.

For instance, we have seen the rise of a partnership between the European Union (Binding Corporate Rules) and Asia-Pacific Economic Cooperation (APEC Privacy framework),[101] with the aim of harmonising perception by highlighting the similarities and differences of each framework.[102] This framework fosters collaboration and aims to give parties a flexible mechanism to demonstrate compliance with data protection standards through a common checklist.[103] This accords Member Economies flexibility to collaborate with multiple stakeholders to adopt mutual recognition approaches to facilitate cross-border data transfer.[104] In the transatlantic area, we have also seen different types of private regulation, such as the Safe Harbor Agreement, which bridges the gap between American and European privacy frameworks beyond interoperability.[105] It has been pointed out that there has been limited progress but a notable convergence through the self-certification process and conformity with data protection rules in both regions.[106] This has seen a progression to flexible adequacy requirements by embracing a partial adequacy requirement.[107] This is a step towards opening market access and the European Union easing the stringent approach of blocking companies from jurisdictions with inadequate data protection safeguards.[108]

In Africa, regulation of cross-border mainly manifests in Free Trade Agreements (FTAs) and Preferential Trade Agreements (PTAs).[109] While bilateral and multilateral agreements exist, only

---

[100] Ibid.
[101] APEC/EU Referential for the Structure of the EU Binding Corporate Rules and APEC Cross Border Privacy Rules System-Draft Endorsement Request concluded on 20 February 2014 at Ningbo China, 2014/SOM1/ECSG/013.
[102] Baker Hostetler 'Moving Towards a Global Harmonized Approach to Cross-Border Data Transfers?' available at https://www.jdsupra.com/legalnews/moving-towards-a-global-harmonized-appro-51399/ accessed on 27 May 2024.
[103] Ibid.
[104] Ibid.
[105] Guillaume Beaumier *The Evolution of Privacy Regulation: Convergence and Divergence in the Transatlantic Space* (published PhD thesis University of Warwick and Université Laval, 2020) 136.
[106] Ibid at 127.
[107] Ibid.
[108] Ibid at 137.
[109] Nelly C. Rotich 'Examining Cross-Border Data Flows Provisions in Africa's Free Trade Agreements' available at https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/, accessed on 27 May 2024.

a few provisions address issues of cross-border data transfer.[110] Overall, though the visible cooperative efforts are a commendable step in establishing flexible frameworks, there seems to be a gap in the transparency of an interpretation guideline that fosters a practical framework within the cooperative mechanisms used to achieve accountability of the agreed data protection principles. It would be misleading to assume that the data protection principles apply automatically when enforced through collaborative instruments such as mutual agreements. Of importance is that we narrow the gap of legal uncertainty in flexible regulatory frameworks, like the Malabo Convention, that give birth to independent regulatory platforms. It is paramount that these principles are operationalised through a defined practical framework that creates legal certainty. For purposes of this paper, I shall limit the proposal of a practical framework for interpreting the data protection principles to cooperative mechanisms that aim to facilitate the safe transfer of personal data to IOs.

c. Data Free Flow with Trust as a framework for interpretating safe personal data transfer to IOs.

The Data Free Flow with Trust (DFFT) concept has been proposed as the foundational principle for legislating on cross-border data transfer issues because it moves away from creating homogeneous frameworks to one founded on trust and responsible data governance.[111] Through this concept, regulatory coordination, as opposed to consensus, is made possible through intergovernmental rule-making founded on trust.[112] Therefore, the focus on interoperability is shifting to national frameworks to ensure national data governance systems are harmonious rather than identical.[113] To achieve this interoperability at the national level, the World Bank has proposed an integrated national data ecosystem founded on a social contract for data.[114] This means intentional collaboration of multiple stakeholders to ensure data is shared based on value, trust, and equity.[115] To operationalise DFFT, the OECD has proposed using an existing legal basis for

[110] Ibid.
[111] Center for Identity Governance 'Data Free Flow with Trust' available at https://identitymanagementinstitute.org/data-free-flow-with-trust/ accessed on 27 May 2024.
[112] World Economic Forum op cit note 78.
[113] Aidan Arasasingham and Matthew P. Goodman 'Operationalizing Data Free Flow with Trust (DFFT)' available at https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft accessed on 27 May 2024.
[114] Declan Deasy, Yaroslav Eferin &Oleg Petrov 'Integrated national data ecosystems: the next stage of digital transformation' available at https://blogs.worldbank.org/en/digital-development/integrated-national-data-ecosystems-next-stage-digital-transformation accessed on 27 May 2024.
[115] The World Bank Development Report on Data for Better Lives 2021.

cross-border data transfer. For instance, there is recognition that the accountability principle is reflected in many data protection laws as a core principle.[116] Therefore, the OECD notes that regulating data transfer through the accountability principle, promotes trust through protection that is context-specific.[117]

DFFT is one flexible approach to managing the free flow of personal data to IO without unnecessary restrictions from the data protection laws of each country.[118] To operationalise and make this approach meaningful, it should not remain a concept or a standard in regulating cross-border data transfer but should evolve into a practical framework for cooperative mechanisms seeking to respond to a regulatory challenge in data protection frameworks. To operationalise this framework for IOs and State Parties seeking to manage the safe transfer of personal data, the following steps should be considered:

a) Transparency on the specific categories of data and the purpose of collection[119] – similar to data protection frameworks that manage transfer of personal data through transparent legal basis, trust must be defined and demonstrated through transparency mechanisms. For instance, IOs and States can agree on transparency databases as a way of building trust.
b) Facilitate interoperability of data protection ecosystem of IOs and State Parties- one way is to build from existing frameworks such as the partnership between the European Union (Binding Corporate Rules) and APEC Privacy Framework that highlights similarities and differences of each regulation and actualise them through the common checklist. This process will facilitate mapping out of common standards and build on a common checklist, which can form flexible adequacy requirements between IOs and the State Parties.
c) Building on internal synergy on regulation of personal data: regulatory sandboxes can be adopted to streamline compliance issues and identify a common approach to promoting interoperable data security mechanisms.[120]

[116] OECD Digital Economy Paper no. 353 on Moving Forward on Data Free Flow with Trust: New evidence and analysis of business experiences (2023).
[117] Ibid.
[118] Digital Agency 'Overview of DFFT' available at *https://www.digital.go.jp/en/dfft-overview-en* accessed on 14 October 2024.
[119] Aidan Arasasingham & Matthew Goodman op cit note 98.
[120] Keita Oikawa 'Future of Data Governance in Asia and Operationalisation of Data Free Flow with Trust' (policy brief published in ERIA no. 2024-01).

d) Appoint a multistakeholder working party to facilitate the process in accordance with the priorities of the data protection common checklist.

In embracing a clearly defined practical framework within the cooperative instruments, we create certainty in what it means to harmonise through commonalities. Nonetheless, we need to ensure that we have a strong regional instrument on which the practical frameworks of cooperative instruments can be operationalised and modelled or else trust will not effectively occur. For this reason, there is an urgent need to reshape our regulatory regime and ensure it does not remain a check-box exercise. Therefore, regional frameworks should move away from an authoritative governance framework[121] to a collaborative governance framework that fosters cooperation at multiple levels of governance.

d. Conclusion

This chapter highlighted how the concept of DFTT can be utilised as a practical framework to foster interoperability. It provides a balanced approach to existing data protection frameworks by ensuring that the system inspires trust rather than standardising all aspects of data protection. However, for this framework to be responsive, the regulatory structures must be flexible but offer robust data protection mechanisms. Therefore, the next chapter shall entail a discussion on how we can strengthen our regulatory structures to enable coherent data protection frameworks that can collaborate across different jurisdictions without compromising privacy.

[121] Christopher Kuner 'A Global Regulatory Framework for Transborder Data Flows' *Transborder Data Flows and Data Privacy Law* ed (2013) 157-188.

V. RECOMMENDATIONS AND CONCLUSION

a. Introduction

In the previous chapters, I have demonstrated the need to adopt an existing flexible regulatory framework that responds efficiently to emerging data protection issues.[122] Regulation is often viewed through different models such as self-regulation, core regulation, and command and control regulations that prioritise different approaches depending on the regulatory demand and goal. Despite the diverse approaches, this chapter notes a worrying trend in legislators prioritising one regulatory model over the others without contemplating the regulatory objectives. In this report, I note that this limitation is advanced by the narrow interpretation of regulatory goals to strictly imposed obligations. As a result, legislators miss out on effectively regulating issues because they bypass the broad objective of regulation in fostering cooperation. For purposes of this chapter, I focus the discussion on command-and-control regulation and core regulation.

Shifting to flexible regulatory structures has proven to be a slow process due to the doubts about its effectiveness in response to regulatory issues. Notably, the OECD, in its report Alternatives to Traditional Regulation, has raised concern about an over-reliance on command-and-control regulations that impose overly prescriptive regulation without examining the effectiveness and efficiency in achieving the objectives.[123] This is despite the possibility of using more flexible forms of regulation, such as core regulation.[124] For this reason, the OECD has encouraged the use of alternative instruments as a factor for regulatory decision-making.[125] On this basis, this chapter recommends a core regulatory approach demonstrating its flexibility in regulating personal data transfer to IOs.

b. Command and Control versus Core regulation: The efficiency conundrum

When determining the most efficient models to adopt in legislation, it is paramount for legislators to adopt a framework that analyses the why, what, where and why aspects of regulation. This involves a contextual case-by-case analysis of the following key questions: what is the nature of command-and-control regulations *as compared* to core regulation? When and how should we use command and control regulations over core regulations? Why should we prioritise one regulation

[122] See chapter 3 and 4.
[123] Glen Hepburn OECD Report on Alternatives to Traditional Regulation.
[124] Ibid.
[125] Ibid.

over the other? These questions provide a framework for examining the correct model that responds to the objectives of data protection regulations. The below comparative analysis of the two models illustrates why priority should be afforded to a core-regulation approach in the context of data protection.

i. Command and Control

Command and control is a top-down regulatory approach backed by legal rules and sanctions.[126] Often, this regulatory approach is mainly preferred when seeking to regulate behaviour because of its predictability and homogeneous application.[127] This is evident in command-and-control data protection regulations, where the prescribed data protection principles have created an inherent universal guideline for collaboration. Not only has it led to a baseline for creating interoperability, but it has lessened ambiguity on standards of mutual recognition by different states. Furthermore, the clear enforcement mechanisms in command-and-control regulations provide specificity and easier monitoring and compliance.[128] This is particularly important now, given the vast data collection and sharing points involving data subjects, which they may be aware of or not, thus creating a need for an accountability instrument.[129] Furthermore, to reduce the policing burden on data subjects, there must be a structure that sets mandatory obligations and defined enforcement structures that address any breaches that arise. As a result, command and control regulations promote this legal certainty in data protection regulations, by minimising state or third parties regulatory capture and restricting their influence on the objectives of regulations. Therefore, the role of a command-and-control approach in effectively regulating data protection should neither be misconstrued nor dismissed.

Cole and Grossman, in their examination of when command-and-control are deemed efficient, make observations that are noteworthy for this discussion.[130] First, is that alternative regulatory regimes often ignore the contextual setting of command-and-control regulations.

---

[126] Michèle Finck 'Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy' (LSE Law, Society and Economy Working Papers 15/2017).
[127] Ibid.
[128] Susan Karr et.al 'What is command and control regulation, and what are its pros and cons? In Susan et.al (ed) *Environmental Science for a Changing World* 47.
[129] Ibid.
[130] Daniel Cole & Peter Grossman 'When is Command and Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes for Environmental Protection (1999) 887 *Wisconsin Law Review* at 1-53.

Second, alternative models tend to overstate the differences of command-and-control frameworks compared to other regulations. As a result, they find that there tends to be a blanket assumption that command-and-control frameworks are typically inefficient though occasionally efficient.[131] They conclude that only upon examining the trade-offs such as costs, should command-and-control frameworks be judged as either efficient and effective.[132] This clarification is useful in scoping this chapter's preference for the core regulation model over the command-and-control model. In agreement with Cole and Grossman, I find that no regulatory model is superior, and they all possess some inefficiency depending on the context, objectives, and costs.

However, while this chapter appreciates the baseline and legal certainty the command-and-control approach lays for other models, an analysis of Cole and Grossman's considerations shows that such an approach offers significant inefficiencies in the context of data protection. This is particularly true when looking at regulation of personal data to IOs. First is the lack of flexible standards to respond to the immunity question. Command and control regulations set mandatory standards that must be met with little consideration to the context, which might not be workable and efficient.[133] This is seen in earlier analyses of the GDPR's adequacy requirements for data transfer and the conflicts with the immunity status of IOs.[134] In most cases, the stringent requirements are not focused on boosting efficiency but on promoting political interests. As a result, there is minimal incentive to improve the responsiveness of legislation beyond the standards set by law.[135] Additionally, the inefficiencies are not only due to stringent standards but also the disconnect in the conceptualisation of privacy in data protection legislation and on the ground. As observed by Bamberger and Mulligan, privacy protection is a '*strategic issue that connects concerns that extend beyond mere compliance of set rules*.[136] The aforementioned authors perceive privacy as an evolving concept determined by context and encompassing agility beyond individual consent and control.[137] Bamberger and Mulligan urge legislators to view privacy as a unique and

[131] Ibid.
[132] Ibid
[133] Susan Karr et.al op cit note 112.
[134] See p.18.
[135]'Command and Control Regulation' in Principles of Microeconomics available at *https://pressbooks.oer.hawaii.edu/principlesofmicroeconomics/chapter/12-2-command-and-control-regulation/* accessed on 13 October 2024.
[136] Kenneth Bamberger & Deirdre Mulligan (eds) 'Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe) in *Privacy on the Ground: Driving Corporate Behaviour in the US and Europe* (MIT 2015) 1-20.
[137] Ibid.

complex concept that cannot be confined through prescriptive rules. Otherwise, our regulatory approaches risk becoming outdated and lacking the required proactivity.[138] Instead, our personal privacy will effectively thrive where there are collaborative approaches, resources, and some level of ambiguity in our legislation.[139] This demands the need for flexible regulatory environments and autonomy among multiple stakeholders to engage in the evolving privacy norms and meaningfully unpack them in practice.[140] To work effectively, a core regulation framework for data protection needs clear, flexible principles and practical, collaborative mechanisms. These include core principles like data minimization and equivalence, which focus on outcomes rather than rigid rules. For implementation, it requires flexible standards, such as a tiered regulatory approach, and core regulatory instruments like model Memoranda of Understanding (MOUs) and interpretive guidelines from a central authority. This principles-based approach allows different systems to be interoperable without being identical, thereby offering a viable solution to the legal and jurisdictional challenges posed by entities like International Organizations (IOs).

ii. Core regulation

Core regulation is a regulatory model that adopts both traditional legislation and self-regulatory instruments.[141] This is so particularly when it comes to regulating the transfer of personal data: the approach recognises the insufficiency of the law in legislating the obligations of the different stakeholders involved in the processing of personal data.[142] The core regulatory model gives the relevant stakeholder processing data independence but with a prescribed framework.[143] This model does not manifest in one form, which demonstrates its agility to adapt, foster the inclusivity of multiple stakeholders,[144] and offer flexibility in implementing data protection general principles based on the relevant context.[145] Furthermore, this flexibility provides for the generation of legal uncertainties that can be resolved through core regulatory instruments.[146] This aligns with the

[138] Ibid.
[139] Ibid.
[140] Ibid.
[141] Irene Kamara 'Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'' (2017) 8 European Journal of Law and Technology 1 at 1.
[142] Ibid.
[143] Rolf H. Weber 'Co-regulation' available at https://platformglossary.info/co-regulation/ accessed on 27 May 2024.
[144] Hans J. Kleinsteuber 'The Internet between Regulation and Governance' available at https://www.osce.org/files/f/documents/2/a/13844.pdf accessed on 27 May 2024.
[145] Ibid.
[146] Francesco Vigna 'Co-regulation Approach for Governing Big Data: Thoughts on Data Protection Law *ICEGOV* 4-7 October 2022, available at *https://dl.acm.org/doi/fullHtml/10.1145/3560107.3560117* accessed on 14 October 2024.

OECD proposal on strengthening cross-border cooperation through international initiatives, such as bilateral or multilateral enforcement arrangements or memoranda of understanding (MOU).[147] This will promote best practice standards between the relevant stakeholders and ensure the policy objectives under the various stakeholders' regulatory frameworks are achieved through cooperation.[148] Additionally, through core regulatory instruments, there is the benefit of shared expertise and access to evolving knowledge, where one group of legislators would not possess when drafting or updating existing legislation.[149] From this perspective, data subjects are assured of innovative responses, efficient enforcement, and accountability from multiple stakeholders.[150] Therefore, this approach will include concrete commitments on purpose limitation, data minimization, and enhanced security standards. The agreements must also establish a clear, independent dispute resolution mechanism that bypasses national courts, directly addressing the immunity question. plays a key role in responding to the legal uncertainties of data protection laws, such as the immunity question identified in this research report.

On the downside, there is a concern about the interest levels by multiple stakeholders in achieving the regulatory objectives of data protection when accorded the flexibility to negotiate on the outcomes of regulation. Often, if there is inadequate representation during high-level negotiations, the regulatory goal would be to boost reputations or avoid fines.[151] There is little confidence in this approach when there are no oversight channels and expertise to negotiate the flexibilities in line with the data protection goals. This creates a bargaining power gap if the flexibilities' relevance is not codified in regulatory instruments. To ensure that this approach is efficient, legislators must not just push for core regulation approaches but ensure they are adopting balanced core regulatory models. This requires a reduction of inflammatory flexibilities through strategically built-in approaches to promote transparency and accountability. This is particularly

[147] OECD (2011), "Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", *OECD Digital Economy Papers*, No. 178.
[148] Ibid.
[149] Laurent Cre´peau 'Responding to Deficiencies in the Architecture of Privacy: Co-Regulation as the Path Forward for Data Protection on Social Networking Sites' (2022) 19 *Canadian Journal of Law and Technology* 2 at 411-454.
[150] Ibid.
[151] Edward Balleisen and Marc Eisner 'The Promise and Pitfalls of Co-Regulation: How Governments Can Draw on Private Governance for Public Purpose' in D. Moss & J. Cisternino (eds) *New Perspectives on Regulation* (2009 The Tobin Project) at 127-149.

important in regional instruments such as the Malabo Convention, which can be used to facilitate the establishment of core regulation instruments.

To this end, the Malabo Convention can adopt a balanced core regulatory framework similar to the Brazilian General Data Protection Law (LGPD)[152] that balances its flexibilities with legal certainty. The legislators can learn from some of the structures in the LGPD that can be utilised to adequately respond to unique regulatory challenges, such as transferring personal data to IOs. For example, article 6 of the LGPD introduces good faith as a principle that governs processing activities. This creates a technical tool for interpretation that mediates the effects between data protection regulatory goals and the immunity status of IOs.[153] As a result, good faith creates a consensus between international law and domestic law in the interpretation of data protection principles. Another observation is that Article 33 of the LGPD creates a closed list for permitted grounds for international data transfer. However, the Act does not give preferential treatment to any ground, and its language is framed with flexibility. For instance, it permits international sharing of personal data when it results from an international cooperation agreement, when it is necessary to protect life and when it is essential for legal cooperation between specified bodies.[154] This provision allows mutual recognition within the law when initiating international data transfers, but based on flexible adequacy requirements. Lastly, Article 40 of the LGPD encourages national authorities to develop standards for interoperability to initiate free access to data while maintaining security.[155] This move is beneficial in building the core regulation network by encouraging national frameworks to adopt flexible approaches and promote the inclusivity of multiple stakeholders. Therefore, this framework provides a valuable guide to build a balanced core regulatory model for the Malabo Convention creating a balance between good faith and clear accountability mechanism with guarantees on data subject rights and express prohibitions on re-transfer.

c. MOUs as a core regulatory instrument to promote safe data transfer to IOs

With the opportunity in the Malabo Convention to explore core regulatory approaches, this research report proposes using MOUs as an adequate core regulatory instrument that states can

[152] Brazilian General Personal Data Protection Act (LGPD) Law No.13,709 of 14 August 2018.

[153] Steven Reinhold 'Good Faith in International Law' (2013) 2 *UCL Journal of Law and Jurisprudence* at 40-63.
[154] Article 33 of LGPD.
[155] Ibid Art. 40.

utilise to impose accountability on IOs, while respecting their immunity status. MOUs provide a framework for cooperation and coordination by outlining the key considerations and broad guidelines regarding the processing of personal data. Due to the non-binding and voluntary basis of such negotiations, MOUs can be utilised in avoiding divergences and promoting compatibility with existing data protection frameworks while respecting jurisdictional boundaries.[156] This approach provides unique mechanisms to create a negotiated and conditional contractual obligation for international organizations (IOs). This obligation is based on mutual consent and the core principles of data protection law. At the same time, it helps to ensure that member states meet the adequacy requirements needed for the safe transfer of personal data. As a result, core data protection principles are not merely wishful in their application, but facilitate a convergence through a practical framework.

d. Conclusion

i) Findings

Overall, this paper's analysis of the Malabo Convention's adequacy requirements demonstrates a responsive avenue to the immunity question while at the same time exhibiting explicit weaknesses that require refinement.[157] The inclusion of state adequacy requirements under Article 8(1) and 14(6)(b) of the Malabo Convention is commendable because it displays a built-in flexible mechanism that can benefit from development to facilitate a core regulation ecosystem. This provides a good baseline to replicate in regional data protection frameworks that are considering adopting a core regulatory approach. Additionally, it also provides a good avenue for the Malabo Member States to develop external mechanisms for collaborations with IOs.

ii) Limitations

However, the weaknesses lie in the fact that the core regulation approach appears coincidental rather than intentional. For this reason, core regulation is likely to be perceived as a tool for interpreting the regulatory deficiencies of the command-and-control approach rather than a default structure of regulation. The danger with this approach is that the ambiguity surrounding

[156] Information Commissioner's Office 'Memorandum of Understanding for Cooperation in the Application of Laws Protecting Personal Data' available at https://www.edps.europa.eu/system/files/2023-11/23-11-08_mou_edps_ico_en.pdf accessed on 27 May 2024.
[157] See chapter 3.

the place of core regulation within the Malabo Convention could oppress the existing and potential flexibilities. In its current state, the Malabo Convention creates an unexploited convergence through its data protection principles and the potential pathways of utilising core regulation. Even so, there is a lack of legislative intervention to bridge the gap between the two, ensuring that the influence of core regulation does not collapse at the national level or within the preferred instruments of cooperation. As it stands, the core regulation approach would benefit from further improvement; or else, the Malabo Convention risk losing its implementation value and retaining the prescriptive inefficiencies of the data protection principles in command-and-control regulations, which assumes that correct application fosters collaboration.

iii) Reforms

Looking forward, there is an opportunity for the Malabo Convention to assert its command in fostering regional cooperation by streamlining its flexibilities through the following specific reforms:

a) **Establish an African Union (AU) Data Protection Authority**: The creation of a dedicated AU Data Protection Authority would provide centralised guidance and approach to utilizing flexibilities through issuance of interpretive guidelines on how Member States can apply the Convention's principles, particularly concerning data transfers to IOs. Therefore, the Authority would act as a central hub for legal expertise and collaboration.
b) **Develop Model Memoranda of Understanding (MOUs)**: The AU Data Protection Authority, in collaboration with IOs, could develop model MOUs. These MOUs though non-binding can serve as influential pre-negotiated templates that outline data protection principles, security requirements, and a dispute resolution mechanism for data transfers between an IO and a Member State. Since MOUs are based on voluntary agreement rather than legal compulsion, they bypass the jurisdictional immunity issue providing a practical, ready to use tool that bridges the gap between the IO's legal status and the Member State's data protection requirements.

a) **Create Interpretive Guidelines for Legal Certainty**: The AU Data Protection Authority should publish **interpretive guidelines** that explicitly state how the Malabo Convention's principles can be applied to IOs. These guidelines would clarify what constitutes an adequate level of protection within the context of an IO's internal framework and

highlighting where Member States can utilize core regulation tools. The guidelines could, for instance, specify that an IO's internal data protection policy, if independently audited and publicly available, can be deemed sufficient for data transfer purposes.

b) **Streamline Mutual Recognition**: The reforms should encourage a system of mutual recognition among Malabo Convention Member States. By establishing a shared baseline of principles, a data transfer framework approved by one Member State's data protection authority would be deemed as valid by others. This avoids the need for repetitive, state by state negotiations with IOs and other partners, promoting efficiency and regional cooperation.

BIBLIOGRAPHY

LEGISLATION

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) adopted on June 27, 2014, by the twenty third Ordinary Session of the African Union Assembly, EX.CL/846(XXV).

European Union Regulation 2016/679 of the European Parliament (General Data Protection Regulation) in OJ L119/1 of 27 April 2016.

Brazilian General Personal Data Protection Act (LGPD) Law No.13,709 of 14 August 2018.

Kenya's Data Protection Act Cap. 411C.

Protection of Personal Information Act (POPIA) Act 4 of 2013.

CASES

CJEU, Grand Chamber, *Maximilian Schrems v Data Protection Commissioner* Case C- 362/14 OF 6 October 2015.

CJEU, Grand Chamber, *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems* Case C- 311/18 of 16 July 2020

JOURNAL ARTICLES

Bjørn Aslak Juliussen, Elisavet Kozyri, Dag Johansen and Jon Petter Rui 'The third country problem under the GDPR: enhancing protection of data transfers with technology' (2023) 13 *International Data Privacy Law 3* at 225-243.

Christopher Kuner 'International Organizations and the EU General Data Protection Regulation' (2019) 16 *International Organizations Law Review* at 158.

Christopher Kuner 'The GDPR and International Organizations' (2020) 114 *American Journal of International Law* at 16.

Christian Pauletto 'Options towards a global standard for the protection of individuals with regard to the processing of personal data' (2021) 40 *Computer Law & Security Review* at 14-17.

Daniel Cole & Peter Grossman ‘When is Command and Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes for Environmental Protection (1999) 887 *Wisconsin Law Review* at 1-53.

Itumeleng Shale ‘Historical perspective on the place of international human rights treaties in the legal system of Lesotho: Moving beyond the monist-dualist dichotomy’ (2019) 19 *African Human Rights Law Journal* 1

Ioannis Ntouvas ‘Exporting personal data to EU-based international organizations under the GDPR’ (2019) 9 *International Data Privacy Law* 4

Irene Kamara ‘Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardization 'mandate'’ (2017) 8 European Journal of Law and Technology 1 at 1

J Neethling ‘The protection of the right to privacy against fixation of private facts: notes’ (2004) 121 *SALJ* 3

Kenneth Bamberger & Deirdre Mulligan (eds) ‘Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe) in *Privacy on the Ground: Driving Corporate Behaviour in the US and Europe* (MIT 2015) 1-20.

Kgothatso Shai et. Al ‘A critical analysis of the difficulties faced by international organisations within the context of the role of the United Nations (2019) 7 *APSDPR* 1

Laurent Cre´peau ‘Responding to Deficiencies in the Architecture of Privacy: Co-Regulation as the Path Forward for Data Protection on Social Networking Sites’ (2022) 19 *Canadian Journal of Law and Technology* 2 at 411-454

Massimo Marelli ‘Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms’ (2024) 14 *International Data Privacy Law* 1

Massimo Marelli ‘The law and practice of international organizations’ interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders’ (2023) 50 *Computer Law & Security Review*

Michelle Barnard 'Legal Reception in the AU against the Backdrop of the Monist/Dualist Dichotomy' (2015) 48 *Comparative and International Law Journal of Southern Africa* 1

Orla Lynskey 'Complete and Effective Data Protection' (2023) 76 *Current Legal Problems* 1

Olumide Babalola 'Transborder flow of personal data (TDF) in Africa: Stocktaking the ills and gains of a divergently regulated business mechanism' (2024) 52 *Computer Law & Security Review* at 4

Steven Reinhold 'Good Faith in International Law' (2013) 2 *UCL Journal of Law and Jurisprudence* at 40-63

Wilfred Mutubwa 'Monism or Dualism: The Dilemma in The Application of International Agreements Under the South African Constitution' (2019) 3 *Journalofcmsd* 1

Xi Yang 'Regulatory Approaches of Cross-border Data Flow in the Big Data Era: China's Choice' (2021) 1848 *Journal of Physics*: *Conference Series* at 1-9.

BOOKS

Christopher Kuner 'A Global Regulatory Framework for Transborder Data Flows' *Transborder Data Flows and Data Privacy Law* ed (2013) 157-188.

Christopher Kuner and Massimo Marelli 'Basic Principles of Data Protection' *Handbook on Data Protection in Humanitarian Action* (2017) 27

David P. Stewart & Ingrid Wuerth 'The Jurisdictional Immunities of International Organisations: Recent Developments and the Challenges of the Future' in Paul B. Stephan & Sarah A. Cleveland (ed) *The Restatement and Beyond: The past, present and future of U.S. Foreign Relations Law* (2020) 411-432.

Edward Okeke 'The tension between the Jurisdictional Immunity of International Organisations and the Right of Access to Courts' in Peter Quayle (ed) *The Role of International Administrative Law at International Organisations* (2020) 25-53.

Edward Balleisen and Marc Eisner 'The Promise and Pitfalls of Co-Regulation: How Governments Can Draw on Private Governance for Public Purpose' in D. Moss & J. Cisternino (eds) *New Perspectives on Regulation* (2009 The Tobin Project) at 127-149.

Julia Hornle ‘Heads in the Clouds: The clash between Territorial Sovereignty, Jurisdiction, and the Territorial Detachment of the Internet’ in Julia (ed) *Internet Jurisdiction Law and Practice* (2021) 4-32.

Lee A. Bygrave ‘Core Principles of Data Privacy Law’ *Data Privacy Law: An International Perspective* ed (2014) 145.

Raphaël Gellert ‘Data protection as command-and-control regulation’ *The Risk-Based Approach to Data Protection* ed (2020) 54.

Rosanne Van Alebeek *The Immunity of States and Their Officials in International Criminal Law and International Human Rights Lawed* ed (2008).

Susan Karr et.al ‘What is command and control regulation, and what are its pros and cons? In Susan et.al (ed) *Environmental Science for a Changing World* 47.

Tom Ruys, Nicolas Angelet and Luca Ferro *The Cambridge Handbook of Immunities and International Law* ed (2019) i-ii.

van der Merwe ‘Data Privacy Law’ (ed) *Information Communications and Technology Law* 3 ed (2021) 372.

INTERNET SOURCES (OTHER)

ALT Advisory ‘THE MALABO ROADMAP: Approaches to promote data protection and data governance in Africa’ available at https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf. accessed on 26 May 2024.

Aidan Arasasingham and Matthew P. Goodman ‘Operationalizing Data Free Flow with Trust (DFFT)’ available at https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft. accessed on 27 May 2024.

Antonio Muñoz Marcos ‘The future of privacy is convergence’ available at https://www.telefonica.com/en/communication-room/blog/the-future-of-privacy-is-convergence/. accessed on 26 May 2024.

Alexander Beck and Christopher Kuner ‘Data Protection in International Organizations and the New UNHCR Data Protection Policy: Light at the End of the Tunnel?’ available at

https://www.ejiltalk.org/data-protection-in-international-organizations-and-the-new-unhcr-data-protection-policy-light-at-the-end-of-the-tunnel/. accessed on 26 May 2024.

APEC/EU Referential for the Structure of the EU Binding Corporate Rules and APEC Cross Border Privacy Rules System-Draft Endorsement Request concluded on 20 February 2014 at Ningbo China, 2014/SOM1/ECSG/013.

Baker Hostetler 'Moving Towards a Global Harmonized Approach to Cross-Border Data Transfers?' available at https://www.jdsupra.com/legalnews/moving-towards-a-global-harmonized-appro-51399/. accessed on 27 May 2024.

Center for Identity Governance 'Data Free Flow with Trust' available at https://identitymanagementinstitute.org/data-free-flow-with-trust/. accessed on 27 May 2024.

Christopher Kuner and Massimo Marelli 'Creating International Frameworks for Data Protection: The ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action' available athttps://www.ejiltalk.org/creating-international-frameworks-for-data-protection-the-icrcbrussels-privacy-hub-handbook-on-data-protection-in-humanitarian-action/. accessed on 26 May 2024.

Casalini F., J. López González and T. Nemoto 'Mapping commonalities in regulatory approaches to European Commission, 'The New Standard Contractual Clauses—Questions and Answers Overview' at ad14 available at https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf. cross-border data transfers' (2021) *OECD Trade Policy Papers*, No. 248.

Command and Control Regulation' in Principles of Microeconomics available at https://pressbooks.oer.hawaii.edu/principlesofmicroeconomics/chapter/12-2-command-and-control-regulation/. accessed on 13 October 2024.

Declan Deasy, Yaroslav Eferin &Oleg Petrov 'Integrated national data ecosystems: the next stage of digital transformation' available at https://blogs.worldbank.org/en/digital-development/integrated-national-data-ecosystems-next-stage-digital-transformation. accessed on 27 May 2024.

Digital Agency ‘Overview of DFFT’ available at https://www.digital.go.jp/en/dfft-overview-en. accessed on 14 October 2024.

European Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework available at https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf. para 185 accessed on 27 May 2024.

Francesco Vigna ‘Co-regulation Approach for Governing Big Data: Thoughts on Data Protection Law *ICEGOV* 4-7 October 2022, available at https://dl.acm.org/doi/fullHtml/10.1145/3560107.3560117. accessed on 27 May 2024.

Guillaume Beaumier *The Evolution of Privacy Regulation: Convergence and Divergence in the Transatlantic Space* (published PhD thesis University of Warwick and Université Laval, 2020) 136

Glen Hepburn OECD Report on Alternatives to Traditional Regulation

Hans J. Kleinsteuber ‘The Internet between Regulation and Governance’ available at https://www.osce.org/files/f/documents/2/a/13844.pdf. accessed on 27 May 2024.

Internet Society ‘The Future of Privacy’ available at https://www.internetsociety.org/wp-content/uploads/2017/09/future-privacy-20100914.pdf. accessed on 26 May 2024.

Information Commissioner’s Office ‘Memorandum of Understanding for Cooperation in the Application of Laws Protecting Personal Data’ available at https://www.edps.europa.eu/system/files/2023-11/23-11-08_mou_edps_ico_en.pdf. accessed on 27 May 2024.

Keita Oikawa ‘Future of Data Governance in Asia and Operationalisation of Data Free Flow with Trust’ (policy brief published in ERIA no. 2024-01)

Madelaine Chiam ‘Monism and Dualism in International Law’ available at https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0168.xml. accessed on 26 May 2024.

Michèle Finck 'Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy' (LSE Law, Society and Economy Working Papers 15/2017).

Nelly C. Rotich 'Examining Cross-Border Data Flows Provisions in Africa's Free Trade Agreements' available at https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/. accessed on 27 May 2024.

OECD Digital Economy Paper no. 353 on Moving Forward on Data Free Flow with Trust: New evidence and analysis of business experiences (2023).

OECD (2011), "Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", *OECD Digital Economy Papers*, No. 178.

OECD Trading Policy 'Mapping commonalities in regulatory approaches to cross-border data transfer' (2021) available at https://issuu.com/oecd.publishing/docs/mapping_commonalities_in_regulatory_approaches_to_. accessed on 27 May 2024.

OECD Digital Economy Paper no. 353 on Moving Forward on Data Free Flow with Trust: New evidence and analysis of business experiences (2023).

Rolf H. Weber 'Co-regulation' available at https://platformglossary.info/co-regulation/. accessed on 27 May 2024.

Robinson L. K. Kizawa and E. Ronchi (2021) 'Interoperability of privacy and data protection frameworks' Going Digital Toolkit Note No. 21 available at https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf. accessed on 26 May 2024.

Status list of countries that have signed, ratified/acceded to African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) as of May 11, 2020, by the African Union available at 29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf. accessed on 24 February 2025.

The World Bank Development Report on Data for Better Lives 2021.

The *White Paper on Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy* (published by the Centre for Information Policy Leadership of 25 September 2017 updated 7 July 2017).

UNCTAD 'Data protection regulations and international data flows: Implications for trade and development' available at https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. accessed on 26 May 2024.

United Nations 'G20 Members' Regulations of Cross-Border Data Flows (2023) available at https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf. accessed on 27 May 2024.

World Economic Forum 'Every country has its own digital laws. How can we get data flowing freely between them?' available at https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/. accessed on 27 May 2024.