



Prosperity Insight Series

DIGITAL TRADE REGULATORY READINESS

A Global Database

Martín Molinuevo, Nigorakhon Sadikova, Alexandra Schwind,
Lillyana Sophia Daza Jaller



DIGITAL TRADE REGULATORY READINESS

A Global Database

Martín Molinuevo, Nigorakhon Sadikova, Alexandra Schwind,
Lillyana Sophia Daza Jaller



WORLD BANK GROUP

© 2025 International Bank for Reconstruction and Development / The World Bank
1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean the World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.

Cover photo courtesy of the World Bank Group. All other photos courtesy of Shutterstock.com.



TABLE OF CONTENTS

Abbreviations	vi
Acknowledgements	vii
Executive Summary	1
1. Introduction	4
A. Digital trade and regulation	5
B. Existing databases	8
2. DTRR Regulatory Areas	12
A. Policies and measures covered	14
i. Regulatory solutions	15
B. Regulation on electronic transactions	16
i. Electronic documents	17
iii. Paperless trade	18
C. Trust building regulation	18
i. Online consumer protection	18
ii. Data protection	19
iii. Artificial intelligence	19
iv. Cybersecurity & cybercrime	19

D. Platform regulation	20
i. Cross-border data	20
ii. Intermediary liability	21
3. DTRR Database Methodology	24
A. Data collection and review methodology	24
i. Traceability to its original source	25
ii. Scope of the data collection	25
iii. Interpretation	26
iv. Deviations I: Restrictions on cross-border data flows	28
v. Deviations II: Paperless Trade and Digital ID	28
B. Geographical scope	29
C. Caveats	29
i. Sub-set of regulation	30
ii. Legal interpretation	31
iii. Implementation / <i>de facto</i> Regulation	31
iii. Different legal systems	31
v. Presenting regulatory “Readiness” trends: quintiles	33
D. Next steps	33
i. Data update and validation	33
ii. Expansion of data coverage	34
iii. Uses	34
iv. Analytical and Quantitative work	34
v. Feedback	35
4. Looking Ahead	36
Bibliography	38
Annex I: List of Regulatory Solutions Captured in DTRR Database	40



Abbreviations

AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
B2B	business-to-business
B2C	business-to-consumer
BPO	Business processing outsourcing
C.A.R.	Central African Republic
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEPA	Digital Economy Partnership Agreement
D.R.C.	Democratic Republic of Congo
DTRR	Digital Trade Regulatory Readiness
DTI	Digital Trade Integration
ECIPE	European Center for International Political Economy
EU	European Union
KPO	Knowledge processing outsourcing
ICT	information and communications technology
LDC	Least Developed Country
OECD	Organization for Economic Co-operation and Development
UAE	United Arab Emirates
WDR	World Development Report
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNGCP	UN Guidelines for Consumer Protection
USITC	US International Trade Commission
US / USA	United States of America
USMCA	United-States-Mexico-Canada Free Trade Agreement
WB	World Bank
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Acknowledgements

This study has been prepared by a team of World Bank experts led by Martín Molinuevo (Senior Counsel, ETIRI) and including Nigorakhon Sadikova (ETC, ETIRI), Lillyana Sophia Daza Jaller, Alexandra Schwind, Joseph Ashraf El-Cassabgui, Philipp Hlatky, and Prakhar Bhardwaj under the guidance of Sebastien Dessus (Manager, ETIRI) and Mona Haddad (Director, TIC).

The team is highly indebted to Javier López González (OECD), Torbjörn Fredriksson (UNCTAD), Melissa Metz (World Bank) and Adele Barzelay (World Bank) for comments as peer reviewers, as well as to Erik van der Marel (ECIPE), Mark Wu (Harvard law School), and Andrea Barone (World Bank) for comments in an earlier version of this report. The team is grateful to OECD experts Janos Ferencz, Chiara Del Giovane, and Karin Gourdon; UNCTAD expert Thomas Van Giffen; and World Bank colleagues Martha Martínez Licetti, Natalija Gelvanovska-Garcia, David Satola, Adele Barzelay, Pierre Sauvé, Elena Gasol-Ramos, Tania Begazo, Rocio Sanchez Viguera, Hunt La Cascia, Cecilia Paradi-Guilford and Rong Chen for their comments and advice at various stages of the project. This study benefited from an editorial review by Chris Wellisz and website portal development by Marlon Amorim.

The team gratefully acknowledges funding for this activity through the Umbrella Facility for Trade Trust Fund (UFT). The UFT is supported by development partners, including the Department of Foreign Affairs and Trade of Australia, the Foreign Commonwealth & Development Office of the United Kingdom, the Norwegian Agency for Development Cooperation (NORAD), the Norwegian Ministry of Foreign Affairs, the Ministry of Foreign Affairs of the Netherlands, the State Secretariat for Economic Affairs of Switzerland (SECO), and the Swedish International Development Cooperation Agency (SIDA).





EXECUTIVE SUMMARY

The digital revolution is changing every aspect of our lives. International trade, as one of the main pillars of a globalized world, is at the center of this revolution, as cross-border transactions of goods and services become an integral, often invisible, part of our daily digital routine.

Digital trade benefits from a comprehensive, modern and non-discriminatory regulatory framework. Regulation can provide the legal tools necessary for remote contracts, clarify the rights and obligations of the multiple actors involved in digital transactions, and establish a framework that promotes trust in digital markets, even when the consumer does not know the merchant or that the merchant is in a different country. However, regulation can also further strengthen segmentation of digital trade, de facto restricting digital transactions.

The report presents the Digital Trade Regulatory Readiness (DTRR) database compiled by a team of World Bank experts. The database offers novel information on laws and regulations on digital trade for 121 economies around the world, out of which 95 are developing countries. The database reflects countries' regulatory framework on specific matters directly relevant to digital trade, structure on nine "regulatory areas" (i.e., i) electronic documents; ii) electronic signature & digital ID; iii) paperless trade; iv) online consumer protection; v) data protection; vi) artificial Intelligence; vii) cybersecurity & cybercrime; viii) cross-border data; and ix) intermediary liability) distributed along three policy pillars, namely electronic transactions, trust-building regulation, and platform regulation. Altogether, the DTRR offers more than 13,000 datapoints, including over 5,200 regulatory

measures currently in effect. “Traceability,” a central feature of the DTRR, ensures the quality of the information, so that each of positive datapoints can be traced back to the specific provision, paragraph, and/or section number that supports them.

The DTRR’s goal is to inform digital trade policy by identifying priorities for strengthening regulation. By readily assessing progress on digital regulations, while also providing granular information on specific regulatory solutions (or lack therefore) within a country’s legal framework, the DTRR can help policymakers, international experts, practitioners and academics identify regulatory priorities for strengthening regulation on digital trade. The database also serves as a starting point for assess-

ing how a country’s regulatory framework complies with international obligations, such as digital trade agreements or the plurilateral WTO e-commerce agreement.

The DTRR database serves as an invaluable tool for policymakers and regulators in developing countries, offering access to a global repository of digital trade regulations from around the world. The database offers insights into current practices and regulatory frameworks that have been successfully implemented elsewhere. It can guide the development and update of their own digital trade policies, fostering an environment conducive to digital economic growth and integration into the global digital economy.





1c

INTRODUCTION

The digital revolution is changing every aspect of our lives. The COVID pandemic and its stay-at-home measures demonstrated how communications technologies can help shrink distances. International trade, as one of the main pillars of a globalized world, is at the center of this revolution, as cross-border transactions of goods and services become an integral, often invisible, part of our daily digital routine.

In a rapidly changing digital world, governments confront new challenges in the regulation of digital trade. Digital devices come alive with services from around the world—with software covering the whole spectrum from entertainment to productivity. Classic trade problems like expediting trade procedures take on new resonance as shipments cross international borders in varied forms—indi-

vidually packaged to consumers rather than in palletized cargo to wholesalers. Obstacles to trade are taking new shapes: issues like cross-border data flows and cybersecurity require international coordination to ensure the efficient and timely flow

of information. Furthermore, the policy challenges lie not only in fostering cross-border transactions, but also in ensuring that benefits and opportunities from digital trade are equitably distributed in society.

A. Digital trade and regulation

Multiple regulatory areas are crucial to the development of digital trade. Digital trade, understood as the purchase and/or delivery of goods and services through digital means (see Box 1 for a definition), benefits from a comprehensive, modern and non-discriminatory regulatory framework. Regulation can provide the legal tools necessary for remote contracts, clarify the rights and obligations of the multiple actors involved in digital transactions, and establish a framework that promotes trust in digital markets,¹ even when the consumer does not know the merchant or that the merchant is in a different country. However, regulation can also reinforce the fragmentation of digital trade, effectively restricting digital transactions.

Rules affecting digital trade extends beyond measures explicitly targeting foreign transactions. As is often the case in services trade more broadly, digital trade is typically governed by general laws and regulations that shape market conditions for a given activity—regardless of whether that activity is carried out by domestic or foreign providers. In this context, what makes a regulation relevant to digital trade is the inherently cross-border nature of the activities it covers. For example, legal liability rules for intermediary platforms often apply to domestic and foreign services alike. However, due to the borderless nature of digital platforms, such rules are more likely to affect foreign transactions than purely domestic ones.

Regulation plays three essential roles in digital transactions:

- **Providing essential regulatory tools for remote digital transactions.** One of the roles of economic regulation is providing legal recognition of innovative ways of making business interactions—while ensuring that the new practices are not harmful to third parties or can be otherwise deemed contrary to public interest. In the digital era, tools like *electronic documents* and *electronic signatures* require a regulation that affords them legal recognition to do business. Lack of electronic signatures may mean, for instance, that parties may need to physically travel or mail a hard copy to sign a document, increasing time and costs for the transaction. Further, the ability to complete *paperless trade* procedures is also a supporting element for cross-border B2B trade.
- **Enhancing trust in digital markets by ensuring that consumers are protected and that their information is safe and remains private.** Lack of trust in digital markets remains the top reason for not engaging in online purchases. In a 24-country survey, almost half the respondents said they never buy goods or services online because they do not trust online transactions (CIGI-Ipsos, 2017). Important limiting factors in both developed and developing economies are the perceptions that

1. We refer to “digital markets” as the ability to conduct commercial transactions over electronic channels, be it through the internet or peer-to-peer systems based on public telecommunications networks. A “digital transaction” is a transaction conducted through digital means where at least side of the transactions is fully automated and does not require direct human intervention.

cross-border online transactions and delivery are less secure, and that no remedies exist for when something goes wrong (World Economic Forum, 2019). Indeed, domestic regulations often lack rules addressing the cross-border elements of e-commerce. The limited jurisdiction of regulators means that they cannot impose their regulations on players outside of their national territory. Regulations that are particularly relevant to promoting citizens' trust in digital markets include:

- *A strong data protection regime*, which gives individuals control over their personal and financial information and fosters trust in how that data is collected, used, and shared;
- *An effective framework for online consumer protection*, which helps users make informed decisions about goods, services, and transaction terms—enhancing their confidence and understanding of digital exchanges;
- *A robust cybersecurity framework*, which improves trust by requiring firms to meet minimum technical standards for data protection and ensures that unauthorized access is appropriately prosecuted and penalized; and
- *Clear rules on artificial intelligence*, particularly those ensuring unbiased and transparent processes, which reassure citizens that safeguards govern how machines use the information they provide.
- **Regulating the operation of firms involved in the digital trade ecosystem**, with a focus on preventing market failures, especially information asymmetry in digital businesses (e.g., platforms, telecom services, electronic payments). Regulations related to intellectual property, specifically those focused on *intermediary liability* are a key component of the regulation of e-commerce platforms. Similarly, the ability to transfer data across is an essential element of digital trade, especially for digital services

Identifying regulatory approaches that minimize restrictions on digital trade while offering strong protections to individuals remains a key challenge. Essential aspects of digital trade regulation, such as intermediary liability or data protection, are new and still subject to trial-and-error experimentation. Other aspects of digital rules have been pioneered by high-income countries that can support those regulations with a vast and skilled institutional apparatus, but whether those rules are also suited to smaller or poorer administrations and economies is uncertain. In addition, horizontal regulations need to be completed with modern sector-specific regulations that address the challenges faced in specific activities that disrupt new digital business models, such as online retail (e-commerce) ride hailing, lodging, among others.

This report discusses the role of regulatory policies in digital trade and presents how these regulations are being adopted around the world. Following this introduction, Section 2 describes the key features of the Digital Trade Regulatory Readiness (DTRR) database. Section 3 presents the regulatory areas by the DTRR and their connections with digital trade. Finally, Section 4 offers suggestions for further analysis.

The DTRR database focuses on horizontal regulations that provide essential regulatory tools for remote transactions, promotes trust among the parties to the transaction, and sets out rules on online platforms. The data gathered helps inform global progress on digital governance by identifying regulatory regimes that lack elements essential to digital trade, thereby introducing costs in the form of legal uncertainty for consumers and providers.

An enabling environment for digital trade requires coordination with multiple other regulatory policies. Regulation relevant to digital trade extends well beyond the current scope of the DTRR. For example, an effective regulatory and institutional framework for electronic payments is essential to cross-border transactions.

Box 1: Defining digital trade

There are four forms of digital trade: the Internet enables trade in “traditional” goods and services that are digitally ordered but delivered offline, and it also provides a platform for trading purely “digitally traded” goods and services that are not only ordered electronically but also produced and delivered online.

Under most definitions of e-commerce, electronic transactions can entail the sale of either goods or services. For traditional goods and services, the Internet functions as a global e-commerce marketplace that enables remote transactions of goods and services that would otherwise be sold in brick-and-mortar stores. Digital technologies not only expand the possibilities for trade in existing goods and services but also offer a completely new environment for new “digital” goods and services to be developed—and traded.

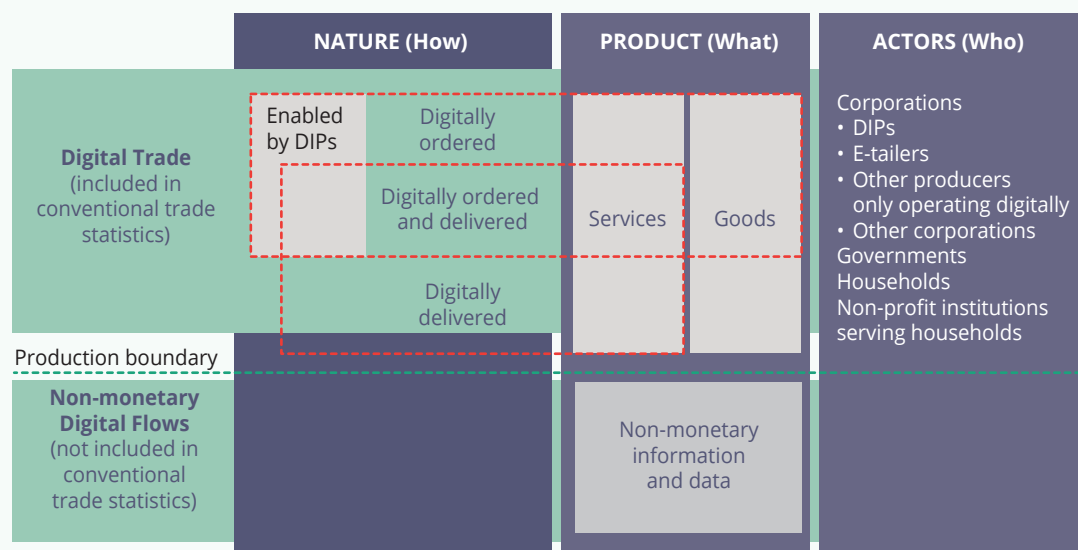
Figure B1 illustrates trade in digital goods and services in quadrants III and IV, respectively. Business reality, especially in the digital environment, however, often blurs these conceptual lines. Software, for example, has been historically traded as merchandise (embodied in the shipping of physical media such as floppy disks or CDs) but is now often provided as a service, based on a subscription fee, that includes the right to updates, technical support, and ancillary digital products. Similarly, some services such as ICT consumer support can blur the lines between “traditional” and “digitally traded” services, as reflected in quadrants I and IV. Finally, some business can be used by final consumers or by other businesses, making it a challenge to clearly distinguish between B2C and B2B activities. This approach is consistent with a similar classification offered by the OECD, WTO, and IMF that focuses on whether goods and services are digitally ordered and/or digitally delivered (Figure B2).

Identifying the differences among the various types of digital trade is more than theoretically valuable. Rather, realizing these different phenomena as part of the broader digital trade or even digital economy analysis has practical implications. For instance, for statistical purposes, e-commerce goods transactions are normally captured by customs as they cross the border in the form of parcels and fall under the goods sections of the current account. Digital goods such as software or e-books should also, in principle, be captured as goods under the current account; however, because they are digitally delivered and do not cross physical borders, customs information will not be available, and such information should be sought elsewhere—for instance, in the international payments for goods and services as recorded by central banks. More importantly, the different expressions of digital trade also face different challenges and call for different policy responses: the logistical challenges of international parcel shipping faced by online retailers are not necessarily relevant to traders of digital goods and services, who, instead, may be much more concerned with intellectual property rights and contract enforcement.

Figure B.1: Types of digital trade I

	GOODS	SERVICES
TRADITIONAL E-COMMERCE	II Jumia ebay Amazon (merchandise) Alibaba	I E lance Freelancer Professional services BPO – KPO E-banking News/information
DIGITALLY TRADED	III App stores (software, music, video, mobile apps) Amazon (e-books, video) 3-D printed goods?	IV Paypal Google Ads E-medicine IT outsourcing Amazon Web Services AI/data analytics Social media

Source: IMF, OECD, UNCTAD and WTO, 2023.

Box 1: Defining digital trade**Figure B.2:** Types of digital trade II

Source: IMF, OECD, UNCTAD and WTO, 2023.

Source: IMF, OECD, UNCTAD and WTO, 2023.

Rules on transport and logistics are directly relevant to e-commerce in merchandise. Competition policies and regulations are also critical, particularly given the network effect associated with third-party platforms. As a result, a comprehensive

review of policies and regulations that go beyond the scope of the DTRR database may be necessary when conducting an in-depth review of the regulatory environment of a specific country.

B. Existing databases

The DTRR database complements existing databases on regulatory restrictions with information on regulations that address regulatory challenges inherent to digital trade. Existing databases cap-

ture regulatory restrictions on digital trade but provide few details on the regulations governing it. For instance, ECIPE's pioneering Digital Trade Restrictiveness Index (DTRI)² and the OECD's Dig-

2. ECIPE's pioneering Digital Trade Restrictiveness Index (DTRI) builds on an underlying database of regulatory restrictions on digital trade for 64 countries. The DTRI assigns a score from zero (fully open) to 1 (virtually closed) based on the trade restrictiveness of digital trade policies (Ferracane, M. F., & van der Marel, E. (2018). The database provides a short description of the restriction, as taken from its source.

ital Services Trade Restrictiveness Index (DSTRI)³ provide relevant information on existing digital restrictions and allow an empirical assessment of the impacts of those restrictions on trade and other aspects of the economy. However, given their focus on trade *restrictions*, they offer little information on the type of measures that can be considered legitimate safeguards that promote consumer trust in digital markets—and where they do, these measures too are assessed as restrictions on trade, without taking into account the positive trade effect they may have. OECD's DSTRI does account for the positive effect of some measures by scoring the absence of regulations on policies like e-signature, e-contract, e-payment and privacy regulation as a restriction on digital trade. UNCTAD's Cyberlaw Tracker⁴ instead monitors the

adoption of certain legislation relevant to e-commerce for 195 countries, in an effort to promote a sound and comprehensive regulatory framework for digital trade. UNCTAD's database does not attempt to build an index or otherwise provide any assessment of the legislation. These datapoints would help inform current indices on restrictiveness by identifying those regulatory regimes that lack essential pieces of regulation on digital trade, thereby introducing costs not in the form of regulatory restrictions, but in the form of legal uncertainty for consumers and providers.

Additionally, the WB Data Governance database provides insights into both safeguards and regulatory restrictions, covering 80 economies. Unlike indices that focus primarily on restrictions, this

Table 1: Comparison of digital regulation databases

	OECD DSTRI	UNCTAD Cyber-law tracker	ECIPE DTRI	DTI	WB Global Data Regulation Survey	DTRR
# economies covered	93	195	64	130	80	121
# of policy areas covered	5	4	13	12	7	9
# total datapoints captured	3,780	776	6,400	13,130	6,480	13,794
Focus on	Regulatory restrictions	Existence of legislation	Regulatory restrictions	Regulatory restrictions + Safeguards	Safeguards + regulatory restrictions	Regulatory restrictions + Safeguards
Methodology	Survey + Regulatory Review	Surveys	Web scraping	Web scraping	Surveys + Regulatory Review	Regulatory review
Quantitative Index	Yes	No	Yes	Yes	Yes	No
Includes sources / traceability	Partial	Yes	Partial	Partial	No	Yes

3. The OECD Digital STRI adds digital elements to the Services Trade Restrictiveness Index (STRI) to capture impediments to services traded digitally, and catalogues and quantifies barriers that affect trade in digitally enabled services across 93 countries. The database includes references and links to some of the underlying regulations. The indices take values between 0 to 1, where 0 is completely open and 1 is completely closed. <https://goingdigital.oecd.org/en/indicator/73>.

4. <https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide>.

database evaluates regulatory safeguards that contribute to fostering trust in digital trade. Furthermore, the DTRR database, which covers 121 economies, distinguishes itself by capturing both regulatory restrictions and safeguards while ensuring traceability. The DTRR methodology relies on regulatory reviews, allowing for a structured assessment of digital trade policies beyond just trade barriers. This approach ensures that not only restrictive measures but also policies that enable digital trade are captured, providing a more nuanced perspective compared to other databases.

The DTI (Digital Trade Integration)⁵ database, which covers 130 economies, is another key regulatory dataset that focuses on both safeguards and reg-

ulatory restrictions. Unlike databases that rely on surveys or purely legal assessments, DTI employs a web-scraping methodology, collecting real-time regulatory data across multiple digital trade policy domains. With 12 policy areas covered, DTI provides a broader regulatory perspective compared to some other indices, making it a valuable resource for understanding the dynamic evolution of digital trade policies globally. By integrating these additional datasets into the analysis, we recognize the complementary nature of various regulatory databases. While some focus strictly on trade restrictions, others incorporate safeguards, and some, like the DTRR, provide a holistic view by bridging both perspectives—offering a more comprehensive understanding of digital trade regulations.

5. <https://dti.eui.eu/>.





2) C

DTRR REGULATORY AREAS

A comprehensive and modern digital regulatory framework is essential for supporting digital trade. Regulation plays three critical roles for digital transactions. It provides the legal tools needed for concluding valid and enforceable electronic contracts, such as rules giving effect to the electronic authentication of documents and e-signatures. Frameworks for personal data protection,

online consumer protection, and cybersecurity offer safeguards that enhance trust in digital markets. Finally, regulations on the legal liability of platforms for unlawful or harmful content and rules on the international transfers of data set out basic rules that support a transparent and predictable framework for digital markets.

Regulation can also introduce unwarranted limitations to digital trade. For instance, unnecessarily restrictive or overly cumbersome requirements for cross-border data transfers limit access to certain digitally delivered services. Limitations on the types of goods and services offered online may be warranted by public policy goals (e.g., restrictions on guns or controlled substances) or may add costs and inefficiencies by segmenting markets (e.g., requiring the use of domestic cloud services). The central challenge for policymakers and regulators is therefore to adopt balanced frameworks that minimize restrictions on digital trade while offering a comprehensive framework for digital transactions and sound safeguards for users. By requiring that public policy measures minimize unnecessary trade restrictions, trade agreements help establish useful benchmarks for setting regulatory boundaries.

The DTRR database focuses on horizontal regulations that provide essential regulatory tools for remote transactions, promote trust in digital markets, and define rules for online platforms. The data gathered helps inform global progress on digital governance by identifying regulatory regimes that lack elements essential to digital trade, thereby introducing costs in the form of legal uncertainty for consumers and providers. In this context, “readiness” is intended as the ability of the regulation to comprehensively address the challenges presented by digital technologies in line with international best practices.

The database offers novel information on laws and regulations on digital trade around the world. The database reflects countries’ regulatory framework on specific matters directly relevant to digital trade, specifically in the areas of electronic transactions, trust-building regulation, and platform regulation. The DTRR offers a total of over novel 13,000 datapoints, which includes over 5,000 regulatory measures effectively in place with explicit reference (“traced”) to the specific legal instrument, including its section and paragraph, that

supports them. The basic premise is that providing effective and transparent regulatory solutions fosters digital trade by enhancing trust in digital markets and reducing costs related to uncertainty and ambiguity in the legal framework.

The goal of the DTRR is to inform policymaking by identifying priorities for strengthening regulation on digital trade. Readily assessing progress on digital regulations, while also providing granular information on specific regulatory solutions (or lack therefore) within a country’s legal framework, the DTRR can help policymakers, international experts, practitioners and academics to identify regulatory priorities for strengthening regulation on digital trade. The database also provides a starting point for assessing compliance of a country’s regulatory framework with international obligations, such as digital trade agreements or the plurilateral WTO e-commerce agreement. In that sense, the DTRR focuses on offering *qualitative* information for over 120 economies in the world in an accessible and user-friendly manner. The data collection is based on laws and regulations related to digital trade, from which the DTRR identifies the specific regulatory measures as set out in formal legal instruments. As such, the information presented in the DTRR reflects *de jure* frameworks only.

The database captures regulations as they apply to digital trade, even when they may have a broader scope. In an effort to zero in on digital trade, the regulation solutions covered address matters inherent to digital trade. In some instances, however, matters relative to digital trade are covered under general, non-digital-specific rules. This is particularly the case in consumer protection, where broad, often dated, consumer-protection regimes also apply to digital transactions, even if they were not designed to do so. The DTRR still recognizes the regulation as applying to digital trade and records it positively wherever the regulatory solution is met, even if contained in a general law or regulation that goes beyond digital trade. This

methodological approach is understood to reflect more accurately the regulatory framework applying to digital trade. In practice, however, general frameworks generally fall short of good practices in digital regulation.

The DTRR focuses on qualitative information but is designed to support further use in quantitative analyses. Unlike other databases in this space—

such as the OECD Digital STRI, ECIPE's DTRI, and the WB-WTO STRI—the DTRR does not provide scores or indexes of the regulatory measures it collects. However, the data can be further processed to support econometric and other quantitative studies aimed at assessing the quality of regulatory frameworks. To this end, the full dataset is available for download, and the authors encourage its use and further development.

A. Policies and measures covered

The Digital Trade Regulatory Readiness data cover nine key regulatory areas for digital trade, grouped into three broader regulatory pillars as captured in Table 2. These areas were selected by the authors based on consultations with WB and external experts and informed by specialized literature:

These topics also reflect the regulatory areas commonly mentioned in digital trade/e-commerce chapters in trade agreements. As global trade in both goods and services increasingly incorporates digital technologies, regulations aimed at fostering digital trade are also becoming a central component of trade agreements. For instance,

the first binding international rules on cross-border data flows are found in trade agreements, namely the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United-States-Mexico-Canada Free Trade Agreement (USMCA). Furthermore, “digital trade agreements” focusing exclusively on digital trade rules are emerging as a new trend in regulation of global trade. The US and Japan concluded a Digital Trade Agreement on October 2019; Singapore, Chile, and New Zealand signed (electronically) their Digital Economy Partnership Agreement (DEPA) in June 2020; and ASEAN countries concluded the “ASEAN Agreement on Electronic Commerce” in

Table 2: Regulatory pillars and areas covered by DTRR database

Policy pillar	Regulatory area	# of regulatory solutions assessed
Regulation on electronic transactions	Electronic documents	4
	Electronic signature & Digital ID	6
	Paperless Trade	3
Trust-building regulation	Online consumer protection	19
	Data protection	19
	Artificial Intelligence	4
	Cybersecurity & Cybercrime	11
Platform regulation	Cross-border data	34 ^a
	Intermediary liability	14
	TOTAL	114

^a Includes 15 enabling and 19 restrictive regulatory solutions.

January 2019. Digital trade rules are also being discussed at the multilateral level. Under the umbrella of the WTO, the current draft plurilateral agreement on e-commerce seeks to adopt a universal set of principles and rules on key aspects of digital trade, such as rules on electronic contracts, online consumer protection, and paperless trade.

These nine regulatory areas are further disaggregated into 114 “regulatory solutions.”

The specific solutions (i.e., individual variables) were selected with a view to providing a progressive understanding of the digital trade regulatory framework. In that sense, countries with limited and/or outdated regulations are likely to answer positively only to the basic **questions** of each area, while countries with a comprehensive and up-to-date framework will tend to answer positively to most of the questions. An effort was made to select broadly uncontroversial questions that indicate a progressive degree of depth and complexity, and to represent the comprehensiveness of the regulatory framework independently, even where those regulations may not be in line with the global “best practices.” Annex I lists all the regulatory solutions reviewed and offers example and additional background on their importance for digital trade.

i. Regulatory solutions

The DTRR focuses on the “regulatory solutions” featured in a country’s legal framework. The main information offered by the DTRR is whether a country has adopted specific statutory actions or safeguards (“regulatory solutions”) meant to overcome policy challenges related to digital trade. Going beyond the title or general context of the legislation, the DTRR digs into the content of laws and regulation to identify whether such regulatory solutions are in place. Regulatory solutions can take the form of statutory requirements, like the mandate to disclose information certain about the vendor in e-commerce platforms or that electronic documents have the same legal value as physical one, or the adoption of certain safeguards, like granting

a right to individuals to request the deletion of their personal information. While the database builds on the assumptions that adopting these regulatory solutions acts as an enabler for digital trade, the section on cross-border data rules also identifies measures that are in fact restrictions on digital trade. These few “negative” regulatory solutions are treated separately from the bulk of the data in most analyses—see section 3.a.iv for details.

The focus on regulatory solutions allows us to assess how comprehensive and modern the regulation is. Regulations can range from basic laws that provide solutions to a few aspects of a given policy area, to frameworks that seek to provide a comprehensive response to various new challenges brought about by digital trade. Consumer trust in remote, digital transactions, for example, is lower than in face-to-face interactions, as the consumer has often little information about its counterpart. Explicitly recognizing that online transactions are covered by consumer protection and requiring online vendors to provide certain information are simple regulatory solutions featured in virtually all effective consumer protection framework; more advanced regulations, however, include rules against the use of “dark patterns” (i.e., user interface designs intended to manipulate behavior—for examples making very easy to sign up for a service, but very difficult to cancel it) or rules against spam. By identifying which regulatory solutions are in place, the DTRR allows users to assess how comprehensive and modern the regulation actually is with greater certainty than verifying the mere existence (or lack thereof) of a legal instrument on any given area.

Based on legal texts, the database captures whether a specific regulatory solution is addressed in the regulation. In the collection stage, the database shows in a binary manner whether each of 114 regulatory solutions is effectively covered in the legal framework of the country under review. Table 3 lists the regulatory solutions assessed under Intermediary Liability, and portrays the data as captured in the DTRR database for the

Table 3: Regulatory solutions on intermediary liability. Selected countries

		Singapore	Chile	U.S.
Intermediary liability	Framework explicitly addresses online intermediary liability	✓	✓	✓
	Online intermediaries are not required to routinely monitor content uploaded by third parties	✓	✓	✓
	Safe harbor provisions exist to shield online platforms/hosting providers from liability for:	✓	—	✓
	• Unlawful activity generally			
	• Infringements related to intellectual property	✓	✓	✓
	Notice and take down procedures required for:	✓	—	—
	• Unlawful activity generally			
	• Infringements related to intellectual property	✓	✓	✓
	Content providers' right to counter notice	✓	✓	✓
	Online platforms'/Hosting providers' right to counter notice/appeal	—	—	—
	Online platforms/Hosting providers are not liable for wrong deletion if they conduct deletion by following a takedown notice	✓	—	✓
	Complainants are liable for wrong deletion following a takedown notice	✓	✓	✓
	Online platforms/Hosting providers are required to disclose the identity of infringers to the extent it is available to them	—	—	—
	If online platforms/hosting providers are required to disclose the identity of infringers, they are not liable for the failure to do so	—	—	—

Source: DTRR.

three countries with the most comprehensive regulatory solutions in that category. In its raw form, the dataset is a matrix of zeros and ones (or their graphical equivalent) with regulatory solutions and countries on each of its axes.

The following sections offer brief reviews of the regulations covered by the DTRR and how they relate to digital trade.

B. Regulation on electronic transactions

Providing legal recognition to the tools necessary for remote, electronic transactions is a necessary initial step toward an enabling framework for digital trade. As communication technologies connect people and businesses around the world with increasing ease and convenience, busi-

nesses engaged in digital trade also expand their network of clients and suppliers across borders. A regulatory framework that is conducive to digital trade should therefore guarantee that contracts concluded remotely through electronic channels are just as valid and legally enforceable as those

concluded in person. Ensuring that electronic documents and signatures are fully recognized and enforceable—while providing citizens with adequate tools—is therefore essential to underpinning the legal validity and practical use of remote electronic contracts and transactions.

i. Electronic documents

A strong and reliable framework for e-documents is particularly important for business-to-business (B2B) transactions. Transactions with final consumers, such as those on e-commerce platforms like Amazon.com, Lazada.com, or MercadoLibre.com, and app-based services like Airbnb, do not typically entail major documentation exchanges and can be concluded even without a specific regulatory framework for electronic transactions.

However, B2B transactions that entail customization of products and services provided over time, such as those that allow suppliers to connect to global value chains or that require peripatetic delivery over extended periods, the ability to conclude or amend contracts across borders in a secure and reliable way is essential for reducing costs and facilitating cross-border business operations.

ii. Electronic signatures & digital authentication

The ability to conclude legally binding contracts remotely depends heavily on capturing the parties' agreement in a secure and reliable manner. Electronic signatures contribute to remote transactions by providing a legal and technological mechanism that ensure the parties that their identities and

Box 2: The EU's eIDAS Regulation: A framework for cross border E-ID and Trust Services

The European Union enacted Regulation No. 910/2014 on 'electronic identification and trust services for electronic transactions in the internal market' ("eIDAS") to remove barriers to the cross-border use of electronic identification means for public services used in the EU Member States. The eIDAS sought to meet this goal by prescribing conditions under which Member States must recognize electronic identification schemes of another EU Member State, laying down rules for trust services for electronic transactions, and by establishing a legal framework for, amongst others, electronic signatures, and documents. The eIDAS regulation requires that mandatory electronic identification schemes to be notified to the Commission along with the appropriate assurance level: either low, substantial and/or high. These assurance levels correspond to minimum technical specifications, standards, and procedures notified by the Commission. Each of the notified electronic identification schemes are required to be interoperable, such that there is no discrimination between any specific national technical solutions for electronic identification. In practice, this has enabled citizens with smartcards and mobile-phone-based digital identification systems issued in one EU Member State to access online services provided in other European countries. By virtue of the Agreement on the European Economic Area, the eIDAS has also been adopted as law in Norway, Iceland, and the Principality of Liechtenstein.

The eIDAS regulation may have also helped countries in establishing electronic identification systems through the legal framework of qualified trust service providers. The eIDAS defines a 'trust service' as an electronic service relating to the creation, verification, preservation, and validation of electronic signatures, electronic seals, and certificates for website authentication. Trust service providers that successfully fulfill the accreditation requirements of the conformity assessment body are listed as 'qualified trust service providers' by each EU Member State. The reliability and credibility associated with being a qualified trust service provider under eIDAS has also made it easier for EU Member States to engage qualified trust service providers to establish digital identity solutions. For instance, the Republic of North Macedonia engaged Evrotrust, a qualified trust services provider of the Mastercard group, to launch the country's first remote digital identity services system.

Source: Authors based on Regulation(EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

expressions of will be secure and reliable, even in contracts concluded at a distance or across countries. Digital identities entail a collection of electronically captured and stored attributes that uniquely describe a person within a given context and are used for electronic transactions (World Bank, 2016), which allow for digital IDs that can be used to prove real-life identity online, and thereby grant access to a range of public and private services in a safe and secure way.

iii. Paperless trade

In paperless trade, digital information is used

instead of paper documents to fulfill customs procedures. Digital customs procedures are a valuable complement not only to traditional, containerized, bulk trade that moves thousands of products at once but also to international e-commerce, where goods are often sold and shipped in individual parcels directly to the final consumer. Bottlenecks in customs clearance and regulatory documentation can be particularly challenging for smaller businesses and digital traders with less experience and resources. (UNECE and WEF, 2017).

C. Trust building regulation

A robust regulatory framework that prevents the misuse of data while facilitating its use and sharing is essential for building trust in data transactions. Despite many recent important advances regarding personal data, legal frameworks for data governance across much of the developing world remain inconsistent, raising concerns about the ability of lower-income countries to benefit from the development opportunities emerging from the burgeoning global data economy (World Bank, 2021).

Regulation plays an essential role in bolstering digital markets by promoting trust. Because digital markets are still in their infancy, lack of trust in remote electronic transactions remains the primary reason consumers avoid online purchases—especially across borders (Figure 7). The very nature of remote electronic transactions means that consumers have no face-to-face contact with vendors, meaning that there are no “visual cues,” such as location, facilities, and personalized interaction, that help consumers gauge a retailer or supplier’s professionalism. In this environment, consumers are asked to disclose sensitive information and personal data either to a retailer, online intermediary, or digital platform.

As a result, one important limiting factor in both developed and developing economies is the perception that cross-border online transactions and delivery are less secure, and that remedies do not exist when something goes wrong (World Economic Forum, 2019).

Trust-building regulation for digital markets focuses on three goals: overcoming information asymmetries, strengthening individuals’ rights and remedies, and making online transactions secure. Under this “trust building” category, the database captures policies on consumer protection, data protection, cybersecurity and AI. Overall, by ensuring that such data is adequately protected and may not be used for purposes other than the specific issue at hand, these regulations seek to provide online users a sense of security in the transaction and control over their own information,.

i. Online consumer protection

Rules governing online consumer protection are needed to overcome information asymmetries between vendors and consumers of online transactions. Distance shopping presents challenges,

such as the inability to assess products in person before confirming a transaction. Online consumer protection laws aim to ensure “a level of protection not less than that afforded in offline commerce” (UNCTAD, 2017). To that end, *online* consumer protection builds on the principles and mechanisms of traditional consumer protection regimes, extending and adapting those protections to digital markets to reduce some of the challenges of buying and selling online (OECD, 2000). Similarly, the UN Guidelines for Consumer Protection (UNGCP) emphasizes that consumer protection in e-commerce should be equivalent to that in traditional commerce. Online consumer protection provisions are typically designed for domestic markets; however, they play an especially important role in international digital trade, where consumer trust tends to be lower—particularly when procedures like cancellations and returns are unclear or poorly communicated.

ii. Data protection

Consumers are increasingly aware of the implications of unrestricted access to personal data. Lack of trust in the way personal data is managed drives users away from electronic transactions, limiting the growth of digital markets. Safeguards governing when and how firms may collect, process and share personal data are essential for building digital markets in which users feel safe providing their personal information, knowing it will only be used and shared as necessary for the original purpose.

Strong and consistent data protection regulations are also essential from digital trade, especially for digital services. Some studies have found that Countries that share strong safeguards for personal data tend to trade more between each other (World Bank, 2021; Ferracane and van der Marel, 2021). Two factors may play a role in this phenomenon. On one hand, consumers are more likely to transact with vendors who, whether due to good practices or regulatory compliance, provide clear assurances about how personal data is used and with whom it may be shared. In parallel, as

data protection regimes expand globally, a growing number of countries now require that foreign partners offer comparable—or “adequate”—protections before allowing cross-border data transfers. This creates incentives to trade with countries that maintain similar data protection standards.

iii. Artificial intelligence

Artificial intelligence (AI) has the potential to boost efficiency and productivity and opens the door to new tradeable services. The ability of machines to “learn” by identifying patterns of data—from a human face, to the risk associated with certain activities, to the potential interests of consumers—can deliver significant productivity gains for businesses. For instance, employee recruitment often involves the costly review of dozens of candidate profiles, a process that can be automated using AI solutions. Similarly, machine learning algorithms can parse large amounts of mobile-phone data to deliver instantaneous credit scores to users in developing countries (Strusani and Hounghonon, 2019). Digital trade plays a critical double role in AI. As machine learning feeds from, and is improved by, large amounts of data, access to information around the world is essential to a well-trained system. Furthermore, because a handful of tech giants control big data and advanced algorithms, most AI users around the world are more likely to access AI services through cross-border digital trade than by developing domestic systems, at least in the short to medium term. At the same time, increasing concerns around data privacy, algorithmic bias, and automated decision making have led to growing regulatory scrutiny of AI and data flows. These tensions underscore the importance of developing international frameworks that enable digital trade while addressing legitimate governance concerns.

iv. Cybersecurity & cybercrime

While less visible to individual consumers, cybersecurity regulation is essential to pro-

moting trust in digital trade. Cybersecurity rules include a broad range of measures addressing the security of network infrastructure and the elements over which data flow, as well as policies to secure the storage and the safe transfer of data. From this perspective, cybersecurity policies seek to bolster broad public confidence in the use of the internet and ICT by addressing the risks that crime, and even armed conflicts may bring to the security of networks such as power grids and urban utilities; devices from consumer phones to computer mainframes; and both per-

sonal and non-personal data (World Bank and United Nations, 2017). From a digital trade perspective, however, the focus is narrower—individuals’ trust and measures to protect personal data from unauthorized access. In that sense, major data breaches, like the one Yahoo! witnessed in 2013 that affected 3 billion user accounts, not only compromise people’s privacy but can have a chilling effect on digital markets as consumers realize how vulnerable their information can be.

D. Platform regulation

Online platforms play an essential role in digital trade by connecting individual consumers with retailers, manufacturers, and service providers from around the world. The internet’s unparalleled ability to connect billions of individuals worldwide has boosted business models based on intermediation between vendors and consumers. E-commerce platforms like Alibaba, eBay, and Mercado Libre are based on offering consumers products from thousands of different providers rather than their own stock. “Gig economy” apps offer services such as rides, lodging, or delivery of food or groceries from firms and individuals. Other services rely on content such as video (YouTube, Vimeo), opinions and reviews of products or services (Yelp, Google), or information (blogs) developed by thousands of users, most of whom remain relatively unknown to the final consumer. The relationship between these intermediaries (websites and apps) and the firms or individuals offering their own products or services is therefore essential to the functioning of those digital transactions. These connections are also possible to the extent that businesses and consumers around the world can transmit the relevant information (i.e., data) in a timely and efficient manner.

i. Cross-border data

Cross-border data flows are an increasingly essential element of international trade. Data flows not only support trade in goods, making production and distribution more effective and less costly, but such flows are in fact the vehicle for trading digital services across borders. As trade in global digital services has increased dramatically in recent years, so have global data flows. Regulation of data flows, especially of personal data, lies at the heart of digital trade governance. More than 40 percent of US firms surveyed by the US International Trade Commission (USITC) consider data localization requirements and market access regulations to be obstacles to trade, particularly larger firms and those in the digital communications, content, and retail services sectors (USITC, 2014). Assessing regulatory restrictions on digital trade, Ferracane and Van Der Marel (2021b) find that restrictive data policies, specifically those related to the cross-border movement of data, result in lower imports of data-intensive services for the countries imposing them, which translates into lower levels of cross-border digital trade.

Restrictions on global data flows can also burden domestic companies using digital technologies,

particularly in the context of global value chains (World Bank, 2020). Swedish manufacturing firms recently reported that data localization requirements and restrictions on cross-border data flows, including for outward transfers, adversely affect the setup and operation of their global production networks (NBT, 2015). The challenge for policy makers is promoting the sharing and transfer of data in a manner that supports the economic benefits of digital trade, while ensuring that sensitive information remains secure and the relevant regulations on personal data protection are respected.

Restrictions on data flows, commonly referred as “data localization” requirements, take multiple forms. Limitations on the management of data are not limited to the explicit regime on cross-border transfers: provisions mandating that certain type of data be stored, processed, or accessed only with the jurisdiction of the country—often referred as “data localization” measures—are also critical in the management of information. Data storage requirements entail the obligations to house certain data on servers physically located in the country. Local processing requirements, on the other hand, mandate that all handling of such data—such as updating, anonymizing, or preparing for any specific use—must take place within the country. Local access requirements require that certain information can only be retrieved from within the country. While these rules do not prohibit cross-border data sharing or offshore storage of copies, they impose significant costs by physically anchoring the data to domestic infrastructure.

Broad, economy-wide, data localization requirements are rare, but are not unusual in specific sectors. No country in the DTRR features general data localizations for personal and non-personal data, but 12 countries in the database have adopted data localization requirements for all personal data—a requirement often considered a major restriction to cross-border data flows. Ten countries from that group demand local storage of all personal data, while two more mandate domes-

tic processing instead, including Kenya which features both.

Non-personal data

Non-personal data flows are important for digital trade, enhancing commercial benefits and technological innovation. Non-personal data plays a key role in digital trade by enabling commercial benefits, driving technological innovation, and facilitating global data flows essential for international business operations. Unlike personal data, it is usually not subject to the same amount of privacy restrictions—such as consent principles or data minimization principles. This relative flexibility in handling and cross-border sharing makes non-personal data especially valuable for improving trade efficiency, enhancing public services, and supporting competitive market strategies. Understanding and managing the flow of non-personal data is key to maximizing the benefits of digital trade while ensuring secure and efficient global trade exchanges.

ii. Intermediary liability

Rules on intermediary liability can make or break business models based on digital platforms. Intermediary liability rules are the set of provisions that distribute the liability between intermediaries (website and apps) and actual vendors or content developers when things go wrong. In other words, intermediary liability is the responsibility that falls upon online intermediaries, such as search engines, application platforms, social networks, and broadband companies, for third-party content featured in, or products and services offered through, their websites or apps. Just as intermediation is not a novel business model, intermediary liability rules are not a new legal concept—most such rules can be traced back to Roman law. Intermediary liability rules can, in fact, be broader rules that apply to online intermediaries (Gasser and Schulz 2015). However, specific rules of digital intermediaries are more likely to adapt to the specific conditions of

digital markets. Lack of provisions specifically oriented to digital platforms leads to courts' decisions to fill the gaps with rules and principles not tailored to the digital context—often with odd or suboptimal results. Even where judicial decisions reach optimal outcomes, having explicit regulations in place increases transparency and predictability, thereby reducing costs for digital business and strengthening user rights.

Given the central role of digital platforms, clear rules on intermediary liability are essential to digital trade. Social media and e-commerce platforms are hallmarks of digital markets, whose inherently global nature provides a natural environment for connecting suppliers and consumers around worldwide. The network effects of digital platforms tend to concentrate market power in a few massive global providers. However, the growth of these services can be hindered by outdated or inadequate rules on intermediary liability, which

may impose harsh penalties for user-generated content or behavior. This regulatory uncertainty also affects domestic start-ups, which may face prohibitive costs if held responsible for their users' misconduct.

Regulations on intermediary liability typically touch on two different policy areas: intellectual property and criminal law. Legal liability for digital platforms may arise from a user's vendor infringement of intellectual property rights. This is the case, for instance, when a vendor offers a counterfeit product that is in violation of trademarks, or uploads a video, song or text in violation of the author's copyright. More egregious conduct may amount to violations of criminal law, for example, if a user uploads a video calling for violence, publishes a deep-fake nude image of a celebrity, or issues a threat to or otherwise harms another person. A comprehensive framework on intermediary liability would cover both types of rules.





DTRR DATABASE METHODOLOGY

A. Data collection and review methodology

The DTRR data is based on the direct review of laws and regulations. The DTRR reflects the regulatory solutions as enshrined in laws, decrees, and other major legal instruments. The strict application of the traceability principle implies that, with the

two exceptions identified below, the data featured in the DTRR originates solely from the actual legal framework of the country in question. In a handful of cases, third-party sources reported on the existence of certain regulatory measures, yet no legal instru-

ment could be found to review, confirm, and *trace* back to that regulation; in those cases, no measure was recorded. Once collected, the legal instruments were carefully reviewed by a team of WB staff and consultants with legal expertise and background. Overall, the DTRR incorporated information from approximately 700 legal instruments and features over 5,200 references to specific provisions.

The data are current as of March 2024 and do not reflect any changes to the legislation after that date. Despite intensive efforts, there were some countries where information could not be gathered. On a few occasions, media or other sources suggested that legislation did exist, but it could not be found online. Because of these potential gaps, the database records missing regulations as “no provision was identified” under the relevant regulatory solution, rather than “no provision exists.” Should interested readers find gaps in the information, they are welcome to contact the authors.

i. Traceability to its original source

DTRR’s information is supported by direct reference to the legal instruments where they are featured. With a view to ensuring the quality of the information, each datapoint can be traced back to the specific provision, paragraph, and/or section number that provides for that specific regulatory solution in the country’s legal framework. For example, the data point indicating that *Argentina’s framework provides that electronic signatures issued abroad have the same legal effect as domestic electronic signature* stems from Article 16 of Argentina’s Digital Signature Law of 2001. Traceability information is readily available to interested parties through the download of the main database file.

“Traceability” ensures the accuracy of the information, and eases any corrections needed. Identifying the specific legal source of the information not only ensures the accuracy of the information but also allows for it to be quickly amended in case of reforms or new develop-

ments in the underlying regulatory framework. This feature is oriented to facilitating informed policy-making and identifying specific needs to improve or reform existing regulatory framework.

This feature sets the DTRR apart from survey-based and from web-scraping database.

While some databases attempt to complement indicator-based information with qualitative information about their sources, the main survey-based databases in the field focus on offering a quantitative index that measures the regulatory framework’s quality and offer little or no access information on the sources of those values. Databases focused on capturing information online (“web-scraping,” whether in an automated or manual way) rely instead on third party sources, such as news media, other databases, and online reports, rather than actual interpretation of the legal instruments. This has the advantage of capturing a much broader range of information, including on how those regulatory measures are applied in practice, but often misses the link to the underlying legal instruments and forces the users to trust the cited third-party source without the ability to verify it directly.

ii. Scope of the data collection

Some procedural steps constrained the scope of data collection for the DTRR. Like the proverbial needle, finding one specific measure that exists in the whole regulatory haystack of a given country can be a time-consuming exercise. To prevent an infinite search, the team adopted a standardized procedure that delivered substantial results while keeping the data collection effort at a feasible scale. The first step of data collection entailed reviewing a number of online databases, repositories, books, studies and similar services that offer legislative information on areas covered by the DTRR. Broad databases like [UNCTAD Cyberlaw Tracker](#), [OneTrust DataGuidance](#), [ECIPE’s Digital Trade Restrictiveness](#) database and the [Digital Trade Integration](#) database were particularly helpful in finding and accessing regulations. Over 20 other databases, some of them specific to

certain topics, like the [UN Global Survey on Digital and Sustainable Trade Facilitation the World](#) or [Intermediary Liability Map of Stanford University](#) were consulted in order to identify the country-specific regulations. Further, where no relevant regulation was identified through those selected databases, the team conducted thorough online research, starting with the official websites of the government as well as broad online searches for third-party information. In many cases, national news media, local law firms, or specialized blogs or articles contained information about whether certain legislation had been adopted, which then facilitated a more granular search. Ultimately, all instruments were taken from publicly available official online sources, mostly government websites such as official gazettes or repositories from specialized government agencies such as sectoral Ministries, data protection authorities, or consumer protection agencies.

Several substantive boundaries were set for the data collection and review. To keep the research feasible, the team applies specific criteria to limit the types of legislation included. These rules comprised:

1. **National / Federal disciplines:** except for the cases of three US states, California, New York and Texas, all legislation featured in the database are disciplines adopted at the national (federal) level. International agreements were not considered,⁶ nor were private industry standards and draft or proposed legislation.
2. **Primary and secondary legislation:** the broad regulatory research and collection effort focused on acts by Parliament / Congress and general decrees by the Executive branch. Ministerial-level regulations were not part of systematic review, but some instruments were considered if they were referred to by either other legal instruments or third-party sources. Court decisions were not considered as legal sources for data collection.

3. **Mandatory regulatory:** All instruments are laws or regulations of mandatory nature. Individual provisions, guidance instruments, or call for certain best practices that are only voluntary compliance were not included in the database. An exception to this rule was made for certain Japanese instruments, such as the “Guidelines for Operational Standards for Bandwidth Control” that are broadly considered mandatory instruments even though they do not feature specific sanctions.

The search was limited to certain types of laws that had been identified as generally featuring the relevant regulatory solutions. Table 4 provides an example for some of the laws that were typically reviewed for each regulatory area. In a handful of situations, certain loosely identified legislation in the media or government websites could not be found. As a result, and given the strict requirement for traceability guiding the data collection, it cannot be ruled out that some relevant pieces of legislation may have been missed, especially for middle- or low-income economies. On the other hand, the regulatory solutions that are mentioned are certainly in effect or would have become effective by June 30, 2024.

iii. Interpretation

The regulatory reviews were guided by a few principles focused on the intent behind the rules. While the database builds on the notion that certain key measures are at the basis of digital trade regulation worldwide, how those laws are drafted and incorporated into the regulatory framework can vary greatly. A same provision may be found featured as a mandate (“shall”) [“Trust services provided by trust service providers established in a third country *shall be recognised* as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union

6. OECD’s Index of Digital Trade Integration and Openness (INDIGO) tracks progress in international arrangements that matter for digital trade.

Table 4: Common legislative sources

	e-document/ e-signature	Online consumer protection	Data protection/ Cybersecurity	Intermediary liability
Law on electronic commerce/ transactions/ trade/exchanges	✓	✓	✓	✓
Digital economy law		✓		✓
Law on electronic communications	✓		✓	
Law on electronic documents	✓			
Law on electronic signature	✓			
Law on consumer protection		✓	✓	
Law on personal data protection			✓	
Law on cybersecurity			✓	✓
Digital security act			✓	✓
Law on information technology crimes				✓
Cyber/computer crimes act			✓	✓
Copyright act				✓
Information and communications act	✓			✓
Law on information society services	✓			✓
Civil code	✓			
Commerce code	✓	✓		
Evidence Act	✓			
Criminal code			✓	

where ...”⁷) or as a prohibition (“A data message, electronic document, electronic record or other communication *must not* be denied legal protection, effect, validity, or enforceability on the ground that it is in electronic form”⁸). Even a prohibition can be expressed through positive language (“It *shall be unlawful* for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity...”⁹), or negative language (“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs ... *shall be prohibited*.”¹⁰”),

or even neutral language but associated to a sanction. Reviewing thousands of regulatory measures from around the world in order to decide whether or not they meet one specific definition necessarily entails a cautious interpretative effort. Even a meticulous reading, however, cannot eliminate occasional doubts and some level of judgement value. Further, to limit the impact of such uncertainties and to make sure that all regulations were being assessed through the same lens, some teleological principles were defined to help the reviewers in the interpretation, namely:

7. Article 14, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
8. Article 5, Fiji Electronic Transactions Act 2008 (No. 26 of 2008).
9. Section 17941(a), Chapter 6, Part 3, Division 7, California Business and Professions Code.
10. Article 9, 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).

1. **Context:** when the language of the provision(s) was not clear enough to determine the answer to our question, context was taken into consideration. This includes the goal of the legislation, whether the legislation was following a given instrument (model law, other country's regulation, etc.). In addition, the position of the provision was considered, for example, what provisions are adjacent, what title and section the provision is housed under, among others.
2. **Governing Ministry/Agency:** the authority over the law will commonly have layman's explanations on their website via Q&As, blog posts, news reports, or short explanatory guides.
3. **Legal blogs and regulatory research websites:** big law firms and domestic specialty firms generally post short blogs regarding recent legislation as well as articles analyzing or describing legal developments. In addition, regulatory research websites (DTI, WIPO, Library of Congress) may have final conclusory data on regulations or links to explanatory texts.
4. **Pro-measure:** when, despite all other interpretative efforts, a provision (or combination thereof) left doubts about whether it in fact featured a specific measure, it was recorded as the regulation being in place—the most favorable interpretation for the country. The opposite is true for the handful of “negative” measures included in the database, particularly those related to cross-border data flows.

iv. Deviations I: Restrictions on cross-border data flows

International flows of machine-readable data are essential for digital trade, especially for trade in services (WDR2021). Specifically, cross-border trade in services relies on information traveling through telecommunications networks (i.e., digital data) to deliver the services from suppliers to consumers located around the world. Digital data plays a role digital services much like shipping containers do in merchandise trade: it serves as the medium for the content of the transaction to reach its consumer. Regulatory restrictions on the cross-border movement of

data are therefore the effective equivalent to direct restrictions on international trade on digital services.

Deviating from its own philosophy, the DTRR includes a set of restrictive regulatory solutions to cross-border data flows. Given the critical role that data flows play in digital trade, it was decided that regulatory restrictions on cross-border data flows, in particular limitations to cross-border transfers and data localization requirements, was inherent to a database focused on digital trade regulation. The DTRR section on cross-border regulations therefore deviates from other DTRR sections as it features both “positive” regulatory solutions that contribute to an enabling environment to digital trade, as well as “negative” regulatory solutions that entail limitations to cross-border data flows, thus hampering the ability to engage in services trade. Nineteen of the 34 regulatory measures collected under the section capture different types of limitations to cross-border data flows.

Regulatory restrictions on cross-border data are sandboxed for the purposes of analysis and visualizations of the regulatory environment. When assessing the progress and “readiness” of the regulatory framework for digital trade, restrictions on cross-border data were considered separately from all other data points in the data. Since the DTRR builds on the notion that a comprehensive and modern regulatory framework acts as an enabler for digital trade, broad analyses and descriptions based on the DTRR, especially aggregate comparative figures that describe the “readiness” to digital trade, effectively exclude all 19 datapoints on data restrictions from the visualizations and analysis. However, these data are brought to light when looking specifically at regulations on cross-border data flows, and wherever reference to data limitations is warranted.

v. Deviations II: Paperless Trade and Digital ID

Digitalization of border procedures play an essential role in facilitating cross-border trade, including

goods traded through e-commerce. Paperless trade refers to the digitalization of information flows required to support the international movement of goods, especially during custom procedures (WTO, 2022). Such procedures include the establishment of “single windows,” recognizing the electronic submissions of documents such as customs declaration, certificates of origin, and sanitary and phytosanitary certificates, as well as accepting electronic payments of custom duties and other fees. For e-commerce, this also includes adopting expedited channels and simplified procedures for processing parcels.

Regulations for paperless trade and digital ID span multiple regulatory levels, which required an exception in the DTRR methodology. While some disciplines relevant to paperless trade are often adopted as laws or decrees it is also often the case that those rules are adopted at lower levels of government, including ministerial declarations or directives from customs or other specialized agencies. Access to these lower-level regulations has proven particularly elusive, limiting the ability to review those regulations and “trace” the DTRR’s dat-

apoints to actual legal instruments, which is the rule for the database. Similarly, many digital ID systems may have been implemented through public-private partnerships, or contractual arrangements where a government may have hired a trust services provider to establish the digital identification system. Rules relating to whether national digital ID systems are accessible by private services providers may have been codified at a departmental level, either as a departmental directive or internal rules of the governmental agency. Considering these challenges in data collection, and taking into account the importance of paperless trade for trade in goods, including those traded through e-commerce, it was decided to deviate from the DTRR “traceability” approach with regard to two regulatory solutions (out of the three covered in that section). Two questions on paperless trade have therefore been answered based on information provided in the UN Global Survey Digital and Sustainable Trade database, in cases without identifying the specific regulations that supports those results. Future revisions of the DTRR database are expected to improve this methodology to be able to trace regulations in this section.

B. Geographical scope

The DTRR database covers 121 economies, including 118 countries and 3 sub-federal states. Countries were selected to ensure broad coverage across all world regions and levels of development, as shown in Table 5 below. The 121 economies include three states of the United States, California, New York, and Texas. These three states were included in the regulatory review to capture the

regulatory differences that are the result of the US federal system, which grants states jurisdiction to regulate various areas relevant to digital trade, such as data governance and consumer protection. The three US states were selected given their size and influence of tech firms (California, Texas) and their global role as a dispute resolution hub for international contracts (New York).

C. Caveats

When using the DTRR database, it is important to be aware of its limitations. Reviewing laws and

regulations from across the globe required certain compromises to make the data suitable for

Table 5: Economies covered in DTRR database^a

	Low income	Lower-middle income	Upper-middle income	High income	Totals
East Asia and Pacific		Cambodia, Lao PDR, Myanmar, Papua New Guinea, Philippines, Samoa, Solomon Islands, Vanuatu, Viet Nam	China, Indonesia, Fiji, Malaysia, Mongolia, Thailand	Australia, Japan, Korea, New Zealand, Singapore	20
Europe and Central Asia		Kyrgyz, Rep., Tajikistan, Uzbekistan	Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Georgia, Kazakhstan, Kosovo, Moldova, Montenegro, North Macedonia, Serbia, Türkiye, Turkmenistan, Ukraine	Croatia, Czechia, Estonia, France, Iceland, Latvia, Lithuania, Norway, Russia, Slovenia, Switzerland, U.K.	30
Latin America & the Caribbean		Bolivia, Haiti, Honduras, Nicaragua	Argentina, Belize, Brazil, Colombia, Costa Rica, Dominican Republic, El Salvador, Jamaica, Mexico, Peru	Chile, Panama, Uruguay	17
Middle East & North Africa		Egypt, Morocco, Tunisia	Algeria, Iran, Iraq, Jordan, Lebanon	Bahrain, Israel, Kuwait, Oman, Qatar, Saudi Arabia, UAE	15
North America				Canada, United States, U.S. – California, U.S. – New York, U.S. – Texas	5
South Asia	Afghanistan	Bangladesh, Bhutan, India, Nepal, Pakistan, Sri Lanka	Maldives		8
Sub-Saharan Africa	Burkina Faso, C.A.R., Chad, D.R.C., Ethiopia, Liberia, Madagascar, Rwanda, Sierra Leone, Somalia, South Sudan, Uganda	Angola, Benin, Cameroon, Congo Rep., Cote d'Ivoire, Ghana, Kenya, Nigeria, Senegal, Tanzania,	Botswana, Gabon, Mauritius, South Africa		26
Totals	15	36	38	32	121

^a Categories are based on World Bank regional and income and classification for 2025–2026. Available at <https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups>

tabulation and user-friendly comparison. These compromises affect how the information is collected, reviewed, and presented, and should be considered when interpreting the database.

i. Sub-set of regulation

The exercise did not review the entirety of

laws and regulations enacted by all covered countries. Collecting and reading every legal instrument in the world would make for a very accurate, but unfortunately not a cost-efficient database. The data collection was thus based on a specific procedure and sub-set of regulations likely to deliver comprehensive and reliable results within a reasonable effort and budget—as

explained in Section 3. This means that there may be some regulatory measures in place that have not been recorded in the database. In fact, in a few cases (less than a handful) there were third-party reports indicating that some measures were in place, but no legal instruments could be found to support that information. Users of the DTRR be aware that different methodological decisions carry certain implications.

Regulatory solutions may exist beyond those featured in the DTRR. This may be the case especially for low-income countries who have not digitalized their legal information. Further, some regulatory areas, like paperless trade, consumer protection, and questions on digital ID, are often governed by decrees or ministerial directive or guidelines that are less likely to be made available online. However, given the breadth of the review, it is possible that specific regulatory measures were missed, but unlikely that instruments governing entire regulatory areas were omitted.

ii. Legal interpretation

Interpreting regulations, especially from foreign legal instruments, is not an exact science. The interpretations of regulations, especially when read directly from legal instruments, invariably involves a degree of subjectivity. As a result, it is possible that the reviewers misread, and thereby misclassified the information. The reviewing team sought to mitigate this risk by ensuring that their reading was in line with other literature as well as the classification in other databases. In particular, the team collaborated closely with the authors of the Digital Trade Integration Project¹¹—the online database most closely related to DTRR—to ensure that interpretations were aligned. However, some regulatory measures may be interpreted differently across databases, or in comparison to how they are intended in the source country.

iii. Implementation / *de facto* Regulation

The dataset does not account for the implementation or enforcement of existing legislation. The information reflected in the database focuses on *de jure* regulatory solutions as captured in mandatory legal instruments. The data does not capture whether or how those measures are being implemented, or whether other informal *de facto* measures apply. This limits the understanding of the effective regulatory framework applying to digital trade, especially in middle- and low-income countries with weak governance practices, where the gaps between written rules and actual enforcement and monitoring practices by government agencies is often substantial. Some studies have focused on assessing implementation and enforcement of regulations on specific policy areas, such as on consumer protection (OECD, 2018), based on surveys or questionnaires answered by policymakers or practitioners. On the contrary, this “weakness” of the DTRR of capturing only *de jure* information is the result of its methodological approach to strictly feature data directly referenced to formal regulatory instruments, ensuring “traceability” of the information.

iii. Different legal systems

It is important to note that the DTRR does not account for differences in legal systems or the various sources of law they may recognize. Instead, it focuses exclusively on written laws and regulations adopted by legislative or executive bodies. Legal systems around the world differ in the sources they recognize for establishing general rules. One key distinction is between civil law and common law traditions. Civil law systems rely primarily on written instruments—laws and regulations enacted by legislatures or, in some cases, adopted by the executive branch under specific conditions. In contrast, common law systems, while also recognizing written legislation, give legal weight to judicial decisions. These decisions,

11. <https://dti.eui.eu/>.

particularly those issued or affirmed by higher courts, contribute to a body of jurisprudence that evolves through precedent.

Another layer of variation arises from how power is distributed within a country. In federal systems, legal authority is shared across multiple levels of government—such as federal, state, or provincial—whereas unitary systems centralize power at the national level. Additionally, some jurisdictions incorporate customary law, which derives from long-standing local traditions or the authority of local or religious leaders. Given the diversity of legal traditions globally, the DTRR standardizes its approach by focusing exclusively on written laws and regulations—typically those adopted by the legislative or executive branches—rather than attempting to account for all possible sources of legal authority.

In practice, few differences exist when it comes to technical economic regulations. The review of

regulations on digital trade did not yield major differences between countries featuring these different legal systems. Economic regulations, specifically those focused on digital transactions, are only marginally affected by customary or religious rules, which tend to govern more traditional legislative aspects, like the criminal and civil justice—in fact, countries based on a customary or religious system also tend to adopt written rules on more modern and complex aspects of legislation, including digital trade. Indeed, the review did not find significant differences between common-law and civil-law systems. Granular matters related to market regulations are rarely regulated through judicial decisions, especially in technical issues like electronic transactions, cybersecurity, or data protection. In fact, comprehensive regulations were found in all regulatory areas in the common law countries under review. However, in common law systems, certain regulatory solutions may not be explicitly written into legislation if they are already established through judicial decisions. As a result, the DTRR may under-

Box 3: Federalism versus unitary systems of government

When gathering laws, the issue of federalist countries commonly gets brought up. This is because most countries in the world subscribe to a unitary form of government, which means that there is one central legal framework that rules over the country. Gathering laws on unitary forms of government is, therefore, much simpler than the alternative—countries that subscribe to federalism. Federalism breaks apart the single system of government into a tiered system, which is usually a state or provincial level and a federal level. In a federal system, both state and national governments hold legal authority. Because states can pass their own laws, a single country may have legal differences across jurisdictions. However, state laws cannot conflict federal laws, which take precedence.

To ensure that a uniform application of the laws was applied when gathering data on the countries, the review did not include data below the federal level. Including laws from state or provincial levels could result in conflicting rules across jurisdictions or inconsistent legal coverage, as not all subnational entities adopt similar legislation. Thus, only federal legal rules were counted: national laws, national regulations, executive/legislative/federal agency decrees, and binding federal agency rules.

However, a case study on the United States was performed to better understand the impact of federalism in a large digital economy. Three states were studied based on the size of their large economies: California, New York, and Texas. All three states include data from both federal and state-level laws, offering a more robust picture of how federal systems function in practice. The findings only significantly differed over new legislation, such as data protection, AI, and cybersecurity. Logically, these findings match with predictions likely because state governments tend to move faster than federal governments that have more competing interests.

count some areas of regulation in these systems. This is particularly relevant for consumer protection and intermediary liability, which is often shaped by long-standing case law on commercial matters, even outside of digital contexts. Still, the decision to adopt comprehensive online consumer protection regulation appears to reflect policy choices more than legal tradition, as some common law countries—such as the United Kingdom—have introduced extensive statutory frameworks in this area.

v. Presenting regulatory “Readiness” trends: quintiles

Regulatory “readiness” to digital trade hinges on a comprehensive and modern legal framework, more than specific regulatory solutions.

An enabling legal environment for digital trade depends on providing effective measures to tackle the novel challenges of digital, international markets. These challenges are addressed by specific regulatory solutions like the ones captured in the DTRR. However, few regulatory measures are by themselves determinants of an enabling environment for digital trade; instead overcoming the challenges of digital markets typically require a set of various interrelated regulatory measures contrib-

uting to the overarching policy goal. For example, multiple regulatory measures can act as safeguards for personal privacy, including explicit limitations on the legal basis for data collection and processing, ensuring a right to access such information by data subjects, the “right for be forgotten,” and specialized and stricter rules on biometric data; while all these measures contribute to the same, the absence of one or some of them does not necessarily make it a poor framework. As a result, when assessing the “readiness” of given regulatory area it is important to consider the regulation as a whole rather than the presence or absence of a specific safeguard.¹²

Graphs based on categories, rather than specific values, help visualize this approach.

To reflect the importance of looking at regulations broadly, rather than merely counting regulatory solutions, it is advisable that analyses based on the DTRR data be best featured in stepped categories of regulatory progress. The DTRR website, for example, portrays regulatory readiness in five categories (quintiles) depending on the percentage of positive answers to the regulatory solutions considered in each regulatory area.

D. Next steps

i. Data update and validation

The DTRR database will maintain accuracy and relevance through structured updates, expert collaborations, and community feedback.

Ensuring the accuracy and timelessness of the DTRR database is important for its efficacy and reliability. A structured strategy will be implemented for data update and validation, including periodic data audits and real-time updates. This strategy

will involve collaboration with international trade experts, stakeholders and regulatory authorities to continuously source and verify new data. In line with the latest development of technologies, a combination of automated data scraping techniques and expert review panels may be adopted to keep the database comprehensive and up to date. Additionally, a user-feedback system will be introduced, allowing users to report discrepancies or outdated

12. When assessing *restrictions on* digital trade, rather than enabling regulatory solutions, the opposite is true. A comprehensive “enabling” framework may be effectively spoiled by the presence of just one regulatory restriction, particularly if it entails a major limitation, such as pre-approval requirements for cross-border data transfers.

information, thereby creating a community-driven verification process that enhances the database's integrity and utility.

ii. Expansion of data coverage

To further enhance the value of the DTRR database, strategic expansion of data coverage will be crucial. This expansion will seek to include newer areas of digital trade that gain prominence, such as regulations around electronic payments, digital taxation, competition between online platforms, e-commerce logistics, paperless trade, customs regulations and the implications of artificial intelligence. By integrating these emerging sectors, the database will offer insights into the fast-evolving landscape of digital trade.

Moreover, the database will expand to include additional countries, focusing on those in emerging markets which are increasingly influential in the global digital economy. Broadening the coverage of these regions will provide a more comprehensive global perspective on digital trade regulations.

Additionally, the questionnaire within the topic areas will also be extended to address these new topics, incorporating additional questions that reflect the latest technological developments. This will ensure the database not only captures a wide range of regulations but also remains at the forefront of digital trade issues.

iii. Uses

The DTRR database is a dynamic platform that provides stakeholders from various sectors with critical insights and data to shape and enhance digital trade policies globally—supporting legal, economic, and policy development. The DTRR database is designed to be an instrumental resource for a diverse array of stakeholders, including developing countries, academic researchers, digital trade companies, and others engaged in the realm of digital trade.

The DTRR database serves as an invaluable tool for policymakers and regulatory bodies in developing countries by providing access to a comprehensive repository of digital trade regulations from around the world, including various level of income group regions. The database offers insights into current practices and regulatory frameworks that have been successfully implemented elsewhere. It can guide the formulation and refinement of their own digital trade policies, fostering an environment conducive to digital economic growth and integration into the global digital economy.

Researchers and scholars may find the DTRR to be a valuable resource for comparative legal studies, policy analysis, and socio-economic research related to digital trade. Its broad coverage of regulatory approaches offers an empirical foundation for academic work, policy development, and teaching materials. The database also supports the exploration of trends, patterns, and regulatory outcomes across jurisdictions.

Other stakeholders—including legal practitioners, international trade organizations, and consumer advocacy groups—can use the DTRR to monitor regulatory developments, anticipate changes in legal frameworks, and engage more effectively in policy discussions. Its detailed insights may also support advocacy efforts by providing evidence to inform digital regulation that balances trade facilitation, consumer protection, and innovation.

iv. Analytical and Quantitative work

The database offers comprehensive regulatory data and analytical resources, assisting stakeholders in effectively developing and implementing informed digital trade policies. The DTRR database serves as both a comprehensive repository of global digital trade regulations and a robust analytical tool that transforms raw data into actionable insights. This dual functionality makes the DTRR database an indispensable resource for pol-

icymakers, industry experts, and researchers focused on the intricacies of digital trade. In practical terms, the database supports detailed analysis of digital trade practices by providing users with access to extensive regulatory information from various countries and sectors. This enables users to conduct comparative analyses, identify regulatory trends, and benchmark against global standards. Companies engaged in cross-border e-commerce, for example, can analyze entry requirements, consumer protection laws, and data privacy regulations across multiple jurisdictions to effectively strategize their market expansion plans.

Based on the previous work done for WDR2021, a deeper analysis of cross-border data transfer regimes can be effectively conducted using the DTRR database. The comprehensive insights and foundational frameworks established in WDR2021 provide a solid groundwork for further exploration. By leveraging the extensive data and detailed regulatory information within the DTRR database, researchers and policymakers can gain a nuanced understanding of how different regulatory regimes impact the flow of non-personal data across borders. This analysis is crucial for identifying best practices, potential barriers, and opportunities to enhance global digital trade and data governance.

Additionally, the DTRR database enables users to model and predict the effects of regulatory changes on their economies or businesses. This functionality supports scenario analysis, risk assessment, and economic impact studies, which are crucial for making informed decisions. By quantifying the potential effects of new regulations,

users can develop strong business strategies and policy frameworks that proactively address market developments.

Access to comprehensive regulatory data allows policymakers to compare their national frameworks with those of other countries, facilitating insights into areas of strength and potential improvement. This capability supports evidence-based policymaking and aids in the development of policies that promote a competitive and efficient digital trade environment. It also enables policymakers to align their regulations with global best practices and international standards, ensuring that their legal frameworks support digital trade while safeguarding consumer rights and promoting data security.

V. Feedback

Recognizing the importance of user input in the continuous development and refinement of the DTRR database, a comprehensive feedback system will be implemented. This system will include regular user surveys and an open channel for ongoing comments and suggestions. Feedback collected through these mechanisms will be systematically reviewed and used to guide updates and enhancements to the database, ensuring it remains relevant and useful. The goal is to establish a development process centered around users, involving them directly in the evolution of the database. This strategy not only enhances the accuracy and relevance of the database but also builds a sense of community and ownership among users, ultimately improving their experience and satisfaction.



4C

LOOKING AHEAD

One day, people will wonder how global trade was even possible before goods and services were seamlessly bought and sold in global digital markets without regard to or even knowledge of where vendors were located. We are not there yet. For the time being, digital trade offers a mixed picture across countries and sectors. In some countries it is thriving, and in others it is still a new, unusual

experience. While some areas of regulation evolve quickly in response to new technologies, others lag behind or struggle to adjust to the pace and complexity of digital change. And, for the most part, digital trade is smooth and effective until something goes wrong, and then it becomes chaotic and hopeless as entailing strong reputational damages.

The DTRR and similar tools contribute to building a global enabling framework for digital trade by helping to identify regulatory gaps, good practices, and regulatory restrictions. For example, DTRR data can help identify regulatory gaps in a given country, provide visual summaries of digital trade policies, and identify where domestic storage and processing requirements exist—and for which sectors.

Some policy areas, such as artificial intelligence or aspects of paperless trade, are still in early stages of regulatory development. Tools like the DTRR can support these emerging areas by offering a clearer picture of current practices and helping guide more consistent and informed policymaking.

This new data also gives rise to further analytical questions. The regulatory research prompts additional questions that can help expand the understanding of regulations and their relationship with international trade. Some of these questions can be addressed through economic empirical analysis:

- *How do these regulations affect the digital trade ecosystem?*
- *Which of these regulatory areas are more relevant for digital trade in goods, services, etc.?*
- *Does a comprehensive and modern digital trade regulatory framework foster investment in digital business and innovation?*

Other research may build upon the DTRR data to further understanding of the enabling legal and institutional environment for digital trade. Some relevant questions to be explored in that sense include:

- *What are the institutional capacity needs behind digital trade regulation?*

- *What digital trade regulations and institutions fit best given the limited capacity (human and financial) of many developing countries and LDCs?*
- *How may private sector initiatives such as codes of conduct complement, or even replace, binding rules like the ones covered in the DTRR database?*

As digital technologies continue to advance and expand, there is little doubt that digital trade will follow—and so will regulation. Regulation on digital trade will continue to play catch-up with reality, one hopes in a way that fosters integration at a global level and inclusion and growth at the local level. Understanding how to achieve those goals, especially in the developing world, cannot wait.

The DTRR and similar tools help advance a global enabling framework for digital trade by identifying regulatory gaps, good practices, and restrictions. However, the lack of policy coordination across countries poses a risk of regulatory fragmentation. If countries develop isolated digital trade frameworks, this could lead to marginalization of certain economies and the formation of suboptimal regulatory blocs that hinder seamless cross-border digital transactions.

To avoid this, fostering international regulatory cooperation is essential. Alignment with global best practices—through multilateral agreements (e.g., WTO e-commerce negotiations), regional initiatives, or bilateral dialogues—can help ensure a cohesive and inclusive digital trade ecosystem. Such coordination is crucial in preventing trade inefficiencies, reducing compliance burdens, and enabling all economies to fully benefit from the digital economy.

Bibliography

CIGI-Ipsos Global Survey on Internet Security and Trust 2017.

IMF, OECD, UNCTAD and WTO (2023), *Handbook on Measuring Digital Trade, Second Edition*, OECD Publishing, Paris/International Monetary Fund/UNCTAD, Geneva 10/WTO, Geneva, <https://doi.org/10.1787/ac99e6d3-en>.

Ferracane, M. F., & van der Marel, E. (2018). Do data policy restrictions inhibit trade in services? ECIPE DTE Working Paper Series No. 2. European Centre for International Political Economy. <https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/Ferracane>, Martina Francesca and Erik van der Marel. 2021. Regulating Personal Data: Data Models and Digital Services Trade. Policy Research Working Paper; No. 9596. © World Bank, Washington, DC. <http://hdl.handle.net/10986/35308> License: CC BY 3.0 IGO.”

Ferracane, Martina and Erik van Der Marel 2021b. Do data policy restrictions inhibit trade in services?. *Rev World Econ* 157, 727–776 (2021). <https://doi.org/10.1007/s10290-021-00417-2>.

Gasser, Urs and Schulz, Wolfgang, Governance of Online Intermediaries: Observations from a Series of National Case Studies (February 18, 2015). Berkman Center Research Publication No. 2015-5, Available at SSRN: <https://ssrn.com/abstract=2566364> or <http://dx.doi.org/10.2139/ssrn.2566364>.

National Board of Trade (NBT), 2015, “No Transfer, No Production—a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods”.

OECD, 2018, “Consumer protection enforcement in a global digital marketplace”, OECD Digital Economy Papers, No. 266, OECD Publishing, Paris, <http://dx.doi.org/10.1787/f041eead-en>.

OECD, 2000. Guidelines for Consumer Protection in the Context of Electronic Commerce. Paris: OECD.

Strusani, Davide, and Georges Vivien Hounghonon, 2019, The Role of Artificial Intelligence in Supporting Development in Emerging Markets, FCI, Encompass n° 69, July 2019.

UNCTAD, 2017. Consumer Protection in Electronic Commerce: A Note by the UNCTAD Secretariat. Geneva: United Nations.

UNECE and WEF 2017: Paperless Trading: How Does It Impact the Trade System?.

USITC, 2014, “Digital Trade in the U.S. and Global Economies”, available at https://www.usitc.gov/publications/industry_econ_analysis_332/2013/digital_trade_us_and_global_economies_part_1.htm.

World Bank, 2016. “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation”, available at <https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf>.

World Bank, 2020. “Payment Systems Worldwide – A Snapshot: Summary Outcomes of the Fifth Global Payment Systems Survey”.

World Bank, 2021. World Development Report 2021: Data for Better Lives. Washington, DC: World Bank. doi:10.1596/978-1-4648-1600-0. License: Creative Commons Attribution CC BY 3.0 IGO.

World Bank and United Nations. 2017. Combating Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

World Economic Forum, 2019. The Global Governance of Online Consumer Protection and E-Commerce. Retrieved from World Economic Forum: http://www3.weforum.org/docs/WEF_consumer_protection.pdf.

Annex I:

List of Regulatory Solutions Captured in DTRR Database

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
ELECTRONIC DOCUMENTS						
1.	Electronic communications are legally valid.	Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message. The form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. ¹	Communications can mean a variety of things. Specifically, for this question, the purpose is to find whether the law specifically recognizes data messages.	- Electronic Transactions Act - Evidence Act	"7. An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is— (a) rendered or made available in electronic form; or (b) not contained in the electronic communication purporting to give rise to such legal effect, but is referred to in that electronic communication." Belize Electronic Transactions Act 2021, Section 7 <i>The provision clearly states the validity of electronic communication, and thus applies to the question at hand.</i>	"84(1). In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question." Nigeria Evidence Act 2011, Section 84(1) <i>The provision only applies to electronic evidence that would transcribe or record oral evidence. Because of its limited scope, the provision does not apply.</i>
2.	Electronic contracts have the same legal effect as paper-based documents	Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose. This is a key step in facilitating electronic transactions, as parties to this type of transaction are usually at different locations. This also boosts the efficiency of ports and customs borders. ²	The purpose is to find a provision which specifically states that contracts can be formed by electronic messages, i.e., the offer and acceptance can be expressed electronically.	- Electronic Transactions Act - Law on E-Commerce	"Where a data message is used in the formation of a contract, such contract shall not be denied validity or enforceability on the sole ground that a legal stamp has not been affixed or has not been attested by witnesses." Bhutan Information Communications and Media Act 2018, Art. 284 <i>The provision applies because the contract formation over electronic means is legally valid.</i>	"Automated Transactions. A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed each of the individual actions carried out by the automated message systems or the resulting contract."

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
3.	Specific provision provides detail on the admissibility of e-documents as evidence	The provision should stipulate that information in the form of a data message shall be given due evidential weight. A provision which prescribes validity for admissibility of e-documents as evidence prohibits judicial authorities from demanding original physical copies of e-documents or treating electronic records as being intrinsically unreliable. ³	A mere statement of admissibility is insufficient. The document must outline criteria for a court to determine its legal validity. Instructions may take the form of limiting the grounds on which the probative value of data messages can be questioned, such as, reliability of the manner in which the data message was	- Law on Electronic Documents - Law on Electronic Signatures	“Formation and validity of contracts 15 (1) In the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records. (2) As between the originator and the addressee of an electronic record, a declaration of intention or other statement or delivery of a deed is not to be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.” Republic of Vanuatu, Electronic Transactions Act No. 24 of 2000, Section 15 <i>Here, the provision specifically states the formation of a contract may occur via electronic means, and thus applies.</i>	Afghanistan Law On Electronic Transactions and Signatures 2020, Art 20 <i>The provision merely applies to automated transactions and is thus too narrow to apply to the question at hand.</i>
					“ARTICLE 11. – Original. Electronic documents signed digitally and those reproduced in digital format digitally signed from first-generation originals in any other medium, will also be considered originals and, as a consequence, have probative value as such, according to the procedures determined by the regulations.” Argentina Digital Signatures Law 2001, Art. 11	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
4.	The law should remain neutral with respect to the storage of e-documents	It is not appropriate to require that information be stored in its original unaltered form, as messages are often decoded, compressed or converted in order to be stored. ⁴	The provision sets out technology-neutral criteria, which, if satisfied, are deemed to fulfill the legal obligation to retain documents.	- Electronic Transactions Act - Law on E-Commerce	This example works because Art. 12(2) specifies what the court must take into account to permit admissibility. “Article 8: Requirements to retain information in original form A legal requirement to retain information that was not made electronic form may be fulfilled by the retention of such information in electronic form if: 1. Such electronic form is a reliable means to determine the completeness of the information; and 2. Such information is easily retrievable for subsequent use.” • Cambodia Law on Electronic Commerce Art. 8 The provision is sufficient to establish technologically neutral principles.	While the text does give the ability to admit an electronic document, it does not provide detail on how to admit electronic documents and thus does not answer the question at hand. “Article 14. Information storage 1. The service provider, who protects the information provided by the recipient at the request of the service recipient, shall not be liable for it if: 1) does not have factual information about the recipient’s illegal activities or that the information provided by the recipient has been obtained, created, modified or used in an illegal manner and, when claiming damages, is not aware of the facts and circumstances indicating the recipient’s illegal activities or that the recipient of the service provides information obtained, created, modified or used in an unlawful manner; 2) upon learning or receiving knowledge about the illegal activities of the service recipient or about the fact that the information provided by the service recipient has been acquired, created, modified or used in an illegal manner, take immediate action to eliminate the possibility of accessing such information.”

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
ELECTRONIC SIGNATURE & DIGITAL ID						
5.	Electronic signatures are legally valid	Countries may provide certain functional criteria for the legal recognition of electronic signatures irrespective of the technology used. This is also known as the minimalist/permissive approach. Laws that require the use of specific technologies such as encryption to recognize the validity of the signature (prescriptive approach) would not meet this requirement. ⁵	This question is aimed at finding explicit and direct language within the law which states that electronic signatures are accepted regardless of the technology utilized. However, although all digital/advanced signatures are electronic signatures, not all electronic signatures are digital signatures. Therefore, the purpose of the question is to see if the basic tenet of recognizing electronic signatures is in place. Please note that different regulations use definitions of “digital” and “electronic” signatures to prescribe different levels of reliability of different electronic/digital signature. The definition of “digital” and “electronic” signatures is only one of the factors to be considered while answering the question.	- Electronic Transactions Law - Electronic Signatures Law - Digital Signatures Law	“Section 5. Subject to the provisions of this Act, an electronic signature shall not be denied legal effect, validity or enforcement solely on the grounds that it is in electronic form.” [Read with] “Section 25. (1) An electronic signature shall be considered to be reliable for the purpose of satisfying the requirements of this Act where - (a) the signature creation data is, within the context in which it is used, linked to the signatory and to no other person; (b) the signature creation data was, at the time of signing, under the control of the signatory and of no other person; (c) any alteration to the electronic signature, made after the time of signing, is detectable; and	Lithuanian Republic of Information Society Services Law 2006, Section 14 <i>The provision here applies to service provider liability and, thus, does not create rules on neutrality.</i>
					“Section 2. For the purposes of this law and its implementing instruments, the following terms shall mean: “Electronic Signature: Signature obtained by an asymmetrical encryption algorithm that helps to authenticate the sender of a message and verify the integrity thereof;” Cameroon Law No. 2010/021 of 21 December 2010 on Electronic Commerce, Section 2 <i>The definition of an electronic signature is the definition of a digital signature. As this creates a higher standard of encryption, the provision does not apply to the question regarding basic electronic signatures.</i>	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
6.	Certificates issued by a qualified certification authority (CA) or using specific technology have the same legal status as handwritten signature	This provision creates a benefit in favor of certain techniques involving certificates issued by qualified certification authorities, which are recognized as particularly reliable, irrespective of the circumstances in which they are used. This ensures that, where any legal consequence would have flowed from the use of a handwritten signature, the same consequence should flow from the use of a reliable electronic signature.	This question may be answered in two ways: that a qualified authority's certification gives the same legal status as a handwritten signature, or that a specific technology gives the same legal status as a handwritten signature. The purpose of this question is to discover if advanced/digital signatures are legally recognized to be secure.	• Electronic Transactions Law • Electronic Signatures Law • Digital Signatures Law	(d) the purpose of a legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. (2) Subsection (1) shall not limit the ability of any person - (a) to establish in any other way, for the purpose of satisfying the requirement referred to in section 6, the reliability of an electronic signature; or (b) to adduce evidence of the non-reliability of an electronic signature.” • Botswana Electronic Communications and Transactions Act, 2014, Sections 5, 25 <i>The two provisions, when read together, create legal validity for electronic signatures.</i>	“10. Signature Requirement for signature (1) If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if: (a) in all cases—a method is used to identify the person and to indicate the person's intention in respect of the information communicated; and (b) in all cases—the method used was either: (i) as reliable as appropriate for the purpose for which the electronic communication was generated

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
		E-signatures that don't meet this requirement are recognized as valid, but not given additional probative value (hybrid/tiered approach). ⁶	Provisions that treat all verification techniques the same—without distinguishing among them—do not qualify as an affirmative response to this question.		Article 9. Equivalent value. Documents and communications signed by digital signature will have the same value and probative value as their equivalent signed in manuscript. In any legal regulation that requires the presence of a signature, both digital and handwritten signatures will be recognized in the same way. Electronic public documents must bear a certified digital signature.” Costa Rica, Decree No. 8454, Law of Certificates, Digital Signatures, and Electronic Documents, 2005, Articles 8,9 Article 8 sets out the requirements for a digital signature that match with the higher encryption standards of one, and Article 9 specifically provides a digital signatures equivalency to handwritten signatures. These provisions sufficiently answer the question.	or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence; and (c) if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements—the entity's requirement has been met; and (d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a).” Australia, Electronic Transactions Act, 2009, Section 10 Although the provision provides that signatures via electronic communications are sufficient to conclude contracts, the provision does not specifically apply to digital signatures as the language of the text is too broad.

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
7.	Digital signatures with a valid certificate are afforded a rebuttable presumption, regardless of certification provider or technology used	The presumption provides legal certainty that a recognized digital signature method—when supported by a valid certificate—carries the same legal effect as a handwritten signature. Without such a provision, courts may require signatures to meet a subjective standard of being “as reliable as appropriate,” creating unpredictability in enforcement. A rebuttable presumption ensures that, in the absence of a dispute over identity or intent, the signature is deemed valid. Legislation may allow parties to use any technology of their choice (permissive approach) or offer additional liberties for parties to adopt technologies or certification providers beyond those officially prescribed (hybrid + approach). ⁷	This question first seeks to know whether digital signature certificates get a presumption of their validity. The “regardless” part of this question means that the type of acquisition of the digital certificate does not matter; there still needs to be some sort of certification provider or technology used to get the classification of a valid digital signature.	- Electronic Transactions Law - Electronic Signatures Law - Digital Signatures Law	“Article 28. Qualified certificates for electronic signatures 1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I. 2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I. 3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures. 4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.” EU Regulation No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market Art. 28 <i>The provision creates a presumption of validity when the text states that no further measures of investigation shall be taken for a qualified certificate.</i>	“Signature. 14(1) If, under any written law in Fiji, the signature of a person is required, or if a written law provides consequences for the absence of a signature, that requirement is taken to have been met in relation to an electronic communication, where – a. a method involving an electronic signature is used by or with the authority of the person to identify the person's and to indicate the person's intention in respect of the information communicated; b. the person to whom the signature is required to be given consent to that requirement being met by way of the use of the method mentioned in paragraph (a); c. the method – (i) having regard to all the relevant circumstances including any relevant agreement, as reliable as appropriate for the purposes for which the information was generated or communicated; or (ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together further evidence; and d. any further requirements prescribed by regulations have been met.” Fiji Electronic Transactions Act, 2008, Article 14 <i>The provision applies to electronic signatures and does not indicate the need for a higher standard of encryption. Thus, as the presumption applies to electronic signatures, the provision does not apply to the question at hand.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
8.	Foreign digital signatures are granted the same legal effect as domestic signatures	While many countries digital signature certificates to be issued by licensed domestic authorities, cross-border commerce demands broader recognition. To support international transactions, legislation should recognize digital signatures based on certificates issued by foreign certification providers, even if those providers are licensed elsewhere. ⁸	This provision establishes a mechanism for recognizing foreign-issued digital certificates, allowing domestic authorities to accept them as legally valid for digital signatures.	- Electronic Transactions Law - Electronic Signatures Law - Digital Signatures Law	"Foreign Electronic Certificates Article 14 – The legal effects of electronic certificates issued by any Electronic Certificate Service Provider established in a foreign country shall be recognized under international agreements. In case that electronic certificates issued by any Electronic Certificate Service Provider established in a foreign country are recognized by an Electronic Certificate Service Provider established in Turkey, such electronic certificates are deemed to be Qualified Electronic Certificates. The Electronic Certificate Service Provider established in Turkey shall be liable for any damages arising from use of those electronic certificates." Turkey Electronic Signature Law, 2004, Article 14 <i>The provision uses language that answers the question directly and thus applies.</i>	N/A
9.	The national digital ID system is accessible by private services providers.	Digital services providers can benefit from accessing the national digital ID systems to validate the identity of their consumers. Many well-functioning digital ID systems only share information between the government and the citizen. However, access by private service	This question can be answered in two ways: (i) a provision which indicates or implies that private service suppliers have access to the national digital ID system; (ii) text from the website of the national digital ID system which indicates the same.	- National Identity Registration Act - Text from the official websites of National Digital ID systems	"8. (1) The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
9.		providers to national digital ID systems can benefit customers by enabling access to key services which usually require identity validation, such as banking or telecom services. ⁹			be specified by regulations.” • India, The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act, 2016, Section 8 <i>The provision directly answers the question by giving private entities the ability to authenticate an ID by requesting authentication from the authority.</i>	
10.	Restrictions exist on the numbers and types of services that may use of the national digital ID system for authentication.	Governments may wish to regulate the types of service providers who have access to the personal data of its citizens in the interest of public safety, national security and integrity of national databases. If every website and any service can subscribe to the digital identity system, there is a risk of watering down the value of the identity, and this can lead to a higher incidence of identity fraud or identity theft. ¹⁰	This question applies to any provision which seeks to limit the number and types of service providers which can access the national digital ID system.	- National Identity Registration Act - Text from the official websites of National Digital ID systems	“8. (2) A requesting entity shall— (a) unless otherwise provided in this Act, obtain the consent of an individual before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations; and (b) ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication. (3) A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication, the following details with respect to authentication, namely:	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
					(a) the nature of information that may be shared upon authentication; (b) the uses to which the information received during authentication may be put by the requesting entity; and (c) alternatives to submission of identity information to the requesting entity. (4) The Authority shall respond to an authentication query with a positive, negative or any other appropriate response sharing such identity information excluding any core biometric information.” India, The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act, 2016, Section 8 <i>The provision applies because it creates a barrier between private entities and the exact details of personal information on the citizen. Thus, the provision applies to the question at hand.</i>	N/A
PAPERLESS TRADE						
11.	Electronic Single Window policy exists for customs procedures	An electronic single window system can decrease search times, reduce capability dependencies and lower transaction costs for parties to a cross-border transaction. ¹¹	The question may be answered by referencing the UNESCAP database.	- Electronic Single Window websites, - UNESCAP database	N/A	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
12.	Electronic transferable records are functionally equivalent to paper-based transferable document or instruments	Certain commercial documents are transferable, i.e., they incorporate the entitlement to the delivery of goods that they describe (e.g., bills of lading, warehouse receipt) or the payment of money (e.g., checks, promissory notes). Bills of lading are particularly relevant for paperless trade facilitation and for logistics. Other transferable documents relate to financing and are relevant for national trade platforms. ¹²	The question may be answered when the text of the provision directly states equivalency exists for electronic transferable records.	- Electronic Transferable Records Law - Customs Law - Law Establishing Single Window Systems - Electronic Commerce Act - Electronic Transactions Act	"An electronic transferable record may not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form." Bahrain Electronic Transferable Records Law Art. 15 <i>The provision applies because the text of the law explicitly gives equivalency to electronic transferable records.</i>	N/A
13.	Foreign origin or use abroad of an electronic transferable record is permitted	This aims to eliminate obstacles to cross-border recognition of an electronic transferable record arising exclusively from the place of origin or use of the electronic transferable record. ¹³	The provision must explicitly state the recognition of foreign electronic transferable records.	- Electronic Transferable Records Law - Customs Law - Law Establishing Single Window Systems - Electronic Commerce Act - Electronic Transactions Act	"An electronic transferable record is not to be denied legal effect, validity or enforceability solely on the ground that it was issued or used outside Singapore." Singapore Electronic Transactions Act Art. 16P(1) <i>The provision explicitly states the answer to the question and thus applies.</i>	N/A
ONLINE CONSUMER PROTECTION						
14.	Framework explicitly addresses online consumer protection	Relevant laws for online consumer protection are crucial to enhance consumer trust in e-commerce. ¹⁴	This question may be answered when there is at least one form of protection over an online transaction. Note that distance contracts and remote contracts are considered online transactions for many countries.	- Consumer Protection Law - Electronic Commerce Law		

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
15.	Online information disclosure requirements prior to conclusion of the contract.	Informed decision-making relies on knowledge about the merchant, about the product or service, and about the parties' rights after purchase. ¹⁵	Multiple choices possible. With every question, ensure first that the requirement occurs prior to the conclusion of the contract.	- Consumer Protection Law - Electronic Commerce Law	"Sec. 3. Scope and Coverage. - This Act shall apply to all business-to-business and business-to-consumer internet transactions within the mandate of the Department of Trade and Industry (DTI), where one (1) of the parties is situated in the Philippines or where the digital platform, e-retailer, or online merchant is availing of the Philippine market and has minimum contacts therein: Provided, That online media content, and consumer-to-consumer (C2C) transactions shall not be covered under this Act." - Philippines Internet Transactions Act Sec. 3 <i>The scope of the law explicitly states that the regulation covers electronic transactions to consumers.</i>	"Article 3 (Definitions and scope): - Consumer is any natural or legal person to whom goods and services are supplied or any rights transferred and who use them as the final recipient, by whom carries out an economic activity aimed at obtaining profits. - Supplier is any natural or legal person, public or private, national or foreign, as well as depersonalized entities that carry out activities of production, assembly, creation, construction, transport, import, export, distribution or commercialization of goods or provision of services.... - Service is any activity provided in the consumer market, for remuneration, including those of a banking, financial, credit and insurance nature, except those arising from employment relationships." - Angola Consumer Protection Law Art. 3 <i>Nowhere in the scope of the law or in other provisions does the law specifically address online protections via electronic goods/services, internet-based goods/services, remote goods/services, or distance contracts. After reviewing the scope and the rest of the text, the question cannot be answered with the laws at hand.</i> See examples for specific questions below. (continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
15a.	Online information disclosure requirements prior to conclusion of the contract: Full business address of merchant	Having an offline means to contact an online business can give customers the stability and trust to move forward with the transaction. ¹⁶	Explicitly find the requirement for an address. Note that laws commonly create different rules for off-premises versus distance contracts. When reading the law, ensure the correct provision has been chosen.	- Consumer Protection Law - Electronic Commerce Law	"Article 16. Requirements for offer in electronic commerce. The offer in electronic commerce must contain: full name of the electronic commerce participant making the offer..." Uzbekistan Law on Electronic Commerce Art. 16 <i>The provision applies to the question because an offer comes before the conclusion of the contract.</i>	"31. Disclosure of information on internet agreement – (1) Before a consumer enters into an internet agreement, the supplier shall disclose the prescribed information to the consumer." Kenya Consumer Protection Law Art. 31 <i>The information provided is not sufficient or specific enough to answer the question.</i>
15b.	Online information disclosure requirements prior to conclusion of the contract: Full description of the product or service	Informed decision-making must balance the need to provide sufficient information to the consumer to make a decision on the product or service while not overwhelming the consumer so as to decrease the rate of understanding that can occur when too much information is presented. This makes regulated descriptions important for consumer trust. ¹⁷	This question may be answered with a main description of the product or service. Countries generally do not require a full description. Note that laws commonly create different rules for off-premises versus distance contracts. When reading the law, ensure the correct provision has been chosen.	- Consumer Protection Law - Electronic Commerce Law	"Sec. 21. Obligations of E-marketplaces. – Except as otherwise provided in this Act, e-marketplaces shall: ... (g) Require all online merchants to clearly indicate the following in their product offers online, regardless of the nature of the goods and services: (3) Description;" Philippines Internet Transactions Act Sec. 21(g)(3) <i>The provision requires e-marketplaces to ensure that merchants provide a description of the goods/services. This description is sufficient to answer the question because any requirement of the description of the goods/services is sufficient.</i>	"31. Disclosure of information on internet agreement – (1) Before a consumer enters into an internet agreement, the supplier shall disclose the prescribed information to the consumer." Kenya Consumer Protection Law Art. 31 <i>The information provided is not sufficient or specific enough to answer the question.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
15c.	Online information disclosure requirements prior to conclusion of the contract: Information about delivery and/or payment	Quick and accessible easy information on costs and delivery leads to better decision-making by the consumers and less cost for the sellers. ¹⁸	Any provision that supplies information on the price or delivery times is acceptable. The information about payment or delivery methods is also acceptable, if needed. Note that laws commonly create different rules for off-premises versus distance contracts. When reading the law, ensure the correct provision has been chosen.	- Consumer Protection Law - Electronic Commerce Law	"Sec. 21. Obligations of E-marketplaces. – Except as otherwise provided in this Act, e-marketplaces shall: ... (g) Require all online merchants to clearly indicate the following in their product offers online, regardless of the nature of the goods and services: (2) Price;" Philippines Internet Transactions Act Sec. 21(g)(2) <i>The provision requires information about the price of the goods/services. As either price or delivery information must be offered, the provision sufficiently answers the question at hand.</i>	"31. Disclosure of information on internet agreement – (1) Before a consumer enters into an internet agreement, the supplier shall disclose the prescribed information to the consumer." Kenya Consumer Protection Law Art. 31 <i>The information provided is not sufficient or specific enough to answer the question.</i>
15d.	Online information disclosure requirements prior to conclusion of the contract: -Information about complaint handling	Giving consumers access to merchants to gain options for redress or to address issues is useful for establishing a stronger client base and trust for new customers. ¹⁹	This may be provided by a requirement in the offer stage. Next, the information about complaint handling does not need to be a detailed description, but it must be more than the conditions for terminating the contract. The purpose of the question is to discover if supports for the consumer exist at the very beginning, leading to a larger sentiment than only termination.	- Consumer Protection Law - Electronic Commerce Law	"(2) A mail order distributor shall indicate, advertise, or notify the following ... 8. Matters concerning compensation for damage, settlement of complaints against the goods, etc., and resolution of disputes between consumers and business operators; ... Republic of Korea Act on Consumer Protection in Electronic Commerce Art. 13(2)(8) <i>The provision here applies to the question because it specifies various types of complaint-handling mechanisms, and all of which are mandatory to discuss.</i>	"The e-supplier must present the electronic commercial offer ... [to] include, but not be limited to, the following information: ... the conditions for terminating the contract, if applicable." Algeria E-Commerce Law Art. 11 <i>The provision does not require enough information to include various types of complaint handling.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
16.	Explicit acknowledgement of obligation to pay for online transaction	Businesses should ensure that the point at which consumers are asked to confirm a transaction, after which time payment is due or they are otherwise contractually bound, is clear and unambiguous, as should the steps needed to complete the transaction, especially for new payment mechanisms. ²⁰	This question seeks to know if the country requires a final and—somewhat—actionable agreement to the payment. The purpose behind this question is to know the level of safety over the consumer's purchase. Thus, this question should be answered when the law requires the consumer to see the final price just before paying, or some action that ensures understanding by the consumer at the end of the transaction.	- Consumer Protection Law - Electronic Commerce Law	“The order of a product or service goes through three mandatory steps: . . . verification of the details of the order by the e-consumer, in particular the products or services ordered, their total and unit price, the quantities ordered with a view to modifying the order . . .” Algeria E-Commerce Law Art. 12 <i>The provision works because, although the word “acknowledgement” is not specifically stated, the consumer must actively agree to the terms just before the conclusion of the contract.</i>	“The seller in e-commerce, before concluding a contract of sale, is obliged to provide the consumer with information on the procedure for paying for goods and on their cost.” Kazakhstan Law on Protection of Consumer Rights Art. 24(12) <i>The provision can be interpreted as merely giving the price of the goods in an advertisement. Further, there is no indication that the consumer must actionably agree to the price.</i>
17.	Requirement to provide online transaction in a format that is appropriate to the means of distance communication used	Businesses should enable consumers to retain a complete, accurate and durable record of the transaction, in a format compatible with the device or platform that the consumers used to complete the transaction. ²¹	Because the purpose/justification of this question, there are two ways to answer the question: the language almost precisely matches the language of the question, or the provision creates a truly durable, complete, and accurate means to provide the data in the exact way the transaction occurred. Note that for the latter, the law must be written so as to ensure that the transaction can only occur in the same way that the information is given, meaning that this type of answer should be exceedingly rare.	- Consumer Protection Law - Electronic Commerce Law	“With respect to distance contracts, the information provided for in Article 57, paragraph (1) of this Act shall be appropriate to the means of distance communication used, and given in plain and intelligible language and if provided on a durable medium, it shall be legible.” Croatia Consumer Protection Act Art. 66(1) <i>This provision is an example of a perfect match to the question.</i>	“Article 78 Reliable information in purchase transactions by electronic means: When the transactions are by electronic means, prior to the conclusion of the transaction, the provider must provide the consumer with true and updated information about their physical address, telephone numbers, electronic address, and other means to which the consumer can go to present their claims or request clarifications. The information about the goods and services offered by suppliers via the Internet or other electronic means must be clear, complete and accurate for potential consumers or users. Likewise, misleading commercial practices regarding the characteristics of the products that may lead to fraud or confusion for consumers or users are prohibited.”

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
			In addition, because the question seeks to understand if protections exist that require a durable record, the provision must discuss such a record after the transaction is concluded.		“Art. 1 – In consumer relations carried out by electronic commerce through the INTERNET... Art. 3 – In addition to the information mentioned in the previous article, the provider must provide the consumer on its INTERNET site, in a clear, precise, and easily accessible manner, at least the following information: (g) electronic copy of the contract.” Argentina Resolution on the Consumer's Right to Information in Commercial Transactions Carried Out over the Internet Art. 3(g) (referencing Art. 1) <i>These provisions provide a good example of the inexact match. First, the resolution is entirely about electronic transactions over the internet. Second, the requirements mean that the supplier must keep the contract of the transaction on the same website the customer used. Thus, the law and articles read together can answer this question.</i>	Nicaragua Consumer Protection Law Art. 78 <i>The provision is discussing the information that must be given prior to the contract. Because the provision does not address the conclusion of the contract or a sustainable record of the individual transaction, the provision does not apply.</i>
18.	Existence of the right of withdrawal	Online customers are unable to inspect a product before purchasing; the right of withdrawal allows them to return the product within a certain period of time, escaping the contractual obligation with no repercussions. ²²	The right to withdraw must be stated to be a right of the consumer. The right to withdraw can be stated in relation to online business contracts or all contracts, which would logically include online contracts.	- Consumer Protection Law - Electronic Commerce Law	“In the sale and in any type of contracting of goods and/or provision of services that are offered or performed outside the supplier's establishment and those for which means are used, such as: ... any means of data messages, internet, ... the	“Article 41 An electronic offer cannot be withdrawn again if the offer has been electronically accepted by another party, unless the cancellation of the electronic offer is also agreed upon by the party receiving the offer.”

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
			Further, the right to withdraw can be counted in the right to terminate a contract—so long as the right to terminate does not preclude online contracts. This rule is needed because laws around the world use the terms “termination,” “cancellation,” and “withdraw” interchangeably. In addition, translation tools may not reliably capture the nuanced distinctions among the three terms.		provider is obliged ... to: (g) Provide and allow the consumer a trial period seven (7) business days minimum, prior to the return of the good or the suspension of the service provision contract.” Dominican Republic General Consumer Protection Law Art. 62(g) <i>This provision applies to the question because the obligation to create a right of withdrawal is written within the distance contract rules. Note that usually a possible right of withdrawal exists in these pre-contractual rules, not a definitive one like in the Dominican Republic.</i>	Indonesia Regulation Concerning Trade Through Electronic Systems Art. 41 <i>The provision specifically states that the offer may not be withdrawn upon acceptance. As the purpose of the question is to understand whether customers have the right to see the good/service in person and decide against it, the question cannot be answered with the provision. Further, the right to withdraw cannot hinge upon another agreement, as the right must be a standalone right by the customer to unilaterally withdraw.</i>
19.	No need to provide a reason for withdrawal	Absence of reason is essential for the right of withdrawal to be effective. ²³	The right to withdraw without reason may be explicitly stated or not stated at all, so long as there is an explicit right to withdraw, cancel, revoke, or terminate. The reason for the ability to count this question with the absence of the law is to see when countries explicitly regulate the reasons for withdraw.	- Consumer Protection Law - Electronic Commerce Law	“30.- (1) Without prejudice to any other law, a consumer may, within seven days or longer period specified in the agreement, after receiving the goods or conclusion of the agreement and the consumer has not received any material benefit from the transaction, cancel the agreement for supply of goods or provision of services. (2) Where a consumer has cancelled the agreement under subsection (1), he shall pay direct cost of returning the goods. ... (5) This section shall not apply to electronic transactions – (a) for financial services;	“In the event of non-compliance by the e-supplier..., the e-consumer may request the cancellation of the contract and request compensation of the damage suffered.” Algeria E-Commerce Law Art. 14 <i>The provision cannot work because the cancellation is dependent on non-compliance.</i>

(continued on next page)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
20.	Rules against dark patterns	Dark patterns include encompass aspects of design such as the placement and color of interfaces, how text is worded, and more direct interventions such as putting pressure on users by stating that the product or service they are looking is about to be sold out. ²⁴ Dark patterns are considered ethically problematic, because they mislead users into making choices that are not in their interest and deprive them of their agency. ²⁵	This question may also be answered “yes” when the loss of the right to withdraw is stated, and this is usually for actions post-delivery. This is because a subsequent loss of rights does not strip the rights from originally existing. However, if there is a reason to withdraw, like non-compliance, then the question must be answered “no”. Currently, the regulation of dark patterns is so new that the term dark patterns is required. Otherwise, too many provisions regarding misrepresentation could be counted towards the question, throwing off the results by not gathering data on the intended purpose of the question.	Children’s Personal Protection Acts	(b) by way of an auction; (c) for the supply of foodstuffs, beverages or other goods intended for daily consumption; ...” Tanzania Electronic Transactions Act Art. 30 <i>The provision does not state that the consumer must provide reasoning or need to meet certain requirements to cancel; rather, the provision gives a list of exclusions.</i>	N/A
					“Online interface design and organisation 1. Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.” <i>/read with/</i> “(67) Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions....” EU Digital Services Act Art. 25 (read with recital para. 67)	(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
21.	Sending unsolicited electronic commercial communications is prohibited, subject to conditions (SPAM)	Spam, which began as messages advertising commercial products or services, grew exponentially. Simple advertising messages have evolved into messages that are potentially dangerous, as opposed to merely annoying. Spam messages nowadays have a deceptive nature, may cause network disruptions, and are used as a vehicle for spreading viruses, thus undermining consumer confidence, which is a prerequisite for the information society and for the success of e-commerce. ²⁶	This question may be answered “yes” when the law states that a prohibition exists or that the communication is only permitted under a certain circumstance. This is because, logically, the prohibition exists except for that certain instance.	- Electronic Transactions Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law - Terms: unsolicited, unauthorized, spam	<i>The provision bans designs that distort or impair services. As the recital paragraph uses the same language to show the purpose of the regulations and references these practices as dark patterns, the provision applies.</i> “1. Unsolicited commercial communications via email or sms are permitted only with the prior approval of their recipient.” - Albania Law on Electronic Commerce Art. 9(1) <i>The provision here answers the question because a prohibition occurs whenever the prior approval has not been given.</i> “Article 28 B. – All communication promotional or advertising message sent by email must indicate the subject or topic it deals with, the identity of the sender and contain a valid address to which the recipient can request the suspension of shipments...” - Chile Decree 3 of 2021 Art. 28B <i>The provision does not directly state that spam messages are prohibited; rather, the logic behind the provision is that spam messages that do not meet its requirements are not permitted.</i>	“Article 8 – Data processing for direct marketing purposes 1. Data obtained from publicly available sources may be processed for direct marketing purposes. 2. Regardless of the purpose of data collection, the following data may be processed for direct marketing purposes: name (names), address, telephone number, e-mail address, fax number. 3. Any data may be processed for direct marketing purposes on the basis of a written consent given by a data subject as determined by this Law. 4. A data subject shall have the right to require at any time that a data controller stop to use of his/her data for direct marketing purposes. 5. A data controller shall be obliged to stop data processing for direct marketing purposes and/or ensure that a data processor stop data processing for direct marketing purposes not later than 10 working days after the request of a data subject is received.

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
22.	Legal basis for sending unsolicited electronic commercial communications	Spam has a negative impact on the digital economy, and results in important economic and social costs. ²⁷	Multiple choices possible. Ensure that the unwanted contact occurs for marketing purposes.	- Consumer Protection Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law	See examples for specific questions below.	6. When data are processed for direct marketing purposes a data controller shall be obliged to notify a data subject of the right under paragraph 4 of this article and to ensure the possibility to stop data processing for direct marketing purposes in the same form as the direct marketing is conducted, and/or to determine the available and adequate means to require discontinuation of data processing for direct marketing purposes.” Georgia Law on Personal Data Protection Art. 8 <i>The provision applies to the processing of personal data in relation to direct marketing. In fact, it does not explicitly state that commercial communications from the processing are regulated here. While small—and perhaps the law is regardless applied to these situations, as the provision does not explicitly extend the scope beyond processing, the provision cannot be read into further. Thus, the provision cannot apply.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
22a.	Legal basis for sending unsolicited electronic commercial communications: -Express consent	Unless threats posed by unsolicited, unwanted, and harmful electronic messages are curtailed, they could erode users' trust and confidence. ²⁸	Consent may be found in provisions where (i) consent is required for every commercial communication, or (ii) consent is one of multiple ways to communicate.	- Consumer Protection Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law	"Article 13 Unsolicited communications: 1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent." EU Directive on Privacy and Electronic Communications Art. 13(1) <i>The provision requires consent to send unsolicited communications. Thus, the provision applies.</i>	"The right of citizens to be protected against abuses and violations of their rights is recognized through the Internet and other electronic means, namely: (a) right to secrecy of communications; (b) right to privacy of your personal information, including the right of access, consultation and rectification thereof and the right to have that information used in strict compliance with constitutional principles and applicable legal rules; (c) right to the security of your information, by improving the quality, credibility and integrity of the systems of information; (d) right to internet security of minors; (e) right not to receive unsolicited electronic messages; (f) right to the protection and safeguard of their rights as consumers, namely, in the acquisition of goods and services through the Internet and in terms of advertising; (g) right to protect and safeguard their rights as users of electronic communications networks or services. Angola Electronic Communications Law Art. 15(e) <i>The provision merely creates the right to not receive unsolicited messages, and it does not create any further ways around the ban like consent. Thus, the provision does not apply.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
22b.	Legal basis for sending unsolicited electronic commercial communications: -Existing relationship	The rationale for the existing relationship exception is that the consumer has already indicated interest both in this type of transaction and in this sender; thus, consent to receive additional and similar communications is implied. ²⁹	This question seeks to understand the higher levels of requirements placed upon the legal basis for spam. Thus, this question should *not* be answered "yes" if the prior existing relationship is purely built on consent.	- Consumer Protection Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law	"(3) Unsolicited Commercial Communications. — The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless: ... (ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; ..." Philippines Cybercrime Prevention Act Sec. 4(c)(3) <i>The provision specifically states that unsolicited communications can occur when a relationship with the consumer and advertiser currently exist.</i>	"Article 86. Obligation not to use user information without authorization. If the service recipient should provide their email address during the ordering process, hiring or subscription to a service and the provider intends to use it later for sending commercial communications, it must inform the client of its intention and request your consent to receive such communications, before complete the recruitment process..." Panama Law 51 of 2008 Art. 86 <i>The provision appears initially to apply to an existing relationship, but upon further reading, the intention is actually about consent. Really, the provision states that if attempting to create a commercial relationship, then the service must gain consent to create such a relationship for commercial communications. Thus, the provision does not apply.</i>
23.	Consumers may opt out of receiving unsolicited electronic commercial communications	Businesses should develop and implement effective and easy-to-use procedures that allow consumers to choose whether or not they wish to receive unsolicited commercial messages, whether by e-mail or other electronic means. ³⁰	This question may be answered when the provision specifically discusses unsolicited commercial communications, when the provision only discusses electronic communications, and when the provision discusses types of electronic communications.	- Consumer Protection Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law	"Article 55 – Suppliers shall provide the customers with the required arrangements that would enable them to choose whether to receive the advertisements at their mailing or e-mail address." Iran E-Commerce Law Art. 55 <i>The provision sufficiently answers whether a consumer may opt-out of any electronic advertisements, including unsolicited advertisements.</i>	"(2) Natural and legal persons may use the electronic contact data for e-mail obtained from consumers of their products and services, for direct marketing and sales only of their similar products and services, provided they have given to those consumers a clear and unambiguous option to object in a simple manner and free of charge to such use of the electronic contact data when said data are being obtained and when each message

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
			The reason for a wider range on this question than others is to find out if the law prescribes ways for the consumer to terminate advertisements being sent to their phone.			is received, in case the consumer have not refused in advance the use of its electronic contact data. (3) Unsolicited communications for the purpose of direct marketing, differing from those stated in paragraphs (1) and (2) of this Article (for instance voice telephone calls), shall be permitted only when the subscribers or users have provided consent thereof, and shall be free of charge.” • North Macedonia Law on Electronic Communications Art. 174(2) <i>The provision here creates a right to opt-out for existing relationships only. This creates a narrow opt-out law that is too narrow for the question at hand. The fact that the opt-out only applies in the certain instance can be further seen via the other sub-articles, like Art. 174(3).</i>
24.	Visible and functioning opt-out process required for unsolicited electronic commercial communications	When consumers have, at any time, indicated that they do not wish to receive such messages, that preference should be respected, as doing so reinforces trust and supports a predictable, consumer-centric regulatory environment.	The purpose of this question is to understand if the law specifically regulates measures that make unsubscribing to advertising content easy. Look for provisions that give enough specification for the process to be apparent and useful to terminate the direct marketing. Ensure the answer provided has language covering both “visible” processes and “functioning” processes.	- Consumer Protection Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law	“...The recipient may revoke, at any time, the consent given for the reception of commercial communications with the simple notification of your will to the sender. To this end, service providers must enable simple and free procedures so that the recipients of services can revoke the consent they have given. Likewise, they must provide accessible information on the Internet about said procedures.” Panama Law 51 of 2008 Art. 86	“6. When processing data for direct marketing purposes, the data processor is obliged to notify the data subject of the right provided for in paragraph 4 of this article and to ensure that the data subject has the opportunity to request the termination of data processing for direct marketing purposes in the same form in which direct marketing is carried out, and/or to determine an accessible and adequate means to request the termination of data processing for direct marketing purposes.” Georgia Data Protection Law Art. 8(6)

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
25.	Sender must honor opt-out requests within a specific period of time	Having a specific timeline for the opt-out procedures creates a more reliable process. ³¹	The provision must either give a numerical amount of days that the operator must comply to the request to opt-out, or the provision must state that the opt-out service will be complied with immediately. Both are sufficient to give a “specific period of time.” Note that the provision requiring compliance within a “reasonable period of time” is not sufficiently specific to answer the question.	- Consumer Protection Law - Advertising Law - Electronic Communications Law - Personal Data Protection Law	The provision applies because the language of the text states simple and free procedures that are accessible, which is equivalent to a visible opt-out system. Further the beginning of the paragraph states that the recipient may revoke consent whenever, which is equivalent to requiring a functional system. Thus, the provision applies. “5. The data processor is obliged to stop the processing of data for direct marketing purposes and/or ensure the termination of data processing for direct marketing purposes by an authorized person no later than 10 working days after receiving the data subject’s request.” Georgia Personal Data Protection Law Art. 8(5) The law gives a specific timeline sufficient to answer the question.	The law does not specify that the processor must make the “unsubscribe button” particularly visible. Because the feature must merely be accessible and the feature does not need to be in the same form as the marketing, the provision does not meet the standards sought here. “Article 39: Any person may notify a service provider directly determined, without charge or indication of reasons, his desire to no longer receive advertisements from him by means of automated calling machines, fax machines or electronic mail. To this end, the service provider: - delivers, within a reasonable time and by an appropriate means, an acknowledgment of receipt confirming to this person the registration of their request; - takes, within a reasonable time, all necessary measures to respect the wishes of this person; - maintains lists of people who have notified their desire to no longer receive advertisements from us by email.” - Congo Rep. Electronic Transactions Law Art. 39 “Within a reasonable time” is not a sufficiently precise time period to apply to the question. The reason is that reasonability can vary greatly, which defeats the purpose of the question—to discover if a specific enough cut-off time exists to create a greater sense of trust in the system. Thus, the provision does not apply to the question as it is too vague.

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
26.	Consumer's right to a refund in case of goods of improper quality	Merchants must provide redress for harm suffered as a consequence of a product that is defective, damaged, does not meet the advertised quality criteria, or if there were delivery problems. ³²	Provisions giving the right to a refund must be linked to inadequate quality or dissatisfaction. Further, ensure that the provision applies to a <i>full</i> refund, not a partial. In addition, the right to refund must be able to be a standalone right. A provision will not apply when the right exists only after other options are exhausted, like the right of repair, but it can be a right that the courts grant.	Consumer Protection Law	"14. To return goods: (1) If anyone wishes to return, being dissatisfied with, any goods purchased from the seller, he or she may return it to the seller within seven days or take other similar goods equal to that price or the payment of the amount which was paid while purchasing such goods." Nepal Consumer Protection Act Art. 14(1) <i>The provision answers the question by allowing a consumer to return the goods for a full refund when unsatisfied with the goods.</i>	"47. (1) The supplier offering goods or services for sale, hire or exchange in an electronic transaction shall make available to the consumer on the electronic platform where the goods or services are offered the following information related to the supplier: ... (m) the return, exchange and refund policy:..." - Ghana Electronic Transactions Act Art. 47(m) <i>Beyond not having any specification about the right coming from the consumer and the defected goods/services, the provision does not state whether the refund policy is mandatory. Thus, for all these reasons, the example cannot apply.</i> "Article 45 Goods with defects: Goods with a current guarantee that do not work properly for reasons attributable to the supplier or due to a product defect, must be repaired. If this is not possible, the supplier will proceed to replace the good with another of the same characteristics or return the sums paid." - Nicaragua Consumer Protection Law Art. 45 <i>The right to refund must stand alone, which it does not here.</i> (continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
27.	Alternatives for redress in case of improper quality, such as repair, replacement, or partial refund	Having variations in redress that are not solely monetary ways to redress improper goods/services is important for addressing the harm suffered. ³³	Provisions giving the right to a refund must be linked to inadequate quality or dissatisfaction.	Consumer Protection Law	"Article 21. Consumer rights in the case non-conformity of the service provided (2) The provider ensures all the operations and bears all the expenses necessary to remedy the deficiencies found in the services provided, to replace the products used in the respective services, including their transport, handling, diagnosis, expertise, disassembly, assembly and packaging, or to refund the value of the inadequate services within the warranty period." Moldova Consumer Protection Law Art. 21(2) <i>The provision applies to goods/services of improper quality because the title of the provision states that it applies to "non-conformity." Further, at least one of the alternatives for redress is listed.</i>	"Article 26 Replacement and return of the product of appropriate quality (1) The consumer has the right to ask the seller in the trade unit where it was purchased, within 14 days, to replace a non-food product of appropriate quality with a product similar to the one purchased if this product does not suit him in terms of shape, dimensions, model, size, color or if he cannot use it as intended for other reasons, with the performance, in the case of the price difference, of the corresponding recalculation." Moldova Consumer Protection Law Art. 26 <i>The provision specifically is titled as pertaining to products of "appropriate quality." This means that the right to redress improper goods/services would not apply.</i>
28.	Penalties for noncompliance with online consumer protection provisions	The imposition of a financial penalty, determined by reference to the nature of the contravention and the trader's circumstances, is likely to be cost-effective in inducing compliance in many cases. ³⁴	The provision cannot merely state that laws of the republic will create liability. The law must indicate the penalties or directly link to a law that indicates the penalties. This is because the purpose of the question is to discover if trust-building measures exist in the law, and measures that do not give sufficient information on what the penalties could entail will not build sufficient trust in the system.	Consumer Protection Law	"51 (1) If, after hearing the application, the court is satisfied that one or more persons have contravened any of the provisions referred to in the application ..., the court may order the person or persons, as the case may be, to pay the applicant... (b) a maximum of (i) in the case of a contravention of section 6, \$200	"If the seller (producer, executor) did not give a respond to the complaint or refuses to remove violations and compensate of inflicted loss (harm) in a voluntary manner, the public association of consumers, associations (unions) shall have the right to go to court." Kazakhstan Law on the Protection of Consumer Rights Art. 42 <i>The provision is too vague to give penalties to the violators, but rather gives liability to their actions of non-compliance.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
			Further, the provision does not answer the question when penalties occur only after the non-complying seller has not responded to a complaint, because the purpose of the question is to understand if there are direct incentives to follow the law.		for each contravention of that provision, not exceeding \$1,000,000 for each day on which a contravention occurred....” Canada Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act Art. 51(1)(b)(i) <i>The provision references the anti-spam provisions. As these provisions are considered an online consumer protection provision, the provision stated can apply. Further, the provision explicitly states numerically what penalties occur. Thus, the provision applies.</i>	
DATA PROTECTION						
29.	General personal data protection law explicitly addresses data protection by private entities	Certainty about online data use and handling increases trust in digital trade. ³⁵	This provision can be found in the scope of the law or another general-purpose provision that expresses governance of data protection by private entities.	Law on Personal Data Protection	“The purpose of this law is to protect... the rights of individuals with regard to the processing of personal data, whatever the nature, method of execution or those responsible.” Burkina Faso Personal Data Protection Law Art. 1 <i>The provision sufficiently states the scope of the law as applying to personal data protection and sufficiently creates a broad enough scope as to cover private entities. Thus, the provision applies..</i>	“Article 1 “ In order to protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information, this law is formulated in accordance with the Constitution.” China Personal Information Protection Law Art. 1 <i>Although the provision discusses that the law applies to the data of personal information, the provision does not work because it does not specifically state that the law applies to private entities.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
30.	Special rules for the treatment of sensitive personal data during processing	Misuse or breach of sensitive information, such as political views or sexual orientation, usually leads to greater consequences for the data subject. ³⁶	This question can be answered whenever sensitive personal data is specifically mentioned, or the definition of certain types of data includes sensitive issues, like political views, sexual orientation, health information, etc.	Law on Personal Data Protection	"Article 12. Specifics for the Processing of Personal Data for a Special Category: (1) The processing of personal data of a specific category without the consent of the person shall be prohibited unless the processing of the data is expressly provided for by law." - Armenia Personal Data Protection Law Art. 12(1) <i>The provision applies because the term "special category" is defined as that of special sensitive information.</i> "Article 2 (Definitions) (3) 'Sensitive personal information' in this Act means personal information as to an identifiable person's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other identifiers or their equivalent prescribed by Cabinet Order as those of requiring special care so as not to cause unjust discrimination, prejudice or other disadvantages to that person." - Japan Act on the Protection of Personal Information Art. 2(3) <i>The definition of the term is sufficient to answer the question presented. Thus, the provision applies.</i>	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
31.	Special rules for the treatment of biometric data	Some laws don't include biometric data under the definition of sensitive data. The ability for companies to extract biometric information, such as face prints, without the user's consent and sell it to third parties poses a risk to personal privacy. ³⁷	Any mention of biometric data in the definitions section or in other provisions is sufficient to answer the question at hand.	Law on Personal Data Protection	"Special categories of data" shall be understood to mean any personal data revealing... biometric data." Bosnia and Herzegovina Personal Data Protection Law Art. 3(c) <i>The provision explicitly discusses biometric data and is, thus, sufficient to answer the question.</i>	What do you think? N/A or does something fit?
32a-d.	Legal basis for data collection and processing: -The data subject's consent; -Performance of a contract to which the customer is party; -Compliance with a legal obligation to which the controller is subject; -Legitimate interests pursued by the controller or by a third party	Common principles for the processing of personal data include the need to have a legitimate reason for any processing activity, obtained either through consent or some other justification designed to acknowledge competing private and public interests. ³⁸	For these provisions, more likely than not, the provisions that apply will use explicit language that matches the question itself. Legitimate interests can be found when the term is explicitly stated and when laws reference serious public interests as a reason.	Law on Personal Data Protection	"The personal information processor may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where the consent is obtained from data subjects; 2. Where special provisions exist in laws or it is unavoidable so as to observe legal obligations... 4. Where it is unavoidable necessary so as to execute and perform a contract with data subjects... 6. Where it is necessary to attain the justifiable interest of personal information processor, which is explicitly superior to that of data subjects..." Korea, Rep. Personal Information Protection Act Art. 15	
33.	The data controller must only collect data for specified purposes	The categories of data chosen for processing must be necessary to achieve the declared overall aim of the processing operations, and a controller should strictly limit collection of data	The provision will likely use the same language as the question or similar language.	Law on Personal Data Protection	"When personal data is collected, the owners must be informed in advance, expressly, precisely and unequivocally of the purpose for which they will be processed and who their recipients or class of recipients may be."	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
34.	Once data are collected, they must not be further processed in a way incompatible with those purposes	to such information as is directly relevant for the specific purpose pursued by the processing. ³⁹ Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. ⁴⁰		Law on Personal Data Protection	- Uruguay Personal Data Protection Law Art. 13 <i>The language of the text is sufficiently synonymous with "specified", and thus applies.</i> "The data may not be used for purposes other than or incompatible with those that motivated its collection." Uruguay Personal Data Protection Law Art. 8	
35.	The data controller must only process information that is necessary for the specified purpose		Law on Personal Data Protection	Law on Personal Data Protection	The data must be deleted when they are no longer necessary or pertinent to the purposes for which they were collected. Uruguay Personal Data Protection Law Art. 8	
36.	Data subject's right to electronic data access	Data subjects must have appropriate rights to access their personal data stored online. ⁴¹	Law on Personal Data Protection	Law on Personal Data Protection	The person who is the subject of a "data message" shall have access to those computer files containing his/her personal "data messages" and be able to remove or amend partial or incorrect "data messages." Iran E-commerce Law Art. 59(d)	
37.	Data subject's right to electronic data rectification		Law on Personal Data Protection			

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
38a-c.	Data subject may ask for their data to be erased if certain conditions are met, such as: - The data is no longer needed for its original purpose - There is no other legal ground to keep processing it - it was being used in a way that was against the law in the first place	Providing data subjects with a right to have their own data erased is particularly important for the effective application of data protection principles. This right is not absolute; it needs to be balanced with other rights specifically the interest and right of the general public in having access to the information.⁴²	Multiple choices possible.	Law on Personal Data Protection	A data subject may request a data controller or data processor... to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully Kenya Data Protection Act Art. 40(b)	
39.	Data subject may withdraw consent under certain circumstances	The inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.⁴³		Law on Personal Data Protection	Consent to the processing of personal data can be revoked by the subject of personal data. Russia Personal Data Law Art. 9(2)	
40.	Data subject's right to demand that their personal data be transmitted directly from one provider to another (personal data portability)	Data portability provides restricted access through which data holders can provide customer data in a commonly used, machine-readable structured format, either to the customer or to a third party chosen by the customer.⁴⁴		Law on Personal Data Protection	The data subject shall have the right to receive the personal data...in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller EU GDPR Art. 19	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
41.	Rules for sharing personal data with third parties	Data sharing is the disclosure of data from one or more organizations to a third-party organization or organizations, or the sharing of data between different parts of an organization. ⁴⁵		Law on Personal Data Protection	The display, publication, transmission, dissemination and/or access opening of Personal Data in an Electronic System may only be conducted: a. upon Approval unless otherwise determined by the provisions of laws and regulations; and b. after the accuracy and suitability for the purpose of acquisition and collection of the Personal Data are verified. Singapore MOCI Regulation 20/2016 Art. 21	
42.	A government agency with a legal mandate to oversee and enforce data protection	Strong support exists for establishing a single central regulator with a combination of oversight and complaints management functions and powers. ⁴⁶		Law on Personal Data Protection	For the purpose of supervising the lawfulness of the undertaken activities while processing and protecting personal data, a Directorate for personal data protection shall be established on the territory of the Republic of Macedonia as an individual and independent state body with the capacity of legal entity. – North Macedonia Personal Data Protection Law Art. 37	
ARTIFICIAL INTELLIGENCE						
43.	Prohibition against AI systems creating discriminatory impacts or its use for the exploitation of vulnerable people.	Aside from the many beneficial uses of AI, AI systems can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful	This question can be answered by provisions which prohibit automated decision-making processes on sensitive personal data such as racial profiling.	- Data Protection Law - Specific law/ regulation on artificial intelligence	N/A	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
		and abusive and may be prohibited in different countries because they contradict values of respect for human dignity, freedom, equality, and democracy. ^a			“Article 39. It is prohibited to make a decision solely on the basis of automated processing by the competent authorities for special purposes, including profiling, if such a decision may have detrimental legal consequences for the data subject or significantly affect the position of that person, unless decisions based on the law and if that law prescribes appropriate measures to protect the rights and freedoms of the data subject, and at least the right to ensure the participation of a natural person under the control of the controller in making the decision.” • Serbia, Law on Personal Data Protection 2018, Article 39 “Article 80(10) The use of automatic license plate recognition systems and systems that process biometric personal data is prohibited in public areas.” • Slovenia, Command on the promulgation of the Personal Data Protection Act 2022, Section 80(10)	

^a Corrigendum to the Position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ of the European Parliament and of the Council laying down Harmonised rules on Artificial Intelligence, Recital 28, as available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.
(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
44.	The law mandates transparency for certain high-risk AI systems by requiring the release of data or publication of independent audits of AI assessments.	Legislations may mandate AI systems to release audits and assessments to allow for appropriate traceability and explainability of the outcomes of AI systems. Such data may also increase user's awareness, inform deployers of the capabilities and limitations of that AI system, and affected persons about their rights.	This question seeks any provision which mandate AI systems to publicly release data or publish independent audits.	- Data Protection Law - Specific law/regulation on artificial intelligence	"6. Requirements. The Assistant Deputy Minister responsible for the program using the automated decision system, or any other person named by the Deputy Head, is responsible for: 6.1 Algorithmic Impact Assessment 6.1.1 Completing and releasing the final results of an Algorithmic Impact Assessment prior to the production of any automated decision system. 6.1.2 Applying the relevant requirements prescribed in Appendix C as determined by the Algorithmic Impact Assessment. 6.1.3 Reviewing and updating the Algorithmic Impact Assessment on a scheduled basis, including when the functionality or scope of the automated decision system changes. 6.1.4 Releasing the final results of the Algorithmic Impact Assessment in an accessible format via Government of Canada websites and any other services designated by the Treasury Board of Canada Secretariat pursuant to the Directive on Open Government." Canada, Directive on Automated Decision-Making 2021, Regulation 6	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
45.	Data subject must be informed of the existence of an automated-decision-making process	Automated decision-making processes, especially in contexts such as employment opportunities or credit scores, can significantly impact the rights of data subjects. Being informed of the existence of automated decision-making processes, may enable the data subject to oppose or inquire about the rationale behind the decision.	This question requires a provision which obligates the data processor to inform the data subject about the existence of automated decision-making processes.	Data Protection Law	"Article 13(2). In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." EU GDPR 2016, Article 13(2)(f)	N/A
46.	Data subjects have the right, under certain circumstances, to have a person intervene in the decision-making process	Automated decision-making processes, especially in contexts such as employment opportunities or credit scores, can significantly impact the rights of data subjects. Providing data subjects the right to require human intervention, may help mitigate the adverse consequences of automated decision-making processes.	The question may be answered in two ways: (i) a provision which either prohibits automated decision-making where there is no human intervention; or (ii) it provides data subjects the right to require human intervention in the process	Data Protection Law	"Art. 22. Automated individual decision-making, including profiling. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Paragraph 1 shall not apply if the decision:	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
					is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.” • EU GDPR 2016, Article 22	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
CYBERSECURITY & CYBERCRIME						
47.	General requirement for data controllers and/or processors to implement measures to keep data secure	Whether physical, logical, or organizational, security measures should protect against deliberate acts of misuse, as well as the accidental loss or destruction of data. This can help companies take full advantage of the data collected without putting data subjects' privacy at risk. ⁴⁷		- Personal Data Protection Law - Cybersecurity Regulations - Law on Cybercrime	The bodies shall... take the appropriate measure to protect the personal data and information referred to in Article 32 against loss, damage, disclosure, replacement with incorrect data or information, or addition of untrue information thereto. Kuwait Law on Electronic Transactions Art. 35	
48.	Data encryption required under certain circumstances	Encryption—the encoding of messages so that only intended recipients can access their contents—is a key tool for insuring data security. It is widely recognized as essential to the digital economy and to the protection of fundamental rights, including privacy and freedom of expression. ⁴⁸			During the processing of personal data, the developer shall use encryption measures – protection of information systems containing personal data from accidental loss, unlawful access to information systems, illegal use, recording, deletion, transformation, blocking, copying, distribution and sharing of personal data. – Armenia Personal Data Protection Law Art. 19	
49.	Requirement to designate a person responsible for overseeing compliance with the data protection law	The appointment of a Data Protection Officer (DPO) can facilitate compliance and further, become a competitive advantage for businesses. ⁴⁹			The personal information processor shall designate the privacy officer who comprehensively takes charge of the personal information processing Korea Personal Information Protection Act Art. 31	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
50.	Risk assessment procedures required	Risk assessment helps organizations classify processing activities by their risks to individuals, prioritize compliance, and implement appropriate mitigations. As a core element of accountability, a risk-based approach helps maximize the potential benefits of data use, while minimizing potential harm to individuals. ⁵⁰			If, given its nature, extent, circumstances or purpose, a particular type of personal data processing is likely to lead to a high risk of unauthorized interference with the rights and freedoms of data subjects, the Management Authority shall draw up an assessment of the personal data protection impact of such processing • Czech, Rep. Personal Data Processing Act Art. 37	
51.	Employee training and awareness program required	Cybersecurity training equips employees to protect both themselves and the company against cyber threats. It provides up-to-date knowledge on recognizing and responding to attacks, including social engineering. Well-trained employees are essential to safeguarding critical business assets and ensuring secure, seamless interactions with customers. ⁵¹			Organizations shall implement policies and practices to give effect to the principles, including. • training staff and communicating to staff information about the organization's policies and practices • Canada Personal Information Protection and Electronic Documents Act Schedule 1 (4.1.4) (c)	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
52a-b.	Controllers are required to report data breaches: -To authority -To data subject(s)	When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Communicating a breach to individuals allows the controller to provide information on the risks resulting from the breach and the steps the affected individuals can take to protect themselves from its potential consequences.⁵²	Multiple choices possible.		The Controller shall inform the Individual and Competent Department of the occurrence of any breach of the precautions provided for in the preceding Article, and if such breach may cause serious damage to Personal Data or individual privacy. • Qatar Personal Data Protection Law Art. 14	
53.	Specific timelines for data breach notifications	A key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner. Timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.⁵³			The manager is obliged to inform about the breach ... the Commissioner without undue delay, or, if possible, within 72 hours of finding out about the injury • Serbia Personal Data Protection Law Art. 52	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
54.	Unauthorized access, alteration, interference, or misuse of systems or databases holding personal data is criminalized	Legal frameworks should establish clear and enforceable penalties—including criminal sanctions—for unauthorized access, use, or alteration of personal data by data controllers or third parties, to deter violations and support the identification and mitigation of cyberthreats. ⁵⁴			(1) Unlawful access to information kept in computer system, net, or machine bearers, along with a violation of the protection system is punishable by a fine of 200 to 400 times the minimum monthly wage or up to 2 years of restriction of liberty. (2) The same actions, if they caused changing, destroying, or blocking of information due to carelessness, as well as disabling computer equipment, or substantial damage are punishable by a fine of 300 to 500 times the minimum monthly wage or up to 2 years of correctional labor, or imprisonment for the same period of time. • Tajikistan Criminal Code Art. 298	
55.	A law, regulation, or policy provides for the creation of a cyber-security strategy	In a constantly changing cyber threat environment, countries need to have flexible and dynamic cybersecurity strategies to meet new, global threats. A national cybersecurity strategy (NCSS) is a coordinated plan of action aimed at enhancing of a country's critical infrastructures, digital services, and information systems. It is a high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. ⁵⁵		• Cybersecurity Strategy	For the purpose of implementation and use in all spheres of social and economic and cultural life of society of modern information technologies, the computer equipment and telecommunications, more complete satisfaction of the growing information needs of citizens, I ... Approve the State strategy "Information and communication technologies for development of the Republic of Tajikistan" it (is applied). • Tajikistan Presidential Decree "About the state strategy "Information and communication technologies for development of the Republic of Tajikistan" Art.1	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
56.	A law, regulation or policy provides for the creation of an institution to identify, investigate, and address cyber-security threats (CERTs)	The creation of clearly defined organizational structures—such as computer incident response teams for banking, telecommunications, and other critical service infrastructures, monitoring as well as cyber threat monitoring response centers—is fundamental ensuring national cybersecurity. ⁵⁶		- Cybersecurity Strategy - National CSERT website	According to Item 8.2 of the State strategy “It is information – communication technologies for development of the Republic of Tajikistan” ... I decide: Form Council for information and communication technologies in case of the President of the Republic of Tajikistan in the enclosed structure on position. Tajikistan Presidential Decree “About formation of Council for information and communication technologies in case of the President of the Republic of Tajikistan Art.1	N/A
CROSS BORDER						
57.	Explicit rules on cross-border general personal data transfers.	These rules increase transparency and require some security over personal data. ⁵⁷	This question seeks to identify whether the country has a provision or law that clearly regulates personal data transfers. This question cannot be answered “yes” unless the law or provision applies to personal data generally, not personal data in a specific act pertaining to a different area of law.	- Personal Data Protection Act - Personal Information Protection Act - Electronic Transactions Act	“A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country . . . ensures an adequate level of protection.” EU GDPR Art. 45(1) “General Data Protection Regulation” <i>Any mention of rules over personal information will work, but try to choose the beginning of the law. The reference to an entire law pertaining to the question also is acceptable.</i>	“4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.” Canada PIPEDA Sched. 1 Prin. 4.1.3 <i>Here, there are only regulations governing 3rd party data transfers. While this incidentally impacts CBDTs, it does not explicitly regulate CBDTs. Thus, rules regarding 3rd parties do not apply to this question, even though other questions in the section may be answered by rules that govern 3rd party data transfers.</i> (continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
58.	Cross-border data protection depends on self-assessment and accountability measures by data controllers and processors without government requirements, even in the absence of explicit regulation.	Understanding the level of security over data subjects' information is valuable to understanding the system the country has set up.	This question seeks to understand if the country does *not* regulate or limit cross-border data transfers (CBDT). By not regulating CBDT, the private parties conducting the deal must create their own privacy constraints. Even when regulated, the government has no say on what privacy restraints are decided between the parties. For example, this means that a country that *only* requires a binding corporate rule before a CBDT would qualify to answer "yes" to this question because the parties themselves decide the privacy protections. Another important note is that this question is not a default question "yes".	Data Protection Act	“(a) DECLARATION OF UNLAWFULNESS; POWER TO PROHIBIT UNFAIR PRACTICES; INAPPLICABILITY TO FOREIGN TRADE (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.” US Federal Trade Commission Act Section 5 <i>Although a long a convoluted explanation, the FTC gives the FTC the power to ensure that companies uphold the international privacy agreements they contract to.</i> “4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.”	“During or after the service is provided, the service provider shall collect and process the data in accordance with the following conditions: 10) Notify the data owner in case the service provider intends to transfer his personal data out of Kuwait in accordance with the data classification policy issued by CITRA.” - Kuwait Data Protection Regulation Art. 6(1) <i>This one rule does not give enough regulatory guidance to answer our question as it's a small provision about processing—not CBDT—in general and the notification has no real bearing on the rights of the data subject.</i> (1.) The personal data of Vietnamese citizens may be transferred abroad in case the Cross-border data transferer has prepared a Dossier for assessment of the impact of cross-border transfer of personal data and conducted the procedures specified in clauses 3, 4 and 5 of this Article... (8.) The Ministry of Public Security shall decide to request the cross-border data transferer to cease the cross-border transfer of personal data in cases where: ...b) The cross-border data transferer fails to comply with the provisions of Clauses 5 and 6 of this Article; c) The personal data of a Vietnamese citizen is disclosed or lost. - Viet Nam Protection of Personal Data Law Art. 25(1), (8) <i>This incorrect answer is a good example of the law needing to be read as a whole for this answer. Here, the law does not specify the privacy requirements needed to transfer; rather, the law merely states that an impact assessment must be sent upon a transfer.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
			This question must look at the law in its entirety to determine if parties will always have the freedom to negotiate privacy protections. If there is absolutely no law or tie to answer this question, then this answer will be a “no”. An example of 62 being a “no” and 63 being a “yes” is that the law regulates third parties but does not specifically mention CBDT.		Canada PIPEDA Sched. 1 Prin. 4.1.3 This provision places the burden on the domestic transfer to uphold whatever data principles it contracts. This provision meets the precise requirements that the question seeks to answer. Further, Principle 4 is titled “Accountability”, which should help inform the researcher that the law is applicable to the question when reading the Principle as a whole.	However, the impact assessment can cause a revocation of the abilities to transfer at any time. Thus, the law heavily regulates CBDTs between the need for an impact assessment upon transfer and that the governments can decree the protections insufficient. This means the answer must be “no”.
59.	Adequacy Requirements Questions		Single choice only. These questions seek to understand what type of adequacy system the country subscribes to, if there is one. Please note, if 63 is a “yes”, then all “64” must be a “no”; and, if any in “64” is a “yes”, then the rest of “64” and “63” must be “no’s”.			
59a.	Who determines adequacy or its equivalent? Data controller on its own terms—with no specific guidance		An adequacy requirement exists in the law, but whether the foreign country’s adequacy is sufficient/ in accordance with the domestic law is entirely determined by the private parties. There is *no* list that expresses what the private parties must evaluate before agreeing to a CBDT.			“10.—(1) For the purposes of section 26 of the Act, a transferring organisation must, before transferring an individual’s personal data to a country or territory outside Singapore ... take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations ... to provide to the transferred personal data a standard of protection that is at least comparable to the (continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
59b.	Who determines adequacy or its equivalent? Data controller based on statutory requirements.		An adequacy requirement for the foreign country exists and there are *explicit*, mandatory safeguards the foreign country must meet before a domestic entity may agree to a CDBT with an entity residing in the foreign country. Usually, the domestic country will require the domestic entity to complete an evaluation of the foreign country's laws/practices by using a list provided within the law. Thus, look for an adequacy requirement with a list.			protection under the Act." Singapore Data Protection Regulations Art. 10(1) <i>The provision uses the word "comparable" and not equivalent, which means that the data controller/processor has the full authority to make a judgement call. This places the example in an evaluation standard (the previous question) rather than an adequacy standard.</i>
59c.	Who determines adequacy or its equivalent? Government agency.		An adequacy requirement exists for the foreign country to meet and the domestic country's government will determine if adequacy in the foreign country is met. The domestic country will publish which countries are acceptable, allowing the domestic entity to trade with a foreign entity residing in the approved foreign country.			

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
60.	When adequacy or equivalent declaration is not found, alternative options for personal data transfers include government approval):		Multiple choices possible. This question seeks to understand what other options entities have to trade data when a foreign country has not met an adequacy standard. These questions may only be answered “yes” when the regulation states that the safeguard is sufficient in the absence of adequacy. The safeguard alone cannot answer the question.			
60a.	When adequacy or equivalent declaration is not found, alternative options for personal data transfers include government approval): Agreement between government, Data Protections Agencies (DPAs), or other governmental agencies.		Governments, data protection agencies, or other government agencies may create binding agreements between each other to trade data. These legal instruments allow for the appropriate safeguards necessary to navigate around the adequacy requirement. Please note, a direct agreement to erect and maintain safeguards between governments is not the same as the laws creating protections sufficient for adequacy, as adequacy is determined by the laws and practices legally mandated without an international agreement.		“2. International transfer of personal data with a state that does not have an adequate level of personal data protection may be done when: a) it is authorised by international acts ratified by the Republic of Albania and are directly applicable; ...” Albania Law on Personal Data Protection Art. 8(2) <i>The law is giving authority for international agreements to be sufficient to allow transfers, if the agreement stipulates to the transfers.</i> “1. A data controller shall not transfer personal data to a country outside the Federal Republic of Somalia or international organisation unless one of the following conditions is met: ...c) the recipient is subject to a law,...”	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
60b.	When adequacy or equivalent declaration is not found, alternative options for personal data transfers include (without additional government approval): Intra-group transfers based on binding corporate rules (reflecting mandatory requirements listed in data protection law).		Binding corporate rules (BCR) generally pertain to an enterprise that is spread between multiple countries. The rules permit data to transfer between the affiliates without needing an adequacy decision. Often, a BCR will be subject to a data protection authority's approval. If the text says "BCR", then the provision would answer this question. If the text does not but discusses a multinational company that needs its internal rules approved by the domestic data protection authority to transfer data, it is likely a BCR.		- Somalia Data Protection Act Art. 30(1)(c) Some countries merely write "law" in the place where "international agreement" would normally be seen. Technically, this works because any citizen is beholden to a binding international agreement as a law. "(Transfer of data to countries that do not guarantee an adequate level of protection) (3) In the case of international data transfer between companies of the same business group, the guarantee of compliance with an adequate level of protection can be achieved through the adoption of uniform internal rules regarding privacy and data protection whose compliance is mandatory." - Angola Personal Data Protection Law Art. 34(3) <i>This provision applies because BCR require the same business or its legal group to have internal rules that bind the company/legal group to perform to the standards set forth.</i>	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
60c.	When adequacy or equivalent declaration is not found, alternative options for personal data transfers include (without additional government approval): Use of government approved contractual clauses between private parties (reflecting mandatory requirements listed in data protection law).		Approved contractual clauses, also called standard contractual clauses (SCCs), are boilerplate terms issued by a government for inclusion in cross-border data transfer (CBDT) agreements. They allow authorities to mandate specific safeguards without evaluating each agreement's adequacy. If a law allows the government to draft clauses that must be included in such contracts, the provision likely qualifies.			"The international transfer of data to a country that does not guarantee an adequate level of protection is subject to authorization from the Data Protection Agency, which can only be granted in one of the following circumstances. . . . (e) If the transfer of data is necessary for the performance of a contract between the data subject and the controller or for steps taken prior to the formation of the contract decided at the request of the data subject; (f) If the transfer of data is necessary for the performance or conclusion of a contract, in the interest of the data subject, between the controller and a third party;..." Angola Personal Data Protection Law Art. 34(1)(e)-(f) Neither example works here because a simple contract does not meet the standards of an SCC that is a government-approved boiler plate addendum to private contracts.
60d.	When adequacy or equivalent declaration is not found, alternative options for personal data transfers include (without additional government approval): Accountability requirement, where domestic controller is liable for data misuse.		Accountability in CDBT refers to holding the domestic entity liable for any wrongdoing concerning personal data misuse, even if the violation occurred abroad. This ensures that someone is held accountable for data protection. Because assigning liability to domestic actors for foreign actions is politically sensitive,			

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
60e.	When adequacy or equivalent declaration is not found, alternative options for personal data transfers include (without additional government approval): Ad hoc approval by government agency.		provisions only meet this standard if they explicitly refer to “accountability” as a safeguard or clearly assign liability to the domestic controller. This safeguard allows the government to authorize transfers without any adequacy reasoning. Look for terms like “ad hoc” or language that granting the government discretion to approve countries without assessing their data protections standards.		“International transfer of data that need to be authorized (1.) In cases other than those provided for in Article 8 herein [conditions for transfer], the international transfer of personal data with a state that does not have an adequate level of data protection, shall be carried out upon an authorization from the Commissioner.” Albania Law on Personal Data Protection Art. 9(1) <i>This example works because the Commissioner is the head of a government agency that can approve transfers on a case-by-case basis.</i>	“Notwithstanding Regulation 1 [requiring adequacy], a database owner may transfer data or enable the transfer of data from his database in Israel abroad, provided that one of the following conditions is met: (8) The data is transferred to a database in a country – (3) in relation to which the Registrar of Databases announced, in an announcement published in the Official
61.	Personal data is explicitly allowed to transfer across border based on consent from the data subject:		Single choice only. This question seeks to know what level of protections are required to use consent as justification for data transfers.			Gazette (“Reshumot”), that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with the said authority. Israel Privacy Protection (Transfer of Data to Databases Abroad) Regulations Art. 2(8) (3) <i>Although the provision gives authority to the government agency to permit transfers of data to an inadequate country, there is nothing stated that shows domestic companies can request approval whenever.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
61a.	Personal data is explicitly allowed to transfer across border based on consent from the data subject: Data subject's approval alone is sufficient.		There are two ways that consent pops up in CBDT: (a) alone as an option to transfer, or (b) a way around adequacy. For both of these, they lead to the same conclusion: only consent from the data subject is needed to transfer data abroad. Thus, we made the question separate from Q60 to cover both possibilities and get any answer that allows for CBDT with consent. Importantly, no further protections are offered to the data subject after their approval. The word "consent" must be used to answer this question as a "yes". If "66b" is a "yes", then "66a" must be a "no", and vice versa.			"Article 39: When a personal information processor provides the personal information outside the People's Republic of China, it shall inform the individual of the name or name of the overseas recipient, contact information, processing purpose, processing method, types of personal information, and personal information to the overseas recipient. The methods and procedures for exercising the rights stipulated in this law [Art. 38: security assessment, certification, standard contract, or other standard], and obtaining the individual's individual consent." China PIPL Art. 39 The law here requires consent to be given to transfer data abroad, but consent alone is not sufficient. Thus, because another requirement beyond consent must also be met, the answer is "no".
61b.	Personal data is explicitly allowed to transfer across border based on consent from the data subject: Additional government approval is required.		Look for any additional safeguard required in addition to the data subject's consent to transfer data abroad. If something more than government approval, please flag and bring to supervisor. If "66a" is a "yes", this answer should be a "no".			(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
62.	Government control questions		Multiple choices possible. If a country has a system where government notification is required for adequate countries and pre-approval is required for adequate countries, then mark the country as requiring notification alone because the authority is being notified in one way or another in every case, but the same cannot be said vice versa.			
62a.	Are the following steps required for cross-border data transfers: Government pre-approval?		This question requires entities to get approval for each CBDT, or a group of CBDTs to a single entity, regardless of the country's safeguard protections. This question cannot be answered as a navigation around adequacy. This question can only be answered when transfers must be approved <u>before</u> the transfer can occur. Importantly, this question will be answered "yes" even when a threshold number of individuals' information is required to trigger the law, if the number will cause the authority to routinely give approval. In addition, this question will be answered "no" if pre-approval is only needed in certain circumstances.		"PIPL Art. 40: ... If it is really necessary to provide it overseas, it shall pass the security assessment organized by the national cybersecurity and informatization department; if laws, administrative regulations, and the national cybersecurity and informatization department stipulate that the security assessment may not be required, follow their provisions." "DESAM Art. 4(3): (3) A data processor that has provided personal information of 100,000 people or sensitive personal information of 10,000 people to overseas countries since January 1 of the previous year has provided personal information overseas;..." China PIPL Art. 40 & Data Export Security Assessment Measures Art. 4	"(Transfer of data to countries that ensure an adequate level of protection): The international transfer of data to countries that ensure an adequate level of protection is subject to notification to the Data Protection Agency," Angola Personal Data Protection Law Art. 33(1) <i>A mere notification is not sufficient to mark this answer as a "yes". Notifications do not necessarily slow the process of transfers and the point of the question is to discover if transfers are inefficient or encumbered by requirements.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
62b.	Are the following steps required for cross-border data transfers: Notification of transfer without authorization/pre-approval?		This question can be answered when pre-authorization of a transfer is not required but the government must be notified about the transfer. The notification requirement can come before, during, or after the transfer—all that matters is that the government does not have to approve the transfer. This question may also be answered when the government may revoke the transfer upon finding an issue. A mere requirement to record the transaction does not sufficiently answer the question but should be marked in the methodology tab of the dataset.		Here, the law requires companies to submit a security assessment that must be reviewed and approved before transfer. The threshold of 100,000 people's data is not so disproportionately high as to preclude it from answering this question, as many companies will be working with more data than that.	“(Preparing of Records on Provision of Personal Data to Third Parties) Article 29 (1) When having provided personal data to a third party ..., businesses handling personal information must prepare a record pursuant to Order of the Personal Information Protection Commission on the date of the provision of the personal data, the name of the third party, and other matters prescribed by Order of the Personal Information Protection Commission; ... (2) A business handling personal information must keep a record under the preceding paragraph for a period of time prescribed by Order of the Personal Information Protection Commission from the date when it prepared the record.” Japan Act on Protection of Personal Information Art. 29 The provision does not mandate that the notification must be sent to the Commission; rather, the record must merely be kept with the possibility that it will be given to the Commission upon request. (continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
62c.	Are the following steps required for cross-border data transfers: Submission of security assessment?	This can create cumbersome administrative and operational burdens and pose unreasonable operational challenges to both domestic companies conducting international business or engaging in any dealing or communications with overseas counterparties and foreign-invested companies who would inevitably share personal information with overseas parents and affiliates on a daily basis. ⁵⁸	Security assessments are reviews done by a domestic entity to be given to the government during authorization approval procedures/applications. This question may only be answered “yes” when the security assessment is a general rule to acquire government approval.		“Article 4 If a data processor provides data overseas under any of the following circumstances, it shall apply to the national cybersecurity and informatization department for a data export security assessment through the local provincial cybersecurity and informatization department: (1) Data processors provide important data overseas; (2) Critical information infrastructure operators and data processors that handle the personal information of more than 1 million people provide personal information overseas.” China Data Export Security Assessment Measures Art. 4(2) <i>The provision requires a full assessment sent to the authority for approval. The law will specify the requirements for the assessment also.</i>	
63.	Data Localization questions	Data localization requirements can significantly hinder the economic benefits enable by Internet of Things (IoT) technologies, reducing potential gains to GDP, growth, employment, trade and investment. ⁵⁹	Multiple choices possible. These questions seek to find the various types of data localization that might be required. Data localization is different from CBDT as it focuses on where the data must be stored. Some countries can allow a CBDT but not storage in a			

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
63a.	*No* general personal data localization requirement exists.		foreign country. This is because storage can be anywhere in the world, regardless of where the data is accessed. For example, VPNs and cloud storage can allow access to data in different locations than where the servers are. 68b through 68p accumulate points by marking each applicable on the different levels.			
63b./g./l	[Combined] Requirement to keep sector specific data stored/processed/accessible within country: All personal and non-personal data.		Some personal data protection laws require personal data to be stored in only the domestic country. Not finding an answer makes this question a “yes” to gain points. This question will be a “yes” for the majority of countries.			
63c./h./m	[Combined] Requirement to keep sector specific data stored/processed/accessible within country: Financial data.				“1.1.1 An automated teller machine operator shall: i) not send any transaction outside Ethiopia for the purpose of processing, authorization or switching (only applies for licensed automated teller machine operator). “3.2 A banking corporation shall not store customer information or data on the cloud outside the borders of the State of Israel, unless it has ascertained that the cloud service provider meets the level of protection in accordance with the directive 95/46/EC on	(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
					Ethiopia Licensing and Authorization of Payment Systems Operators Art. 11.1(j) <i>Here, the provision applies to storage, processing, and accessibility because there is no way to transmit the information abroad, leaving the logical deduction that the information will only be accessible within Ethiopia.</i>	the protection of individuals with regard to the processing of personal data and the free movement of such data directive of the European Union.” Israel Risk Management in Cloud Computing Environment Para. 3.2 <i>Because there is a way around the localization requirement, we count this answer as a “no”. Note: mark in blue in source tab to show it is a close call.</i>
63d/i/n	[Combined] Requirement to keep sector specific data stored/processed/accessible within country: Health data.		Storage only. If “68i/n” are a “yes”, this must be a yes.			
63e/j/o	[Combined] Requirement to keep sector specific data stored/processed/accessible within country: National security related data.		Storage only. If “68j/o” are a “yes”, this must be a yes.			
63f/k/p	[Combined] Requirement to keep sector specific data stored/processed/accessible within country: Telecommunications data.		Storage only. If “68k/p” are a “yes”, this must be a yes.			

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
64.	Explicit framework on non-personal data cross-border data transfers		Legal provisions are narrowed into stating “non-personal” data. Currently, the rules on CBDT for non-personal data are so new that the word will be used when the meaning is intended.	Data Protection Law	“Article 1 Subject matter This Regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.” EU Regulation on a Framework for the Free Flow of Non-Personal Data in the EU Art. 1 <i>The provision expressly states that the entire regulation applies to non-personal data.</i>	
65.	Explicit rules on portability of non-personal data		The word “portability” will likely be used because of how new non-personal data regulations are. Provisions that include portability of all data are not included because the purpose of the question is to determine the countries that specifically regulate non-personal data.	Data Protection Law	“Article 6 Porting of data 1. The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level (‘codes of conduct’), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, (a) best practices for facilitating the switching of service providers...; (d) communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.” - EU Regulation on a Framework for the Free Flow of Non-Personal Data in the EU Art. 6(1) <i>The provision discusses the interoperability of non-personal data. The further explanation in the sub-articles sufficiently provides the explicit rules necessary.</i>	

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
66.	Rules on preventing network providers or ISP from limiting data flow in their systems (net neutrality)	Network neutrality is a principle of equal treatment of data on all platforms and services. The treatment must be done in a way that does not discriminate in favor of certain services over others. ⁶⁰	Because the definition of net neutrality is used differently all over the world, the question uses a broad definition. Provisions that have open access, anti-discrimination, or anti-limitation principles work to answer the question.	Telecommunications Law	"3. Policy Directives on Net Neutrality: 3.1 The Government is committed to the fundamental principles and concepts of Net Neutrality i.e., keep the Internet accessible and available to all without discrimination. Internet Access Services, therefore, need to be governed by a principle that restricts any form of discrimination, restriction or interference in the treatment of content, including practices like blocking, degrading, slowing down or granting preferential speeds or treatment to any content. To ensure that the regulatory framework on Net Neutrality adheres to the fundamental principles and concepts of Net Neutrality, the policy directives as mentioned in the succeeding paras are hereby issued..." India DoT Letter on Net Neutrality Regulatory Framework para. 3 The paragraph above introduces the principles that the rest of the document seeks to apply. This is sufficient to answer the question at hand.	"3. Internet service providers limit access to the Internet resource based on: restricted list – organizations (except for the Ministry of Information, the Ministry of Communications and Informatization, ...), individuals, including individual entrepreneurs, on a free basis..." Belarus Resolution on the Approval of the Regulations on the Procedure for Restricting (Renewing) Access to an Internet Resource para. 3 The provision explicitly permits the limitation of access, which is antithesis to the question. Thus, the provision cannot apply.

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
INTERMEDIARY LIABILITY						
67.	Framework explicitly addresses online intermediary liability	Rules on intermediary liability are trending in two different manners currently: either mandating liability exists for intermediaries or protecting intermediaries from liability. Clear rules are useful for organizations to understand the liability of allowing users to publicly post information on websites. ⁶¹	The provision does not need to limit liability, but merely address liability for intermediaries. This answer can be broad or narrow, and it can specifically give liability to service providers. If any of the safe harbor or notification questions are answered, this question must also be answered, but that is not necessarily true vice versa.	• Electronic Transactions Law • Online Safety Law • Copyright Law • Intellectual Property Law • Telecommunications Law • Internet Services Act	“Article 24. Liability of intermediaries and electronic commerce service providers...” • Cambodia Law on Electronic Commerce Art. 24 <i>The provision or the chapter [titled the same as the article] on intermediaries both work to show that Cambodia has a framework of laws that regulate online intermediary liability. Thus, the provision is sufficient to answer the question.</i>	“27(2.3) It is an infringement of copyright for a person, by means of the Internet or another digital network, to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service.” “29.21 (1) It is not an infringement of copyright for an individual to use an existing work or other subject-matter or copy of one, which has been published or otherwise made available to the public, in the creation of a new work or other subject-matter in which copyright subsists and for the individual — or, with the individual's authorization, a member of their household — to use the new work or other subject-matter or to authorize an intermediary to disseminate it,....” • Canada Copyright Modernization Act Secs. 27(2.3), 29.21 <i>Both of these provisions are good examples of incorrect frameworks for the question at hand. The first provision states that online infringements occur when the “service primarily” enables copyright infringement. That means that the regulation applies when the purpose of the online website is to infringe copyrighted material. As the question seeks to understand regulations for legal websites’ users’ illegal infringements, the provision does not apply. The second provision is about publicly released work that has authorization for use. Thus, neither of these provisions apply to answering the question at hand.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
68.	Online intermediaries are not required to routinely monitor content uploaded by third parties	This requirement may impose too much burden on hosting provider which will unreasonably curb their freedom to conduct business. ⁶²	This question seeks to understand if the law specifically carves out the need to monitor content. Without the specific carve-out, the law is unclear whether or not monitoring might be required. Thus, the answer does not count unless the provision mentions monitoring or its equivalent.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	“45. (1) A service provider shall not ... be generally obliged to – (a) monitor the data which it transmits or stores...” Botswana Electronic Communications and Transactions Act Art. 45(1)(a) <i>The law explicitly states that the online service providers are not required to monitor the data. This provision, thus, applies.</i>	“1 The provider of an internet hosting service which stores information entered by users is required to prevent a work or other protected subject matter from being unlawfully remade available to third parties through the use of its services, if the following requirements are fulfilled: ... b. The provider has been notified of the infringement.” Switzerland Federal Law on Copyrights and Related Rights Arts. 39d(1)(b) <i>The provision does not work because online service providers are subject to prior knowledge. At first glance, the chapeau seems to create a monitoring requirement with the phrase “prevent a work”, but the notification element eliminates a monitoring requirement. Thus, the provision does not apply.</i>
69.	Safe harbor provisions exist to shield online platforms or hosting providers from liability	An unreasonable burden of enforcement on intermediaries may stifle their freedom to operate and is likely to increase their business risks and legal expenses. ⁶³	Multiple choices possible.			
69a.	Safe harbor provisions exist to shield online platforms / hosting providers from liability for: Unlawful activity generally	This relieves intermediaries from liability under certain circumstances, such as where they did not modify third party content before posting or transmitting it.⁶⁴	The provision must be housed within a non-IP law.	- Electronic Transactions Law - Online Safety Law - Telecommunications Law - Internet Services Act	“Article 3(1) If the rights of others are violated due to dissemination of information through specified telecommunications, the specified telecommunications service provider that uses specified telecommunications facilities used for specified telecommunications ... will not be liable for damages resulting from the violation, unless it is technically	“Article 102 (Limitation on Liability of Online Service Providers) (1) Even if copyright or other rights protected pursuant to this Act are infringed in relation to any of the following subparagraphs, an online service provider shall not be responsible for such infringement...” Republic of Korea Copyright Act Art. 102(1) <i>The provision resides within an IP-based law and cannot apply to general unlawful activity.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
69b.	Safe harbor provisions exist to shield hosting providers from liability for: Infringements related to intellectual property	While some countries have rules on the liability of intermediaries regarding topics such as hate speech, intellectual property rights—which are crucial for e-commerce—are not usually covered. This is indicative of a more comprehensive regulatory framework.⁶⁵	The law must clearly state that the limitation applies to IP issues or the provision must be contained in an IP law.	- Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	possible to take measures for preventing the information from being transmitted to unspecified persons and the violation falls under any of the following items; provided, however, that this does not apply if the related service provider is the sender of information violating the rights of others...” Japan Act on the Limitation of Liability of Specified Telecommunications Service Providers for Damages and the Right to Demand Disclosure of Sender Identification Information Art. 3(1) <i>The provision limits liability for other's wrongs.</i>	“Article 3(1) If the rights of others are violated due to dissemination of information through specified telecommunications, the specified telecommunications service provider that uses specified telecommunications facilities used for specified telecommunications ... will not be liable for damages resulting from the violation, unless it is technically possible to take measures for preventing the information from being transmitted to unspecified persons and the violation falls under any of the following items; provided, however, that this does not apply if the related service provider is the sender of information violating the rights of others...”

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
70.	Notice and take down procedures required for: -Unlawful activity generally	Once intermediaries are notified of infringing content on their platform or website, they should have a procedure to remove it expeditiously. This mitigates risks posed by the infringing content. ⁶⁶	Both the take-down requirement and the notification requirement must be triggered by the same act of infringement. If only one—either notification or take-down—is regulated in isolation, the provision does not meet the criteria. Second, ensure that the removal procedures stem from the service provider, not the court system. The purpose of this question is to discover whether the law creates requirements for the service providers themselves. Note that if the notification and takedown procedure comes solely from the government, there is a good chance that the law will answer Q79 on judicial restrictions.	- Electronic Transactions Law - Online Safety Law - Telecommunications Law - Internet Services Act	"Article 497. Liability of online service providers: Online service providers cannot be held civilly liable ... if, from the moment they became aware of it, they acted promptly to remove this data or make access to it impossible ..." Article 498. Notification of illicit content: Knowledge of the disputed facts is presumed to have been acquired by the online service provider when it is notified of the following elements: ... (4) the description of the disputed facts and, if possible, their precise location, ..." Benin Digital Code Arts. 497-498 The two provisions can be linked to answer the question. Importantly, the law creates a take-down requirement upon notification. As the obligation stems from the entity itself as well, the question can be answered with the provision.	- Japan Act on the Limitation of Liability of Specified Telecommunications Service Providers for Damages and the Right to Demand Disclosure of Sender Identification Information Art. 3(1) The provision does not state anywhere that it specifically applies to intellectual property right infringements, and, therefore, does not apply to the question at hand. "20.—(1) Any Minister may instruct the Competent Authority to issue a Part 4 Direction... 22.—(1) A Disabling Direction is one issued to the internet intermediary that provided the internet intermediary service by means of which the subject material has been or is being communicated in Singapore, requiring it to disable access by end-users in Singapore to the subject material provided on or through the service that consists of or contains the subject statement, by the specified time." - Singapore Protection from Online Falsehoods and Manipulation Act Arts. 20(1), 22(1) The notification comes from the authority alone and the obligation to take down the material comes from a written order. Thus, the provision cannot apply as there is no procedure for a user to report issues.

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
71.	Notice and take down procedures required for: -Infringements related to intellectual property	IP can be so widely distributed that notice and takedown procedures can help online service providers find and stop IP infringements more efficiently. ⁶⁷	First, ensure the law/provision specifically applies to IP. Second, ensure that the removal procedures stem from the service provider, not the court system. The purpose of this question is to discover whether the law creates requirements for the service providers themselves. Question 79 answers whether the courts/agencies are the sole authorities for removal.	- Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	"Article 103 (Suspension of Reproduction or Interactive Transmission) (1) Any person who claims that his or her copyright and other rights protected under this Act are infringed ... due to the reproduction or interactive transmission of works, etc. through the use of services by an online service provider ..., may demand the online service provider, ... suspend the reproduction or interactive transmission of the works, etc. ..." Republic of Korea Copyright Act Art. 103 <i>The provision allows users to notify service providers of infringement issues and have those issues removed.</i>	"Article 5. Duty of enterprises providing intermediary service. ... 3. Removing and deleting content of digital information which violates copyright and related rights, cutting, stopping and suspension of the Internet line, telecommunication line as receiving request in written of the inspector of the Ministry of Information and Communications or inspector of the Ministry of Culture, Sports, and Tourism or other competent State agencies as prescribed by law." Viet Nam Joint Circular Regulating the Duty of Enterprises Providing Intermediary Service in Protection of Copyright and Related Rights in the Internet and Telecommunication Networks Environment Art. 5(3) <i>The provision provided does create a notice- and-takedown requirement, but the requirement comes from notice from the government. As this does not apply to the average citizen wanting to notify an enterprise, the provision does not apply to the question at hand.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
72.	Content providers' right to counter notice	Unless there are exceptional circumstances, the providers of material should be informed by the platforms of the removal and have the possibility to contest counter-notice, then out-of-Court dispute resolution mechanisms and, ultimately, before the judicial Courts. ^{68,69}	Ensure that the provision discusses the content provider's right to counter notice. As the terms can change for this from country to country, check the definitions if needed and the purpose of the provision itself.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	“(2)Exception.—Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider— (A)takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material; (B)upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days;.... Contents of counter notification.—To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:....” United States 17 U.S.C. Sec. 512(g)(2)(B), 17 U.S.C. Sec. 512(g)(3) <i>The provision creates the right and ability for the content provider to give a counternotice to the service provider.</i>	“Article 15.7. Extrajudicial measures to terminate the violation of copyright and (or) related rights in information and telecommunication networks, including the Internet, taken at the request of the copyright holder. ... 7. If the owner of a site on the Internet has evidence confirming the legality of posting on his site on the Internet, ... the owner of the Internet site has the right not to take the measures provided for ... and is obliged to send the applicant a corresponding notification with the specified evidence.” Russia Federal Law on Information, Information Technologies and Information Protection Art. 15.7(7) <i>The example does not apply because the notice of legality comes from the service provider, not the content provider. In this instance, there is no right for the content provider to send a counternotice. Rather, the right is that the service provider may keep the material online upon finding justification for its legal use. Thus, the provision does not apply.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
73.	Online platforms' / Hosting providers' right to counter notice/appeal	An adequate system for appealing requests is an important aspect to a strong notice and takedown mechanism. This allows greater safeguards against abusive notices and avoids suppression of legitimate content. ⁷⁰	This question may be answered when a higher authority decides that the website controller (online service provider) has incorrectly permitted an infringement to remain online, and the website controller disagrees with the authority's opinion. The authority could be a government agency, the courts, or a higher level of authority over the telecommunications system. This regulation is currently rare, so expect it to be difficult to find.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	"9. The website owner has the right to apply to the hosting service provider, from whom he received information about the measures taken in accordance with part seven of this article, with a notice of refusal in accordance with part five of this article, demanding the restoration of access to digital content..." Ukraine Law on Copyright and Related Rights Art. 56(9) <i>The law here divides the website owners and the hosting providers to create a situation where a hosting provider can be contacted for infringement removal. Because of this situation, there is a right to counternotice.</i>	"Article 43: After receiving the forwarded notice, the operator of the platform (user) may submit a statement that there is no infringement to the operator of the e-commerce platform. The statement should include preliminary evidence that there is no infringement. After receiving the statement, the e-commerce platform operator shall forward the statement to the intellectual property right holder who issued the notice and inform him that he can lodge a complaint with the relevant competent authority or file a lawsuit with the people's court..." China E-Commerce Law Art. 43 <i>Here, the online service provider is not appealing to a higher authority when disagreeing with the user's argument, nor is the service provider given the right to disagree in the provision. Thus, as the provision does not pertain to appeals or counternotices from a hosting provider or online platform, the provision does not apply.</i>

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
74.	Online platforms / Hosting providers are not liable for wrong deletion if the deletion is conducted following a takedown notice	Copyright owners tend to send notices without diligent investigation, and intermediaries are highly likely to remove the material to reduce the risk of litigation, leading to wrong deletion. ⁷⁰	The provisions that have this answer provide the same or exceedingly similar language as the question.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	"A service provider acting in compliance with subsection 43H(1) and in accordance with this Part shall not be subject to any liability in respect of an action taken in good faith in relation to— a. The removal of an electronic copy of a work from its primary network; or b. The disabling of access to an electronic copy of a work on its primary network or another network. Malaysia Copyright Act Art. 43F(1) <i>The provision uses specific language that matches the question and, thus, answers the question.</i>	"The intermediary or service provider is liable for wrongful takedown in response to a notification." Ghana Electronic Transactions Act Art. 94(4) <i>The provision provides an example of the opposite of the question's intention. This provision shows that Ghana does not have such a system and considered it. Thus, this question is marked as no and the answer is saved in blue on the source tab for any future country-specific research.</i>
75.	Complainants are liable for wrong deletion following a takedown notice		The provisions that have this answer provide the same or exceedingly similar language as the question.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	"A person who knowingly makes a false statement on the notification in subsection (1) is liable to the service provider for the loss or damage suffered by the service provider." Uganda Electronic Transactions Act Art. 31(2) <i>The provision establishes liability for false notifications.</i>	N/A

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
76.	Online platforms / Hosting providers are required to disclose the identity of infringers to the extent it is available to them	Hosting providers normally do not retain enough personal data to have suspected infringers successfully identified, so the effectiveness of identify disclosure is in question. ⁷¹	This question seeks to understand whether an independent obligation exists for service providers to report a user's identity to authorities, without a previous order. Thus, this question should be answered "yes" when a self-reporting structure exists.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	"... The service provider must inform the competent state authority if he has reasonable grounds to suspect that: 1) by using its service, the service user undertakes illegal activities; 2) the user of his service provided inadmissible information. The service provider is obliged to present, on the basis of an appropriate judicial or administrative act, all data on the basis of which the detection or prosecution of perpetrators of criminal acts, ie the protection of the rights of third parties can be undertaken...." Serbia Law on E-Commerce Art. 20, para. 2 <i>The provision creates the necessary obligation to report without a previous order. Thus, the provision applies to the question at hand.</i>	"Article 85 S. The competent court, at the request of the rights holders who have initiated the procedure established in the preceding article, may order the delivery of information that allows the identification of the alleged infringer by the respective service provider." Chile Law on Intellectual Property Art. 85S <i>The provision here does not apply to the question because the disclosure requirement only triggers upon a court order.</i>
77.	If online platforms / hosting providers are required to disclose the identity of infringers (CQ=1), they are not liable for the failure to do so (If CQ=0 à CR=0)		This question may be answered whether or not an independent self-reporting structure exists, unlike the previous question. However, the law must clearly state that the failure to disclose the identity of the infringer would not cause liability. Likely, because failing to comply with a judicial order would create serious liability, this question will only be answered when a self-reporting structure exists.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act		

(continued on next page)

(continued)

#	Regulatory Solution	Reason	What is Captured	Usually Found in	Correct Example	Incorrect Example
78.	Online platforms / Hosting providers may not disclose their users' identity information to third parties without court orders	Because of privacy concerns, hosting ISPs should be forbidden to voluntarily disclose suspected infringers' identities to copyright owners without orders from courts or competent authorities. ⁷²	The provision will restrict sharing the personal information of a user in the same section of the law as the other provisions on intermediary liability. Because this question seeks to know whether the law addresses privacy rights in intermediary liability instances, the provisions should be carefully taken from applicable law, not a general privacy law.	- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act	"(5) An online content host must not disclose any personal information about the complainant or author under information privacy principle 11(1)(e)(iv) set out in section 22 of the Privacy Act 2020, except by order of a District Court Judge or a High Court Judge made on an application under this subsection." New Zealand Harmful Digital Communications Act Sec. 24(5) <i>The provision here directly responds to the question at hand.</i>	"Article 5(1) A person alleging that their rights are violated due to dissemination of information through specified telecommunications, may demand the disclosure of sender identification information..." Japan Act on the Limitation of Liability of Specified Telecommunications Service Providers for Damages and the Right to Demand Disclosure of Sender Identification Information Art. 5(1) <i>The law contains multiple provisions specifying how the victim may demand the identification of the infringer and how the victim cannot use the information further. Thus, these provisions are the opposite answer to the question.</i>
79.	An order from a judicial court or competent authority is required to require content restriction	Such enforcement should be ensured by public authorities, in particular regulatory authorities and judicial courts. ⁷³		- Electronic Transactions Law - Online Safety Law - Copyright Law - Intellectual Property Law - Telecommunications Law - Internet Services Act		

Endnotes

1. UNCITRAL (1996) Model Law on Electronic Commerce.
2. UNCITRAL (1996) Model Law on Electronic Commerce.
3. UNCITRAL (1996) Model Law on Electronic Commerce.
4. UNCITRAL (1996) Model Law on Electronic Commerce.
5. UNCITRAL (1996) Model Law on Electronic Commerce.
6. UNCITRAL (1996) Model Law on Electronic Commerce.
7. UNCITRAL (2007) United Nations Convention on the Use of Electronic Communications in Electronic Contracts; UNCITRAL (2001) Model Law on Electronic Signatures.
8. UNCITRAL (2001) Model Law on Electronic Signatures.
9. ITU (2018), “Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security”, https://digitalregulation.org/wp-content/uploads/D-PREF-BB.POW_ECO-2018-PDF-E.pdf.
10. ITU (2018), “Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security”, https://digitalregulation.org/wp-content/uploads/D-PREF-BB.POW_ECO-2018-PDF-E.pdf.
11. International Trade Centre (2017), International Trade Forum: Trade for the 99%, <https://intracen.org/news-and-events/news/making-trade-work-for-the-99>.
12. ESCAP (2020) “Legal Readiness Assessment Guide”, <https://readiness.digitalizetrade.org/files/documents/legal-readiness-assessment-guide.pdf>.
13. UNCITRAL (2018) Model Law on Electronic Transferable Records.
14. UNCTAD (2017), «Consumer Protection in Electronic Commerce», https://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf.
15. OECD (2018) «Improving Online Disclosures with Behavioural Insights», <https://doi.org/10.1787/39026ff4-en>.
16. OECD (2018) «Improving Online Disclosures with Behavioural Insights», <https://doi.org/10.1787/39026ff4-en>.
17. OECD (2018) «Improving Online Disclosures with Behavioural Insights», <https://doi.org/10.1787/39026ff4-en>.
18. OECD (2018) «Improving Online Disclosures with Behavioural Insights», <https://doi.org/10.1787/39026ff4-en>.
19. OECD (2018) «Improving Online Disclosures with Behavioural Insights», <https://doi.org/10.1787/39026ff4-en>.
20. OECD (2016), «Consumer Protection in E-commerce: OECD Recommendation» <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>
21. OECD (2016), «Consumer Protection in E-commerce: OECD Recommendation» <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.
22. VON BAR Christian / CLIVE Eric (editors), Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR) – Full Edition, Prepared by the Study Group on a European Civil Code and the Research Group on EC Private Law (Acquis Group), Vol. 1, Munich 2009, https://www.law.kuleuven.be/personal/mstorme/european-private-law_en.pdf.
23. VON BAR Christian / CLIVE Eric (editors), Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR) – Full Edition, Prepared by the Study Group on a European Civil Code and the Research Group on EC Private Law (Acquis Group), Vol. 1, Munich 2009, https://www.law.kuleuven.be/personal/mstorme/european-private-law_en.pdf.
24. FORBRUKERRADET (2018), <https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf>.
25. UIE (2017) Dark Patterns and the Ethics of Design, <https://medium.com/adventures-in-ux-design/dark-patterns-and->

- [the-ethics-of-design-31853436176b](#).
26. OECD (2005) Report of the OECD Task Force on SPAM: Anti-SPAM Toolkit of Recommended Policies and Measures, <https://www.oecd.org/digital/consumer/36494147.pdf>.
 27. OECD (2005) Report of the OECD Task Force on SPAM: Anti-SPAM Toolkit of Recommended Policies and Measures, <https://www.oecd.org/digital/consumer/36494147.pdf>.
 28. OECD (2005) Report of the OECD Task Force on SPAM: Anti-SPAM Toolkit of Recommended Policies and Measures, <https://www.oecd.org/digital/consumer/36494147.pdf>.
 29. ITU (2005), «A Comparative Analysis of SPAM Laws: The Quest for a Model Law», https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf.
 30. OECD (2016), «Consumer Protection in E-commerce: OECD Recommendation» <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.
 31. FCC (2024), “FCC Fact Sheet: Strengthening Consumer Protections Against Unwanted Robocalls”, <https://docs.fcc.gov/public/attachments/DOC-400039A1.pdf>.
 32. OECD (2016), «Consumer Protection in E-commerce: OECD Recommendation», <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.
 33. OECD (2016), «Consumer Protection in E-commerce: OECD Recommendation», <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.
 34. OECD (2006), “Best Practices for Consumer Policy: Report on the Effectiveness of Enforcement Regimes”, [https://one.oecd.org/document/DSTI/CP\(2006\)21/FINAL/en/pdf](https://one.oecd.org/document/DSTI/CP(2006)21/FINAL/en/pdf).
 35. UNCTAD (2016): Data protection regulations and international data flows: Implications for trade and development https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
 36. Opinion WP29 06/2014, <http://www.dataprotection.ro/servlet/ViewDocument?id=1086>.
 37. EFF (2021), “EFF Transition Memo to Incoming Biden Administration”, <https://www.eff.org/wp/eff-transition-memo-incoming-biden-administration#Contents>.
 38. UNCTAD (2016), “Data protection regulations and international data flows: Implications for trade and development”, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
 39. European Union Agency for Fundamental Rights (2018), “Handbook on European data protection law”, <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>.
 40. CoE (2018) Convention 108+: Convention for the protection of individuals with regard to the processing of personal data, <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.
 41. UNCTAD (2016), “Data protection regulations and international data flows: Implications for trade and development”, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
 42. European Union Agency for Fundamental Rights (2018), “Handbook on European data protection law”, <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>.
 43. Working Party Article 29 Guidelines on consent under Regulation 2016/679, <https://ec.europa.eu/newsroom/article29/items/623051>.
 44. OECD (2020), “Mapping Approaches to Data and Data Flows”, <https://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf>.
 45. ICO (2011), “Data sharing code of practice”, https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.
 46. UNCTAD (2016), “Data protection regulations and international data flows: Implications for trade and development”, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
 47. UNCTAD (2016), “Data protection regulations and international data flows: Implications for trade and development”, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

48. EDPS (2021), “Encryption”, https://www.edps.europa.eu/data-protection/our-work/subjects/encryption_en.
49. WP29 (2016), “Guidelines on Data Protection Officers (‘DPOs’)”, <https://ec.europa.eu/newsroom/article29/items/612048/en>.
50. CIPL (2016), “Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR”, https://iapp.org/media/pdf/resource_center/cipl_gdpr_risk_21_dec_2016.pdf.
51. Ramesh Ramachandran, “The Importance of Training: Cybersecurity Awareness like a Human Firewall”, Entrepreneur India (2019), <https://www.entrepreneur.com/en-in/growth-strategies/the-importance-of-training-cybersecurity-awareness-like-a/340838>.
52. Working Party Article 29 Guidelines on consent under Regulation 2016/679, <https://ec.europa.eu/newsroom/article29/items/623051>.
53. Working Party Article 29 Guidelines on consent under Regulation 2016/679, <https://ec.europa.eu/newsroom/article29/items/623051>.
54. World Bank (2019), “ID4D Practitioners Guide”, <https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>.
55. European Union Agency For Cybersecurity (2021), “ENISA’s work on National Cybersecurity Strategies”, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>.
56. World Bank (2019), “Global Cybersecurity Capacity Program Lessons Learned and Recommendations towards Strengthening the Program”, <https://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf>.
57. UNCTAD (2016), “Data protection regulations and international data flows: Implications for trade and development”, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
58. Baker McKenzie (2019), “China Proposes More Stringent Rules on Security Assessment of Export of Personal Information”, <https://www.globalcompliancenews.com/2019/07/31/china-proposes-more-stringent-rules-security-assessment-export-personal-information-20190703/>.
59. GSMA (2021), “Cross-Border Data Flows: The impact of data localization on IoT”, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf.
60. EFF (2024), “Net Neutrality” <https://www.eff.org/issues/net-neutrality#:~:text=-Network%20neutrality%20is%20the%20idea,idea%20that%20ISPs%20could...>
61. EFF (2022), “Platform Liability Trends Around the Globe: Taxonomy and Tools of Intermediary Liability”, <https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-taxonomy-and-tools-intermediary-liability>.
62. Wang, Jie, “Regulating Hosting ISPs’ Responsibilities for Copyright Infringement: The Freedom to Operate in the US, EU and China”, Springer Singapore Pte. Limited, 2018. ProQuest Ebook Central, <https://ebookcentral-proquest-com.libproxy-wb.imf.org/lib/jointlib-ebooks/detail.action?docID=5358158>.
63. Wang, Jie, “Regulating Hosting ISPs’ Responsibilities for Copyright Infringement : The Freedom to Operate in the US, EU and China”, Springer Singapore Pte. Limited, 2018. ProQuest Ebook Central.
64. Manila Principles on Intermediary Liability (2015), <https://www.manilaprinciples.org>.
65. Beatrice Martinet & Reinhard J. Oertli, “Liability of E-Commerce Platforms for Copyright and Trademark Infringement: A World Tour”, American Bar Association (2015), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2014-15/may-june/liability-e-commerce-platforms-copyright-trademark-infringement-world-tour/.
66. EFF (2022), “Platform Liability Trends

- Around the Globe: Taxonomy and Tools of Intermediary Liability”, <https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-taxonomy-and-tools-intermediary-liability>.
67. CREATE (2021), “21 for 2021: Notice-and-Takedown in Copyright Intermediary Liability”, <https://www.create.ac.uk/blog/2021/06/25/21-for-2021-notice-and-takedown-in-copyright-intermediary-liability/>.
 68. CERRE (2018), “Liability of online hosting platforms: should exceptionalism end?”, <https://cerre.eu/publications/liability-online-hosting-platforms-should-exceptionalism-end/>.
 69. CREATE (2021), “21 for 2021: Notice-and-Takedown in Copyright Intermediary Liability”, <https://www.create.ac.uk/blog/2021/06/25/21-for-2021-notice-and-takedown-in-copyright-intermediary-liability/>.
 70. Wang, Jie, Regulating Hosting ISPs> Responsibilities for Copyright Infringement : The Freedom to Operate in the US, EU and China, Springer Singapore Pte. Limited, 2018. ProQuest Ebook Central.
 71. Wang, Jie, Regulating Hosting ISPs> Responsibilities for Copyright Infringement : The Freedom to Operate in the US, EU and China, Springer Singapore Pte. Limited, 2018. ProQuest Ebook Central.
 72. Wang, Jie, Regulating Hosting ISPs> Responsibilities for Copyright Infringement : The Freedom to Operate in the US, EU and China, Springer Singapore Pte. Limited, 2018. ProQuest Ebook Central.
 73. De Streel, A. et al., Online Platforms> Moderation of Illegal Content Online, Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.



THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

TRADE, INVESTMENT AND COMPETITIVENESS