Politics and Governance
2025 • Volume 13 • Article 10422
https://doi.org/10.17645/pag.10422

cogitatio

ARTICLE

Open Access Journal

The EU's Digital Footprint: Shaping Data Governance in Japan and Singapore

Danni Zhang [1,2]

[1] Faculty of Politics and International Relations, Northeastern University London, UK
[2] Institute of Cyber Security for Society, University of Kent, UK

Correspondence: Danni Zhang (dz3501phd@nulondon.ac.uk)

Submitted: 28 March 2025 **Accepted:** 8 May 2025 **Published:** 16 July 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

The rapid development of the internet and information and communication technologies over the past few decades has led to the emergence of a new digital order, attracting significant attention from both academia and policymakers. In the global digital domain, the EU has assumed a distinctive role in shaping and influencing digital norms and standards. This status stems from the EU's pioneering efforts, ranging from the Council of Europe's Convention 108 (1981) to the more recent General Data Protection Regulation, which has exerted far-reaching extraterritorial effects, influencing data laws and regulatory practices beyond the EU's borders. However, there remains a lack of sufficient research on how these actors have progressively enacted and revised their data regulations in response to evolving EU standards. To address this gap, this article adopts a qualitative approach to examine how the EU's evolving data regulations have diffused to and been adopted by two Asian countries—Japan and Singapore. By categorising diffusion mechanisms into incentive, socialisation, learning, competition, and emulation, this research further explores the operative mechanisms underpinning the diffusion process. This research argues that the EU's diffuse-ability in Japan has demonstrated a gradual strengthening trend, with socialisation functioning as the primary mechanism driving this process. In contrast, the EU's diffuse-ability in Singapore has remained relatively weak, with competition serving as the dominant mechanism.

Keywords

data governance; diffuse-ability; EU; Japan; Singapore

1. Introduction

In the digital era, data has emerged as a key geopolitical and economic asset, influencing everything from global trade to national security. More specifically, since data is often referred to as "the new oil" (Humby, 2006, as cited in Palmer, 2006), governments have embraced this metaphor to emphasise its transformative power in the modern economy (Kuneva, 2009; World Economic Forum, 2011). This analogy underscores the strategic value of data, which, much like oil, has become a vital resource central to geopolitical competition. While traditional geopolitics has historically focused on physical geography, the rapid development of information and communication technologies (ICTs) and the internet has introduced cyberspace as an increasingly salient dimension (Brunn, 2000; Deibert, 2008). This expansion has extended the scope of geopolitics to the virtual sphere, making data governance—including its collection, storage, transfer, and protection—a critical issue in shaping international relations and geopolitical dynamics. Moreover, governments advocate divergent models of data governance, thereby creating barriers to global data flow and complicating international cooperation and trade (O'Hara & Hall, 2021). As a key player in both global geopolitical competition and the digital economy, the EU, alongside the US and China, supports a model of data governance that is widely regarded as rights-based, emphasising privacy and data protection (Bradford, 2023; O'Hara & Hall, 2021).

The EU has historically been recognised as a normative power (Manners, 2002), with its strategies often characterised as the "soft version of geopolitics" (Edwards, 2008), extending the norms, values, and standards developed within its geographic space to other countries (Christou, 2010). As the EU strives to promote its norms, values, and standards globally, its role in diffusing these principles provides valuable insights for diffusion research. Specifically, in existing policy diffusion research, two main perspectives explain why external actors selectively adopt EU standards or policies. First, the EU's substantial economic market acts as a powerful incentive, a phenomenon known as the "Brussels effect," where external actors align with EU standards to gain access to its lucrative market (Bradford, 2020). Hopkins and McNeill (2015) illustrate this phenomenon through the case of New Zealand's wine regulations. To gain access to the EU market—accounting for approximately 70% of the global wine market—New Zealand largely adopted the EU model for its wine regulations (Hopkins & McNeill, 2015). Second, geographic proximity is often associated with a higher likelihood of adopting EU laws and standards (Schimmelfennig & Sedelmeier, 2004). During the EU's Eastern enlargement, countries such as Ukraine and Morocco adopted EU-aligned policies through instruments such as the European Neighbourhood Policy and associated agreements (Schimmelfennig & Sedelmeier, 2004). Russia's adoption of antitrust law further demonstrates the influence of geographic proximity (Bradford et al., 2024).

In the context of diffusion research on data laws and regulations, despite an extensive body of scholarship on the global diffusion of EU data policies, several limitations persist. First, some scholars have extended the concept of the Brussels effect and geographic proximity as the two primary factors explaining why external actors selectively adopt the EU's standards or policies in the context of data regulation diffusion. However, this perspective tends to overemphasise EU-driven factors, placing excessive focus on the EU's influence while overlooking the local context and agency recipient actors, including their domestic priorities and strategic adaptations. For instance, Cervi (2022) underscores the appeal of the EU's internal market as a key factor contributing to the GDPR's global reach. Similarly, Akcali Gur (2020), through a case study of Turkey's data protection legislation, highlights the EU's normative power in shaping regulatory frameworks beyond its

jurisdiction, particularly in neighbouring states. By contrast, Corning (2024) challenges this EU-driven perspective, arguing that the prevailing explanation for GDPR diffusion—the Brussels effects—fails to account for how local contexts, including political, institutional, and socio-economic conditions within affected countries, shape both the adoption and implementation of data protection policies.

Second, although recent scholars have increasingly extended their focus beyond the EU's immediate neighbourhood to examine the global diffusion of EU data regulations, much of the research remains centred on the influence of the General Data Protection Regulation (GDPR) in prompting other international actors to formulate or amend their data legislation, while overlooking the impact of earlier EU data regimes. Asia has become a focal point of scholarly attention, given its strategic importance in the EU's digital agenda and its growing role in global data governance. As a result, a growing body of literature examines how EU data regulations have shaped the development and reform of data laws in Asian countries (Bentotahewa et al., 2022; Corning, 2024; Creemers, 2022). Based on case studies of data privacy law reforms in four ASEAN countries—the Philippines, Singapore, Thailand, and Indonesia—Corning (2024) highlights how internal regulatory demands, driven by the accelerating digitalisation of these societies, intersect with the role of the GDPR as a legal template. Similarly, Bentotahewa et al. (2022) demonstrate the influence of the GDPR on South Asian countries, showing how the EU's regulatory framework has informed legislative developments in the region. Additionally, Creemers (2022), through a systematic analysis of China's data protection framework, argues that China's personal information protection model has been significantly influenced by the GDPR. Although China largely adopted the GDPR's consumer protection components, it has explicitly rejected the EU's foundational principle of privacy as a fundamental right. While existing research widely acknowledges the GDPR's influence on the development of data legislation in Asia, it often overstates its role as a global gold standard and neglects the EU's longer-standing regulatory influence in this field. The EU's external regulatory power did not emerge solely with the GDPR, rather, it evolved gradually through earlier instruments such as the Council of Europe's Convention 108 (Convention 108; Council of Europe, 1981) and the 1995 EU Data Protection Directive (1995 Directive; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, 1995). These earlier frameworks laid critical normative and legal foundations for global data governance, influencing legislative developments across various regions well before the GDPR's adoption.

To address these gaps, this article conducts a case study analysis of the development of data regulations in Japan and Singapore, guided by two research questions:

1. To what extent have the data governance frameworks of Japan and Singapore been influenced by the evolution of EU data regulations?
2. What mechanisms contributed to Japan and Singapore's regulatory convergence with EU data regulations, and under what conditions did this convergence occur?

The first question assesses the EU's diffuse-ability in the digital governance domain within Japan and Singapore. The second question further explores the mechanisms that contributed to regulatory convergence, focusing specifically on key periods of convergence to interpret how and under what conditions EU influence took effect.

This article is structured as follows: Section 2 reviews the literature on diffusion theory, including policy diffusion and diffusion mechanisms within the field of international relations (IR), and outlines the

theoretical framework. Section 3 discusses the methodology and case selection. Section 4 presents detailed case studies of Japan and Singapore. Each case study sheds light on the diffusion mechanisms that played significant roles in enabling these countries to adopt EU-inspired regulatory elements and to establish or amend their data laws. Section 5 summarises the key findings and presents the conclusion.

2. A Theoretical Framework Based on Diffusion Literature

To develop a more nuanced understanding of the EU's diffuse-ability and the means through which it transmits regulations to Asian countries, this study employs a theoretical framework grounded in existing diffusion literature. Specifically, in IR scholarship, policy diffusion research focuses on how specific policies spread across different jurisdictions including countries, states, cities, and organisations (Bradford et al., 2024; Graham et al., 2013; Shipan & Volden, 2008). Scholars regard the term "diffusion" as a process of spreading ideational frameworks, instruments, and institutional settings at national, regional, and international levels (Elkins & Simmons, 2005; Simmons et al., 2008). In this study, diffusion is understood as the process through which data regulations are transmitted from the EU to the two Asian countries.

Moreover, "diffusion items" refer to the ideational frameworks, instruments, and institutional settings that are transmitted in the diffusion process. Scholars categorise these items into three levels of specificity: (a) overarching ideas and norms, (b) policy instruments, and (c) precise institutional settings (Klingler-Vidra & Schleifer, 2014). Since legal provisions constitute binding commitments that operationalise regulatory standards within domestic systems, offering codified evidence of convergence or divergence vis-à-vis EU data governance standards, this study relies on formal legal documents, including official policy documents and cooperation agreements, as primary data sources for diffusion analysis. In this research, these diffusion items—referred to as "EU elements" (detailed in Section 3)—are derived from the EU's data regulatory frameworks, including Convention 108, the 1995 Directive, and the GDPR.

To evaluate diffusion outcomes, scholars have used measures such as varying degrees of convergence (Klingler-Vidra & Schleifer, 2014; Solingen, 2012) or a conceptual framework distinguishing between adoption, adaptation, resistance, and rejection (Björkdahl et al., 2015) to capture differing degrees of recipient acceptance. Accordingly, this study adopts diffusion outcomes as analytical tools to assess both the extent and effectiveness of the EU's diffuse-ability in Asian countries over the past three decades (see Table 1).

Scholars acknowledge multiple mechanisms underpinning the spread of diffusion items to varying degrees (Gilardi & Wasserfallen, 2019; Meseguer & Gilardi, 2009; Risse, 2016). To analyse the diffusion mechanisms

Table 1. Conceptual tools of evaluating EU's diffuse-ability.

Conceptual tool	Type and definition	EU's diffuse-ability
Diffusion outcomes	Adoption: Local practices have complied with the EU's diffusion items	Strong
	Adaptation: Local practices have integrated EU's diffusion items but have localised them to fit the local demands and context	Mid-strong
	Resistance: Few local practices imported EU's diffusion items	Weak
	Rejection: Local practices rejected any EU's diffusion item	No

Source: Adapted from Björkdahl et al. (2015).

driving the transmission of EU data regulations to Asian countries, this study adopts five commonly cited mechanisms: (a) incentive, (b) socialisation, (c) learning, (d) competition, and (e) emulation. Building on Risse's (2016) research, this study advances the conceptualisation of interactive diffusion by categorising the five mechanisms according to the identity of the initiator: (a) sender-driven (direct mechanisms) and (b) adopter-driven (indirect mechanisms). Given this study's focus on how the EU induces the adoption of its regulatory frameworks, direct mechanisms are defined as EU-driven, while indirect mechanisms are shaped by recipient actors. Specifically, the incentive is a direct mechanism that includes both positive instruments (e.g., financial support or technical assistance) and negative pressures (e.g., penalties or sanctions) imposed by the senders to promote the uptake of diffusion items (Chen & Gao, 2024; Risse, 2016). The second direct mechanism is socialisation, commonly understood as the process by which actors internalise such items through sustained interaction with external agents or institutions (Risse, 2016; Strang & Meyer, 1993). Given that this study focuses on the EU's effort to actively induce the adoption of its regulatory frameworks in external jurisdictions, it deliberately adopts a more sender-driven interpretation of socialisation, consistent with Risse's (2016) definition. Accordingly, socialisation is conceptualised in this research as a sender-driven, one-way process.

The remaining three mechanisms—competition, learning, and emulation—are classified as indirect mechanisms. Competition refers to the process by which actors adopt the diffusion items to gain advantages or avoid falling behind rivals in the competitive environment (e.g., economic competition, technological innovation, or security threats; Meseguer & Gilardi, 2009). While learning and emulation share conceptual similarities, they differ in the degree of reflexivity. Learning involves a reflective process in which actors selectively adopt or localise diffusion items perceived as effective or contextually appropriate (Shipan & Volden, 2008). In contrast, emulation is a more superficial process in which actors replicate diffusion items with minimal adaptation, motivated by the perceived legitimacy or success of prior adopters (Simmons & Elkins, 2004). Table 2 outlines the five diffusion mechanisms and the indicators used to identify them in the case studies.

Table 2. Diffusion mechanisms and indicators.

Diffusion mechanisms		Indicators
EU-driven mechanisms	Incentive	Positive: • Foreign direct investment (FDI) • Development aid and technical assistance Negative: • Trade restrictions targeting non-compliant countries • Threats of fines or financial penalties
	Socialisation	• Membership in international organisations and forums • Diplomatic engagements and bilateral dialogues
Recipient-driven mechanisms	Competition	• Regional rivalries and competitive adaptation • Legal convergence to enhance the business environment
	Learning	• Explicit references to foreign models in policy debates • Government-sponsored comparative studies
	Emulation	• Replication of foreign legal texts without domestic adaptation

Note: Mechanisms and indicators are summarised from key studies in diffusion literature (see references cited in the theoretical framework).

3. Methodology

This article employs a case-study approach to analyse the evolution of the EU's diffuse-ability in two Asian countries—Japan and Singapore—over the past three decades (1990s–2020s). It further investigates the diffusion mechanisms underlying this process. This research is based on a combination of open-source primary materials, including official policy documents, cooperation agreements, and declarations, complemented by secondary sources such as policy analysis, white papers, and academic journal articles published between the 1980s and the 2020s.

This section explains how the core analytical units—referred to as "EU elements"—were extracted from EU legal instruments and categorised into six provision types. It then outlines the case selection strategy and comparative logic, using Mill's (1843) method of difference and the most similar systems design (MSSD).

3.1. The Categories of Provision Type and EU Elements

To facilitate a systematic comparison of data protection regimes across jurisdictions, this study categorises legal provisions into six functional types, reflecting widely recognised building blocks of data protection frameworks. These include: (a) scope and definitions; (b) data processing; (c) data subject rights; (d) obligations of data controllers/processors; (e) cross-border data transfers; and (f) supervisory authorities and enforcement. This typology is informed by the regulative profile approach to legal analysis, which focuses on the structural and functional roles of legal provisions within a broader regulatory architecture (Francesconi & Passerini, 2007).

Based on this categorisation, the study identifies a set of "EU elements"—previously introduced as the diffusion items in this research—as the core analytical indicators for assessing regulatory convergence. These elements refer to specific concepts and legal requirements that were first introduced or uniquely developed within the EU's data protection instruments, ranging from Convention 108 and the 1995 Directive to the GDPR. Following Greenleaf's (2012) methodology of identifying "European elements" as benchmarks for convergence assessment, this study draws on a close reading of EU legal texts and existing diffusion literature to extract key elements. These are then organised under the six provision types described above and serve as the primary criteria for evaluating the extent of EU influence in the domestic data regulations of Japan and Singapore. Table 3 provides an overview of these provision types, including their definitions and corresponding EU elements.

3.2. Case Selection: Japan and Singapore

This study adopts a comparative case-study design, specifically employing an MSSD grounded in the logic of Mill's (1843) method of difference. MSSD has been widely used in IR research, particularly in small-n comparative case studies that aim to identify causal mechanisms under conditions of limited variation (Lai, 2024). The method of difference involves comparing cases that are similar in most respects but differ in both outcomes and at least one potential causal factor (Mills et al., 2010, pp. 558–559). It enables researchers to isolate explanatory variables by holding background conditions constant. Furthermore, the method of difference can be applied not only across cases but also within a single case over time, thereby enabling a dynamic analysis of policy evolution under otherwise stable structural conditions.

Table 3. Provision types and EU elements.

Provision types	Definitions	EU elements
Scope and definitions	Defines the jurisdictional scope of the regulation and clarifies key legal terms	• Protection of fundamental rights and freedoms, particularly the right to personal data protection • Geographic applicability of data regulations • Concept of sensitive data • Concept of anonymised data • Concept of pseudonymised data
Data processing	Covers principles and rules governing the collection, use, storage, and sharing of personal data	• General requirement of "fair and lawful processing" • Data collection must be limited to what is necessary for the stated purpose • Obligation to destroy or anonymise personal data after a retention period • Restrictions on automated decision-making
Data subject rights	Defines the ability of individuals to exercise control over their personal data	• Right to opt-out of direct marketing uses of personal data • Right to understand the logic behind automated data processing • Requirements to inform the DPA within 72 hours of a data breach and notify individuals if their rights are at risk
Obligations of controllers/processors	Specifies the responsibilities of data controllers and processors, including their roles in managing and executing data processing	• Additional safeguards required for processing sensitive data • Obligation to notify, and in some cases conduct prior checking of, certain types of data processing
Cross-border data transfers	Covers the rules governing the transfer of personal data to third countries or international organisations	• Restrictions on data transfers to countries lacking adequate privacy protection standards
Supervisory authorities and enforcement	Outlines the structure and powers of regulatory bodies and the mechanisms for enforcement	• Requirement of an independent Data Protection Authority • Access to judicial remedies for the enforcement of data privacy rights

Accordingly, Japan and Singapore are selected as two high-exposure, economically advanced Asian states with mature data governance systems and strong relations with the EU. Despite these similarities, they display divergent levels of regulatory convergence with the EU data standards. To trace the mechanisms underlying these divergent trajectories, the study further employs a process tracing approach. Process tracing is a qualitative method used to identify and test causal mechanisms within individual cases (Collier, 2011). It helps establish a temporal link between cause and outcome through detailed within-case analysis (Beach & Pedersen, 2016). In this study, process tracing is applied separately to Japan and Singapore to examine how their domestic data protection regimes evolved from the 1990s to the 2020s, and how EU elements were selectively adopted or resisted over time.

3.3. Case Contexts of Japan and Singapore

In the 1990s, the EU recognised the growing strategic importance of Asia and sought to strengthen ties with Asian countries and regional organisations. The 1994 policy paper Towards a New Asia Strategy and its subsequent updates emphasised expanding bilateral and multilateral cooperation in areas such as trade, technology, and rule-based global governance (European Commission, 2001). As a result, the EU established multiple dialogue mechanisms and signed cooperation agreements with key Asian actors, including Japan, South Korea, and ASEAN. This study selects Japan and Singapore as two geographically diverse, economically advanced Asian states with extensive relations with the EU, to assess the diffusion of EU data protection regulations. The following section provides a brief overview of their data governance trajectories, EU relations, and the temporal benchmarks used in the analysis.

Japan, the world's fourth-largest economy by nominal GDP, maintains strong cooperation with the EU across various domains. The EU is Japan's third-largest trading partner, while Japan ranks as the EU's second-largest in Asia (European Commission, 2024a). Japan was the first country in Asia to enact a privacy law in the late 1990s, initially focused on protecting personal data held by public agencies (Suda, 2020), followed by the adoption of the Act on the Protection of Personal Information (APPI) in the early 2000s to cover the private sector (Adams et al., 2009). As a key EU strategic partner, Japan offers a valuable case for examining the EU's diffuse-ability in data governance. This study divides Japan's regulatory evolution into three periods—2005, 2016, and 2022—each corresponding to major EU developments. It systematically assesses the extent of convergence, identifying specific provisions that incorporate EU elements, and explores the mechanisms that enabled such diffusion.

Singapore, a leading city-state in Southeast Asia, ranks second globally in GDP per capita as of 2023 (WorldData.info, 2024). It is the EU's top trading partner in ASEAN and a major investment destination (European Commission, 2024b). While its engagement with data governance dates back nearly three decades, early efforts focused on voluntary codes such as the Model Data Protection Code for the Private Sector (2002 Model Code; Wong, 2017). Comprehensive legislation was not introduced until 2012, with the Personal Data Protection Act (PDPA) covering both public and private sectors (Singapore Attorney-General's Chambers, 2012). As the EU's most important ASEAN partner, Singapore presents a contrasting case for examining EU regulatory diffusion. The study identifies 2002, 2013, and 2022 as key reform milestones and evaluates the extent to which Singapore's regulations incorporated EU elements. It also investigates the mechanisms driving selective adoption and regulatory localisation.

By selecting Japan and Singapore as case studies, this research captures both convergence and variation in EU influence across the Asian region. It finds that Japan pursued deeper alignment, culminating in GDPR adequacy recognition, while Singapore selectively adapted EU elements within a more flexible regulatory framework. Through cross-case comparison and within-case process tracing, the study identifies both outcome variation and the underlying diffusion mechanisms.

4. Case Study: Data Regulations in Japan and Singapore

This section evaluates the EU's diffuse-ability by examining whether, when, and how Japan and Singapore incorporated EU elements into their domestic data protection frameworks. As outlined in Table 1,

diffuse-ability is assessed based on observable diffusion outcomes—adoption, adaptation, resistance, or rejection—which reflect varying degrees of regulatory convergence.

Moreover, the analysis identifies and explains the underlying diffusion mechanisms that contributed to convergence where it occurred. Rather than assigning mechanisms to every stage of legal development, the study focuses on periods of clear convergence, where EU elements were substantially adopted or adapted. This approach allows for a more targeted and meaningful interpretation of how and under what conditions EU elements gain traction in domestic contexts. While a single mechanism may dominate in a given period, this study supports the insight in diffusion theory that multiple mechanisms often operate simultaneously and interact to shape diffusion outcomes.

4.1. Data Regulation in Japan: From the 1990s to the 2020s

This article argues that the EU's diffuse-ability in Japan has progressively increased over time, reaching its peak between 2006 and 2016, when significant regulatory convergence occurred. During this period, socialisation served as the primary diffusion mechanism driving this regulatory alignment.

To evaluate this trajectory, the analysis draws on the diffusion outcomes typology introduced earlier and uses the matrix in Table 4 to compare the adoption of EU elements across three key time points—2005, 2016, and 2022. This table tracks newly incorporated provisions reflecting EU elements and illustrates the cumulative trajectory of regulatory convergence.

Table 4. Convergence of data regulations of Japan's and EU's.

Provision type/year		2005		2016		2022	
		EU	Japan	EU	Japan	EU	Japan
Scope and definitions	Objectives	✓	✓	✓	1	✓	✓
Scope and definitions	Geographic applicability	✓	✓	✓	1	✓	✓
Scope and definitions	Definitions	✓	✓	✓	1	✓	✓
Data processing	Lawfulness, fairness, and transparency	✓		✓		✓	1
Data processing	Purpose limitation	✓	1	✓	✓	✓	✓
Data processing	Data minimisation	✓		✓	1	✓	✓
Data processing	Accuracy	✓	✓	✓	✓	✓	✓
Data processing	Storage limitation	✓		✓	1	✓	✓
Data processing	Integrity and confidentiality	✓	✓	✓	1	✓	✓
Data processing	Accountability	✓		✓	✓	✓	✓
Data subject rights	Consent before collecting	✓	1	✓	✓	✓	✓
Data subject rights	Access	✓	✓	✓	1	✓	✓
Data subject rights	Correction	✓	✓	✓	1	✓	✓
Data subject rights	Erasure			✓		✓	✓
Data subject rights	Restriction			✓		✓	

Table 4. (Cont.) Convergence of data regulations of Japan's and EU's.

Provision type/year		2005		2016		2022	
		EU	Japan	EU	Japan	EU	Japan
Data subject rights	Objection	✓		✓		✓	
Data subject rights	Portability			✓		✓	1
Obligations of data controllers/processors	Security measures	✓	1	✓	✓	✓	✓
Obligations of data controllers/processors	Breach notification	✓		✓	1	✓	✓
Obligations of data controllers/processors	Maintain records			✓	1	✓	✓
Obligations of data controllers/processors	Data Protection Impact Assessments (DPIAs)			✓		✓	
Obligations of data controllers/processors	Data Protection Officers (DPOs)	✓		✓		✓	
Cross-border data transfers	Consent	✓		✓	✓	✓	✓
Cross-border data transfers	Adequacy level of protection	✓		✓	1	✓	✓
Cross-border data transfers	Standard Contractual Clauses (SCCs)	✓		✓		✓	
Cross-border data transfers	Binding Corporate Rules (BCRs)	✓		✓		✓	
Supervisory authorities and enforcement	Independent supervisory authorities	✓		✓	1	✓	✓
Supervisory authorities and enforcement	Sanctions	✓	✓	✓	✓	✓	✓
Total score			3		12		2

Notes: A checkmark (✓) indicates that the provision was already present in the data regulation at each time point; a blank cell signifies the absence of the provision in the respective regulation; in the Japan provision columns, a score of 1 denotes the first instance where a specific EU element was incorporated, which signals a point of regulatory convergence; the cumulative total score reflects the aggregate number of newly adopted EU elements at each time point.

In the period prior to 2005, Japan integrated only three EU elements, each localised to fit domestic priorities—an outcome that corresponds to resistance, suggesting weak diffuse-ability. However, between 2005 and 2016, Japan introduced a significant number of new EU elements into its data regulations. Although adapted to local contexts, the scale and depth of convergence indicate adaptation and reflect mid-strong diffuse-ability. From 2016 to 2022, only two additional EU-aligned provisions were adopted, yet this should not be interpreted as declining EU influence. The matrix reflects only newly incorporated EU elements, allowing the analysis to highlight key regulatory shifts rather than cumulative harmonisation. Moreover, since legal reforms typically emerge from long-term regulatory and policy engagement, Japan's 2016 data protection reforms should not be seen as a direct response to the GDPR. Rather, they reflect a broader and more gradual alignment with the EU's data governance model—one that had already been shaped by earlier instruments such as Convention 108 and the 1995 Directive, which had exerted sustained influence on Japan's regulatory development over the preceding decades.

From the late-1990s to 2005, Japan's data regulations selectively adopted the basic concepts and principles of the EU's data regulations. More specifically, the 2003 APPI introduced three EU elements in its provisions, including "purpose limitation," "consent of the person before collecting and processing personal information,"

and "security controls" (Japan Ministry of Justice, 2003). These provisions were integrated into Japan's data regulations to address early domestic demands for fundamental data protection. During this period, although Japan's data laws were primarily recognised as being influenced by the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 OECD Guidelines; Suda, 2020), Birnhack (2008) pointed out that Japan regarded the EU directive as a policy target in its 1998 governmental report and modelled the EU directive's basic data protection principles including purpose limitation, security controls, basic data subject rights, and consent before disclosing to third parties. Additionally, Horibe (2013) pointed out that Japan's data laws considered European legislation as early as the 1980s, with particular reference to Convention 108.

Subsequently, Japan's data regulations have demonstrated a high degree of convergence, gradually aligning with the EU's data regulations since 2005. First, in terms of scope and definitions, the amended 2015 APPI, issued by the Personal Information Protection Commission (PPC; 2016), broadened its scope to introduce the concept of "extraterritorial jurisdiction," meaning that certain provisions applied to business operators outside Japan, rather than being limited to domestic application, as stated in Article 75 of the 2015 APPI. The 2020 APPI further expanded its extraterritorial scope to include any business operators processing data related to Japanese residents, regardless of their geographic location (PPC, 2020, p. 45). Japan also incorporated EU elements into the definitions of key terms in its legislation. For instance, the 2015 APPI added the term "sensitive personal information," encompassing key elements such as an individual's "race, creed, social status, medical history, etc." (PPC, 2016, p. 3). This aligns with the concept of "sensitive data" as emphasised in both the EU Directive and Convention 108.

Regarding the provision type of data processing, Japan's data regulations have been revised since 2005 to align more closely with the EU's data processing principles. In addition to the previously adopted principle of "purpose limitation," the amended data regulations introduced the principles of "data minimisation," "storage limitation" and "integrity and confidentiality" in the 2015 APPI (PPC, 2016, pp. 6–9). For instance, under Article 19 of the APPI (Maintenance of the Accuracy of Data), business operators are required to collect personal data "within the scope necessary for achieving the purpose of use" and to "delete such personal data without delay when its use is no longer required" (PPC, 2016, p. 9), thereby incorporating identified EU elements. The 2015 APPI also introduced a new security measure, "de-identified information" (a concept similarly referenced in the 2012 GDPR proposal), to help prevent the leakage, loss, or damage of processed personal data and to enhance data confidentiality (European Commission, 2012; PPC, 2016). Furthermore, the 2020 APPI introduced a new provision to specifically emphasise the principle of "lawfulness and fairness" (PPC, 2020, p. 9).

Additionally, although Japan's data regulations prioritise economic objectives over recognising the right to data privacy as a fundamental human right, as is emphasised in the EU's approach (Wang, 2020), the amended APPI still revised its provision related to the data subject rights to better align with the EU regulations. For instance, the 2015 APPI revised its provisions related to rights to access, correction, and deletions, and required business operators to provide "the name of the business operator handling personal information, the purpose of use of all retained personal data, etc." upon a data subject's request and must "respond without delay" (PPC, 2016, p. 12). In alignment with the GDPR, the 2020 APPI introduced "data portability rights," as outlined in Article 28 (PPC, 2020). In terms of obligations of data controllers/processors, the 2015 and 2020 APPI respectively introduced and revised the requirements for "timely

breach notifications" and mandated that business operators maintain records of data processing activities both domestically and internationally (PPC, 2016, pp. 8–11; 2020, pp. 10–12).

Finally, Japan's amended data regulations introduced specific provisions related to cross-border data transfers, as well as establishing an independent supervisory authority to ensure an adequate level of personal data protection (PPC, 2016, 2020). These changes were also intended to meet the EU's requirements and to address the challenges posed by the globalisation of data flows (Council of Europe, 1981; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, 1995; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016). Specifically, the Act required business operators to obtain the prior consent of individuals before transferring personal data to third parties outside Japan, while stipulating that the receiving country maintain a "level of protection for the rights and interests of individuals" equivalent to that in Japan (PPC, 2016, p. 11, 2020). Meanwhile, the amended regulations also established the PPC to align with the broader trend of strengthening independent supervisory authorities and to fulfil the EU's adequacy criteria under its data protection framework (Horibe, 2013; Ishiara, 2019).

In sum, Japan's convergence with EU data regulations has been gradual but increasingly substantial, particularly between 2005 and 2016. Regulatory alignment is most evident in foundational areas such as the categories of scope and definitions and data processing, where multiple EU elements have been incorporated and localised. These patterns suggest that the EU's diffuse-ability in Japan has strengthened over time. To understand how this process unfolded, the following section turns to the diffusion mechanisms that underpin Japan's regulatory transformation.

As mentioned at the beginning of Section 4, multiple diffusion mechanisms often operate simultaneously and interactively, making it difficult to isolate them with precision. To guide the identification of the primary mechanisms during key stages of convergence, Table 5 presents the key indicators used to identify the mechanisms of learning and socialisation, along with their corresponding behavioural patterns. While learning played a notable role during the early phase of Japan's data governance in the 1990s and 2000s, much of the evidence observed—particularly during the period of regulatory convergence—corresponds more closely to indicators associated with socialisation. Accordingly, the remainder of this section focuses on explaining how socialisation served as the primary mechanism underpinning the diffusion process.

Table 5. The mechanisms behind the diffusion process in Japan.

Diffusion mechanisms	Indicators	Examples of appropriate behaviour
Learning	Explicit references to foreign models in policy debates	• During the drafting of the 2003 APPI, Japanese officials explicitly referenced the EU's Convention 108 and the 1995 Directive
Socialisation	Membership in international organisations and forums	• Japan's accession to the OECD in 1964 enabled its participation in drafting the 1980 Guidelines and laid the groundwork for later cooperation with EU member states
	Diplomatic engagements and bilateral dialogue	• The EU and Japan signed the 1991 Joint Declaration on Relations between the European Community and its Member States and Japan • Negotiations for the EU–Japan Economic Partnership Agreement (EPA)

First, this study argues that Japan's accession to the OECD in 1964 played a foundational role in shaping its long-term engagement with European regulatory models. Through active participation in the drafting of the 1980 OECD Guidelines, Japan became familiar with data protection principles that closely aligned with EU standards. This early exposure contributed not only to the subsequent incorporation of selected EU elements into Japan's data laws but also laid the groundwork for establishing scientific and technological cooperation and trade relations with founding members of the OECD—primarily EU member states. In a 2013 speech marking the establishment of the PPC, Masao Horibe, then Chair of the PPC and a key figure in drafting the APPI, explicitly acknowledged that Japan's data regulations drew upon the EU's data regulations. Notably, Horibe had also served as a member of the OECD expert group responsible for drafting the 1980 Guidelines, which were themselves heavily influenced by European privacy principles (Kirby, 2017). His dual involvement reflects both the learning mechanism, whereby EU elements were selectively incorporated into Japan's legal framework, and the socialisation mechanism, whereby sustained participation in international forums facilitated normative engagement. These expert-level, rule-setting interactions promoted the diffusion of norms and standards not through coercion or conditionality, but through shared participation in the transnational shaping of data governance principles. Moreover, Japan signed bilateral cooperation agreements with EU member states, such as Germany and France, emphasising collaboration in science and technology (Ministry of Foreign Affairs of Japan, 1999, 2023). Japan also engaged in both inward and outward FDI with the UK in 1983 and expanded the activities to include Germany, France, and Italy since 1987 (Japan External Trade Organization, 2024). These longstanding ties with European partners not only laid the foundation for later Japan-EU cooperation but also created a context of increasing economic and normative proximity that eventually facilitated Japan's regulatory convergence with the EU in the digital era.

Second, this study observes that since the 1990s, the EU has primarily leveraged bilateral cooperation to encourage Japan to adopt its diffusion items, reinforcing regulatory alignment in data governance. Building on Japan's collaborations with EU member states, the EU further established a partnership with Japan across various sectors, including trade, policymaking, and technology. For instance, the 1991 Joint Declaration on Relations between the European Community and its Member States and Japan (Ministry of Foreign Affairs of Japan, 1991) was signed by Japan and the EU, serving as a formal framework for cooperation and dialogue between the two parties. Furthermore, the two parties launched the Action Plan for EU–Japan Cooperation, in which the EU further promoted the principles of "respect for human rights," "promotion of democracy," and "good governance" (Ministry of Foreign Affairs of Japan, 2001).

Moreover, Japan and the EU have expanded their cooperation due to the rapid development of ICTs. Under the EU–Japan Science and Technology Agreement (European Commission, 2009), both parties confirmed new cooperation in Future Internet/New Generation Networks research—a key element of the Digital Agenda for Europe—during the 2011 EU–Japan Dialogue (European Commission, 2011). Additionally, since 2013, negotiations for the EU–Japan EPA have been launched, covering a range of issues including cross-border data flows and regulation cooperation (European Parliament, 2019). During the 22nd EU–Japan Summit (European External Action Service, 2014) and the first EU–Japan Cyber Dialogue (Ministry of Foreign Affairs of Japan, 2014), the EU and Japan discussed governmental structures and principles related to cyber regulations to address the increasing challenges of cybersecurity. As Japan–EU cooperation deepened, the European Commission and Japan engaged in negotiations on adequate data protection levels based on the EPA (European Commission, 2018). These collaborations created channels for

sustained normative interaction, progressively familiarising Japanese regulators with European regulatory standards and expectations and facilitating the adaptation of EU elements.

In sum, although diffusion is a highly complex process involving the interaction of multiple diffusion mechanisms, it is undeniable that socialisation has played a predominant role in Japan's gradual adoption of EU elements in the evolution of its domestic data regulations.

4.2. Data Regulations in Singapore: From the 1990s to the 2020s

This study argues that the EU's diffuse-ability in Singapore has remained weak over time, with only limited incorporation of EU elements across three decades of regulatory development. The overall pattern suggests that convergence has been marginal, with competition emerging as the primary diffusion mechanism.

To examine the EU's diffuse-ability in Singapore, this study applies the diffusion outcomes typology to trace the evolution of regulatory convergence. Table 6 compares key developments in EU and Singaporean data regulations from the 1990s to the 2020s. The number of newly adopted EU elements remained low and relatively stable across the three periods examined (2003, 2012, and 2022), with no clear upward trajectory. These findings suggest that the EU's diffuse-ability in Singapore has remained consistently weak, with most diffusion outcomes falling into the category of resistance.

Table 6. Convergence of data regulations of Singapore's and EU's.

Provision type/year		2002		2013		2022	
		EU	Singapore	EU	Singapore	EU	Singapore
Scope and definitions	Objectives	✓	✓	✓	✓	✓	✓
Scope and definitions	Geographic applicability	✓	1	✓	✓	✓	✓
Scope and definitions	Definitions	✓		✓	✓	✓	✓
Data processing	Lawfulness, fairness, and transparency	✓	✓	✓	✓	✓	✓
Data processing	Purpose limitation	✓	1	✓	✓	✓	✓
Data processing	Data minimisation	✓	1	✓	✓	✓	✓
Data processing	Accuracy	✓	✓	✓	✓	✓	✓
Data processing	Storage limitation	✓		✓	✓	✓	✓
Data processing	Integrity and confidentiality	✓		✓	✓	✓	✓
Data processing	Accountability	✓	✓	✓	✓	✓	✓
Data subject rights	Consent before collecting	✓	✓	✓	✓	✓	✓
Data subject rights	Access	✓	✓	✓	✓	✓	✓
Data subject rights	Correction	✓	✓	✓	✓	✓	✓
Data subject rights	Erasure					✓	✓
Data subject rights	Restriction					✓	
Data subject rights	Objection	✓		✓	1	✓	

Table 6. (Cont.) Convergence of data regulations of Singapore's and EU's.

Provision type/year		2002		2013		2022	
		EU	Singapore	EU	Singapore	EU	Singapore
Data subject rights	Portability					✓	1
Obligations of data controllers/processors	Security measures	✓	✓	✓	✓	✓	✓
Obligations of data controllers/processors	Breach notification	✓		✓		✓	1
Obligations of data controllers/processors	Maintain records				✓	✓	✓
Obligations of data controllers/processors	DPIAs					✓	
Obligations of data controllers/processors	DPOs	✓		✓	1	✓	✓
Cross-border data transfers	Consent	✓	✓	✓	✓	✓	✓
Cross-border data transfers	Adequacy level of protection	✓	1	✓	✓	✓	✓
Cross-border data transfers	SCCs	✓		✓		✓	
Cross-border data transfers	BCRs	✓		✓		✓	
Supervisory authorities and enforcement	Independent supervisory authorities	✓		✓	1	✓	✓
Supervisory authorities and enforcement	Sanctions	✓		✓	✓	✓	✓
Total score			4		3		2

Notes: A checkmark (✓) indicates that the provision was already present in the data regulation at each time point; a blank cell signifies the absence of the provision in the respective regulation; in the Singapore provision columns, a score of 1 denotes the first instance where a specific EU element was incorporated, signalling a point of regulatory convergence; the cumulative total score reflects the aggregate number of newly adopted EU elements at each time point.

During the first period, Singapore's data code incorporated four EU elements and adapted them into domestic data regulations. First, in terms of scope and definitions, Singapore's data regulations began to consider the "territorial scope," which aligned with the EU Directive, as the 2002 Model Code specified that it would apply to "any personal data processed in Singapore, whether the data controller is within Singapore" (National Internet Advisory Committee, 2002, pp. 30–31). Second, in relation to data processing provisions, the 2002 Model Code introduced two principles: "identifying purposes" (Clause 4.2) and "limiting collection" (Clause 4.4), which correspond to the EU elements of "purpose limitation" and "data minimisation" (National Internet Advisory Committee, 2002, pp. 61-67). Specifically, the Code stated that organisations should inform individuals of the purpose "at or before the time of collection" and that the data should not be used for a new purpose (National Internet Advisory Committee, 2002, p. 61). The principle of "limiting collection" required organisations to ensure that the data collected "shall be limited to that which is necessary for the identified purposes" (National Internet Advisory Committee, 2002, p. 67). Additionally, the 2002 Model Code introduced provisions for cross-border transfers, aligning with the EU's regulations. The principle of

"transborder data flows" required organisations to ensure "an adequate level of protection" when transferring data to "any recipient outside Singapore" (National Internet Advisory Committee, 2002, p. 31). Although the 2002 Model Code was a voluntary code designed to align with Article 25 under the framework of the EU Directive, its principles were carried forward into subsequent data regulations. Moreover, in the evolution of Singapore's data regulations, the 2002 Model Code has been regarded as a transitional step toward enacting mandatory legislation to keep pace with global digitalisation (Wong YongQuan, 2017).

During the second period, Singapore enacted its formal data protection law, the 2012 PDPA, which incorporated three provisions containing EU elements. More specifically, Singapore introduced the provision of "withdrawal of consent," meaning that individuals can "withdraw any consent given" at any time, while organisations are required to inform them of the "likely consequences" (Singapore Attorney-General's Chambers, 2012, p. 20). This provision is comparable to the "right to object" under the EU data protection framework. Regarding obligations of data controllers/processors, the 2012 PDPA aligned with the EU Directive by requiring organisations to designate one or more "reasonable persons" to ensure that data is collected and processed in compliance with relevant data protection regulations (see Article 11, Singapore Attorney-General's Chambers, 2012). Finally, Singapore established the Personal Data Protection Commission (PDPC) in 2013 as an independent supervisory authority responsible for administering the PDPA and providing advisory guidelines to individuals and organisations (Singapore Attorney-General's Chambers, 2012). As mentioned earlier, the "requirement of an independent data protection authority" is a key regulatory component emphasised by the EU (Greenleaf, 2012, p. 73). Thus, this development reflects an alignment with EU data regulations and the evolving global landscape of data governance.

Finally, during the third period, Singapore incorporated only two EU elements, adapting them to fit its domestic regulatory framework. This limited adoption further reflects the EU's persistently weak diffuse-ability in Singapore. More specifically, the 2020 PDPA introduced the "notification of data breach" requirement, mirroring the GDPR's provision that organisations must notify the PDPC "no later than three calendar days" and inform affected individuals as soon as possible (Personal Data Protection Commission, 2020, p. 35). Additionally, the amended PDPA incorporated the concept of "anonymised information," first introduced in the 2012 GDPR proposal and later adopted in the final regulation. In alignment with EU data regulations, the PDPA provides that "re-identification is not authorised by the organisation or public agency" (Personal Data Protection Commission, 2020, p. 59).

Overall, by tracing the evolution of Singapore's data regulations, this research finds that the EU's diffuse-ability in Singapore has remained persistently weak. Moreover, the EU elements adopted in Singapore's data regulations are primarily concentrated in the provision types of "data processing" and "cross-border data transfer," particularly provisions governing cross-border data flows.

In terms of diffusion mechanisms, this study finds that while multiple mechanisms operated concurrently, their effects were uneven. Some signs of socialisation—such as bilateral cooperation with the EU and participation in ASEAN-led regional initiatives—became more visible after the 2010s, but did not lead to greater regulatory convergence. In fact, most EU elements were adopted between the 1990s and the 2010s, indicating that socialisation had limited influence on the timing of adoption. Instead, the evidence points to competition as the dominant mechanism. Singapore's strategic aim to position itself as a global trade and data hub, along with regulatory competition with regional actors, better explains its selective adoption of EU elements. This strategic logic is elaborated in the following analysis and summarised in Table 7.

Table 7. The mechanism behind the diffusion process in Singapore.

Diffusion mechanisms	Indicators	Examples of appropriate behaviour
Competition	Legal convergence to enhance the business environment	• Singapore aimed to be the international e-commerce hub • Singapore referenced multiple national data protection regimes in its working papers
	Regional rivalries and competitive adaptation	• Hong Kong enacted the Personal Data (Privacy) Ordinance (PDPO) in 1996

First, this study observes that Singapore's establishment and modification of its data governance framework have been primarily driven by its goal to facilitate cross-border business operations and attract foreign investment. In the early 1990s, Singapore recognised the importance of data protection regulations, and the Singapore Academy of Law issued a working paper stating that the primary objective of the legislation was to strike a balance between the "interests of data subjects, data users and the wider community" (Wong, 2017, p. 288). Although this approach was later reflected in Singapore's data protection framework, the government initially opted to develop voluntary codes for the private sector—following a review of the international data protection landscape—rather than enacting formal legislation for both the public and private sectors (National Internet Advisory Committee, 2002; Wong, 2017). In 2002, the National Internet Advisory Committee Legal Subcommittee noted that the 1999 E-Commerce Code had failed to consider EU data regulations, particularly Article 25 of the EU Directive concerning transborder data flows (National Internet Advisory Committee, 2002). This neglect was seen as potentially undermining Singapore's competitive position in the rapidly evolving global e-commerce landscape.

Second, this study argues that the integration of EU elements into Singapore's data provisions is a result of regulatory adjustments in response to regional competition, enabling Singapore to maintain its economic and strategic advantages in an increasingly competitive digital economy. Singapore, one of Asia's major developed economies since the 1960s, has built its growth largely on its strategic geographic location and "entrepôt trade" (Hundt & Uttam, 2017). For instance, driven by proactive government policy initiatives and global technological developments, the ICT manufacturing sector has become a major economic pillar since the late 1980s. However, Singapore's ICT manufacturing remained heavily export-oriented, rendering it highly sensitive to fluctuations in the global ICT market (Vu, 2013). As one of the Asian Four Tigers alongside Singapore, Hong Kong shared a similar development model, leveraging its geographic advantages to foster international trade and economic growth (Paldam, 2003). To maintain its status as an "international trading centre," Hong Kong enacted the PDPO in 1996, drawing on the 1980 OECD Guidelines to ensure an "adequate level of data protection" (Office of the Privacy Commissioner for Personal Data of Hong Kong, 2024). Tang (2003) highlighted that the success of e-commerce depends heavily on "securing the confidence of consumers over the flow of personal data across territorial boundaries" and emphasised that data protection legislation is a "pre-requisite" for ensuring "an adequate level of data privacy protection" and gaining consumers' confidence.

However, Singapore lacked a comparable data protection framework necessary to ensure its position as a "trusted node" and sustain its status as an "international e-commerce hub" (National Internet Advisory Committee, 2002; Parliament of Singapore, 2012). This absence of an adequate data protection regime posed a particular challenge, given that the EU—Singapore's third-largest export market after Malaysia and

the US—could "place Singapore businesses at disadvantage in the global economy" (National Internet Advisory Committee, 2002, p. 13). Therefore, the National Internet Advisory Committee Legal Subcommittee incorporated EU data regulations into the development of Singapore's data protection framework, publishing the 2002 Model Code and the subsequent 2012 PDPA to address domestic economic demands. Although the PDPA formally recognises the "right of individuals to protect their personal data" (Singapore Attorney-General's Chambers, 2012, p. 12), it primarily emphasises two key objectives: "maintaining individuals' trust in organisations that manage data" at the domestic level and "enhancing Singapore's competitiveness and strengthening its position as a trusted business hub" at the international level (Parliament of Singapore, 2012).

Over the past two decades, the EU and Singapore have engaged in multilevel cooperation across political, economic, and digital domains, signing multiple agreements, including the EU-Singapore Free Trade Agreement and the EU–Singapore Digital Trade Agreements (European Commission, 2024b). Additionally, the EU and ASEAN have established longstanding cooperation and dialogue mechanisms across political, security, and economic areas. In particular, during the EU–ASEAN Commemorative Summit, the EU and its member states—acting under the Team Europe initiative—announced the mobilisation of €10 billion as part of the Global Gateway strategy to accelerate digital infrastructure investment in ASEAN countries (European Commission, 2022). These investments are not purely economic, rather, they involve sustained engagement with technical standards, data security framework, and regulatory practices, thereby providing channels for the gradual socialisation of the European data regulatory approach within ASEAN countries, including Singapore. However, there is limited evidence to support that such dynamics have driven the incorporation of additional EU elements into Singapore's data legislation. In other words, Singapore's data regulations do not show a pattern of increasing adoption of EU elements, despite intensified negotiations and cooperation.

In sum, since most EU elements were incorporated during the early stages of Singapore's data policy development, competition emerged as the dominant diffusion mechanism in this process.

5. Conclusion

This research examines the establishment and evolution of data protection regimes in Japan and Singapore over the past three decades, with a focus on how, when, and to what extent their domestic regulations have converged with the EU's data governance framework. By applying a provision-level analytical approach and identifying key EU elements, the analysis evaluated convergence as a diffusion outcome and accounted for variation through the lens of diffusion mechanisms. The findings reveal two distinct patterns: Japan gradually incorporated a large number of EU elements and demonstrated progressive structural alignment with the EU's data governance model, while Singapore adopted only selected EU elements, reflecting minimal convergence.

Theoretically, this research contributes to diffusion research by complementing existing literature that overemphasises EU-driven factors, such as market size, legal externalities, or normative superiority. This study highlights the role of recipient actors, emphasising how domestic context, strategic orientation, and institutional priorities shape the selective adoption—or rejection—of external regulatory models. It particularly draws attention to the normative tensions between the EU's rights-based data governance model and the market-oriented priorities of some recipient countries. While both Japan and Singapore engaged in adaptation rather than direct adoption, their regulatory trajectories diverged significantly. Japan's

reforms have progressively aligned with EU standards, incorporating stronger rights protections and supervisory structures. In contrast, Singapore initially relied on voluntary, non-legislative codes, such as the 2002 Model Code, to regulate data protection. As global regulatory standards evolved, it introduced the PDPA in 2012 to formalise its framework. However, the PDPA retained a business-oriented, flexible approach that prioritised trade facilitation and cross-border data flows. Rather than fully aligning with the EU's rights-based model, Singapore has continued to selectively adapt global standards in ways that support its competitive positioning as an international data hub. This contrast illustrates that regulatory convergence is not merely a function of external pressure, but a negotiated outcome shaped by the domestic logic of strategic regulatory positioning.

Empirically, this comparison reveals that the EU's regulatory power in global data governance is both conditional and uneven. Its influence depends not only on market size or legal sophistication but also on the institutional receptivity and strategic interests of recipient states. In Japan, longstanding institutional ties and economic interdependence created favourable conditions for socialisation and deeper regulatory convergence. In Singapore, by contrast, the need to remain agile and competitive, in a multipolar regulatory environment led to selective and instrumental alignment. These findings suggest that the diffusion of European standards should be understood not as a linear or automatic process, but as one shaped by reciprocal engagement, institutional filtering, and regulatory competition.

The findings also offer broader implications for future research on global diffusion. The mechanisms identified in this study are not exclusive to Japan and Singapore but are likely to influence regulatory outcomes across a wide range of emerging economies. As countries increasingly navigate between competing regulatory models, understanding how external norms and standards are domestically interpreted, adopted, or resisted is critical for capturing variation in convergence outcomes. Future studies could build on this framework by applying it to a broader set of cases and by examining how domestic political coalitions, legal traditions, and global alignments mediate the influence of external normative pressures in shaping data governance trajectories.

Acknowledgments

The author would like to thank the academic editors of this thematic issue, Dr Xuechen Chen and Dr Xinchuchu Gao, for their efforts in organising the issue and for their valuable feedback during the drafting process. Sincere thanks also go to Professor Benjamin Farrand for his insightful comments and to the three anonymous reviewers for their constructive and thoughtful suggestions.

Funding

The author would like to thank Northeastern University London for funding the open access publication of this article.

Conflict of Interests

The author declares no conflict of interests.

References

Adams, A. A., Murata, K., & Orito, Y. (2009). The Japanese sense of information privacy. *AI & Society*, *24*(4), 327–341. https://doi.org/10.1007/s00146-009-0228-z

Akcali Gur, B. (2020). The normative power of the EU: A case study of data protection laws of Turkey. *International Data Privacy Law*, *10*(4), 314–329. https://doi.org/10.1093/idpl/ipaa013

Beach, D., & Pedersen, R. B. (2016). *Causal case study methods: Foundations and guidelines for comparing, matching, and tracing*. University of Michigan Press. https://doi.org/10.3998/mpub.6576809

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The normative power of the GDPR: A case study of data protection laws of South Asian countries. *SN Computer Science*, *3*, Article 183. https://doi.org/10.1007/s42979-022-01079-z

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *The Computer Law and Security Report*, *24*(6), 508–520. https://doi.org/10.1016/j.clsr.2008.09.001

Björkdahl, A., Chaban, N., Leslie, J., & Masselot, A. (2015). Introduction: To take or not to take EU norms? Adoption, adaptation, resistance, and rejection. In A. Björkdahl, N. Chaban, J. Leslie, & A. Masselot (Eds.), *Importing EU norms* (Vol. 8, pp. 1–9). Springer. https://doi.org/10.1007/978-3-319-13740-7_1

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bradford, A., Chilton, A., & Linos, K. (2024). Dynamic diffusion. *Journal of International Economic Law*, *27*(3), 538–557. https://doi.org/10.1093/jiel/jgae034

Brunn, S. D. (2000). Towards an understanding of the geopolitics of cyberspace: Learning, re-learning and un-learning. *Geopolitics*, *5*(3), 144–149. https://doi.org/10.1080/14650040008407697

Cervi, G. V. (2022). Why and how does the EU rule global digital policy: An empirical analysis of EU regulatory influence in data protection laws. *Digital Society*, *1*(2), Article 18. https://doi.org/10.1007/s44206-022-00005-3

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440. https://doi.org/10.1093/ia/iiae237

Christou, G. (2010). European Union security logics to the East: The European neighbourhood policy and the Eastern partnership. *European Security*, *19*(3), 413–430. https://doi.org/10.1080/09662839.2010.526110

Collier, D. (2011). Understanding process tracing. *PS, Political Science & Politics*, *44*(4), 823–830. https://doi.org/10.1017/S1049096511001429

Corning, G. P. (2024). The diffusion of data privacy laws in Southeast Asia: Learning and the extraterritorial reach of the EU's GDPR. *Contemporary Politics*, *30*(5), 656–677. https://doi.org/10.1080/13569775.2024.2310220

Council of Europe. (1981). *Convention for the protection of individuals with regard to automatic processing of personal data* (European Treaty Series No. 108). https://rm.coe.int/1680078b37

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), Article tyac011. https://doi.org/10.1093/cybsec/tyac011

Deibert, R. J. (2008). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of internet politics* (pp. 323–336). Routledge. https://doi.org/10.4324/9780203962541

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *Official Journal of the European Union*, L 281. https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng

Edwards, G. (2008). The construction of ambiguity and the limits of attraction: Europe and its neighbourhood policy. *Journal of European Integration*, *30*(1), 45–62. https://doi.org/10.1080/07036330801959465

Elkins, Z., & Simmons, B. (2005). On waves, clusters, and diffusion: A conceptual framework. *The Annals of the American Academy of Political and Social Science*, *598*(1), 33–51. https://doi.org/10.1177/0002716204272516

European Commission. (2001). *Europe and Asia: A strategic framework for enhanced partnerships* (COM(2001) 469 final). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0469:FIN:EN:PDF

European Commission. (2009, November 30). *European community signs a science & technology cooperation agreement with Japan* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_09_1844

European Commission. (2011). *Digital agenda: EU and Japan agree to strengthen cooperation in future internet research* (MEMO/11/432). https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_11_432/MEMO_11_432_EN.pdf

European Commission. (2012). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012) 11 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011

European Commission. (2018, September 5). *International data flows: Commission launches the adoption of its adequacy decision on Japan* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_18_5433

European Commission. (2022, December 14). *Global gateway: EU and its member states to mobilise €10 billion for South-East Asia* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7678

European Commission. (2024a). *Japan—EU trade relations with Japan: Facts, figures and latest developments*. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan_en

European Commission. (2024b). *Singapore: EU trade relations*. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore_en

European External Action Service. (2014, May 7). *22nd EU-Japan Summit joint press statement* [Press release]. https://eeas.europa.eu/archives/delegations/japan/en/resources/news-from-the-eu/news2014/20140507/210016/index.html

European Parliament. (2019). *EU-Japan Economic Partnership Agreement (EPA)*. https://www.europarl.europa.eu/legislative-train/theme-international-trade-inta/file-eu-japan-epa

Francesconi, E., & Passerini, A. (2007). Automatic classification of provisions in legislative texts. *Artificial Intelligence and Law*, *15*(1), 1–17. https://doi.org/10.1007/s10506-007-9038-0

Gilardi, F., & Wasserfallen, F. (2019). The politics of policy diffusion. *European Journal of Political Research*, *58*(4), 1245–1256. https://doi.org/10.1111/1475-6765.12326

Graham, E. R., Shipan, C. R., & Volden, C. (2013). The diffusion of policy diffusion research in political science. *British Journal of Political Science*, *43*(3), 673–701. https://doi.org/10.1017/S0007123412000415

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Hopkins, W., & McNeill, H. (2015). Exporting hard law through soft norms: New Zealand's reception of European standards. In A. Björkdahl, N. Chaban, J. Leslie, & A. Masselot (Eds.), *Importing EU norms* (pp. 153–172). Springer. https://doi.org/10.1007/978-3-319-13740-7_8

Horibe, M. (2013). *Privacy culture and data protection laws in Japan* [Speech transcript]. Personal Information Protection Commission. https://www.ppc.go.jp/files/pdf/290928_en_horibespeech.pdf

Hundt, D., & Uttam, J. (2017). *Varieties of capitalism in Asia: Beyond the development state*. Palgrave Macmillan. https://doi.org/10.1057/978-1-349-58974-6_5

Ishiara, T. (2019). Japan. In A. C. Raul (Ed.), *The privacy, data protection and cybersecurity law review* (6th ed.,

pp. 233–250). Law Business Research Ltd. https://datamatters.sidley.com/wp-content/uploads/sites/2/2019/11/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6.pdf

Japan External Trade Organization. (2024). *Japanese trade and investment statistics*. https://www.jetro.go.jp/en/reports/statistics.html

Japan Ministry of Justice. (2003). *Act on the protection of personal information* (Act No. 57 of May 30, 2003). Japanese Law Translation. https://www.japaneselawtranslation.go.jp/en/laws/view/130

Kirby, M. (2017). Privacy today: Something old, something new, something borrowed, something blue. *Journal of Law, Information and Science*, *25*(1), 1–25. https://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html

Klingler-Vidra, R., & Schleifer, P. (2014). Convergence more or less: Why do practices vary as they diffuse? *International Studies Review*, *16*(2), 264–274. https://doi.org/10.1111/misr.12137

Kuneva, M. (2009). *Meglena Kuneva—European Consumer Commissioner—Keynote Speech—Roundtable on online data collection, targeting and profiling* [Speech transcript]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156

Lai, D. (2024). Reimagining comparisons in international relations through reflexivity. *International Studies Review*, *26*(4), Article viae043. https://doi.org/10.1093/isr/viae043

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies*, *40*(2), 235–258. https://doi.org/10.1111/1468-5965.00353

Meseguer, C., & Gilardi, F. (2009). What is new in the study of policy diffusion? *Review of International Political Economy*, *16*(3), 527–543. https://doi.org/10.1080/09692290802409236

Mill, J. S. (1843). *A system of logic, ratiocinative and inductive: Being a connected view of the principles of evidence, and methods of scientific investigation*. J. W. Parker. https://doi.org/10.5962/bhl.title.25118

Mills, A. J., Durepos, G., & Wiebe, E. (Eds.). (2010). *Method of difference*. In *Encyclopedia of case study research* (pp. 558–559). Sage. https://doi.org/10.4135/9781412957397.n206

Ministry of Foreign Affairs of Japan. (1991). *Joint declaration on relations between the European Community and its member states and Japan*. https://www.mofa.go.jp/region/europe/eu/overview/declar.html

Ministry of Foreign Affairs of Japan. (1999, December 16). *Japan–France bilateral summit between Prime Ministers Obuchi and Jospin*. https://www.mofa.go.jp/region/europe/france/visit9912/joint/index.html

Ministry of Foreign Affairs of Japan. (2001). *An action plan for EU–Japan cooperation*. https://www.mofa.go.jp/mofaj/area/eu/kodo_k_e.html#1-3

Ministry of Foreign Affairs of Japan. (2014, October 3). *First meeting of Japan–EU cyber dialogue* [Press release]. https://www.mofa.go.jp/press/release/press4e_000447.html

Ministry of Foreign Affairs of Japan. (2023, February 3). *The 24th Japan–Germany joint committee meeting on science and technology cooperation* [Press release]. https://www.mofa.go.jp/press/release/press3e_000540.html

National Internet Advisory Committee. (2002). *Report on a model data protection code for the private sector*. https://www.agc.gov.sg/docs/default-source/publications/law-reform-reports/2002_report-on-a-model-data-protection-code-for-the-private-sector.pdf

O'Hara, K., & Hall, W. (2021). *Four internets: Data, geopolitics, and the governance of cyberspace*. Oxford University Press. https://doi.org/10.1093/oso/9780197523681.001.0001

Office of the Privacy Commissioner for Personal Data of Hong Kong. (2024). *The personal data (privacy) ordinance*. https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

Paldam, M. (2003). Economic freedom and the success of the Asian tigers: An essay on controversy. *European Journal of Political Economy*, *19*(3), 453–477. https://doi.org/10.1016/S0176-2680(03)00012-0

Palmer, M. (2006, November 3). Data is the new oil. *ANA Marketing Maestros Blog*. https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Parliament of Singapore. (2012). *Personal data protection bill*. https://sprs.parl.gov.sg/search/email/link/?id=023_20121015_S0003_T0002&fullContentFlag=false

Personal Data Protection Commission. (2020). *Personal data protection (amendment) act 2020*. Singapore Statutes Online. https://sso.agc.gov.sg/Acts-Supp/40-2020

Personal Information Protection Commission of Japan. (2016). *Act on the Protection of Personal Information (APPI)*. https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf

Personal Information Protection Commission of Japan. (2020). *Act on the Protection of Personal Information (APPI)*. https://www.ppc.go.jp/files/pdf/APPI_english.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Risse, T. (2016). The diffusion of regionalism. In T. A. Börzel & T. Risse (Eds.), *The Oxford handbook of comparative regionalism* (pp. 87–108). Oxford University Press.

Schimmelfennig, F., & Sedelmeier, U. (2004). Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe. *Journal of European Public Policy*, *11*(4), 661–679. https://doi.org/10.1080/1350176042000248089

Shipan, C. R., & Volden, C. (2008). The mechanisms of policy diffusion. *American Journal of Political Science*, *52*(4), 840–857. https://doi.org/10.1111/j.1540-5907.2008.00346.x

Simmons, B. A., Dobbin, F., & Garrett, G. (2008). *The global diffusion of markets and democracy*. Cambridge University Press.

Simmons, B. A., & Elkins, Z. (2004). The globalization of liberalization: Policy diffusion in the international political economy. *The American Political Science Review*, *98*(1), 171–189. https://doi.org/10.1017/S0003055404001078

Singapore Attorney-General's Chambers. (2012). *Personal Data Protection Act 2012* (No. 26 of 2012). https://sso.agc.gov.sg/Act/PDPA2012/Historical/20130102?DocDate=20121203&ValidDate=20130102

Solingen, E. (2012). Of dominoes and firewalls: The domestic, regional, and global politics of international diffusion. *International Studies Quarterly*, *56*(4), 631–644. https://doi.org/10.1111/isqu.12034

Strang, D., & Meyer, J. W. (1993). Institutional conditions for diffusion. *Theory and Society*, *22*(4), 487–511. https://doi.org/10.1007/BF00993595

Suda, Y. (2020). Japan's personal information protection policy under pressure: The Japan-EU data transfer dialogue and beyond. *Asian Survey*, *60*(3), 510–533. https://doi.org/10.1525/AS.2020.60.3.510

Tang, R. (2003). *A short paper on implementing data privacy principles: How are governments making it work in the real world?* Office of the Privacy Commissioner for Personal Data, Hong Kong. https://www.pcpd.org.hk/english/news_events/speech/apec_feb03.html

Vu, K. M. (2013). Information and communication technology (ICT) and Singapore's economic growth. *Information Economics and Policy*, *25*(4), 284–300. https://doi.org/10.1016/j.infoecopol.2013.08.002

Wang, F. Y. (2020). Cooperative data privacy: The Japanese model of data privacy and the EU–Japan GDPR adequacy agreement. *Harvard Journal of Law & Technology*, *33*(2), 661–728. https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf

Wong YongQuan, B. (2017). Data privacy law in Singapore: The Personal Data Protection Act 2012. *International Data Privacy Law*, *7*(4), 287–302. https://doi.org/10.1093/idpl/ipx016

WorldData.info. (2024). *Economy of Singapore* [Data set]. https://www.worlddata.info/asia/singapore/economy.php

World Economic Forum. (2011). *Personal data: The emergence of a new asset class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

About the Author

Danni Zhang is a joint PhD researcher at Northeastern University London and the University of Kent, affiliated with the Institute of Cyber Security for Society. Her research focuses on digital governance in the EU and China, especially in digital economy, data governance, and AI regulation.