Policy Research Working Paper 9615

World Development Report 2021

Background Paper

Mapping Data Governance Legal Frameworks Around the World

Findings from the Global Data Regulation Diagnostic

Rong Chen

WORLD BANK GROUP
Development Economics
World Development Report 2021 Team
April 2021

Policy Research Working Paper 9615

Abstract

A robust data governance regulatory environment, encompassing both safeguards that protect the rights of market players and enablers that facilitate use/reuse of data, provide an important foundation for trust in the data economy. This paper presents the methodology and findings from a Global Data Regulation Diagnostic. The Global Data Regulation diagnostic is a detailed assessment of laws and regulations on data governance, covering both safeguards and enablers for data governance across 80 countries ranging from low to high income groups. Diagnostic results show that countries have put in greater effort in adopting enabling regulations than regulatory safeguards. However, the development of both enablers and safeguards remains at an intermediate stage: only 41 percent of good practices for safeguards and 47 percent for enablers have been adopted across countries. The diagnostic identifies gaps in the regulatory framework across several important dimensions including safeguards for personal and nonpersonal data, cross-border data flows and cybersecurity, as well as enablers for public and private intent data, as well as e-commerce. While higher income countries are typically more advanced than their lower income counterparts, significant gaps nonetheless remain in the regulatory framework for data across all income groups.

This paper is a product of the World Bank's *World Development Report 2021* Team, Development Economics. It is part of a larger effort by the World Bank to provide open access to its research and make a contribution to development policy discussions around the world. Policy Research Working Papers are also posted on the Web at http://www.worldbank.org/prwp. The author may be contacted at rchen5@worldbank.org.

Mapping Data Governance Legal Frameworks Around the World: Findings from the Global Data Regulation Diagnostic[1]

Rong Chen

Key words: data protection, laws, regulatory framework

JEL codes: K19, K24, L86, O38

[1] The paper is a background paper for the World Development Report 2021: Data for Better Lives. The author would like to thank the following colleagues from the World Bank Group for their review and valuable feedback on the paper: Mark Williams (Practice Manager, Digital Development Global Practice) and Silvia Muzi (Program Coordinator, Development Economics Vice Presidency). The author is also grateful to participants to the World Development Report 2021 Seminar Series (Seminar 2: Data policies, laws and regulations) for their comments and suggestions.

1. Introduction

Digital data is growing at exponential rates. Individuals are leaving digital footprints through their daily activities. Businesses accumulate data about customer behaviors and preferences, using them to improve efficiency and to facilitate exchanges. Governments are also taking initiatives on data accumulation by creating, for example, smart cities and incorporating data analytics into their policy making. If used well, data can foster inclusive economic growth and improve the delivery of public services. Concerns regarding data protection and security are mounting, however, as data breaches and potential violations of individual rights increase.

Governments have been adopting various approaches to improve data protection and security. For instance, the European Union has adopted the General Data Protection Regulation (GDPR), which emphasizes the rights of data subjects who might be either identified or identifiable. The United States and the Asia-Pacific Economic Cooperation (APEC) opt for a laissez-faire, or market-centric, approach by relying on voluntary private sector standards. But data sets that could serve as a reference point to assess the robustness a country's regulatory environment on data governance are limited.

This Global Data Regulation Diagnostic (or "diagnostic" hereafter) aims to develop objective and standardized indicators to measure the regulatory environment for the data economy across countries. The structure of the indicators follows a "trust" framework proposed in the *World Development Report 2021: Data for Better Lives* (WDR21). The framework identifies the legal and normative "safeguards" and "enablers" needed to engender trust and facilitate the development of a data-driven economy, using a conceptual framework developed specifically for the WDR21.

The indicators aim to serve as a diagnostic tool so countries can assess their adoption of regulatory elements that comprise a "trust" framework for the data economy. Diagnostic results could also be used to form a baseline to track relevant regulatory reforms over time. Understanding gaps in regulatory good practice is a necessary first step for governments when identifying and prioritizing reforms. This is especially important for emerging economies that need to catch up on reaping the benefits of the data economy while avoiding the risks associated with it. Meanwhile, it is important to emphasize that there is no one-size-fits-all approach to data governance. Although the diagnostic helps governments understand where they are with regard to the adoption of good practices in building a robust legal framework to promote the data economy, the design of such a sound regulatory environment needs to be responsive to local circumstances. Extensive consultation with citizens and market players, efficient enforcing authorities, and flexible mechanisms to ensure that the legislation is adapted to new technologies or business models are all indispensable to making sure that the regulatory environment is robust and effective.

This paper has six sections. The next section, section 2, provides a literature review and explains the theoretical background of the study, while section 3 describes the methodology and section 4 presents key findings from the diagnostic. The penultimate section (section 5) shares case studies on data governance and regulatory reforms during the COVID-19 pandemic. The final section, section 6, discusses policy implications and provides conclusions.

2. Literature Review

In the evolving global data economy, trust has come under the spotlight. As the Organisation for Economic Co-operation and Development (OECD) observes, the data-rich and hyperconnected digital environment calls for trust to exploit the potential of the digital economy to support economic and social prosperity (OECD 2016). An influx of brand-new data-based products or services, as well as the virtual-interaction environment, imposes challenges for traditional ways to develop trust (O'Neill 2012). There is a lack of

prior knowledge about the newly emerged and constantly changing data-based products or services. The authenticity and reliability of entities behind the products are also difficult to assess or verify. How to build trust in data-based technologies, service providers, and other individuals and groups online becomes important to promote data economic activities.

Data regulations could play an essential role in shaping trust in the data economy. On the one hand, by legally recognizing data-related products (e.g., e-signatures) and setting rules or standards for data use/reuse, regulations provide certainty. Standards can help facilitate data use/reuse, just as accounting rules improve efficiency in conventional business transactions. On the other hand, regulations that lay out rights and responsibilities of market players provide them "a recourse to institutionalized forms of redress in the case of trust breaches." Some empirical evidences also show the impact of laws on engendering trust. For instance, presence of government regulation in a platform rule helps reduce the likelihood of non-compliance behaviors among sellers (Koo, 2019). AlGhamdi, Drew, and Al-Ghaith (2011) argue that laws and regulations in internet transactions affect consumers' attitudes toward technologies. Cyber-law is among the factors that affect the adoption of e-commerce by residents in Saudi Arabia (Alqahtani, Al-Badi, and Mayhew 2012). Similarly, González, Hasker, and Sickles (2009) find that eBay consumers are less likely to make a transaction if they do not get protection from the government.

The impact of data regulations on shaping trust in the data economy can be traced back to the theory of new institutional economics. Institutions provide the structure for exchange that determines transaction costs (North 1990). As North argues, transaction costs involve information gathering and measurement, policing and enforcing the agreement, as well as an uncertainty discount to compensate transacting parties for imperfect measurement and the enforcement process.

First, the cost of measuring the valuable attributes of what is being exchanged involves devoting resources to search and gather information about legal and physical attributes of the goods/services. For instance, data regulations that define characteristics of certain valid data products or services, such as a digital ID or electronic signature, saves assessing or evaluation time for market participants. Data regulations that clearly define the responsibilities of data processors or controllers lower transaction costs by vetting service providers on behalf of customers. Due to the complexity of data economy activities, such a vetting function can be more economically performed by a centralized regulator through adopting rules or standards than by individual customers.

Second, when a transaction happens, efficient institutions can help police and enforce the agreement. Legislatures regulate rights and obligations of parties involved in a transaction and exercise the coercive power of the state to make those parties abide with the requirements. Data regulations that grant rights to data subjects, such as the right to access or erase their individual data, protect individuals from data controllers or processors. Such protection might increase their willingness to participate in data economic activities without worrying about exploitation. Moreover, an effective and independent data protection agency that supervises the application of data protection legislation and handles complaints lodged against legal violations could further boost market stakeholders' confidence in data protection.

Third, institutions may exert influence on the transaction cost by affecting the uncertainty of transaction parties (North 1990, 1986). It is worth noting that in a business transaction, the collection of information is unlikely to be exhaustive, while the information shared by the parties to a transaction are asymmetric. One party can deliberately hide or forge information. Regulatory enforcement can also be inefficient. An enabling institutional environment can serve as a foundation and safety net to engender trust for market participants. With regard to burgeoning data economy activities, a regulatory environment that has

cybersecurity requirements for data processors or controllers and provisions safeguarding the rights of data subjects may engender certainty and trust to promote data-based transactions.

Given the essential role of data regulation in promoting trust in the data economy, this diagnostic builds on a trust framework proposed in the WDR21, which advocates for the adoption of both *safeguards* and *enablers* to achieve an efficient environment for data governance (World Bank 2021). The trust framework embeds rule of law and good governance principles, including certainty, transparency and accountability, nondiscrimination, fairness, inclusiveness, and openness. Rule of law that emphasizes certainty, rules, and predictability as well as procedural due process supports the creation of trust in the data economy (Crawford and Schultz 2014; Tamanaha 2004; Waldron 2008).

This diagnostic builds on earlier efforts to document the regulatory environment for digital economy activities across countries. The United Nations Conference on Trade and Development (UNCTAD) developed a database tracking the existence of legislation related to e-transactions, consumer protection, data protection/privacy, and cybercrime in 194 countries. DLA Piper, a global law firm, also launched a data protection law tracker that covers116 jurisdictions (DLA Piper 2020). Ferracane, Lee-Makiyama, and van der Marel (2018) have developed a digital trade restrictiveness index to map and measure policy restrictions to digital trade in 64 countries. Greenleaf (2019) conducted a stocktaking of data privacy laws in 132 countries. However, most of the existing data collection efforts focus only on collecting information about the adoption of certain types of legislation, such as the existence of e-commerce or data protection laws, without providing a more granular level of information about the contents of the legislation. What makes this diagnostic unique is that it goes beyond documenting the presence or absence of legislation. It assesses whether the laws contain specific good practice provisions or regulatory attributes, thereby conveying something about the quality of the regulatory environment. In doing so, it builds on the conceptual framework described above.

3. Methodology

Within the trust framework, the term *safeguards* stands for norms and legal frameworks that aim to protect the rights of individuals and entities participating in the data economy by addressing misuse of data, or data breaches. Cybersecurity requirements imposed on data processors or controllers are typical safeguards. The term *enablers* refers to norms and laws that facilitate the use and reuse of data, such as data portability mechanisms, open data legislation, and so on. Although safeguards and enablers include both formal legal frameworks as well as social norms, the diagnostic assesses only formal regulatory environments. While the diagnostic goes beyond identifying the presence or absence of legislation, by examining different attributes of the regulatory framework, it is not possible to assess the implementation or enforcement of the regulatory frameworks.

Moreover, according to the WDR21, a legal framework with enablers and safeguards to build trust in the data economy needs to be multidimensional, covering different types of data, actors, and transactions. Personal data—data directly provided by an individual that involved personally identifiable information—as well as nonpersonal data have different levels of sensitivity, thus requiring tailored safeguards. According to international law, individuals have fundamental rights regarding their personal data, such as the right to object to the data usage, file complaints, and seek redress. Safeguarding nonpersonal data instead requires protection of intellectual property rights. Depending on the "domain" of the data—whether data are generated and/or controlled by the public or private sector—enablers would also vary. Government can directly adopt regulatory or policy reforms to mandate access or use of public data, while in the case of private data, the government's role is more limited to creating incentives and removing barriers to facilitate

voluntary data sharing involving private sector actors. For instance, granting data portability rights to individuals allows them to legally obtain and reuse their personal data across services, provides legal grounds for data sharing among different service providers, and prevents existing players from walling off data. Finally, although many enablers and safeguards apply to both domestic and cross-border data flows, particular regulatory provisions for cross-border data transactions are needed to ensure adequate protection in receiving jurisdictions and the accountability of parties involved in transactions.

The diagnostic is based on a detailed assessment of domestic laws, regulations, and administrative requirements in 80 countries (see annex 1 for the list of countries covered). Countries are selected to ensure a balanced coverage across income groups, regions and different levels of digital technology development. Standard questionnaires are used to collect the data and are completed mainly by lawyers specializing in data governance and information and communication technology (ICT). The team has sent the questionnaire to more than 2,000 professionals in 80 countries and received about 300 responses. Data were further verified through detailed desk research of legal texts and rounds of follow-up inquires with respondents. After this, data collection results and preliminary findings were shared with regional operational colleagues at the Digital Development Global Practice of the World Bank Group for final validation based on their direct knowledge of the countries concerned.

The questionnaire comprises 37 questions designed to determine if a country has adopted good regulatory practice on data governance. The responses are then scored and assigned a normative interpretation. Related questions fall into seven clusters so that when the scores are averaged, each cluster provides an overall sense of how it performs in its corresponding regulatory and legal dimensions. These seven dimensions are:

1. E-commerce/e-transaction
2. Enablers for public intent data
3. Enablers for private intent data
4. Safeguards for personal data
5. Safeguards for nonpersonal data
6. Cybersecurity and cybercrime
7. Cross-border data transfers

The detailed calculation process is as follow: at the question level, a score of 1 was assigned to the presence of good regulatory practices, and 0 otherwise. For example, a score of 1 is assigned if there is a law or regulation that explicitly governs e-commerce/e-transactions. For multiple choice questions, a score of 1 is divided by the number of options. For instance, a score of 1/6 is assigned to each of the six cybersecurity requirements for data processors/controllers. For each of the dimensions *i*, the score for country *j* is calculated as follows:

$$X_{ij} = 100 * \left[\frac{GP_{ij} - GPmin_i}{GPmax_i - GPmin_i}\right]$$

where *GP* is the number of the adopted regulatory good practices in country *j* under dimension *i*, and *GPmin* and *GPmax* are the minimum and maximum numbers of regulatory practices measured under dimension *i*.[2] The obtained scores are normalized between 0 and 100, with 100 (0) representing the best (worst) score for the robustness of the regulatory framework. The unweighted average of a country's scores on all questions pertaining to a specific dimension yields the score for that dimension (For more on the questions for each dimension, see annex 2).

[2] The minimum number of regulatory practices measured under dimension *i* is always 0.

Further, the unweighted average of all dimensions pertaining to a particular pillar yields the score for that pillar, whether enablers or safeguards. The average scores for dimensions 1–3 provide an overall sense of how enablers are performing, while dimensions 4–7 do the same for safeguards. No attempt is made, however, to average the scores obtained for enablers and safeguards into an overall country score. This avoids the creation of country rankings, as the purpose of the exercise is not to rank countries but rather to help them identify gaps in their respective regulatory frameworks.

Under the safeguards pillar, data governance regulatory environments for personal data and non-personal data are assessed differently. The personal data dimension collects information on the regulatory practices adopted to protect data that convey information specific to a known (or knowable) individual. Personal data protection that takes a human rights approach is considered good practice—emphasizing the rights of data subjects, including the right to challenge the accuracy of data and obtain corrections. An independent data protection authority also plays an important role in enforcing compliance of those requirements. With nonpersonal data, a balance must be struck between data sharing and protecting intellectual property rights. Cybersecurity and cybercrime are additional dimensions covered under the safeguards pillar. The cost of malicious cyberactivity in the US economy was estimated in 2016 at $57 billion to $109 billion (Council of Economic Advisers 2018). For the sustainable development of the data economy, there needs a regulatory framework that criminalizes illegal cyber-activities, specifies cybersecurity measures and requires the establishment of organizations such as national Computer Security Incident Response Teams (CSIRT). Finally, the safeguards pillar, includes cross-border data flows, the global volume of which increased twentyfold between 2007 and 2017, with a further threefold increase expected in the 2017–22 period (Cisco 2018). How cross-border data flows are regulated may shape a country's competitiveness and opportunities in international trade. For instance, data localization conditions may deter some firms from opening offices in some countries.

The enablers pillar begins with an examination of the regulatory environment for e-commerce/e-transactions. According to the UNCTAD (2020), the global value of e-commerce sales was estimated at $25.6 trillion in 2018, accounting for about 30 percent of global GDP. Comprehensive e-commerce regulations support inclusive e-commerce by suppressing digital inequities (UNCTAD 2019). They also could increase trust in the use of data to facilitate e-transactions. In addition, public intent data dimension measures regulatory provisions related to data collected for public purposes. An enabling regulatory environment that promotes the use and reuse of public intent data not only allows governments to achieve better development outcomes through evidence-based policy but also to create opportunities for private sector growth and innovation, as well as contribute to the development of the society as a whole through improved transparency and accountability. Private intent data dimension covers provisions regulating data collected with the original intent of pursuing commercial purposes. The recent booming of data-driven businesses has shown the potential of private intent data in supporting innovation, efficiency, and inclusion.

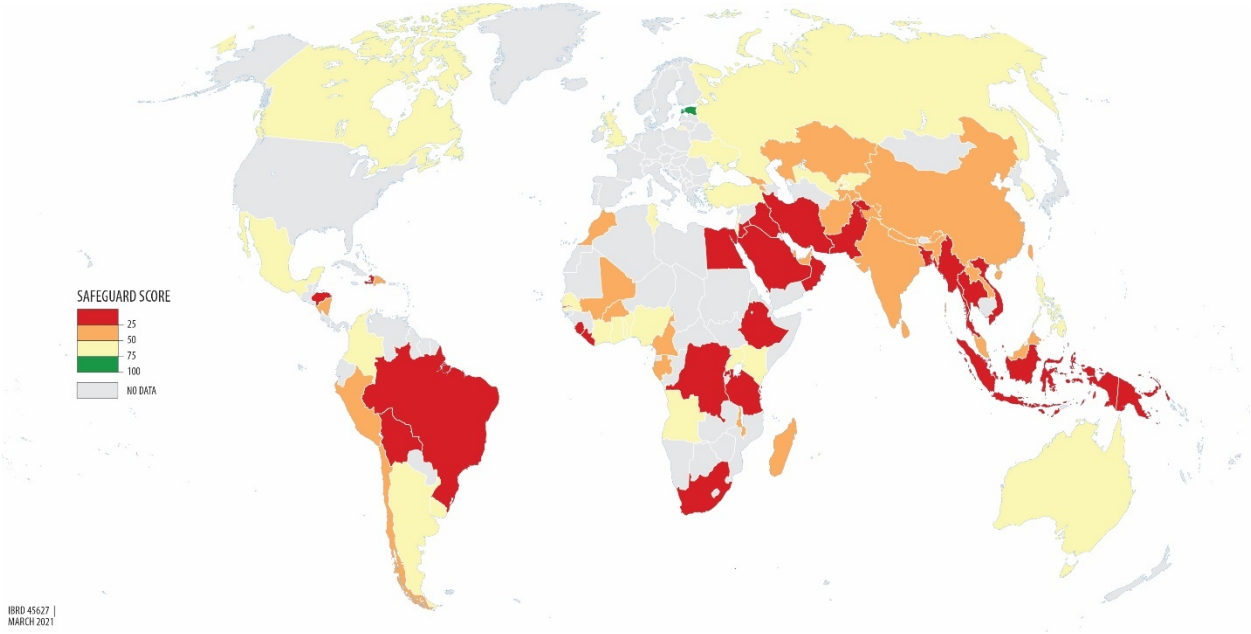
4. Findings

4.1 The global picture

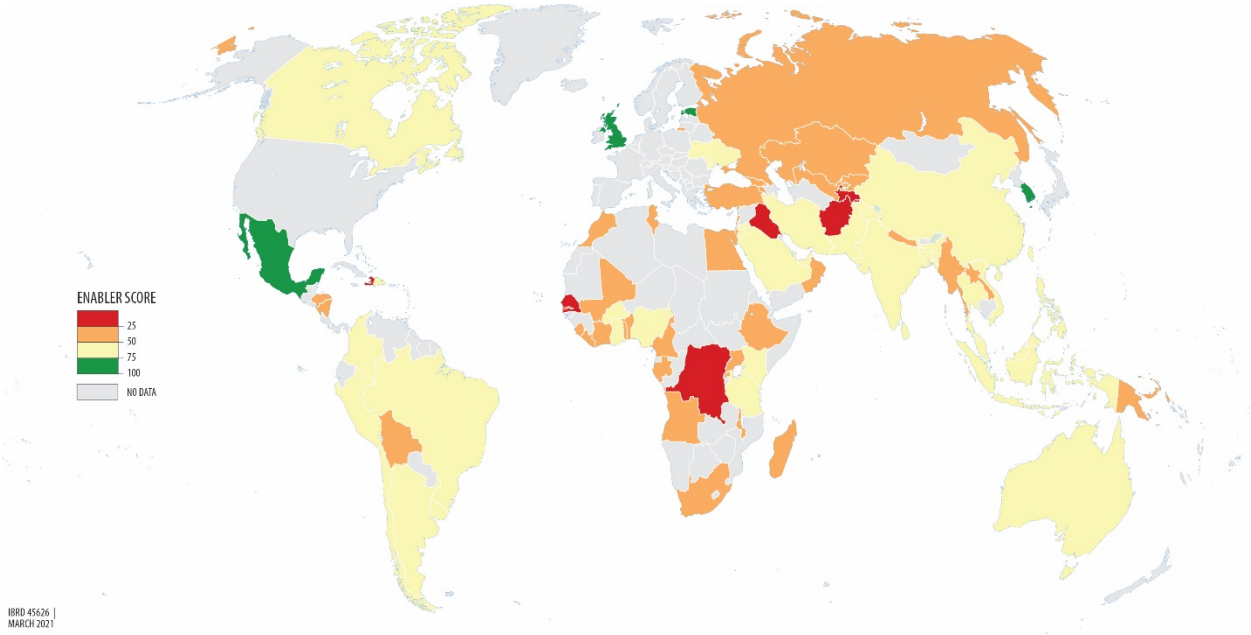
Diagnostic results show the different regulatory environments that countries have adopted, enabling data use for market players on the one hand while safeguarding the rights of data subjects on the other (map 1). According to their scores on the safeguards and enabler pillars, countries fall into four groups: advanced, moderate, evolving, and basic. A score of 75–100 confers an advanced level for enabling/safeguarding and is coded green; a score of 50–75 confers a moderate level, coded yellow; a score of 25–50 indicates an evolving regulatory level, coded orange; while a score below 25 is considered basic and coded red.

Map 1. Overall country scores on the enablers and safeguards pillars

Map 1.a Country scores on safeguards pillar



Map 1.b Country scores on enablers pillar



Source: Author's calculation based on results from the diagnostic.
Note: The highest performers are denoted with dark green, the lowest with red.

With regard to safeguards, only Estonia falls under the advanced category, while more than 60 percent of countries sampled have only reached an evolving or basic level of regulatory framework to safeguard rights of participants involved in data economic activities (table 1). Following the GDPR, Estonia has adopted comprehensive regulatory provisions to safeguard rights of data subjects, such as requiring that the collection and use of personal data be proportionate, relevant, adequate, and limited to what is necessary in relation to the purpose for which it is processed, in addition to which personal data shall not be kept longer than is necessary. Nigeria, Moldova, and Benin have the highest scores in the safeguards pillar among the lower-middle-income group. All three countries have passed personal data protection legislation and adopted a cybersecurity strategy, entailing infrastructure and institutions to identify, investigate, and address cybersecurity threats. Togo and Uganda are the only low-income countries showing a moderate level of regulatory framework for data safeguards. Both countries created a regulatory framework on personal data protection in recent years (in Togo, the law is LOI N° 2019-014 of October 29, 2019; in Uganda it is the Data Protection and Privacy Act 2019).

Table 1. Safeguards pillar by country income (number of countries by category)

	Advanced (75–100)	Moderate (50–75)	Evolving (25–50)	Basic (0–25)
High income	1	8	3	2
Upper middle income	0	6	8	7
Lower middle income	0	13	7	10
Low income	0	2	6	7
	1	*29*	*24*	*26*

Source: Author's calculation based on results from the diagnostic.

Turning to enablers, only four countries were shown to possess advanced legal frameworks, while more than half the countries sampled possessed regulatory environments at evolving or basic levels (table 2). Of the countries surveyed, the United Kingdom, Estonia, Mexico, and the Republic of Korea are among the best performers under this pillar, adopting an array of regulatory best practices regarding e-commerce and public and private data. For example, Estonia's "X-tee" data exchange platform is a good practice example on system interoperability among government entities. Mexico grants data portability rights to individuals, enabling the smooth legal transfer of personal data as individuals switch between services or product providers. In Korea, individuals can authenticate themselves with an online digital ID system to gain access to governmental services; meanwhile private sector service providers can digitally verify or authenticate the identity of a person against data stored in the ID system. It is worth noting that Burkina Faso is the best-performing low-income country under the enabler pillar. It has adopted an open data policy; meanwhile, another of its laws (N ° 051-2015 / CNT of August 30, 2015) grants individuals the right to request access to government records or data, while still another law (045-2009/AN) facilitates e-transactions, for instance, by granting legal equivalence to paper-based and electronic communications.

Figure 1 provides more detail on disparities across income groups and regions. While high-income countries tend to perform well on average, there are notable disparities in their regulatory development. For instance, in Mauritius, the regulatory environment for enablers is far from complete. Private sector service providers are unable to digitally verify or authenticate the identity of a person against data stored in the ID system. The country has no government data classification policy, nor are individuals entitled to data portability

rights. Low-income countries present low, closely clustered scores for enablers and safeguards alike. Overall, performance is more widely distributed for safeguards than enablers, across income groups.

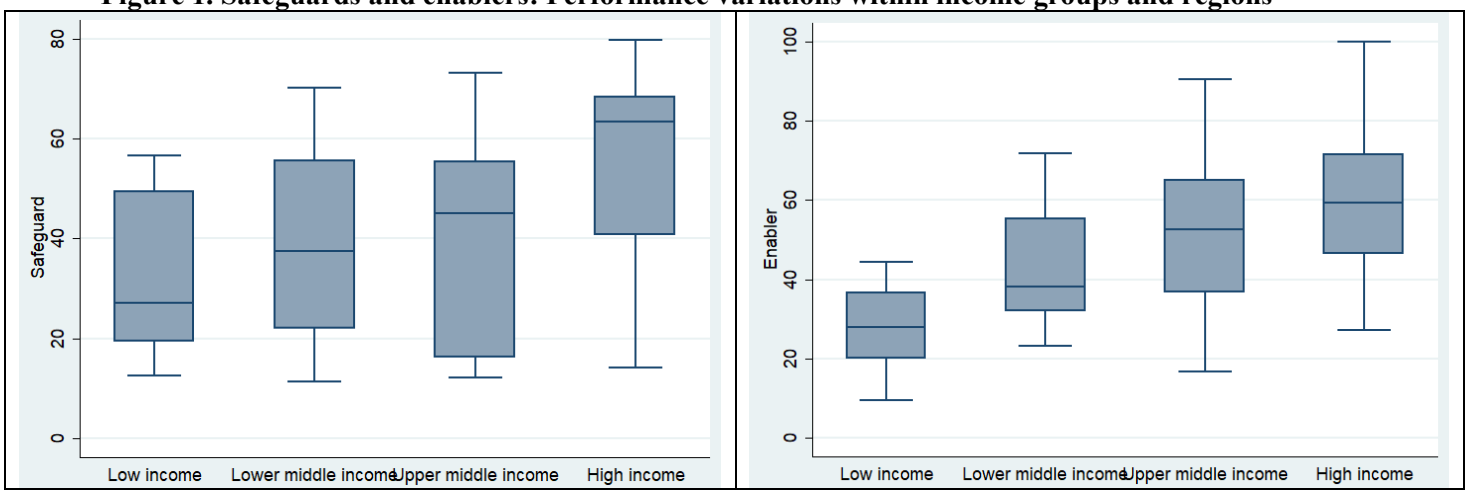
Table 2. Enablers pillar (number of countries per income group by category)

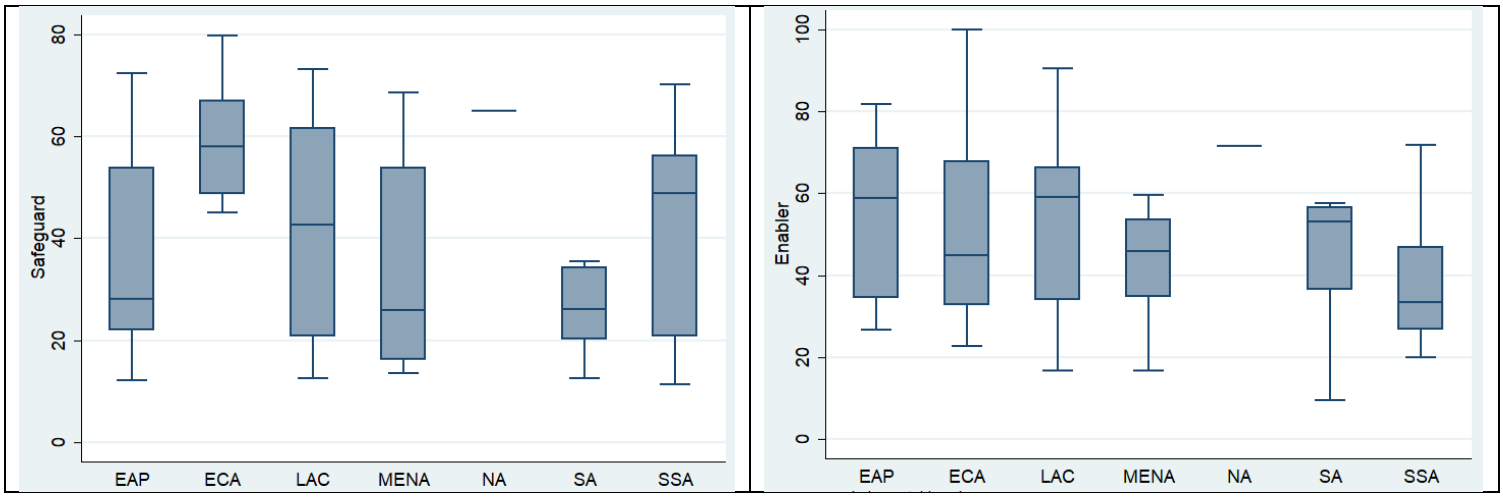
	Advanced (75–100)	Moderate (50–75)	Evolving (25–50)	Basic (0–25)
High income	3	7	4	0
Upper middle income	1	11	8	1
Lower middle income	0	12	16	2
Low income	0	1	9	5
Total	*4*	*31*	*37*	*8*

Source: Author's calculation based on results from the diagnostic.

There is a notable overlap across geographic regions regarding the performance of enablers, whereas safeguards development is more advanced in North America and in Europe and Central Asia. Disparities in performance across countries within regions is considerable. For example, within Latin America and the Caribbean, Mexico has established an advanced regulatory environment for enablers, while Haiti remains at a basic level. Colombia's law (no. 1581 of 2012) protects personal data rights of data subjects, while in Bolivia the legal framework does little to safeguard data subjects.

Figure 1. Safeguards and enablers: Performance variations within income groups and regions





Source: Author's calculation based on results from the diagnostic.
Note: The line on the upper whisker stands for the upper adjacent value, while the line on the lower whisker stands for the lower adjacent value. The upper adjacent value (UAV) is the largest observation that is less than or equal to the upper inner fence (UIF), which is the third quartile plus 1.5*IQR (interquartile range). The lower adjacent value (LAV) is the smallest observation that is greater than or equal to the lower inner fence (LIF), which is the first quartile minus 1.5*IQR. The line within the box refers to the median; the upper hinge of the box refers to the 75th percentile, and the lower hinge of the box refers to the 25th percentile. Outside values are excluded from the figure. Canada is the only North American country covered in the sample. EAP = East Asia and Pacific; ECA = Europe and Central Asia; LAC = Latin America and the Caribbean; MENA = Middle East and North Africa; NA = North America; SA = South Asia; SSA = Sub-Saharan Africa.

4.2 Safeguards versus Enablers

Overall, the adoption rate of good regulatory practices pertaining to enablers is higher than that of safeguards across countries. Countries in the diagnostic sample adopt 47 percent of regulatory good practices measured for enablers, with the adoption rate ranging from 30 percent in low-income countries to 62 percent in high-income countries (table 3). In comparison, 41 percent of good regulatory practices measured for safeguards are adopted. The lower rate is mainly due to the relatively worse performance of the high- and upper-middle-income countries on safeguards. The difference between enablers and safeguards becomes less obvious at lower levels of country income group. Lower-middle and low-income country performance on both pillars is consistent.

Table 3. Scores for enablers and safeguards (by country income group)

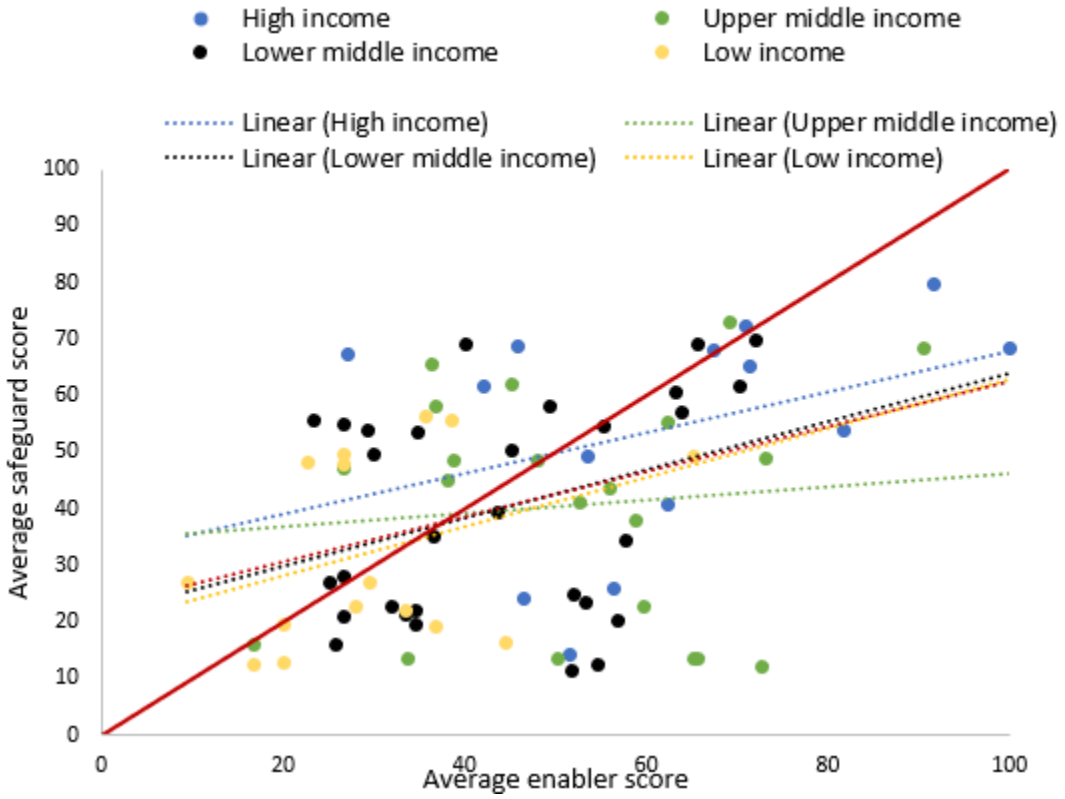
Average of safeguard score		Average of enabler score	
High income	54	High income	62
Upper middle income	40	Upper middle income	52
Lower middle income	40	Lower middle income	44
Low income	33	Low income	30
Grand total	**41**	**Grand total**	**47**

Source: Author's calculation based on results from the diagnostic.

A scatterplot showing enabler and safeguard scores also confirms that enabler regulatory practices are more prevalent than those for safeguards (figure 2): consistently across country income groups, some 60 percent of countries exhibit higher scores for enablers than safeguards. Estonia is alone in having an advanced

regulatory environment for both enablers and safeguards. Indonesia, Thailand, and Tanzania have frameworks with moderate environments for enablers, coupled with minimal adoption of safeguards. Although it is true that these countries have overarching e-commerce laws and implemented regulations supporting the utilization of public intent data, such as open data laws, they nonetheless lack regulatory safeguards for personal and nonpersonal data.[3] Conversely, Mauritius has adopted more regulatory good practices on safeguards than on enablers. It lacks legislation that supports the use/reuse of public and private intent data, but the country's 2017 Data Protection Act established comprehensive safeguards for personal data in addition to cybersecurity requirements. It's also worth highlighting that the correlation coefficient between enablers and safeguards is 0.38, demonstrating a moderate degree of positive correlation. In other words, countries that adopt a robust regulatory environment on data enabling are more likely to have strong regulatory environments for data safeguards, and vice versa.

Figure 2. Country scores on enablers and safeguards: A scatterplot



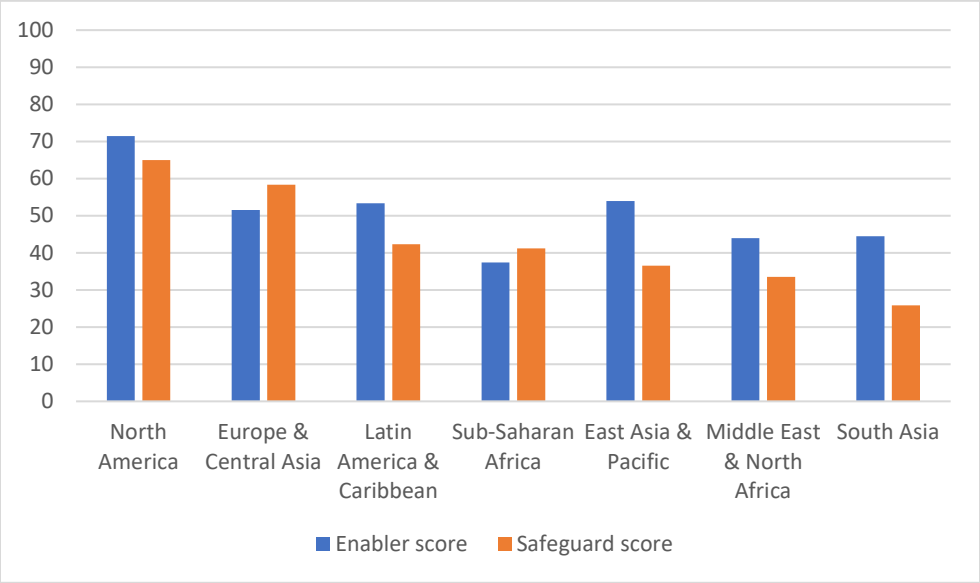
Source: Author's calculation based on results from the diagnostic.

Regional performance shows slightly different patterns (figure 3), with most regions performing better on enablers than on safeguards; Europe, Central America, and Sub-Saharan Africa are exceptions. On enablers, good regulatory practices remain at the "evolving" stage in Sub-Saharan Africa. For instance, the digital ID system that allows individuals to authenticate themselves online to access governmental services (e.g., e-tax filing and online benefits application) does not exist in most of the Sub-Saharan African countries in the sample. Few have adopted an open licensing regime (such as a Creative Commons license by Attribution) to facilitate the use/reuse of public intent data. Europe and Central Asia is the other region where the regulatory environment for safeguards is more robust than it is for enablers. In the diagnostic sample, all

[3] At the time of data collection, Thailand's Personal Data Protection Act had not been enforced yet.

the countries in Europe and Central Asia have data protection laws explicitly governing the use, collection, and processing of personal data. Estonia, Moldova, and the United Kingdom have also imposed a full range of cybersecurity requirements on data processors and controllers. But when it comes to the regulatory environment for enablers, the region is still lagging. For instance, the Kyrgyz Republic is still in the process of drafting an e-commerce law.

Figure 3. Scores on enablers and safeguards across regions



Source: Author's calculation based on results from the diagnostic.

4.3 Comparison across dimensions under the enabler and safeguard pillars

In addition to the uneven development of regulatory environments for enablers and safeguards, country performance on the underlying dimensions also varies significantly (table 4). On average, countries in the higher-income group tend to perform better across all dimensions. However, no country income group demonstrates an advanced regulatory framework across all dimensions, indicating room for significant improvement. All income groups achieve their highest scores on the dimension of e-commerce, with more than 70 percent of the regulatory good practices adopted on average. Public intent data and cybersecurity and cybercrime are two other dimensions where most countries are performing relatively well, except for those in the low-income category. All income groups show a basic or evolving level of development for the regulatory framework related to cross-border data flows and private intent data. On average, only 17 percent of regulatory best practices are adopted under the private intent data dimension, ranging from 3 percent in low-income countries to 30 percent in high-income countries.

The average correlation coefficient among country scores across all seven dimensions is 0.27; the coefficients between two dimensions range from -0.22 (between regulations for sharing public intent data and protecting nonpersonal data) to 0.82 (between regulations for protecting personal data and allowing cross-border data flows) (table 5). The extent to which such bilateral correlation coefficients are statistically significant, and indeed rather large in some cases, suggest that governments may tend to simultaneously address certain clusters of issues in the regulatory framework. For instance, countries with regulatory frameworks that allow cross-border data flows are highly likely to allow access to private intent data, provide protection for personal data, and have strong cybersecurity regulations in place. Or again, countries

with strong e-commerce legislation are much more likely to promote sharing of both public and private intent data. Of some concern is the finding that governments with a well-established regulatory framework to facilitate e-commerce/transactions, appear not to be adopting adequate safeguards to protect personal data. Take Indonesia as an example, where Law No. 11 of 2008 on Electronic Information and Transactions (and amendments to the law) establishes an enabling environment for e-commerce and e-transactions by granting the equivalence of paper-based and electronic communications, recognizing e-signatures, and adopting the technological neutrality principle. But there is no general law protecting data, despite scattered, sector-specific regulations.

Table 4. Regulatory good practices, by country income across dimensions (in percentages)

	Safeguards				*Enablers*		
Country income level	**Personal data**	**Non-personal data**	**Cybersecurity and Cybercrime**	**Cross border data flows**	**E-commerce /transactions**	**Public intent data**	**Private intent data**
High income	59	43	73	42	86	69	30
Upper middle income	46	29	57	30	74	62	20
Lower middle income	43	38	55	24	72	44	15
Low income	31	47	39	13	59	28	3
Total	**44**	**38**	**56**	**27**	**73**	**50**	**17**

Source: Author's calculation based on results from the diagnostic.

The high correlation between personal data and cross-border data flows merits further scrutiny. Countries with sufficient regulatory safeguards on personal data may not only engender trust for domestic market but also enhance its competitiveness in international digital trade, thus further incentivizing governments in adopting regulatory practices to facilitate cross-border data transactions. The correlation between nonpersonal data protection and other dimensions is at a rather low level, even falling into negative territory, suggesting lack of attention to this issue.

Table 5. Enablers and safeguards: Correlations among regulatory scores across dimensions

	E-commerce/ transactions	Public intent data enablers	Private intent data enablers	Personal data protection	Non-personal data protection	Cybersecurity and cybercrime	Cross-border data flows/ transactions
E-commerce/transactions	1						
Public intent data	0.2979*	1					
Private intent data	0.3496*	0.3998*	1				
Personal data	0.0875	0.1736	0.4589*	1			
Nonpersonal data	-0.1046	-0.2214*	-0.0853	0.1249	1		
Cybersecurity and cybercrime	0.2924*	0.4031*	0.6232*	0.5423*	-0.1744	1	
Cross-border data transactions/flows	0.1329	0.2458*	0.5573*	0.8216*	0.0348	0.6087*	1

Source: Author's calculation based on results from the diagnostic.
Note: * indicates that correlation coefficients are significant at the 5 percent level or better.

4.3.4 Safeguards: Personal data

The first dimension under safeguards covers personal data—regulatory practices that seek to protect personally identifiable data. Given the sensitivity of personal data, which may include an individual's health or financial information, the level of regulatory protection could have an impact on individuals' trust in data products or services, thus affecting their willingness to participate in data economy activities.

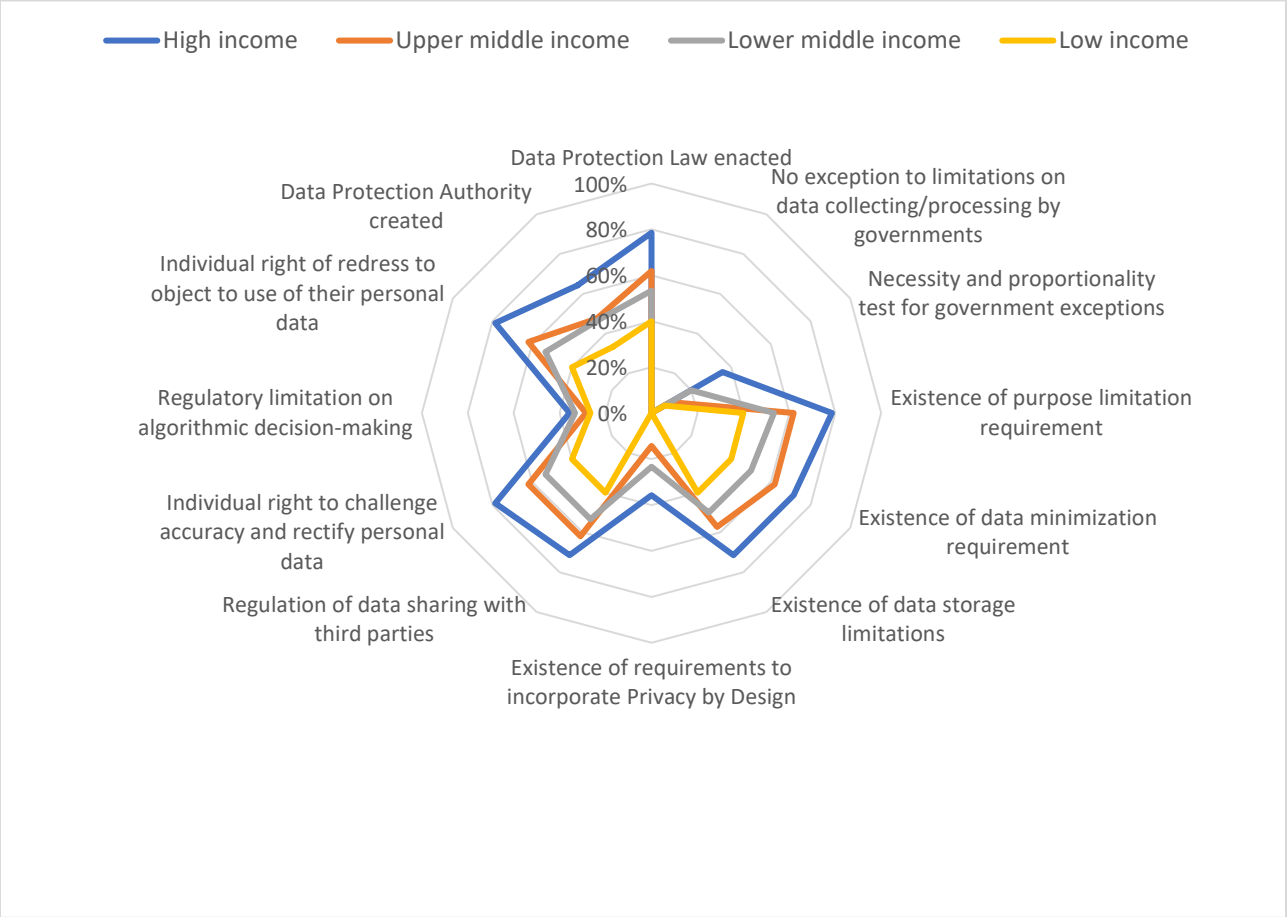
The personal data dimension measures 12 different features of the data protection law of a given jurisdiction.[4] It first examines whether an overarching data protection law has been enacted, then it surveys the implementation of data subject rights such as redress; objection to the use of personal data and limitation of sharing with third parties; data minimization, purpose limitation, and storage limitation requirements. Furthermore, this dimension looks at whether limitations exist on the possibility that decisions about individuals are taken only on the basis of automated processes, which might lead to social discrimination (Article 29, Working Party 2018). Finally, this dimension provides information on whether data subject rights are effectively protected on the technical side through the implementation of measures based on the privacy-by-design and privacy-by-default principles in the surveyed jurisdictions (UK Information Commissioner's Office 2020b), as well as by the monitoring activity of a data protection authority.

Overall, 58 percent of the countries surveyed enacted an overarching data protection law, such as Nigeria's Data Protection Regulation 2019 or Ukraine's Law on the Protection of Personal Data of 2010. Data protection laws are found in 40 percent of low-income countries, 53 percent of lower-middle-income countries, 62 percent of upper-middle-income countries, and close to 80 percent of high-income countries (figure 4). All these laws include exceptions to the limitations on data collection and processing by governments, but a necessity and proportionality test for such exceptions appears in 18 percent of the countries measured. Such limitation can be found in Côte d'Ivoire's data protection law, whereby the processing of personal data carried out on behalf of the state, or a public or private legal entity managing a public service authorized by decree, is subject to the reasoned opinion of the Data Protection Body.[5]

Interestingly, the performance of income groups on a few specific provisions of personal data protection legislation is quite consistent. Provisions on purpose limitation, individual's right to challenge accuracy of personal data, and seek redress are found in 79% of high income countries, 62% of upper middle-income countries, 53% of lower middle-income countries and 40% of low-income countries. This indicates that when countries adopt personal data protection legislation, the above mentioned regulatory good practices are usually embedded in the regulatory framework, implying a convergence on regulatory practices in personal data protection across countries. However, there emerges a potential gap between the enactment of regulatory frameworks and their implementation. Though personal data protection legislation is relatively prevalent at 58 percent, supervisory authorities for data protection are found in 47 percent of the countries surveyed and only 33 percent in low-income countries.

[4] While scores are averaged on the basis of the full set of countries surveyed, the DBI methodology assigns a score for the specific safeguards adopted only if a country adopted an overarching data protection law.
[5] See *Loi 2013-450 relative à la protection des données à caractère personnel*, art. 13. Accessible at: https://www.artci.ci/images/stories/pdf/lois/loi_2013_450.pdf.

Figure 4. Countries with good regulatory practices safeguarding personal data, by country income group (in percentages)



Source: Author's calculation based on results from the diagnostic.

There is significant potential for implementing further improvement in two areas: data protection by design (or by default) principle and automated decision-making. Data protection by design seeks to deliver the maximum degree of protection by ensuring the automatic protection of personal data in any given information technology system or business practice, from the design stage right through the life cycle (Cavoukian 2011; UK Information Commissioner's Office 2020b). On a global scale, this requirement is found in 18 percent of the countries assessed—36 percent of high-income countries, as in the case of Uruguay,[6] 14 percent of upper-middle-income countries, and 23 percent of lower-middle-income countries. Not one low-income countries has adopted a similar provision. For instance, art. 12 of Uruguay's Ley de Proteccion de Datos Personales n. 18331 requires data controllers to adopt technical measures such as *privacidad desde el diseño* and *privacidad por defecto* to protect personal data.[7] A similar requirement can

[6] See Ley de Proteccion de Datos Personales n. 18331, art. 12. Accessible at: https://www.impo.com.uy/bases/leyes/18331-2008/12.
[7] See Ley de Proteccion de Datos Personales n. 18331, art. 12. Accessible at: https://www.impo.com.uy/bases/leyes/18331-2008/12.

be found in Section 41(3) of Kenya's Data Protection Act No. 24 of 2019, which mandates the adoption of the data protection-by-default principle.[8]

Limiting decision-making solely based on automated processing becomes important with the increasing practice of profiling used in various data economic activities. Profiling is the practice of using personal data, specifically data on individuals' various personal attributes, in order to analyze and predict their behavioral preferences based on their economic status, interests, health, or work performance. On top of this, the data controller may also make decisions about data subjects through automated means, without human oversight. While profiling and automated decision-making may boost efficiency and cost savings for data controllers, these practices may have serious negative impacts on data subjects, perpetuating bias and discrimination. Individuals may see their freedom to purchase products online diminished due to an algorithm that has locked them into a specific category or, in the worst cases, subjected them to unjustified discrimination (Article 29, Working Party 2018). A limitation to the making of decisions about individuals solely as a result of automated processing of personal data is found in about 30% of the countries sampled, with minimal differences recorded across income groups.

4.3.5 Safeguards: Nonpersonal data

The level of safeguards for nonpersonal data is another dimension assessed under the safeguards pillar. It mainly covers two issues: whether IPRs can be cited to prevent the sharing of data and whether a country's regulatory framework includes provisions on the confidentiality of third-party rights in nonpersonal government data, such as company registers or business data underlying official statistics.

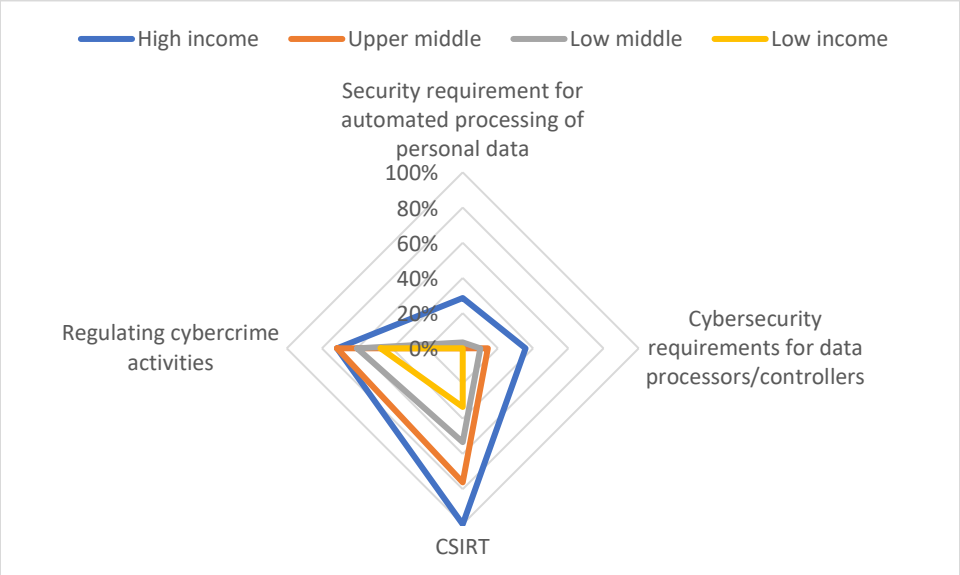
Results show that 70 percent of countries do not allow the use of IPRs to prevent data sharing or have no specific provision for the matter. Most low-income countries have not established relevant legislation on IPRs at all, not to mention the leveraging of such rights to facilitate or prevent data sharing. With regard to the confidentiality of third-party rights in nonpersonal government data, it is not regulated in any low-income country but is addressed by 14 percent of high-income countries. For instance, Canada protects third-party rights in nonpersonal government official statistics made available publicly, preventing the manipulation of databases to identify individuals, businesses, or organizations.[9] Only 7 percent of the sampled countries worldwide regulate third-party confidentiality in nonpersonal government data.

4.3.6 Safeguards: Cybersecurity and cybercrime

In order to be effective, safeguards for personal and nonpersonal data should be linked with legal and technical cybersecurity measures. Mandating the implementation of security measures in technical infrastructure, as well as adopting provisions against cybercrime—that is, the criminalization of unlawful or illegal access or use of infrastructure, systems, and data—are crucial to build a robust safety net for data economy activities. Therefore, the cybersecurity and cybercrime dimension collects information on four elements: security requirements for automated processing of personal data; cybersecurity requirements for data processors/controllers; existence of a national computer emergency response team (CERT); and existence of provisions that criminalize cybercrime.

[8] The law can be accessed at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.
[9] The terms and conditions of Statistics Canada Open Licence can be accessed at the following link: https://www.statcan.gc.ca/eng/reference/licence.

Figure 5. Countries with good regulatory practices on cybersecurity and cybercrime, by income group (in percentages)



Source: Author's calculation based on results from the diagnostic.
Note: CSIRT = Computer Security Incidence Response Team.

Diagnostic results show that data processors and controllers have to comply with security requirements for automated data processing in 29 percent of high-income countries (figure 5). Kenya is the only country in the lower-middle-income group with a similar security requirement. In particular, Kenya requires data controllers and data processors to: encrypt personal data, implement measures for pseudonymization, restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident, verify that the safeguards are effectively implemented, and ensure that the safeguards are continually updated in response to new risks or deficiencies.[10] Furthermore, no low-income country has adopted the full range of cybersecurity requirements for data processors and controllers, whereas these can be found in 10 percent of the lower-middle-income group, 14 percent of the upper-middle-income group, and 36 percent of high-income countries.

Although they lack cybersecurity measures in their regulatory frameworks, many countries (66 percent) have national cybersecurity plans and a national Computer Security Incident Response Team (CSIRT). Stark differences remain across income groups—100 percent of high-income countries have endorsed these cybersecurity strategies while only a third of low-income countries have done so. With regard to provisions that criminalize different forms of cyber activities, income groups have more consistent performance. Globally, 62 percent of the countries assessed have comprehensive cybercrime provisions, along with 47 percent of the low-income countries. Rwanda's Law on Governing Information and Communication Technologies 2016 (ICT Law) addresses unauthorized access to computer data, modification of data held in a computer system, interception of computer services, access to a computer system with intent to commit an offense, damaging or denying access to a computer system, and computer-related theft, fraud, and forgery.[11]

[10] See Section 41(4) of the Data Protection Act 2019. Accessible at: https://www.ict.go.ke/wp-content/uploads/2019/11/TheDataProtectionAct__No24of2019.pdf.
[11] See art. 197-203. Accessible at: https://govca.rw/eng/lawspdf/RWA_2016_LAW%20N0%2024-2016_INFORMATION_AND_COMMUNICATION_TECHNOLOGY-OG_N0_26_OF_27_JUNE%20_2016.pdf.

4.3.7 Safeguards: Cross-border data flows

As digital trade becomes more important in international trade, an appropriate regulatory approach is required to support cross-border data flows. On the one hand, data subjects' rights and national security should be safeguarded during international data flows. On the other hand, smart regulation is needed to avoid negative impacts on a country's competitiveness in international trade. The cross-border data flow dimension monitors the conditions under which personal data can be transferred abroad. In particular, it measures whether a country's regulatory framework allows data transfer through both adequacy and accountability approaches, recording the specific conditions that permit data transfer.

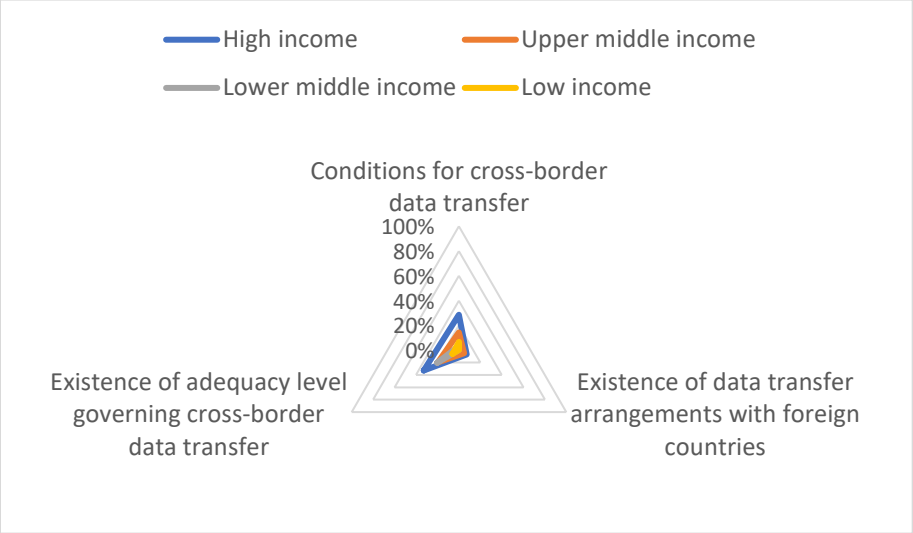
Countries regulate the transfer of local personal data to nondomestic third parties by adopting various approaches. The "adequacy" approach was introduced in the 1981 Council of Europe's Convention 108. Countries that adopt this approach allow international data transfer to a set of jurisdictions that guarantee comparable data protection safeguards, generally following the decision of the data authority. Conversely, the OECD Guidelines recommend a more flexible approach, leaving to an organization the responsibility to assess and determine which protections are to be put in place before proceeding with the international data transfer (OECD 2013). Regulatory frameworks inspired by this view adopt an "accountability" approach (Phillips 2018). Moreover, some countries have begun to adopt a restrictive government-control approach on cross-border data flows by mandating data localization within the country. For instance, Nigeria, Russia, and Vietnam require that personal data about their citizens must be stored and processed with country borders. In China, "critical information infrastructure operators" are required to store "important data" collected and generated in their operations within its territory. Although some governments cite national security in support of such data localization requirements, concerns about citizen surveillance and disrupted business operations are increasing.

Almost 50 percent of the countries adopt an adequacy approach. Circumstances constituting an "adequate level of protection" for international transfers of personal data include the purposes and time period for which data are intended to be processed, the existence of relevant domestic law in the host country (such as data minimization and individual rights), the existence and effective functioning of one or more independent supervisory authorities in the third country to enforce compliance, and so on. Around one-third of high-income countries have specified a full range of circumstances constituting this "adequate level of protection," while few low-income countries have done so. Countries can also have mutual arrangements with foreign countries or multinational entities or schemes to require, permit, or limit transfers of personal data between countries. Such agreements include whitelisting, mutual recognition, and treaties. Mutual recognition agreement and treaties are more prevalent, with about 30 percent of countries surveyed having such arrangements. For instance, the Philippines and Singapore agreed to develop compatible mechanisms to facilitate trusted cross-border data flows, including mutual recognition of comparable protection afforded by their respective laws to safeguard citizens of both the Philippines and Singapore.

More in detail, figure 6 shows that 29 percent of high-income countries use both adequacy and accountability approaches to regulate data transfers, but the ratio is at only 3 percent and 7 percent among lower-middle- and low-income countries, respectively. These shares are even lower when it comes to data transfer arrangements with foreign countries, such as adequacy decisions/whitelists, binding corporate rules, mutual recognition, and international treaties. Only 7 percent of high-income- and 5 percent of upper-middle-income countries have incorporated all these requirements to facilitate cross-border data transfers. On average, the regulations of high-income countries generally include at least two conditions in order to

allow adequacy-based data transfer, while upper-middle- and lower-middle-income countries generally take into account only one condition.[12]

Figure 6. Countries by income group adopting good regulatory practices on cross-border data flows (percentages)



Source: Author's calculation based on results from the diagnostic.

4.3.1 Enablers: e-commerce/e-transactions

Country performance on each of the key regulatory dimensions (summarized above) can be further explored with reference to the scores on the "component" question underlying each dimension. Such analysis makes it possible to pinpoint where the data governance framework may be deficient.

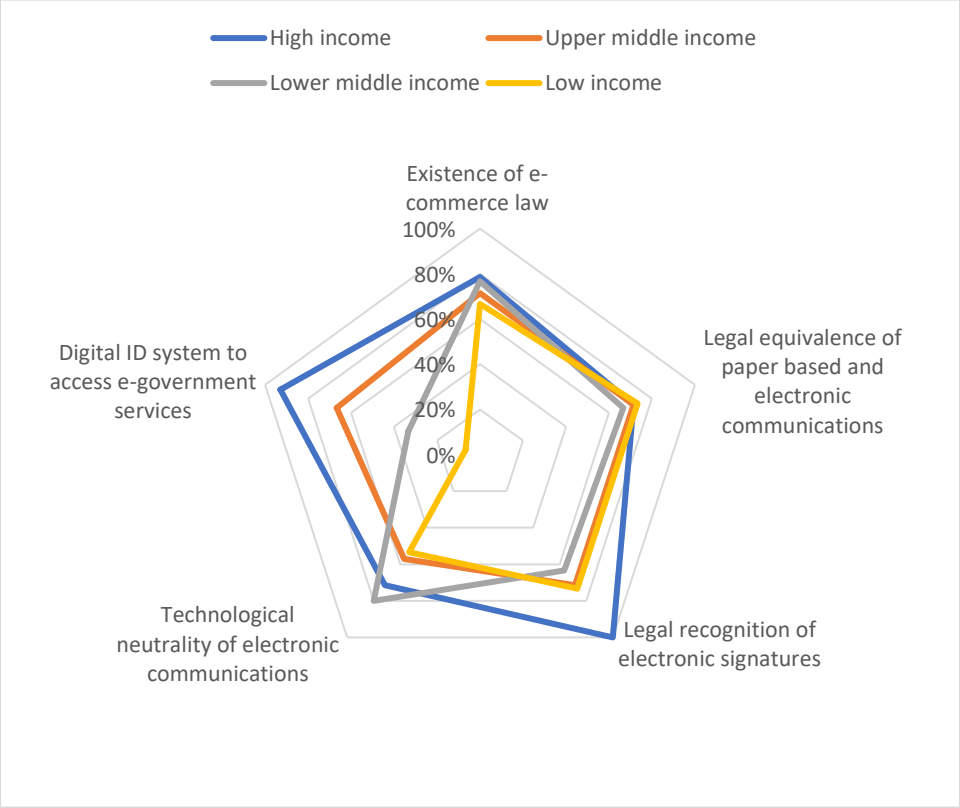
Firstly, supporting the development of e-commerce calls for a regulatory environment that is adapted to fast-evolving technologies to allow a full participation in the opportunities brought by e-commerce without increasing digital inequalities (UNCTAD 2019). The e-commerce dimension encompasses the following elements: existence of an overarching e-commerce law; legal equivalence of paper-based and e-communications; legal recognition of e-signatures; adoption of principles of technological neutrality of e-communications; and implementation of a digital ID system so users can access e-government services.

Country performance varies significantly on technological neutrality in electronic communications and a digital ID system for accessing e-government services (figure 7). The technological neutrality principle advocates a flexible regulatory framework. Applied in the arena of e-commerce/transactions, it ensures openness to technologies needed for e-signatures and e-communications. Rules that are neutral regarding technology accommodate innovation and change without further legislative work. Regulations should define the expected output without imposing requirements favoring, or consolidating the position of, technological winners (Maxwell and Bourreau 2014). For instance, the Ukrainian Law on Electronic Trust Services stipulates technological neutrality of e-services.[13] The principle of technological neutrality has been implemented in the regulation of 53 percent and 57 percent of low- and upper-middle-income

[12] The DBI project measures how many adequacy conditions can be found on average in each jurisdiction. This average score is calculated on the basis of the full set of countries; the score is not restricted to countries that regulate adequacy-based data transfer only.
[13] See art. 1 (42). The text of the law is accessible at: https://zakon.rada.gov.ua/laws/show/2155-19.

countries, respectively, in contrast to 71 percent in high-income countries and 80 percent in lower-middle-income countries.

Figure 7. Countries adopting good regulatory practices on e-commerce/e-transactions by income group (in percentages)



Source: Author's calculation based on results from the diagnostic.

Digital authentication allows users to be verified, uniquely and securely, through digital technologies or biometrics.[14] Digital IDs allow users to effectively access sensitive applications, data, and e-services, which enhances equality and inclusion.[15] A digital ID system to access e-government services is found in 30 percent of lower-middle-income countries and only 6 percent of countries in the low-income group; the system is adopted by 93 percent and 62 percent of high- and upper-middle-income countries, respectively. Singapore's SingPass is a well-functioning digital ID system.[16] Users can access SingPass on their smartphones, logging in through biometric data, using their digital identity to sign e-documents or access more than 200 e-government services, such as tax or property information.[17] Instruments like SingPass allow citizens to interact easily with government services and save on administrative costs and fees.[18]

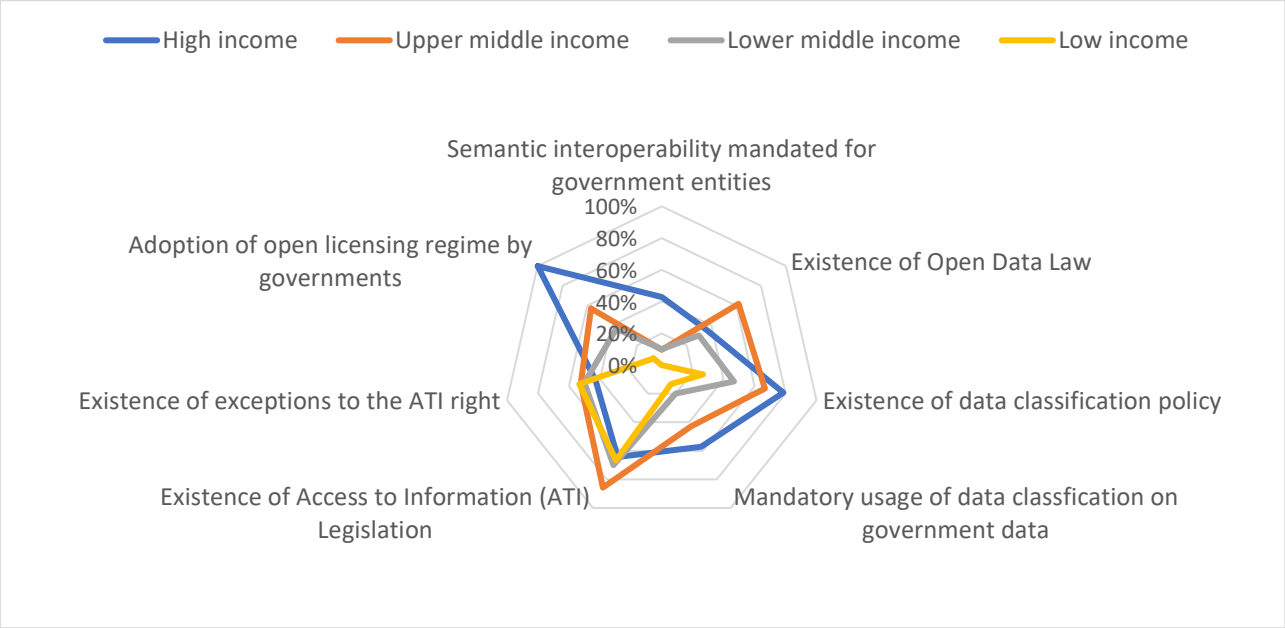
[14] See World Bank, *Identity for Development* (ID4D), glossary, available at: https://id4d.worldbank.org/guide/glossary.
[15] See, generally, World Bank, *Identity for Development* (ID4D), available at: https://id4d.worldbank.org/global-dataset; and Sustainable Development Goals (SDGs), available at: https://sustainabledevelopment.un.org/sdgs. SDG 16.9 provides that, "By 2030, provide legal identity for all, including birth registration."
[16] The SingPass portal can be accessed at: https://www.singpass.gov.sg/.
[17] For further information, see also: https://www.tech.gov.sg/products-and-services/singpass/.
[18] For information about the benefits of SingPass, see also: https://www.smartnation.gov.sg/docs/default-source/press-release-materials/factsheet---national-digital-identity.pdf?sfvrsn=ea1d279f_2.

4.3.2 Enablers: public intent data

"Public intent data" refer to data collected for public purposes, regardless of the collection instrument or the entity that manages the data. Traditionally, public intent data are collected by censuses and household surveys, although newer sources of such data have become available and more prominent in recent years, such as data collected through digital identification and facial recognition through public cameras. Issues measured under the dimension of public intent data include: the existence of open data laws, the interoperability of government data exchange platforms, the existence of a data classification policy and its mandatory use for government data, the existence of access to information (ATI) legislation and related exceptions, and, finally, the adoption by governments of an open licensing regime.

Country performance on the abovementioned aspects vary significantly, except on ATI legislation (figure 8), which has been adopted by 70 percent of the countries surveyed, while about half the countries include exceptions regulating ATI rights.[19] ATI legislation provides citizens a legal instrument to obtain public sector disclosure. Access and circulation of information held by public actors is a cornerstone for freedom of information and expression. This is one of the SDGs as it increases accountability and transparency of government action.[20]

Figure 8. Percentage of countries with good regulatory practices to facilitate the use of public intent data (by country income)



Source: Author's calculation based on results from the diagnostic.

Compared with ATI legislation that provides an ex post channel for citizens to obtain information, open data laws establish an ex ante responsibility for the disclosure of public data. Korea's Act on the Promotion

[19] Countries score points if they regulate all the following exceptions to ATI rights: (1) sensitive information on national security, defense, or foreign policy grounds; (2) trade secrets or other commercial interests; (3) personal data; (4) law enforcement; (5) privileged information; and (6) public investigations and audits.
[20] Goal 16.10.2, see: https://sdgs.un.org/goals/goal16.

of Provision and Use of Public Data[21] is a good example of such legislation. Sixty percent of upper-middle-income countries have adopted an open data law. However, open data laws are not as prevalent as ATI legislation, especially in low-income countries. Another issue that is partially linked to the publication of open data is the adoption of an open licensing regime, such as a Creative Commons License. This allows users to reuse "public sector information for a purpose other than the initial public task it was produced for," with few or no restrictions, including commercial purposes (UK Information Commissioner's Office 2020a). Therefore, a sharing-friendly licensing regime maximizes the benefits of making open data available, enhancing opportunities for economic growth (European Commission 2019). Adoption rates for this regulatory practice vary across country-income groups: an open licensing regime has been adopted in all the high-income countries surveyed, while the adoption rate decreases to 57 percent of upper-middle-income countries, 37 percent of lower-middle-income countries, and 7 percent of countries in the low-income group.

To facilitate the use of public data, another regulatory good practice is a mandatory requirement among government entities to use common technical standards to enable interoperability of systems, registries, and databases. Examples of such initiatives include establish standards for open APIs for G2G/G2B/G2C services, implement the "ask once" principle, utilize standardized communications protocol for accessing metadata, and rely upon semantic catalogues for data and metadata.[22] Saudi Arabia's Yesser E-Government Program provides a good example of an interoperable data exchange platform, which allows citizens and companies to access e-government services on the Gov.sa portal (World Bank 2020). Similar platforms can be found in 43 percent of high-income countries and 10 percent of upper-middle and lower-middle-income countries, while this system is not found in any low-income country.

It is worth noting that certain categories of government data may not be suitable for publication under open data policies—for instance, in the case of personal data or data entailing national security concerns. Thus, public entities should evaluate potential issues of sensitivity in light of a data classification policy. This requires an ex ante assessment of the risks associated with the publication and adoption of protective measures to ensure the safe publication of personal information on open data portals, while allowing accountability. Data should be categorized taking into account the different levels of sensitivity across the different stages of the data life cycle, enabling effective and safe data reuse (Digital Guardian 2018). A data classification policy has been adopted by more than half of the countries across income groups, ranging from 26 percent of countries in the low-income group to 78 percent of high-income countries. The use of such classification is mandatory for government data in 13 percent of low-income countries, 20 percent of lower-middle-income countries, 42 percent of upper-middle-income countries, and 57 percent of high-income countries.

4.3.3 Enablers: private intent data

The private intent data refers to data collected with the original intent of pursuing commercial purposes. Private data can generate productivity gains and growth in both developed and developing countries, supporting innovation, efficiency, and inclusion (World Bank 2016). Data on consumer behavior and preferences become the secret weapon to further propel business growth (Argenton and Prüfer 2012). MYbank, an online private commercial bank in China, uses big data to assess loan applications instead of hiring thousands of loan officers or lawyers for offline, face-to-face due diligence work. It provided loans

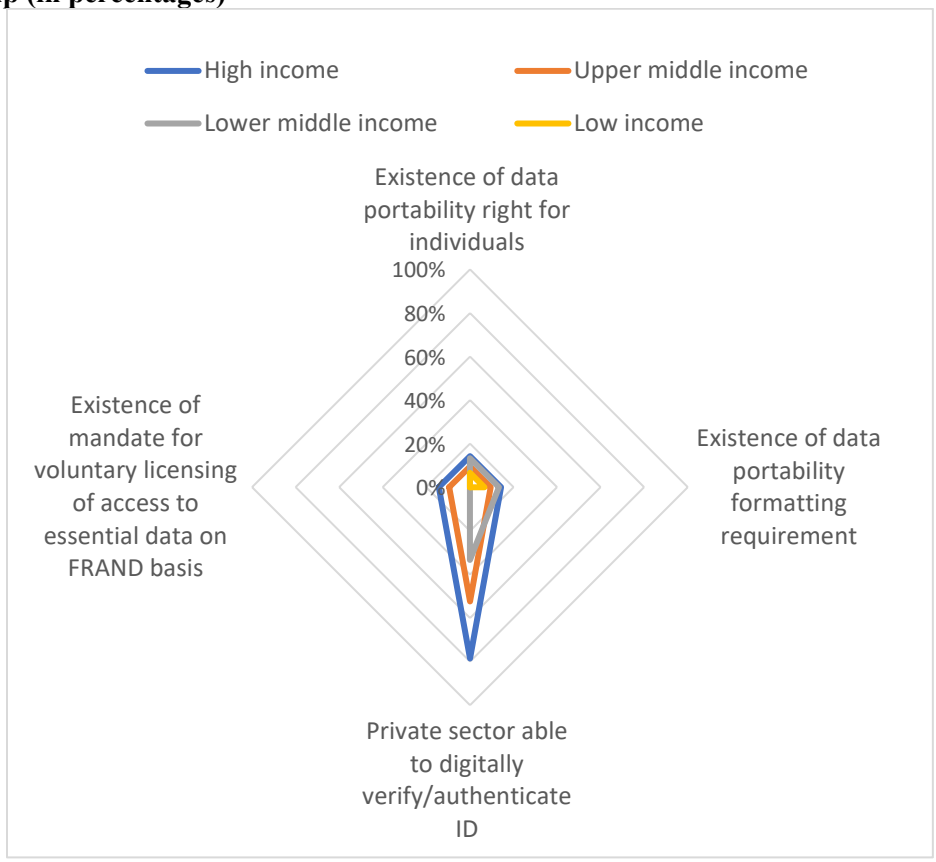
[21] The text of the law can be accessed at: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EA%B3%B5%EB%8D%B0%EC%9D%B4%ED%84%B0%EC%9D%98%EC%A0%9C%EA%B3%B5%EB%B0%8F%EC%9D%B4%EC%9A%A9%ED%99%9C%EC%84%B1%ED%99%94%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0.

[22] Countries score points if their data exchange platforms adopt all these features.

exceeding $600 billion to more than 22 million small and medium enterprises (SMEs) from 2014 to 2019. However, these positive outcomes may be counterbalanced by the potentially negative impact of data collection and exploitation on society. Extensive data collection for private intent requires the implementation of adequate protection safeguards, which will be covered in the safeguards pillar.

The private intent data dimension analyzes the existence of data portability rights for individuals and its formatting requirements, the possibility for the private sector to digitally verify and authenticate users, and the possibility for standard-setting organizations to mandate patent holders to provide voluntary licensing access to "standard essential" data or applications on FRAND (fair, reasonable, and nondiscriminatory) terms (figure 9).

Figure 9. Countries with good regulatory practices to facilitate use of **private** intent **data, by country-income group (in percentages)**



Source: Author's calculation based on results from the diagnostic.

Granting data portability rights is one of the good regulatory practices to facilitate the use of private intent data. According to the European regulators, data portability rights allow data subjects to obtain the personal data they provided to a company or organization in a structured machine-readable format and can be transmitted to another data controller by virtue of clear legal and technical standards. Therefore, data portability has the double effect of increasing users' control over their own data while enhancing competition between companies (European Commission 2020). Data portability for individuals and related formatting requirements have been adopted by only 10 percent of the surveyed countries. This is the case of Benin, among others, which gives users the right to request a controller to transfer their personal data to

another service or product provider in a structured readable format.[23] More in detail, the right to portability has been adopted approximately by 14 percent of high- and lower-middle-income countries, 9 percent of upper-middle-income countries, and 6 percent of countries in the low-income group.

Another issue investigated under the private intent data dimension is the voluntary licensing on FRAND terms, which enables companies and patent holders to share technology and data. On the one hand, holders of data-related intellectual property rights (IPRs) are encouraged to invest in products and markets, as they can control access to licensed products and receive returns on their investments. On the other hand, sectoral or international standard setting organizations may require patent rights to be applied on FRAND terms when these are considered standard essential patents. The diagnostic results show that voluntary licensing to access essential data on FRAND terms is regulated in 14 percent and 9 percent of high- and upper-middle-income countries, respectively, while the matter is not regulated by any lower-middle- and low-income country.

As more and more economic transactions occur online, the ability of private sector actors to digitally verify the identity of users against the ID system becomes essential for efficient digital transactions. High-income countries are taking the lead on adopting such practices, with more than 79 percent of them allowing so. For instance, Canada's SecureKey Technology digitally identifies users through the online credentials used with private partners.[24] A comparable solution is found in approximately half of the upper-middle-income countries. However, no low-income country allows private sector actors to digitally verify the identity of users against the ID system.

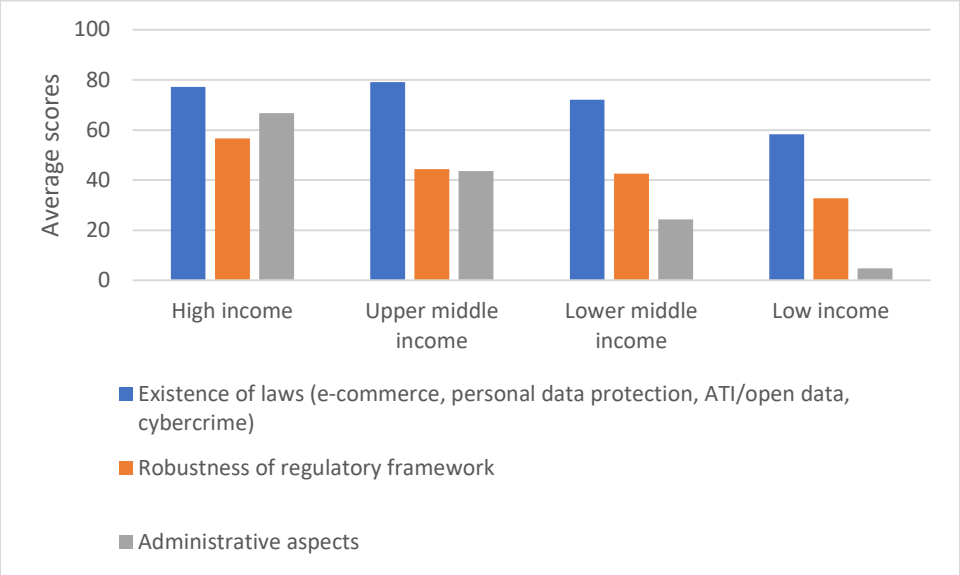
4.4 Existence of laws vs. robustness of laws

The details presented above on data regulation frameworks seek to capture the existence of foundational laws, the robustness of these laws, and data governance administration. These additional details comprise the value this diagnostic provides compared with efforts like UNCTAD's e-transaction database and DLA Piper's data protection law tracker. Besides collecting information on the existence of any e-commerce and data protection laws, ATI, or open data legislation, the diagnostic also measures the robustness of such laws to assess whether they contain specific provisions or regulatory attributes. Moreover, in order to capture information on the implementation of those regulatory frameworks, the diagnostic also includes a few questions on administrative aspects of data governance, such as any digital ID systems for e-services, key institutions such as CSIRTs for cybersecurity and data protection authorities, common technical standards to ensure government system interoperability, mandatory data classifications used across government systems, and so on.

The diagnostic results show that although many countries have established various data regulations, those regulatory frameworks are not extensive enough or sufficiently aligned with good regulatory practices to ensure that the legal framework can create an enabling environment for the data economy (figure 10). Low-income countries in particular are weak on technical infrastructure or institutional settings that enable robust data governance, such as the existence of digital ID system for e-services, mandatory use of common technical standards to ensure government system interoperability. In comparison, high-income countries show a high score on the administrative aspects of data governance even though some legislation is not robust enough with a full range of regulatory good practice incorporated. This reflects quite a pragmatic approach in exploring the most appropriate regulatory framework for their countries.

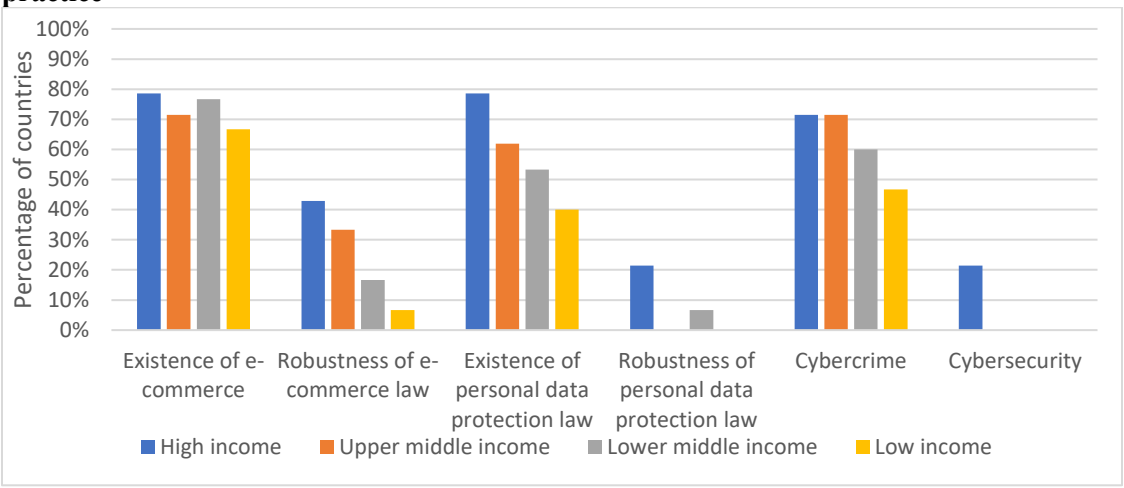
[23] See art. 438 of the Digital Code Act, accessible at: https://sgg.gouv.bj/doc/loi-2017-20/
[24] Additional information available at: https://www.canada.ca/en/revenue-agency/services/e-services/cra-login-services/sign-partners-help-faqs/using-a-sign-partner.html

Figure 10. Performance on different elements of the data governance framework, by country income



Source: Author's calculation based on results from the diagnostic.
Note: Administrative aspects include existence of digital ID system for e-services, mandatory use of common technical standards to ensure government system interoperability, mandatory use of data classification categories across government systems, adoption of open licensing regime, private sector ability to digitally verify/authenticate ID, and existence of mandate for voluntary licensing of access to essential data on FRAND basis. Robustness of regulatory framework is based on the average score of all regulator attributes measured under the Global Data Regulation diagnostic except for the administrative aspects questions, as well as the questions on the existence of e-commerce law, personal data protection law, ATI law, open data law or policy, and cybercrime provisions.

Figure 11. Comparison between existence of key legislation and its coverage of regulatory good practice



Source: Author's calculation based on results from the diagnostic.
Note: Robustness means that the corresponding legal framework contains all the regulatory attributes (getting a full score on all relevant questions) assessed under the Global Data Regulation diagnostic.

The contrast between the existence of laws and the robustness of those laws is particularly salient for data protection legislation (figure 11). Though more than 60 percent of upper-middle-income countries have legal frameworks on data protection, none of them has adopted all the regulatory good practices measured

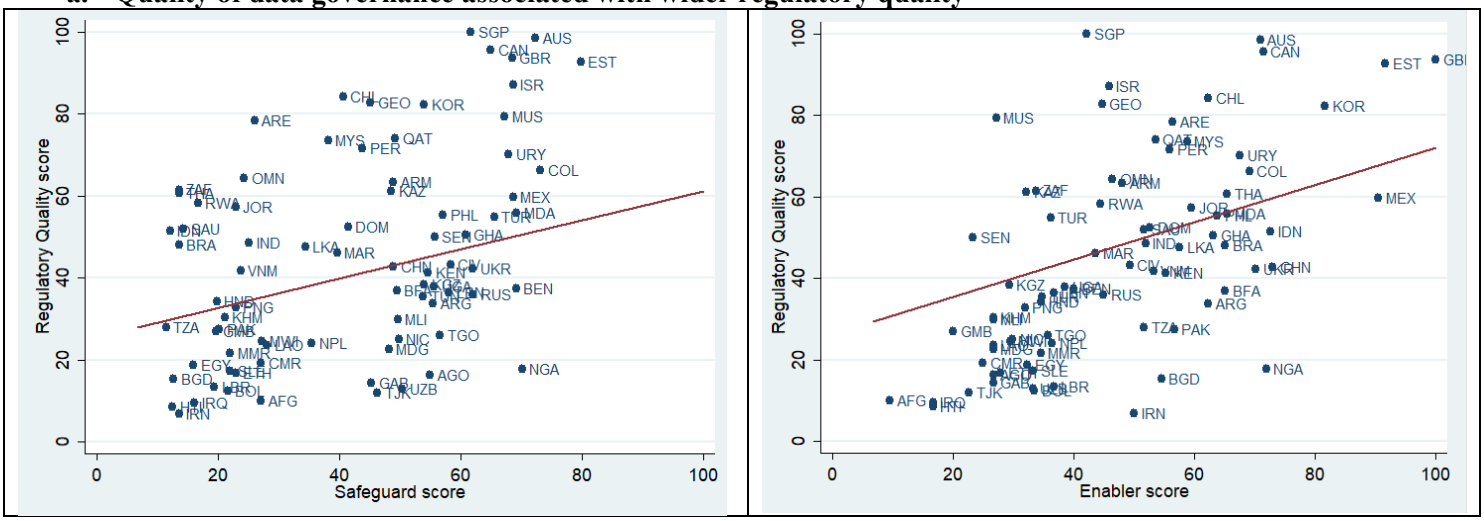
under the diagnostic; this is similarly true for low-income countries. In the same vein, though more than 60 percent of countries surveyed have adopted comprehensive provisions to regulate cybercrime, there are widespread, glaring gaps in the regulatory framework for cybersecurity. Only a few high-income countries (such as the United Kingdom) have adopted a full range of regulatory good practices on cybersecurity, including security requirements for the automated processing of personal data, cybersecurity requirements imposed on data processors/controllers, as well as the creation of cybersecurity strategies, infrastructure, and institutions to identify, investigate, and address cybersecurity threats.

4.5 Data regulation diagnostic vs. other governance assessments

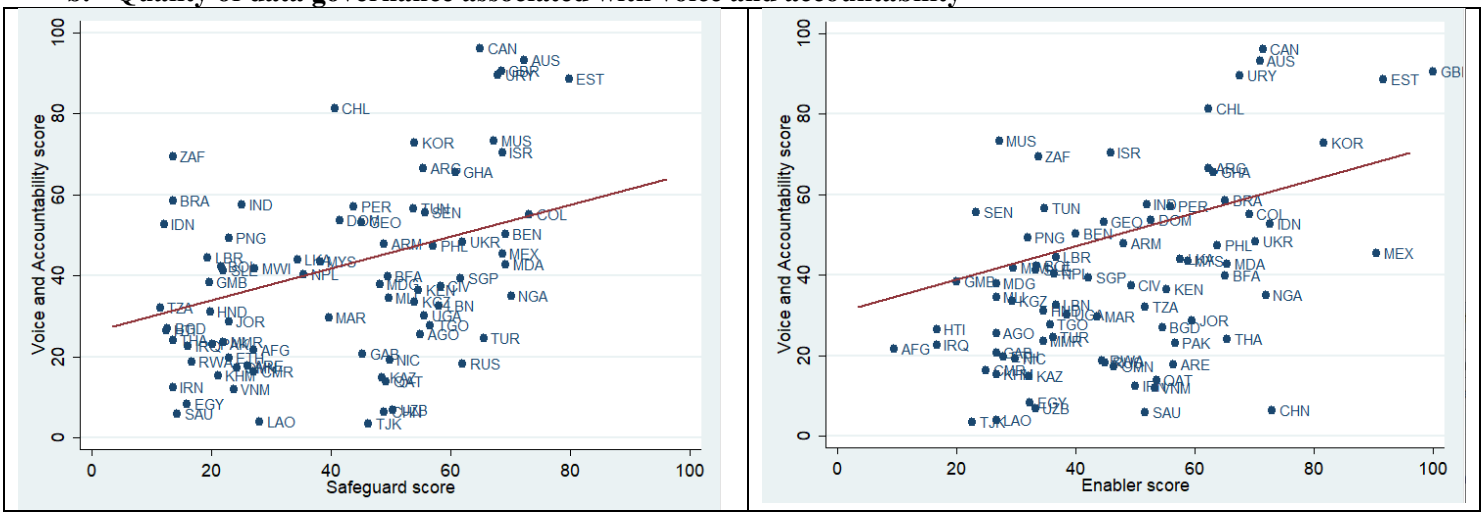
As argued above, the regulatory environment for data governance shapes public trust in the data economy. The diagnostic can also be used, in combination with other data sources, to examine the association between a country's level of regulatory development for data governance and public perceptions, using the Word Governance Indicators (figure 12).

Figure 12. Correlations between the quality of data governance and wider governance characteristics

a. Quality of data governance associated with wider regulatory quality



b. Quality of data governance associated with voice and accountability



Source: Author's calculation based on results from the diagnostic and World Governance Indicators.

Note: Data on "regulatory quality" and "voice and accountability" are from the world governance indicators. The regulatory quality score reflects perceptions of the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development. This indicator has a correlation of 0.45 with the safeguard score and 0.60 with the enabler score. The voice and accountability score reflects perceptions of the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media. This indicator has a correlation coefficient of 0.45 with the safeguard score and 0.50 with the enabler score.

The first point to note is that the safeguard and enablers scores show quite a high correlation with the wider regulatory quality index from the World Governance Indicators (figure 12a). This makes sense as countries with a relatively strong regulatory culture tend to do well on regulation across a wide range of sectors, including data. The regulatory quality indicator reflects the public's trust in the government's ability to formulate and implement sound policies and regulations that permit and promote private sector development. Moreover, more regulatory good practices in enablers are associated with greater confidence in various government functions and entities, including public services, the civil service and its independence from political pressures, policy formulation and implementation and the government's commitment to policies. This could be related in particular to the dimension of public intent data under the enabler pillar, which aims to facilitate the use/reuse of public data to improve government efficiency.

Furthermore, the author finds that more robust regulatory frameworks for data governance are associated with countries where citizens feeling more empowered in terms of both voice and accountability, as reflected in their perceived ability to participate in selecting their government, along with their freedom of expression, freedom of association, and a free media (figure 12b).

Though no causal relations can be drawn from these correlations, the high level of positive associations indicate that the regulatory framework for data does not exist in isolation from a country's wider governance framework and tends to do better in country contexts where citizen perceptions indicate relatively high levels of trust in the regulatory environment. One additional caveat is that the World Governance Indicators measure public trust in governance environment in general, rather than direct measurements of public trust in data economy.

5. COVID-19-specific provisions

The ongoing COVID-19 pandemic makes a robust data governance environment more salient than ever, as many governments have been exploring data-driven options to halt the spread of the virus. For instance, "contact tracing" mechanisms hinge upon the collection and processing of personal data by public authorities—and private actors on their behalf such as app developers. Data protection and cybersecurity concerns regarding such initiatives are rapidly rising. This calls for transparent and consistent rules and regulations on enabling data usage for public health purposes while safeguarding individual rights.

As the pandemic unfolded during the implementation of this diagnostic, the team examined the adoption of COVID-19 emergency regulations in the surveyed countries to assess whether emergency regulations led to the implementation of additional data protection safeguards or the suppression of the existing ones. Overall, 15 countries in the diagnostic sample adopted emergency regulations that had data protection implications. Nine of them had a preexisting data protection law (including Armenia, Côte d'Ivoire, Israel, Korea, Madagascar, Mauritius, Morocco, Peru, and the United Kingdom) and the remaining six did not (Brazil, China, Indonesia, the Islamic Republic of Iran, Jordan, and Papua New Guinea).

For countries that had a pre-existing robust regulatory framework for personal data protection, the legislation usually contained provisions specifying legal grounds or conditions enabling public authorities to collect personal data to preserve public safety and permitting private actors to do so for the public interest.

In this sense, emergency regulation may not necessarily have been required for authorities to carry out their duties. This is the view of the Council of Europe (2020). Protecting the rights of data subjects and preserving public health are goals easily reconciled in jurisdictions that are signatories to the Convention 108 and Convention 108+, as long as data are collected in line with the principles of necessity, proportionality, temporariness, effective (parliamentary and judicial) scrutiny, predictability of emergency legislation, and loyal cooperation among state institutions such as data protection authorities.[25]

As of June 1, 2020, 20 percent of countries with data protection laws adopted emergency regulations to contain the spread of COVID-19 through the collection of personal data. None of those emergency regulations suppressed existing rights of data subjects on the pretext of fighting the pandemic. Take Mauritius as an example. In May 2020, the government adopted emergency regulations that included an amendment to the Data Protection Act 2017, which modified Section 44(1) of the act. This section regulates the "necessary and proportionate" exceptions to the application of the act,[26] which now includes the "issue of any license, permit or authorisation during the COVID-19 period." This amendment sought to facilitate the issuance of documents like work permits during the pandemic, although a test of necessity for such exceptions remains in place.[27] Similarly, the Israeli government declared a temporary state of emergency with the Emergency Regulations (Authorization of the General Security Service to Assist the National Effort to Reduce the Spread of the Novel Coronavirus, 5780-2020), and empowered the national security agency, also known as the Shabak, to conduct contact tracing. This measure raised concerns, but the Israeli Supreme Court confirmed its compliance with the principle of data minimization, and the processing is restricted to what is necessary for the purpose of fighting the pandemic within the time frame of the state of emergency.[28]

On the other hand, 18 percent of countries with no data protection laws promulgated emergency regulations that addressed individual rights with regard to the collection of personal data. Some of the emergency regulations embed certain good regulatory practices on personal data protection, but none provide the full range of safeguards. For instance, Brazil's Law no. 13,979, adopted in response to the pandemic, did not include specific data protection safeguards other than a generic provision that requires personal data sharing among public authorities be limited to the purpose of preventing the spread of COVID-19.[29] Similarly, in Papua New Guinea's National Pandemic Act 2020, although authorities managing the pandemic emergency are required to limit their actions to what is "necessary to achieve the purposes and objectives" of the act and to be "the least intrusive and invasive as possible," they wield extensive powers in data collection and surveillance, such as the unspecified power to "require a person to provide information or answer questions" when needed.[30]

---

[25] With regard to the European Union, the European Data Protection Board (2020) adopted a similar view with its *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, stating that there is no tradeoff between responding to the COVID-19 emergency and the protection of data subject rights.

[26] The act can be accessed at: https://dataprotection.govmu.org/Documents/The%20Law/Act%20No.%2020%20-%20The%20Data%20Protection%20Act%202017.pdf.

[27] See the Covid-19 (Miscellaneous Provisions) Act 2020, Section 13. Accessible at: https://www.mra.mu/download/COVID19Act.pdf .

[28] The Emergency Regulations (Authorization of the General Security Service to Assist the National Effort to Reduce the Spread of the Novel Coronavirus), 5780-2020 is accessible at: https://perma.cc/96V9-HJSS – For further information see also: https://www.pearlcohen.com/israeli-privacy-and-data-protection-in-the-context-of-the-coronavirus-pandemic/

[29] See Lei Nº 13.979, de 6 de Fevereiro de 2020, Art. 6. Accessible at: https://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735; At the time of our data collection, the implementation of Brazil's Federal Law No. 13,709/2018, that is the Brazilian General Data Protection Law (LGPD), had been postponed to 2021.

[30] National Pandemic Act 2020, Sections 9 and 35. Accessible at: https://covid19.info.gov.pg/files/June2020/18062020/National%20Pandemic%20Act%202020-%28Certified%29.pdf

6. Conclusion

The rapid development of the data economy, entailing as it does a boom in various data-driven products, services, and business models, calls for adaptive policies and regulations. A robust regulatory framework for data governance, ecompassing both safeguards to protect rights of market players and enablers to facilitate use/reuse of data, is important to engender trust and encourage participation in the data economy. However, a comprehensive global stocktaking of various good data governance regulatory practices is missing. Governments, especially those in developing countries, lack a reference point to understand their distance from the global frontier of regulatory best practices, and help prioritize regulatory reforms.

The Global Data Regulation diagnostic is so far the most comprehensive assessment of laws and regulations on data governance. It covers the regulatory practices for both safeguarding and enabling across 80 countries. Under the safeguarding and enabling pillars, the diagnostic produces quantitative measurements of the regulatory environments for country data governance, across the dimensions of safeguards for personal and nonpersonal data, cross-border data flows, and cybersecurity, as well as enablers for public and private intent data, and e-commerce transactions. Two aggregated indicators—covering enablers and safeguards—are constructed to summarize good practice policies for benchmarking country performance.

Diagnostic results show that countries have put in greater effort in adopting enablers than safeguards. However, the regulatory development of both safeguards and enablers remains at an intermediate stage: just 41 percent of good safeguard practices and 47 percent of enabler good practices are adopted across countries. High-income countries perform better than lower-income countries in general, but nonetheless present significant regulatory gaps. Except for Sub-Saharan African countries, presently lagging, other regions have relatively similar performance on the enabler pillar, with the East Asia and Pacific region taking a slight lead. Europe and Central Asia is doing better than many other regions on its regulatory safeguards.

Across all dimensions measured, no income group demonstrates advanced regulatory frameworks. All country income groups achieve their highest scores on the e-commerce dimension. Enabling access to public intent data as well as safeguarding cybersecurity are two dimensions where countries are performing relatively well, except for low-income countries. On average, countries have adopted about half the recommended regulatory practices for enabling access to public intent data. Although more than 60 percent of the countries surveyed have adopted comprehensive regulatory provisions on cybercrime, significant regulatory gaps persist in the framework for cybersecurity. Meanwhile, all income groups are at evolving or basic levels for enabling the use/reuse of private intent data and facilitation of cross-border data flows. The recent COVID-19 pandemic has provided the impetus for many countries either to adopt missing personal data protection legislation or to strengthen or clarify such legislation already in place.

An important value addition of the diagnostic, compared with other tools, is that it does not merely track the existence of legislation but captures the overall robustness and completeness and completeness of that regulation by recording the presence or absence of key provisions within the legislation. The diagnostic finds that countries are typically far more advanced with the passage of overarching legislation, than they are with the robustness of that legislation, or with administrative measures to support its implementation. A better characterization of the enforcement of data governance frameworks, as well as a deeper understanding of their economic and social impact, remain topics for future research.

Acknowledgements

This diagnostic builds on the experience and resources of the Digital Business Indicator (DBI) project, a joint initiative started among the Indicators Group of the Development Economics Vice Presidency (DECIG), Macroeconomics, Trade, and Investment (MTI), and Digital Development Global Practices. In 2018, the DBI project collected information on the regulatory environment for the digital economy, covering topics of broadband connectivity, digital payment, data privacy and security, as well as logistics, in 21 pilot countries. Information about data privacy and security, regulatory practices regarding the rights of data subjects, cross-border data flow, and cybersecurity is collected. This study refines the methodology of the data privacy and security indicator (now named as "data governance" indicator) of the DBI project to ensure its consistency with the new framework proposed in WDR21.

The diagnostic project team appreciates funding support from WDR21 and USAID. Vivien Foster provided guidance throughout the diagnostic. Rong Chen was the Project Lead managing the diagnostic. David Satola and Adele Barzelay helped design the questionnaire used in the diagnostic. Yasmin Zand and Olga Kuzmina helped to disseminate questionnaires. Aliaksandra Tyhrytskaya, Federico Cardenas Chacon, Lillyana Sophia Daza Jaller, New Doe Kaledzi, Nicolas Conserva, and Paris Gkartzonikasm contributed to data collection. Nicolas Conserva also provided research support for the paper. David Medine, Malarvizhi Veerappan, Martín Molinuevo, and Sara Nyman provided valuable comments on the methodology of the diagnostic.

References

AlGhamdi, Rayed, Steve Drew, and Waleed Al-Ghaith. 2011. "Factors Influencing E-Commerce Adoption by Retailers in Saudi Arabia: A Qualitative Analysis." *The Electronic Journal of Information Systems in Developing Countries* 47 (1): 1–23.

Alqahtani, Mohammed A., Ali H. Al-Badi and Pam J. Mayhew. 2017. "The Enablers and Disablers of E-Commerce: Consumers' Perspectives." The Electronic Journal of Information Systems in Developing Countries, 10.1002/j.1681-4835.2012.tb00380.x, 54, 1, (1-24).

Argenton, Cédric, and Jens Prüfer. 2012. "Search Engine Competition with Network Externalities." *Journal of Competition Law and Economics* 8 (1): 73–105.

Article 29 Working Party. 2018. "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679." Accessed December 15, 2020. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Cavoukian, Ann. 2011. "Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices." https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf.

Cisco. 2018. "Cisco Visual Networking Index: Forecast and Trends, 2017–2022." Accessed December 15, 2020. https://cloud.report/whitepapers/cisco-visual-networking-index-forecast-and-trends-2017-2022/9017.

Council of Europe. 2020. *Digital Solutions to Fight COVID-19: 2020 Data Protection Report*. Accessed December 15, 2020. https://www.coe.int/en/web/portal/full-news/-/asset_publisher/y5xQt7QdunzT/content/digital-solutions-to-fight-covid-19-shortcomings-protecting-privacy-and-personal-data.

Crawford, Kate and Jason Schultz. 2014 "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*. Vol 55, Rev. 93. http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4

Digital Guardian. 2018. "What Is a Data Classification Policy?" Accessed December 15, 2020. https://digitalguardian.com/blog/what-data-classification-policy.

DLA Piper. 2020. *Data Protection Laws of the World: The Full Handbook*. London, UK: DLA Piper. https://www.dlapiperdataprotection.com/.

European Commission. 2019. "Commission Makes It Even Easier for Citizens to Reuse All Information It Publishes Online." EU Science Hub, European Commission. Accessed December 15, 2020. https://ec.europa.eu/jrc/en/news/commission-makes-it-even-easier-citizens-reuse-all-information-it-publishes-online.

European Commission. 2020. "Shaping Europe's Digital Future: A European Strategy for Data." Accessed December 15, 2020. https://ec.europa.eu/digital-single-market/en/european-strategy-data.

European Data Protection Board. 2020. "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak." Accessed December 15, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

Ferracane, Martina Francesca, Hosuk Lee-Makiyama, and Erik van der Marel. 2018. *Digital Trade Restrictiveness Index.* Brussels, Belgium: European Center for International Political Economy (ECIPE).

González, Raul, Kevin Hasker, and Robin Sickles. 2009. "An Analysis of Strategic Behavior in eBay Auctions." *Singapore Economic Review* 54 (2): 1–32.

Greenleaf, Graham. 2019. "Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)." Supplement to 157 Privacy Laws & Business International Report (PLBIR), 16 pgs. https://ssrn.com/abstract=3380794.

Koo, Wesley Wu-Yi. 2019. "An Institutional Perspective on Platform Rules and Government Regulation." *Academy of Management Annual Meeting Proceedings*. Vol. 2019, No. 1.

Maxwell, Winston, and Marc Bourreau. 2014. "Technology Neutrality in Internet, Telecoms and Data Protection Regulation." SSRN Scholarly Paper, Social Science Research Network, Rochester, NY. Accessed December 15, 2020. https://papers.ssrn.com/abstract=2529680.

North, Douglass C. 1986. "The New Institutional Economics." *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft* 142 (1): 230–37.

North, Douglass C. 1990. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press. Accessed December 15, 2020. https://www.cambridge.org/core/books/institutions-institutional-change-and-economic-performance/AAE1E27DF8996E24C5DD07EB79BBA7EE.

OECD (Organisation for Economic Co-operation and Development). 2016. "Managing Digital Security and Privacy Risk." Accessed December 15, 2020. https://www.oecd-ilibrary.org/science-and-technology/managing-digital-security-and-privacy-risk_5jlwt49ccklt-en.

OECD (Organisation for Economic Co-operation and Development). 2013. "Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data" Accessed December 15, 2020. http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

O'Neill, Brian. 2012. "Trust in the Information Society." *Computer Law & Security Review* 28 (5): 551–59.

Phillips, Mark. 2018. "International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR)." *Human Genetics* 137 (8): 575–82.

Tamanaha Brian Z. 2004. *On the rule of law: history, politics, theory*. Cambridge University Press, Cambridge.

UK Information Commissioner's Office. 2020a. "Data Protection by Design and Default." Accessed December 15, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.

UK Information Commissioner's Office. 2020b. "What Is Re-Use of Public Sector Information?" Accessed December 15, 2020. https://ico.org.uk/for-organisations/guide-to-rpsi/what-is-rpsi/.

UNCTAD (United Nations Conference on Trade and Development). 2019. "UNCTAD Rapid eTrade Readiness Assessments of Least Developed Countries: Policy Impact and Way Forward." Accessed December 15, 2020. https://unctad.org/webflyer/unctad-rapid-etrade-readiness-assessments-least-developed-countries-policy-impact-and-way.

UNCTAD. 2020. "Global E-Commerce Hits $25.6 Trillion—Latest UNCTAD Estimates." Accessed December 15, 2020. https://unctad.org/press-material/global-e-commerce-hits-256-trillion-latest-unctad-estimates.

United States Council of Economic Advisers. 2018. *The Cost of Malicious Cyber Activity to the U.S. Economy*. Washington, DC: Executive Office of the President of the United States. Accessed

December 15, 2020. https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/.

Waldron, Jeremy. 2008. "The Concept and the Rule of Law." *Georgia Law Review*. NYU School of Law, Public Law Research Paper No. 08-50.

World Bank. 2016. *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank.

World Bank. 2020. "In Saudi Arabia, Investments in Digital Infrastructure Are Paying Off." Accessed December 15, 2020. https://blogs.worldbank.org/digital-development/saudi-arabia-investments-digital-infrastructure-are-paying.

World Bank. 2021. *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank.

Data Annexes

Annex 1. Country list

High income	Upper middle income	Lower middle income	Low income
Australia	Argentina	Angola	Afghanistan
Canada	Armenia	Bangladesh	Burkina Faso
Chile	Brazil	Benin	Congo, Dem. Rep.
Estonia	China	Bolivia	Ethiopia
Israel	Colombia	Cambodia	Gambia, The
Korea, Rep.	Dominican Republic	Cameroon	Haiti
Mauritius	Gabon	Côte d'Ivoire	Liberia
Oman	Georgia	Egypt, Arab Rep.	Madagascar
Qatar	Indonesia	Ghana	Malawi
Saudi Arabia	Iran, Islamic Rep.	Honduras	Mali
Singapore	Iraq	India	Rwanda
United Arab Emirates	Jordan	Kenya	Sierra Leone
United Kingdom	Kazakhstan	Kyrgyz Republic	Tajikistan
Uruguay	Lebanon	Lao PDR	Togo
	Malaysia	Moldova	Uganda
	Mexico	Morocco	
	Peru	Myanmar	
	Russian Federation	Nepal	
	South Africa	Nicaragua	
	Thailand	Nigeria	
	Turkey	Pakistan	
		Papua New Guinea	
		Philippines	
		Senegal	
		Sri Lanka	

Annex 2. Data Notes

The Global Data Regulation Diagnostic measure laws and regulations concerning key aspects of a data economy. It consists of two pillars—enablers and safeguards—covering seven dimensions as below:

1. Enablers
    - E-commerce
    - Public intent data
    - Private intent data

2. Safeguards
    - Personal data
    - Nonpersonal data

- Cybersecurity
- Cross-border data

Data are obtained from lawyers specialized in data protection regulations, electronic transactions, cybersecurity, and information and communication technology (ICT), as well as from data protection supervisory authorities. Data collection includes questionnaires completed by specialized respondents and telephone interviews with contributors. Data are also verified through analyses of laws and regulations, including a review of public information sources on relevant topics. More details on each dimension, including the scoring methodology for each data point and specific terms, are set out below.

1. Enablers

Dimension name	Regulatory attribute	What is measured	How it is scored
E-commerce	Legal basis	Is there a law or regulation that explicitly governs e-commerce/e-transactions?	**A score of 1 if "yes"** **A score of 0 if "no"**
	Legal/functional equivalence	Does any law include provisions that grant legal (functional) equivalence between paper-based and electronic communications, contracts, signatures, and records? - Electronic communications/ messages - Electronic contracts - Electronic signatures - E-evidence	**A score of .25 for each of the four options** **A score of 0 if "no"**
	E-signature	What types of electronic signatures are legally recognized in your country? - All legal signatures - Only digital signatures (e.g. PKI)	**A score of 1 if "All legal signatures"** **A score of .5 if "Only digital signatures (e.g., PKI)"**
	Technological neutrality	Does the law or regulations prescribe a specific form or condition for any of the following: - Electronic communications/ messages - Electronic contracts - Electronic signatures	**A score of 0 if "yes"** **A score of 1 if "no"**

	Digital ID system for e-services	Is there a digital ID system that enables individuals to authenticate themselves online to access governmental services? (E.g., e-tax filing, online benefits application)	**A score of 1 if "yes"** **A score of 0 if "no"**
Public intent data	Semantic interoperability	Are governmental/official entities mandated to use common technical standards (e.g. "FAIR") that enable interoperability of systems, registries, databases? - Established standards for open APIs for G2G/G2B/G2C services - Mandated "ask once" principle - Standardized communications protocol for accessing metadata - Semantic catalogues for data and metadata	**A score of .25 for each** **A score of 0 if "no"**
Public intent data	Open data	Is there an Open Data Act or open data policy applicable across the entire public sector? - Yes, an Open Data Act - Yes, an Open Data policy - No	**A score of 1 if "yes, an Open Data Act"** **A score of .5 if "yes, an open data policy"** **A score of 0 if "no"**
Public intent data	Data classification	Is there a government data classification policy/directive?	**A score of 1 if "yes"** **A score of 0 if "no"**
Public intent data	Data classification	Is it mandatory to use common data classification categories across all government database applications or document management systems?	**A score of 1 if "yes"** **A score of 0 if "no"**
Public intent data	ATI	Has right to information/access to information (ATI) legislation been passed that grants individuals the right to request access to government records or data?	**A score of 1 if "yes"** **A score of 0 if "no"**
Public intent data	ATI	Does the law provide for limitations or exceptions to this right of requesting access to government records or data? Please check all that apply: - Sensitive information on national	**A score of 1/6 if any of the options other than "other";** **A score of 0 if "other"**

		security, defense, or foreign policy grounds - Trade secrets or other commercial interests - Personal data - Law enforcement - Privileged information - Public investigations and audits - Other (please explain):	
Public intent data	Sharing-friendly license	Has the government adopted an open licensing regime (such as a Creative Common license by attribution)?	**A score of 1 if "yes"** **A score of 0 if "no"**
Private intent data	Data portability	Do individuals have the right to request that a controller transfer their personal data to another service or product provider?	**A score of 1 if "yes"** **A score of 0 if "no"**
Private intent data	Data portability	Do individuals have the right to obtain their data processed by a controller in a structured, commonly used, and machine-readable format?	**A score of 1 if "yes"** **A score of 0 if "no"**
Private intent data	Private sector verification/authentication through ID	Can private sector service providers digitally verify or authenticate the identity of a person against data stored in the ID system?	**A score of 1 if "yes"** **A score of 0 if "no"**
Private intent data	Voluntary licensing of IPRs	Can standard-setting organizations mandate patent/IPR holders to provide voluntary licensing access to "standard essential" data or applications on FRAND (fair, reasonable and non-discriminatory) terms?	**A score of 1 if "yes"** **A score of 0 if "no"**

2. Safeguards

Personal data	Legal basis for personal data protection	Is there a data protection/privacy law of general application explicitly governing the use, collection, and processing of	**A score of 1 if "yes"** **A score of 0.5 if "no, there are only sector-specific personal data protection**

		governing personal data (including sensitive data) and PII ("personally identifiable information)? - Yes, there is a data protection law of general application governing personal data, PII, and sensitive data; - No, there are only sector-specific personal data protection and/or privacy laws; - No, there are privacy and/or data protection rights protected in the country's constitution - No, no laws exist but there have been significant court or administrative decisions that form the basis of or clarify privacy or data protection rights	**and/or privacy laws"** **A score of 0.25 if "no, there are privacy and/or data protection rights protected in the country's constitution"** **A score of 0.25 if "no, no laws exist but there have been significant court or administrative decisions that form the basis of or clarify privacy or data protection rights"** **A score of 0 if "no"**
Personal data	Government exception to liability	Does the relevant law/regulation provide exceptions to limitations on the collection or processing of data by government?	**A score of 0 if "yes"** **A score of 1 if "no"**
Personal data	Necessity and proportionality	Are these exceptions subject to a "necessary and proportionate" test to determine whether the exception is legitimately applied?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Purpose limitation	Does any law or regulation require that the collection and use of personal data be made for a stated purpose (or similar standard)?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Data minimization	Does any law or regulation require that the collection and use of personal data be proportionate, relevant, adequate, and limited to what is necessary in relation to the purpose for which it is processed (or similar standard)?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Storage limitations	Does any law or regulation require that personal data not be kept longer than is necessary for the	**A score of 1 if "yes"** **A score of 0 if "no"**

		purposes for which it is processed (or similar standard)?	
Personal data	Privacy by design	Does any policy, law, or regulation require data processors to incorporate technical and organizational privacy-by-design or privacy-by-default principles or use privacy-enhancing technologies (PETs) in the design and implementation of processing systems?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Data sharing with third parties	Do any laws, regulations, or policies authorize, restrict or otherwise address sharing of personal data with third parties?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Right to challenge accuracy and rectify personal data	Do individuals have the right to challenge the accuracy of information and have it rectified, completed, amended, and/or deleted?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Automated decisions	Are there rights to limit the making of decisions about individuals solely as a result of automated processing of personal data (i.e., without any human intervention)?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Redress	Do individuals have a right to object to the use of personal data about them, file complaints, and seek redress?	**A score of 1 if "yes"** **A score of 0 if "no"**
Personal data	Enforcement mechanisms	Does the law/regulation provide for the creation of a data protection authority/office (DPA/DPO)?	**A score of 1 if "yes"** **A score of 0 if "no"**
Nonpersonal data	IPRs to prevent data sharing	Can intellectual property rights be used to prevent the sharing of data?	**A score of 0 if "yes"** **A score of 1 if "no"**
Nonpersonal data	IPRs to prevent data sharing	Does the law include a provision regulating confidentiality or third-party rights in non-personal	**A score of 1 if "yes"** **A score of 0 if "no"**

		government data (e.g. company registers, business data underlying official statistics)?	
Cybersecurity	Data security	Do data processors/controllers have to comply with the following security requirements for the automated processing of personal data? Please check all that apply: - Encryption of personal data - Anonymization/ pseudonymization of personal data - Integrity of data and systems that use or generate personal data - Ability to restore data and systems that use or generate personal data after a physical or technical incident - Ongoing tests, assessments, and evaluation of security of systems that use or generate personal data	**A score of .20 for each "yes"** **A score of 0 if "no"**
Cybersecurity	Internal adoption of cybersecurity standards	Do data processors/controllers have to comply with the following cybersecurity requirements? Please check all that apply: - Adoption of an internal policy establishing procedures for preventing and detecting violations - Confidentiality of data and systems that use or generate personal data - Appointment of a personal data processing office/manager - Performance of internal controls - Assessment of the harm that might be caused by a data breach - Awareness program among employees	**A score of 1/6 for each "yes"** **A score of 0 if "no"**
Cybersecurity	CERT	Does any law, regulation, or policy provide for the creation of a cyber-security strategy, infrastructure and institutions to identify, investigate, and address cyber-security threats? - A cyber-security plan to protect	**A score of .5 for each "yes"** **A score of 0 if "no"**

		key national infrastructure - A national CERT	
Cross-border data	Adequacy and mutual recognition agreements for personal data	Under what conditions can local personal data be transferred to non-domestic third parties? - Adequacy approach - Accountability approach	**A score of .5 if "adequacy approach"** **A score of .5 if "accountability approach"** **A score of 0 if local personal data cannot be transferred to nondomestic third parties**
Cross-border data	Adequacy and mutual recognition agreements for personal data	Does the country have arrangements with foreign countries or multinational entities or schemes, including decisions of domestic and foreign bodies or agencies, to require, permit, or limit transfers of personal data between countries? Please check all that apply: - Adequacy decisions/ whitelists - Binding corporate rules - Mutual recognition arrangements - Required information sharing through the Advance Passenger Information System - Treaties - Self-certification/self-assessment under a specific agreement - Standard contractual clauses	**A score of .25 for (i) adequacy, (ii) BCR, (iii) mutual recognition arrangements, and (iv) treaties; 0 otherwise**
Cross-border data	Adequacy and mutual recognition agreements on personal data	If the regime requires an "adequacy" or similar mechanism, what circumstances constitute an "adequate level of protection" when transferring personal data internationally? Please check all that apply: - The nature of the personal data - The country of origin of the information contained in the data - The country of destination - The purposes for which and period during which the data are intended to be processed	**Except for "country of origin" and "country of destination", a score of 1/7 for each remaining option**

		- The domestic law in force in the host country (general and sectoral, including defense and access of public authorities to personal data) - The existence and effective functioning of one or more independent supervisory authorities in the third country to enforce compliance - Presence of effective rule of law and judicial redress for data subjects - The international treaties the host country is a party to - Relevant codes of conduct or other rules enforceable in the host country (SCCs; BCRs)	

Annex 3. Country scores on different dimensions, and on the enablers and safeguards pillars

Country name	E-commerce/transaction	Public intent data	Private intent data	Personal data	Non-personal data	Cybersecurity and cybercrime	Cross border data transactions/ flows	Enablers	Safeguards
Afghanistan	0.00	28.57	0.00	4.17	50.00	54.17	0.00	9.52	27.08
Angola	80.00	0.00	0.00	83.33	50.00	43.69	42.86	26.67	54.97
Argentina	80.00	82.14	25.00	75.00	0.00	76.67	70.24	62.38	55.48
Armenia	50.00	69.05	25.00	83.33	0.00	69.17	42.86	48.02	48.84
Australia	95.00	92.86	25.00	75.00	50.00	91.67	72.62	70.95	72.32
Bangladesh	60.00	78.57	25.00	4.17	0.00	46.43	0.00	54.52	12.65
Benin	70.00	0.00	50.00	83.33	50.00	82.50	60.71	40.00	69.14
Bolivia	35.00	40.48	25.00	4.17	50.00	32.14	0.00	33.49	21.58
Brazil	100.00	95.24	0.00	4.17	0.00	50.00	0.00	65.08	13.54
Burkina Faso	80.00	65.48	50.00	75.00	50.00	47.86	25.00	65.16	49.46
Cambodia	80.00	0.00	0.00	4.17	50.00	30.36	0.00	26.67	21.13
Cameroon	75.00	0.00	0.00	4.17	50.00	54.17	0.00	25.00	27.08
Canada	100.00	89.29	25.00	75.00	50.00	85.00	50.00	71.43	65.00
Chile	75.00	86.90	25.00	58.33	50.00	54.17	0.00	62.30	40.63
China	100.00	69.05	50.00	4.17	50.00	95.00	46.43	73.02	48.90
Colombia	80.00	52.38	75.00	75.00	100.00	67.50	50.00	69.13	73.13
Congo, Dem. Rep.	60.00	0.00	0.00	2.08	50.00	0.00	0.00	20.00	13.02
Côte d'Ivoire	80.00	42.86	25.00	83.33	50.00	64.17	35.71	49.29	58.30
Dominican Republic	65.00	92.86	0.00	50.00	0.00	63.33	52.38	52.62	41.43

Egypt, Arab Rep.	45.00	32.14	0.00	4.17	0.00	59.76	0.00	25.71	15.98
Estonia	100.00	100.00	75.00	91.67	50.00	100.00	77.38	91.67	79.76
Ethiopia	55.00	28.57	0.00	4.17	50.00	37.50	0.00	27.86	22.92
Gabon	80.00	0.00	0.00	75.00	50.00	34.52	29.76	26.67	47.32
Gambia, The	60.00	0.00	0.00	4.17	50.00	24.29	0.00	20.00	19.61
Georgia	45.00	44.05	25.00	66.67	0.00	67.50	46.43	38.02	45.15
Ghana	100.00	64.29	25.00	91.67	50.00	76.67	25.00	63.10	60.83
Haiti	50.00	0.00	0.00	0.00	50.00	0.00	0.00	16.67	12.50
Honduras	80.00	23.81	0.00	4.17	50.00	25.00	0.00	34.60	19.79
India	70.00	60.71	25.00	4.17	0.00	50.00	46.43	51.90	25.15
Indonesia	100.00	92.86	25.00	4.17	0.00	44.29	0.00	72.62	12.11
Iran, Islamic Rep.	80.00	70.24	0.00	4.17	0.00	50.00	0.00	50.08	13.54
Iraq	50.00	0.00	0.00	2.08	50.00	12.50	0.00	16.67	16.15
Israel	65.00	47.62	25.00	58.33	50.00	90.00	76.19	45.87	68.63
Jordan	100.00	78.57	0.00	4.17	50.00	37.50	0.00	59.52	22.92
Kazakhstan	45.00	71.43	0.00	58.33	50.00	56.19	29.76	38.81	48.57
Kenya	80.00	35.71	50.00	91.67	0.00	95.83	30.95	55.24	54.61
Korea, Rep.	95.00	100.00	50.00	75.00	50.00	53.21	37.50	81.67	53.93
Kyrgyz Republic	45.00	42.86	0.00	66.67	50.00	51.43	47.62	29.29	53.93
Lao PDR	80.00	0.00	0.00	4.17	50.00	58.33	0.00	26.67	28.13
Lebanon	60.00	50.00	0.00	66.67	100.00	35.95	29.76	36.67	58.10
Liberia	60.00	50.00	0.00	2.08	50.00	25.60	0.00	36.67	19.42
Madagascar	80.00	0.00	0.00	66.67	50.00	38.33	37.50	26.67	48.13
Malawi	60.00	28.57	0.00	4.17	50.00	54.76	0.00	29.52	27.23
Malaysia	80.00	46.43	50.00	66.67	0.00	47.86	38.10	58.81	38.15
Mali	80.00	0.00	0.00	83.33	50.00	34.17	30.95	26.67	49.61
Mauritius	60.00	21.43	0.00	83.33	50.00	100.00	35.71	27.14	67.26
Mexico	100.00	96.43	75.00	83.33	50.00	90.00	51.19	90.48	68.63
Moldova	100.00	71.43	25.00	83.33	50.00	77.86	65.48	65.48	69.17
Morocco	100.00	30.95	0.00	66.67	0.00	35.95	55.95	43.65	39.64
Myanmar	75.00	28.57	0.00	4.17	50.00	33.93	0.00	34.52	22.02
Nepal	45.00	64.29	0.00	41.67	50.00	50.00	0.00	36.43	35.42
Nicaragua	35.00	54.76	0.00	75.00	50.00	38.33	35.71	29.92	49.76
Nigeria	80.00	60.71	75.00	75.00	50.00	90.00	65.48	71.90	70.12
Oman	100.00	39.29	0.00	4.17	50.00	42.86	0.00	46.43	24.26
Pakistan	95.00	50.00	25.00	4.17	50.00	26.79	0.00	56.67	20.24
Papua New Guinea	60.00	35.71	0.00	4.17	50.00	37.50	0.00	31.90	22.92
Peru	50.00	92.86	25.00	75.00	0.00	60.83	39.29	55.95	43.78
Philippines	70.00	71.43	50.00	83.33	0.00	95.00	50.00	63.81	57.08
Qatar	100.00	35.71	25.00	50.00	50.00	71.67	25.00	53.57	49.17

Russian Federation	60.00	50.00	25.00	75.00	50.00	85.00	38.10	45.00	62.02
Rwanda	100.00	33.33	0.00	4.17	0.00	62.50	0.00	44.44	16.67
Saudi Arabia	80.00	50.00	25.00	4.17	0.00	52.86	0.00	51.67	14.26
Senegal	70.00	0.00	0.00	83.33	50.00	46.67	42.86	23.33	55.71
Sierra Leone	50.00	50.00	0.00	4.17	50.00	33.93	0.00	33.33	22.02
Singapore	80.00	21.43	25.00	66.67	50.00	67.50	62.50	42.14	61.67
South Africa	75.00	26.19	0.00	4.17	0.00	50.00	0.00	33.73	13.54
Sri Lanka	80.00	92.86	0.00	0.00	100.00	37.50	0.00	57.62	34.38
Tajikistan	25.00	42.86	0.00	66.67	50.00	33.93	42.86	22.62	48.36
Tanzania	80.00	75.00	0.00	4.17	0.00	41.67	0.00	51.67	11.46
Thailand	100.00	96.43	0.00	4.17	0.00	50.00	0.00	65.48	13.54
Togo	50.00	57.14	0.00	75.00	50.00	55.00	46.43	35.71	56.61
Tunisia	40.00	64.29	0.00	66.67	50.00	55.60	42.86	34.76	53.78
Turkey	55.00	28.57	25.00	75.00	50.00	63.33	73.81	36.19	65.54
Uganda	80.00	35.71	0.00	75.00	50.00	80.83	16.67	38.57	55.63
Ukraine	100.00	85.71	25.00	83.33	50.00	68.10	46.43	70.24	61.96
United Arab Emirates	80.00	89.29	0.00	4.17	50.00	50.00	0.00	56.43	26.04
United Kingdom	100.00	100.00	100.00	91.67	0.00	100.00	82.14	100.00	68.45
Uruguay	80.00	97.62	25.00	91.67	50.00	64.40	65.48	67.54	67.89
Uzbekistan	70.00	65.48	0.00	66.67	50.00	46.67	38.10	45.16	50.36
Vietnam	80.00	54.76	25.00	4.17	0.00	90.83	0.00	53.25	23.75