

G20

Members' Regulations of Cross-Border Data Flows



United
Nations

G20

Members' Regulations of Cross-Border Data Flows



**United
Nations**

Geneva, 2023

© 2023, United Nations

This work is available through open access, by complying with the Creative Commons licence created for intergovernmental organizations, at <http://creativecommons.org/licenses/by/3.0/igo/>

The findings, interpretations and conclusions expressed herein are those of the author(s) and do not necessarily reflect the views of the United Nations or its officials or Member States.

The designations employed and the presentation of material on any map in this work do not imply the expression of any opinion whatsoever on the part of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Photocopies and reproductions of excerpts are allowed with proper credits.

This publication has not been formally edited.

United Nations publication issued by the United Nations Conference
on Trade and Development

UNCTAD/DTL/ECDE/2023/1

eISBN: 978-92-1-002423-5

Photos: (cc) Unsplash



Note

In accordance with the mandate given to it by member States, UNCTAD's E-Commerce and Digital Economy (ECDE) Branch in the UNCTAD Division on Technology and Logistics aims to contribute to enhanced inclusive and sustainable development gains from e-commerce and the digital economy for people and businesses in developing countries, particularly least developed countries (LDCs). The ECDE Programme works with government policymakers and development partners, civil society and the private sector to strengthen the readiness of developing countries to harness the opportunities and address the risks presented by digitalization in four main ways, by:

- Providing better evidence on what policy changes are needed at the national, regional and international level to generate more inclusive and sustainable outcomes in the data-driven digital economy, including through the biennial Digital Economy Report;
- Offering tailored assistance to low-income countries to build their capacities to engage in and benefit from e-commerce and the digital economy (eTrade Readiness Assessments, E-commerce Strategies, E-commerce and Law Reform, Measuring the Digital Economy);
- Empowering women digital entrepreneurs in developing countries to become more visible as role models and therefore better heard by policy makers to foster change in the business enabling environment (eTrade for Women);
- Paving the way for more collaborative efforts and effective partnerships to make better use of scarce resources in the area of digital for development and build consensus (eTrade for all, eCommerce Weeks, Intergovernmental Group of Experts).

Foreword

BY **SHAMIKA N. SIRIMANNE**

DIRECTOR, DIVISION ON TECHNOLOGY
AND LOGISTICS

Accelerated digitalization has marked the experience of many in the past few years. This has led to a surge in digital data and data flows across borders. It is fair to say that we are still looking for answers on the best approaches to handling data to ensure favourable outcomes. However, how we deal with data and data flows will have significant implications for our ability to meet the Sustainable Development Goals. And it will affect the lives of people in countries at all levels of development. This therefore remains one of the main policy challenges of our time.

This report, and its underlying survey of G20 member States and invited guests during Indonesia's 2022 G20 Presidency, highlight the multidimensional nature of data and consequently the multitude of legislation which impact many areas for policy making, including child protection, health, competition, financial markets, and data governance.

Harnessing data for all people and the planet will require new thinking on and innovative approaches to the governance of data. The discussions within the G20's Digital Economy Working Group fostered efforts to strengthen stakeholders' understanding of commonalities, complementarities, and elements of convergence between regulatory approaches, including the existing regional and multilateral arrangements, that enables data to flow with trust.

Previous UNCTAD publications and research have demonstrated that the challenge going forward is to govern data and data flows in such a way that gains can be shared more equitably. And this process must allow for sufficient policy space for countries at varying levels of digital capabilities, to promote national priorities and development objectives, while also addressing possible risks from digitalization.

This report reflects UNCTAD's commitment to providing new knowledge and insights to policy makers and to contribute to the much needed dialogue among member States on how to govern cross-border data flows with a view to fostering sustainable development.

While the body of this report looks at G20 participants, the United Nations has a key role to play, being the most inclusive forum in terms of country representation.



Important lessons can perhaps be drawn from the work on climate change, ensuring that all development aspects are considered. In the Digital Economy Report 2021, we recommended the establishment of a body or mechanism to facilitate more dialogue and coordination on data governance. It would need to be multilateral, multidimensional and multistakeholder in its approach.

This report can contribute to building greater awareness of all the relevant areas that Governments are considering in the context of data governance, and support evidence-based consensus-building towards improving a balanced global approach to governing data.



Acknowledgements

This report was prepared under the overall guidance of Shamika N. Sirimanne, Director of the Division on Technology and Logistics, by Torbjörn Fredriksson and Laura Cyron. An earlier version was presented to the G20 Digital Economy Working Group at the request of the Indonesia G20 Presidency in 2022.

UNCTAD would like to thank the Government of Indonesia and all G20 Members and invited guests that provided responses to the questionnaire, based on which the following report was compiled, as well as to those that provided feedback to the report.

The cover, graphics and desktop publishing were designed by Jesús Alés. Diana Quirós provided administrative support.

Financial support from the Core Donors of the ECDE Programme – Germany, the Netherlands, Sweden and Switzerland – is gratefully acknowledged.

Contents

NOTE	V
FOREWORD	VI
ACKNOWLEDGEMENTS	IX

1. Introduction	1
-----------------	---

2. Survey methodology	4
-----------------------	---

Description of the questionnaire	4
Motivation to include questions	4
Response rates by section	4

3. Survey results	5
-------------------	---

Analysis of laws and regulations presented	5
Policy coordination and consultation	11

4. Conclusions	14
----------------	----

Implications for international cooperation on data governance	14
Areas for potential further discussion	15

5. References	16
---------------	----

6. Annex	17
----------	----

ANNEX TABLE 1: PERSONAL DATA DEFINITIONS	17
ANNEX TABLE 2: SENSITIVE DATA DEFINITIONS	20
ANNEX TABLE 3: OVERVIEW OF SUBMISSIONS CATEGORIZED BY DATA TYPE	22
RECENT UNCTAD PUBLICATIONS ON E-COMMERCE AND THE DIGITAL ECONOMY	26

Acronyms and abbreviations

G20	Group of Twenty
OECD	Organisation for Economic Co-operation and Development
UNCTAD	United Nations Conference on Trade and Development



1. Introduction

Data have become a key strategic asset for the creation of both private and social value. If well managed, data can help address global development challenges such as pandemics and climate change while promoting prosperity. However, negligent handling of data can contribute to highly unequal development outcomes and undermine the functioning of the Internet.

Unified measurement of global data flows does not exist. However, it is clear that an already existing upward tendency was accelerated by COVID-19 when many activities moved online. One estimate suggested that the global Internet Protocol traffic in 2022, both international and domestic, would exceed all Internet traffic up to 2016.¹ Meanwhile, this increase in data traffic and extent of value capture from the digital economy is not equally distributed across and between countries; available information suggests that traffic, which can be seen as a rough proxy for value, is predominantly concentrated on two main East-West routes, between North America and Asia and North America and Europe (see Figure 1).²

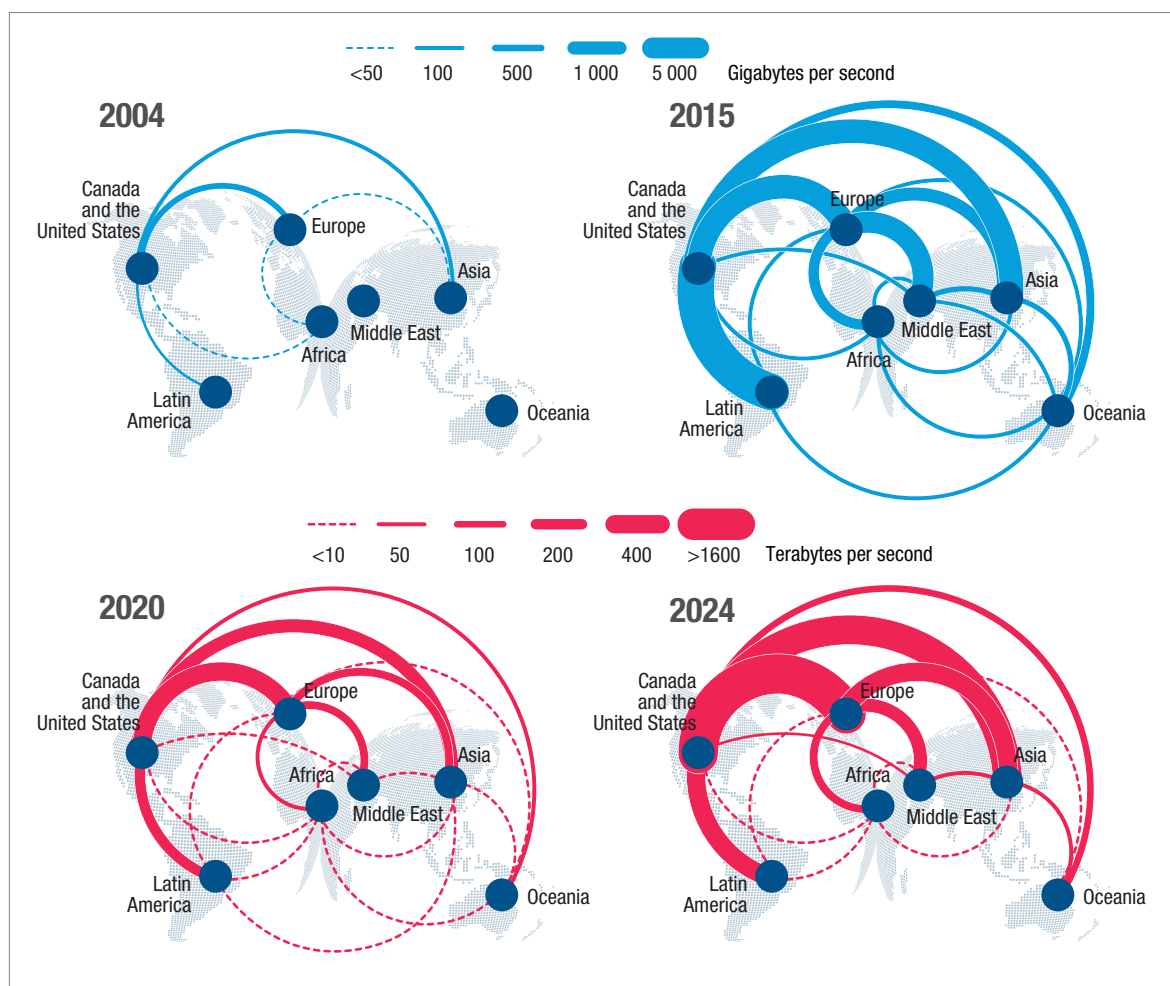
As highlighted in the [Digital Economy Report 2021](#) (UNCTAD, 2021), the global landscape for the governance of data is fragmented, with countries adopting different approaches to regulate and safeguard data flows across borders. There is a lack of globally agreed common definitions and understanding of basic concepts related to data and data flows. The various taxonomies that are used to classify types of data are sometimes based on different criteria. For example, data may be collected for commercial or governmental purposes; used by the private or the public sector; may be instant or historic; sensitive or non-sensitive; personal or non-personal. Different understandings of key terms and approaches may undermine the interoperability of data access and sharing, including across borders.

Regardless of the different definitions and concepts related to data and data flows, there are initiatives in the G20 and beyond to identify and unify convergences, commonalities and complementarities, in order to help in the adequate development on the subject, through the experiences and authorities in the field of personal data protection of each country.

1. See Cisco, 27 November 2018, Cisco Predicts More Internet Protocol Traffic in the Next Five Years Than in the History of the Internet.

2. This statement refers to openly available information from TeleGeography, the largest provider of data and analysis on long-haul networks and the undersea cable market. More information is available for subscription. Thus, it could be the case that more detailed statistics exist, but are proprietary.

Figure 1: Evolution of interregional international bandwidth, selected years



Source: UNCTAD (2021), based on TeleGeography (2015, 2019, 2021).

Note: One Terabyte is equal to 1,000 Gigabites. Data for 2024 are forecasts.

The interface between the use of different taxonomies and cross-border data flows has not yet been much explored. This report analyses the responses to a survey of G20 Members' current laws and regulations pertaining to cross-border data flows. It seeks to establish a better understanding of where there are commonalities, complementarities, convergence and divergence, and contribute to further dialogue on how to shape governance frameworks that can facilitate cross-border data flows and data free flow with trust.

This report focuses predominantly on domestic policies of G20 member States and invited guests³ affecting data flows. Consequently, they highlight unilateral ways of handling data-related issues and indirectly illustrate countries' national priorities in safeguarding data and enabling data flows. For international discussions in this area to succeed, a better understanding of the national perspectives can be a beneficial component.

3. The nine invited guest countries under the Indonesian presidency: Cambodia, Fiji, the Netherlands, Rwanda, Senegal, Singapore, Spain, Suriname, and United Arab Emirates.

Data free flow with trust and cross-border data flows are topics of discussion among G20 members since the Japanese Presidency in 2019. They continued under the Saudi Presidency in 2020 and the Italian Presidency in 2021. In 2022, under the Indonesian Presidency, the Digital Economy Working Group met for the first time, taking over from its predecessor, the Digital Economy Task Force.

Discussions on cross-border data flows concern all countries, beyond the G20. This is also reflected in the growing body of relevant initiatives since 2021 such as the African Union Data Policy Framework,⁴ the G7 Trade Ministers' Digital Trade Principles,⁵ multiple United Nations' initiatives – the Secretary General's "Our Common Agenda"⁶ and UNICEF's Global Development Commons⁷ – and initiatives from civil society, for instance, the Datasphere Initiative⁸.

Furthermore, there is an increasing body of policy relevant research on cross-border flows, as demonstrated by the Digital Economy Report 2021 (UNCTAD, 2021). Moreover, the OECD reports on *Mapping approaches to data and data flows* (OECD, 2020) and on *Mapping commonalities in regulatory approaches to cross-border data transfers* (Casalini et al., 2021) inform on the existing approaches for governance of data flows and options on regulatory approaches. The latter report put an emphasis on trade related aspects.

To complement these insights, this report is based on G20 Members' responses to a survey asking for any type of law and regulation linked to cross-border data flows. Given the growing role of data for all aspects of life, broadening the perspective for international cooperation in the area of cross-border data flows will be essential to ensure that in the future the gains from digitalization can be shared more broadly across countries for the benefit of society, economies, people and the environment.

4. <https://au.int/en/documents/20220728/au-data-policy-framework>

5. <https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles>

6. <https://www.un.org/en/common-agenda>

7. <https://gdc.unicef.org/>

8. <https://www.thedatasphere.org/>

2. Survey methodology

Description of the questionnaire

Responses by G20 Members and invited guests inform this report and analysis. The underlying survey elicited information on existing laws and regulations and some proposals that include provisions affecting cross-border data flows. This report aims to provide a description of the existing landscape in member States of laws and regulations that take cross-border data flows into account.

The survey aimed to categorize which types of data certain laws and regulations are linked to and how these categories are defined. Categories include personal, non-personal, critical and sensitive data.

This information was complemented by information on whether the law or regulation is specific to a sector and on the ministries and agencies responsible for its implementation. Moreover, the survey aimed to find out how these laws and regulations impact cross-border data flows. In a second part, the survey asked about national (multistakeholder) coordination on data governance issues.

Motivation to include questions

The survey was as open ended as possible for countries to submit their laws and regulations. Given the growing importance of data in all areas, the results presented here are indicative, but not exhaustive. The questions aimed to create basic profiles of laws and regulations that pertain to cross-border data flows. They may indicate certain country-specific priorities but also highlight how pervasive data are in all areas of the economy and society.

Response rates by section

The response rate and level of engagement were high, with 90 per cent of G20 Members submitting responses plus contributions from five guests. Overall, the submissions included 92 national laws, regulations, and guidelines.

3. Survey results

Analysis of laws and regulations presented

Definitions

Discussions in international fora on data and data flows can be facilitated by using common definitions for various concepts and terms when regulating data and data flows. Against this background, the survey requested respondents to specify, where possible, the definitions used in the different laws.

Personal data

At a basic level, definitions appear to be aligned, as also pointed out in OECD (2020). In the submissions to the survey, the definitions of “personal data” overlap to a great extent across Members, although the level of detail provided varies (see Annex table 1). As some laws and regulations predate the recent years of accelerated digitalization, the definitions referring to personal or sensitive information are included as well.

Some national laws limit the definition of personal data to information on identified or identifiable persons without any further details.

In a law of Mexico, a further clarification on “identifiable” is added, by stressing “when his/her identity may be directly or indirectly determined from any information”. Similar clarifications are also found in legal texts from the European Union, the Republic of Korea and the United Kingdom of Great Britain and Northern Ireland.

Definitions also vary with respect to the level of detail on the kind of information that may make someone identifiable. For example, Canada’s Privacy Act includes, but is not limited to, 23 specific features of information. Saudi Arabia lists 11 features in its Personal Data Protection Law, the United States of America includes 11 in its Privacy Act, the definitions offered by the European Union and United Kingdom of Great Britain and Northern Ireland cover 10 categories, while the personal information protection act of the Republic of Korea contains three (see Annex table 1). Singapore’s Advisory Guidelines on Key Concepts in the Personal Data Protection Act extends the Act’s definition by providing examples of possible features that make an individual identifiable.

Another way to group the definitions is by their inclusion of provisions on whether and how these data are recorded or stored. Elements to this effect are included in the definitions used by, for example, Australia, China, Indonesia and the United States of America.



Sensitive data

The term “sensitive data” in the submissions is universally understood to be a subset of personal data (see Annex table 2). National definitions vary with regard to the kind of elements which are included as sensitive information (see Table 1).

Table 1: Elements included in sensitive data definitions

Categories	Argentina	Australia	Brazil	Mexico	Saudi Arabia	Republic of Korea	Türkiye	United Kingdom
Biometric information								
Credit data								
Criminal records								
Ethnic/racial/tribal origin								
Genetic information								
Health information								
Location data								
Philosophical/moral conviction								
Political assoc. membership								
Political opinions								
Religious belief								
Sex life								
Trade union membership								
Unknown parentage								

Source: UNCTAD, based on survey responses by G20 member States and invited guests.

Critical data

Another term used in discussions around cross-border data flows and their regulation is “critical data”, which is often left intentionally ambiguous (UNCTAD 2021: 129). The laws and regulations submitted seem to confirm this observation. Three countries refer to critical data in their submissions (Republic of Korea with respect to cloud computing, Saudi Arabia for critical systems cybersecurity controls and Türkiye in the context of statistics). Critical data are defined only in one instance, in the Republic of Korea’s Standards for Cloud Computing Service Information Protection (see Table 2).

Table 2: Critical data definition

	Definition
Republic of Korea <i>Standards for Cloud Computing Service Information Protection</i>	Critical data: Important internal information data such as electronic approval, HR, and accounting management

Areas and sectors covered by the data regulations

The survey submissions highlight the multi-dimensionality of data and the diversity of areas potentially affected by data flows. Forty-two laws and regulations were predominantly linked to personal data, 9 relate to non-personal data, and 41 refer to all types of data (see Annex table 3).

As the term data free flow with trust implies, transferring data internationally requires a certain level of trust or legal safeguards which ensure that data are protected to a similar extent outside the country as within. In line with this, a large share of submitted laws and regulations that are linked to cross-border data flows are focused on personal data and provisions allowing their transfer abroad, specifically with respect to personal data protection and privacy (see Annex table 3, column 1). It is therefore not surprising that 28 submissions primarily focus on these aspects of safeguarding.

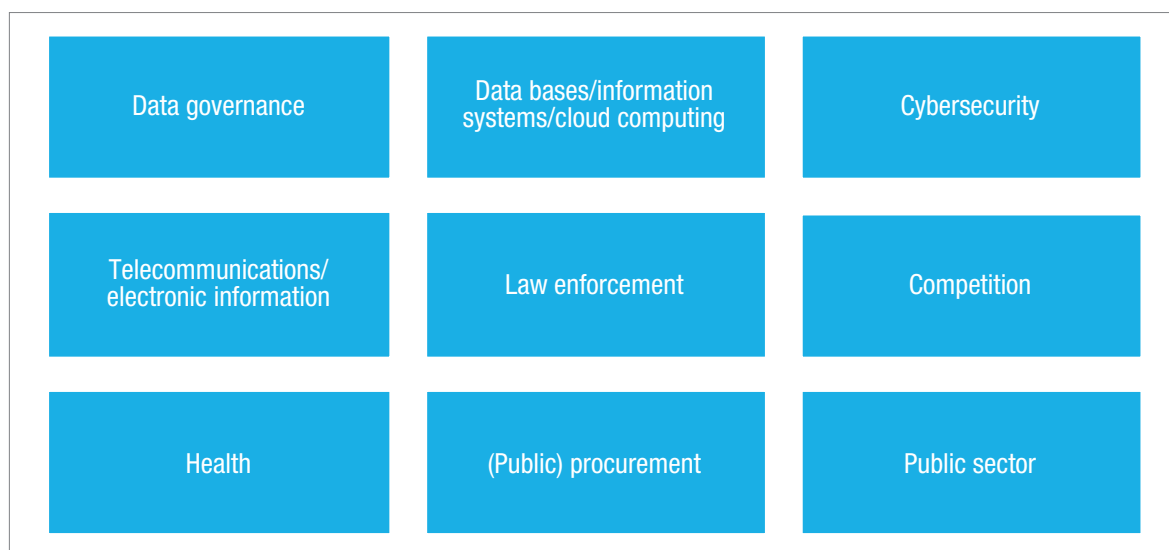
These are complemented by laws that are less broad and more specific to electronic communications, health, financial transactions and the public sector. One law specifically addresses children’s privacy protection online, an aspect of the digital economy that was included for the first time in the Declaration of G20 Digital Ministers in Trieste under the Italian Presidency and in the included G20 High Level Principles for Children Protection and Empowerment in the Digital Environment (G20, 2021).⁹

In the domain of submissions pertaining to non-personal data (see Annex table 3, column 2), submissions can be grouped into four categories: geospatial data (2 submissions), trade secrets and intellectual property (4), trade (1) and cybersecurity (1).

Laws and regulations touching on all types of data (see Annex table 3, column 3) are related to the categories shown in Figure 2.

9. <https://innovazione.gov.it/notizie/articoli/en/the-declaration-of-g20-digital-ministers/>

Figure 2: Categories of laws and regulations affecting “all data”



Source: UNCTAD, based on survey responses from G20 member States and invited guests.

These main themes are also mirrored in the list of sectors shown in Table 3, to which some of the laws and regulations are specific.

Table 3: Sector-specific legislation

Sector concerned	G20 Members with relevant laws
Banking, financial sector, capital markets	Saudi Arabia, Türkiye, United States
Defense and related private sector	United States
Geospatial	Indonesia, Republic of Korea
Health	Indonesia, United States
ICT and telecommunications	European Union, Indonesia, Saudi Arabia, Türkiye, United Kingdom, United States
Public sector	Brazil, Canada, Mexico, Republic of Korea, Saudi Arabia, United States
Trade	European Union, Indonesia, United States

Source: UNCTAD, based on survey responses from G20 member States and invited guests.

Data governance and the handling of data-related policy questions are not limited to one single ministry or agency. Instead, the multifaceted nature of data touches policymaking of many government institutions (see Figure 3). This suggests a growing need to ensure having relevant expertise in data-related aspects across all ministries involved in data governance.

Given the diversity of legal areas emerging from the submissions, it is clear that policies to enable data free flow with trust go well beyond the trade domain, which is

where most of the international discussions on cross-border data flows are currently happening as evidenced by international and regional agreements related to trade.¹⁰ Indeed, a lot of legislation is primarily concerned with personal data related aspects that may not be linked to trade, such as health or law enforcement. For example, the recent experience of COVID-19 and the international collaboration to fight the pandemic, brought the role of responsible scientific use of health and related data to the centre of attention.

Cross-border data flow provisions

Policy approaches to governing cross-border data flows can be divided into unilateral, bilateral and multilateral ones, as reflected in the survey submissions.

Unilateral approaches

First, most Members use [adequacy](#), [standard contractual clauses](#) or [binding corporate rules](#) to enable international data transfers. These provide an assessment of data protection (for personal data) before allowing data flows to take place.

Second, [data transfer plans requiring government approval](#) are another unilateral mechanism to facilitate data free flow with trust. These are employed by Indonesia with respect to geospatial data, health data and personal data protection. Similarly, Türkiye's banking law has provisions which allow the Board of the Banking Regulation and Supervision Agency to prohibit international data flows as does their regulation on private archival material.

Third, multiple submitted laws and regulations require [consent from the data subject](#) as a condition for international data flows. This is often used in the context of personal data.

Another approach relates to [data localization requirements](#). It is unilateral, but limits or conditions data to flow freely. *Personal data* generated in the Russian Federation and by its inhabitants must be stored locally first before it can be transferred abroad. In the context of *cloud computing*, Brazil requires a recent data backup to be maintained in its territory. Saudi Arabia requires data and data infrastructure for cloud and IoT systems to be maintained within the country.¹¹ The same holds for the Republic of Korea's cloud computing services for public procurement, for which data need to be stored in the country. Türkiye has a provision which requires data from the *financial sector and capital markets* to have their primary and secondary versions stored domestically, beyond this there are no explicit restrictions on data flows.

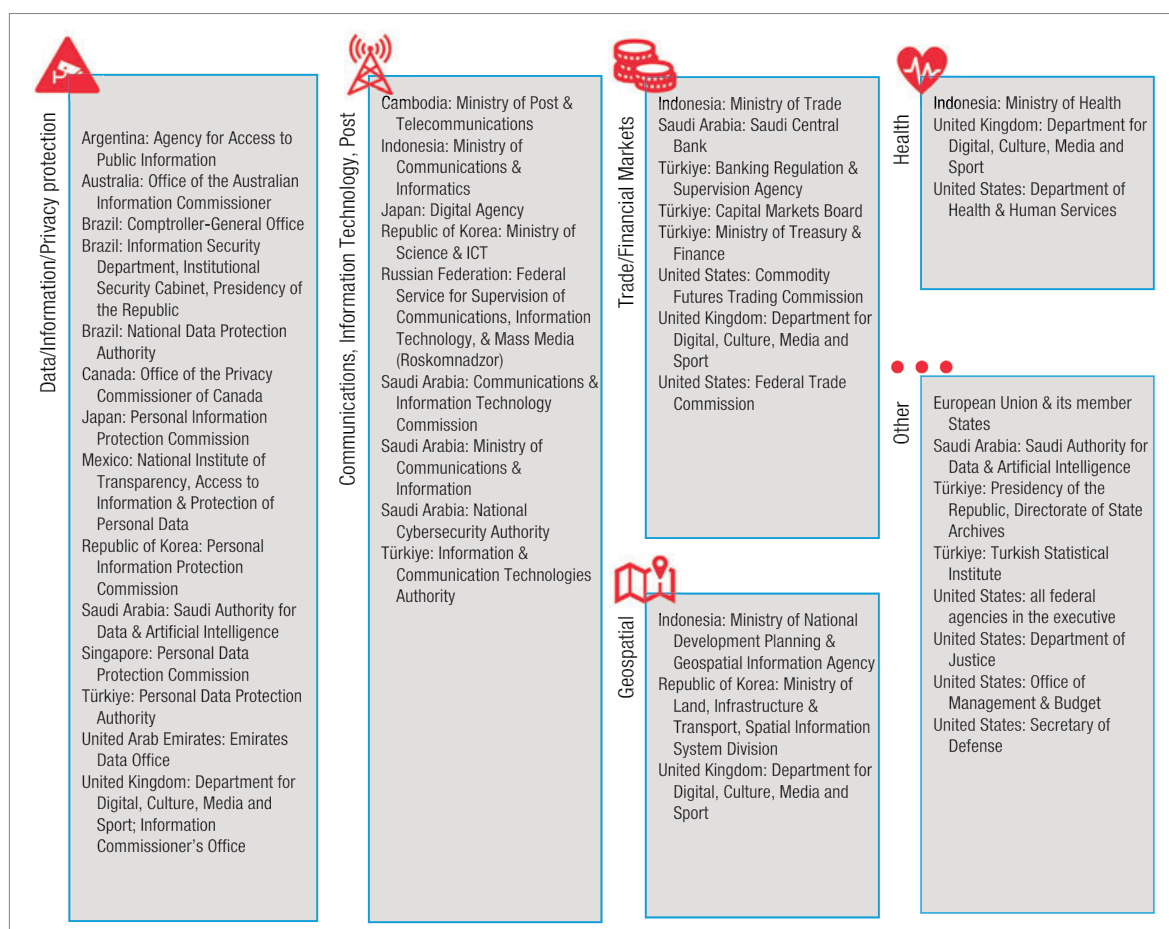
Indonesia and the Republic of Korea mandate that *geospatial data* are saved and processed domestically. Although, Indonesia's regulation on implementation of geospatial information includes an exception where, when trained labour or equipment is not available within the country, processing can take place abroad.

Finally, Indonesia requires the domestic storage of *health data*, although under specific circumstances processing can take place abroad.

¹⁰. For instance, discussions as part of the Joint Initiative Negotiations on E-commerce, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, the Regional Comprehensive Economic Partnership and the United States-Mexico-Canada Agreement.

¹¹. See the cloud computing regulatory framework, the IoT regulatory framework, and the essential cybersecurity controls.

Figure 3: Ministries and agencies responsible for different areas of data and data flows based on survey submissions



Source: UNCTAD, based on survey responses from G20 member States and invited guests.

Bilateral approaches

The submitted laws from Canada, Mexico, Singapore and the United States of America refer to [contracts](#) and [memoranda of understanding](#) for international parties to enable data flows, predominantly for personal data as well as data linked to commodities trading. Similarly, they put the responsibility on the local data controller to ensure that (foreign) data processors adhere to the relevant safeguards.

[Judicial cooperation](#) is an essential element of enabling cross-border data flows. Argentina, Canada, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland and the United States of America refer to bilateral judicial cooperation in this context.

[Regulatory cooperation](#) on data protection also plays an important role in creating a regulatory environment that enables, and builds trust in, data flows. Enhanced international regulatory cooperation can be secured through arrangements between regulators on issues such as enforcement, and through dialogues and agreements between Governments. Regulatory cooperation is also a key area mentioned in the 2021 G7 Roadmap for Cooperation on Data Free Flow with Trust.¹²

Multilateral approaches

Given the focus of the survey on domestic laws, references to multilateral approaches are limited in the submissions. However, one of Türkiye's laws approves the Multilateral Convention on Mutual Administrative Assistance in Tax Matters to improve exchanges between countries on data related to taxation. Furthermore, European Union directives and regulations on establishing a digital single market involve by nature of this political and economic union multiple countries, with an aim of fostering free flow of data *within* the European Union member States as much as possible – while using adequacy for transfers outside of the single market's borders. Singapore makes reference to using the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System in a multilateral arrangement for cross-border data flows.

Policy coordination and consultation

The multidimensional character of data that plays a role for the economy and society can be harnessed to generate much private and societal economic value. At the same time, many non-economic aspects, such as children's privacy, other human rights, and security, are also of concern to G20 member States. Given all these dimensions that cannot be disentangled for clear-cut policymaking, data have become a strategic resource for countries, firms and individuals. This suggests that to address existing and future opportunities and challenges related to data and data flows, it becomes increasingly important to develop holistic approaches to data governance (including management and implementation) in cross-border data protection to incorporate the cross-dimensional impact of various policy measures. A whole-of-government approach can be beneficial to determine broad

¹². <https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration>

guiding principles and to coordinate policymaking across ministries and agencies. Furthermore, various actors are differently impacted by data and their governance. Consequently, multistakeholder consultations, which can elicit the needs outside the public sector, can add value for countries' policy development.

Lead agencies and departments for data governance

Whole-of-government approaches which clearly identify one lead organization for the government's strategy on data governance may help coordinate requirements and demands from society and economy. Six out of 13 countries that answered this part of the survey questionnaire responded affirmatively to the question of whether they had a ministry or agency that has the primary responsibility for coordinating issues related to data governance. In the United Kingdom of Great Britain and Northern Ireland this responsibility is shared between two entities. The Department for Digital, Culture, Media & Sport leads on general data governance frameworks while the Central Digital and Data Office leads on government data. The responsible agencies and ministries are listed in Figure 4.

Figure 4: Lead agencies for data governance in selected countries

Argentina Agency for Access to Public Information	Cambodia Ministry of Post and Telecommunications of Cambodia	Mexico National Digital Strategy Coordination, direct report to the Office of the President
Saudi Arabia Saudi Data and AI Authority	United Arab Emirates Emirates Data Office	United Kingdom Department for Digital, Culture, Media and Sport & Cabinet Office, Central Digital and Data Office

Source: UNCTAD, based on survey responses from G20 member States and invited guests.

Mechanisms for multistakeholder dialogue on data governance

A growing number of countries have set up multistakeholder dialogues to secure inputs into the policymaking process. In the survey, ten out of 15 countries that responded to this part indicated that they have such a mechanism in place.

Canada introduced its Digital Charter following multistakeholder consultations. A Digital Charter Implementation Act is currently being discussed in parliament.

Mexico introduced the “Abramos México” initiative in February 2022. It aims to develop a National Open Data Policy in a public, open and collaborative way with multisectoral inputs. This endeavour is promoted by multiple agencies – including



the National Institute for Transparency, Access to Information and Protection of Personal Data, the National Transparency System, the regulatory body for statistical and geographical information – civil society and academia.

The Republic of Korea has set up an “Open Data Strategy Council” under the prime minister, with participation of other ministers, and co-chaired by the private sector. The council guides and coordinates the Government’s policies, plans on open government data, and monitors their implementation. It is led by the Ministry of Interior and Safety.

Saudi Arabia’s national regulatory committee provides a collaborative regulation mechanism through which various regulations linked to digital are harmonised and implemented.

The Data Protection Advisory Committee of Singapore, consisting of public and private sector as well as civil society representatives, advises the Personal Data Protection Commission with respect to reviewing and administering the personal data protection framework.

In the United Arab Emirates, federal government entities and the private sector engage in consultations for the co-drafting of policies.

The United Kingdom of Great Britain and Northern Ireland incorporates multistakeholder feedback through various mechanisms and fora, including the National Data Strategy Forum and the International Data Transfers Expert Council, expert and advisory groups and expert networks from academia and the private sector. Furthermore, the Government publishes public and stakeholder consultations for policy interventions linked to data.

Finally, three members regularly hold discussions with various stakeholders on data governance issues.

4. Conclusions

The responses to the questionnaire highlight the diversity of laws and regulations which are linked to cross-border data flows. Given the growing importance of data, this trend is likely to continue and ever more sectors may be affected by data and laws governing data flows.

Implications for international cooperation on data governance

The survey highlights that, for some aspects of data, national definitions do overlap a great deal, although there remain differences at a more granular level, for example with regard to the definition of personal data. While the bulk of the submissions is on governing personal data, the responses highlight that several countries also govern non-personal data. Building a deeper understanding of where commonalities and differences may exist is important to explore future opportunities for finding common ground.

The survey responses also illustrate that data flows are not equal to trade, nor are the laws and regulations confined to trade contexts.¹³ In none of the countries that responded to the data governance section of survey is the Ministry of Trade or Commerce the lead for issues related to data governance. Nevertheless, at the international level, cross-border data flows are currently discussed predominantly in the context of trade agreements. Furthermore, current international agreements, particularly trade agreements but also discussions within the OECD, the Council of Europe and regional initiatives, tend to be too limited geographically, especially low-income countries are often not parties to these agreements, and in scope, possibly failing to govern cross-border data flows in a way that allows for an equitable sharing of economic development gains while properly addressing possible risks.

The current situation may serve as a point of departure towards broadening the discussion on how data governance frameworks may be developed to support global development goals while allowing sufficient policy space for countries at varying levels of digital capabilities to secure national priorities and development objectives.

13. For a longer discussion on this aspect, please refer to UNCTAD's [Digital Economy Report 2021](#).

Areas for potential further discussion

Based on the results from this survey, the G20 may in the future wish to discuss possible ways forward to agreeing on common terminology of key concepts related to data governance. In view of the different approaches adopted by Members, further sharing of experiences may be useful with a view to identifying good practices that might be emulated by others. Discussions within the G20 would be part of a broader move towards reaching consensus on the global scale, with participation of all countries. At the same time, discussions on data governance frameworks that enable combining global development goals and countries' policy space may be helpful. This aspect may be taken up further by the coming Presidencies of India, Brazil and South Africa. Special attention may be warranted to approaches that may help to fully factor in the multi-dimensional character of data, and perspectives of multiple stakeholders, when designing and implementing different laws and regulations affecting data and data flows.



5. References

Casalini F, López González J and Nemoto T (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. OECD Trade Policy Paper, No. 248, OECD Publishing, Paris. Available at: <https://doi.org/10.1787/ca9f974e-en>.

G20 (2021). Declaration of G20 Digital Ministers: Leveraging Digitalisation for a Resilient, Strong, Sustainable and Inclusive Recovery.

OECD (2020). Mapping Approaches to Data and Data Flows. Report for the G20 Digital Economy Task Force, Saudi Arabia. OECD, Paris.

TeleGeography (2015). International Bandwidth Trends in Africa. What Has (and Hasn't) Changed in the Past Five Years, 27 August. Available at: http://isoc-ny.org/afpif2015/AfPIF2015_Teleography.pdf.

TeleGeography (2019). Back to the Future. Presentation by Alan Mauldin, TeleGeography Workshop at Pacific Telecommunications Council (PTC), 20 January. Available at: <https://www2.telegeography.com/hubfs/2019/Presentations/TeleGeo-PTC2019.pdf>.

TeleGeography (2021). Exploring the Cloud, Overland and Undersea. Trends in Cloud Infrastructure and Global Networks, 17 February. Available at: <https://www2.telegeography.com/hubfs/2021/Presentations/2021%20Cloud%20Trends.pdf>.

UNCTAD (2021). Digital Economy Report 2021 – Cross-border data flows and development: For whom the data flow. UNCTAD/DER/2021.

6. Annex

Annex table 1: Personal data definitions

Country	Definition
Argentina <i>Law n° 25.326 on Personal Data Protection (Art. 2)</i>	Personal data: Information of any kind referring to specific or identifiable natural or legal persons.
Australia <i>Privacy Act</i>	Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Brazil <i>General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, Art. 5 I)</i>	Personal data: information regarding an identified or identifiable natural person.
Canada <i>Personal Information Protection and Electronic Documents Act (Definitions)</i>	Personal information means information about an identifiable individual.
Canada <i>Privacy Act (Definitions)</i>	Personal information means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

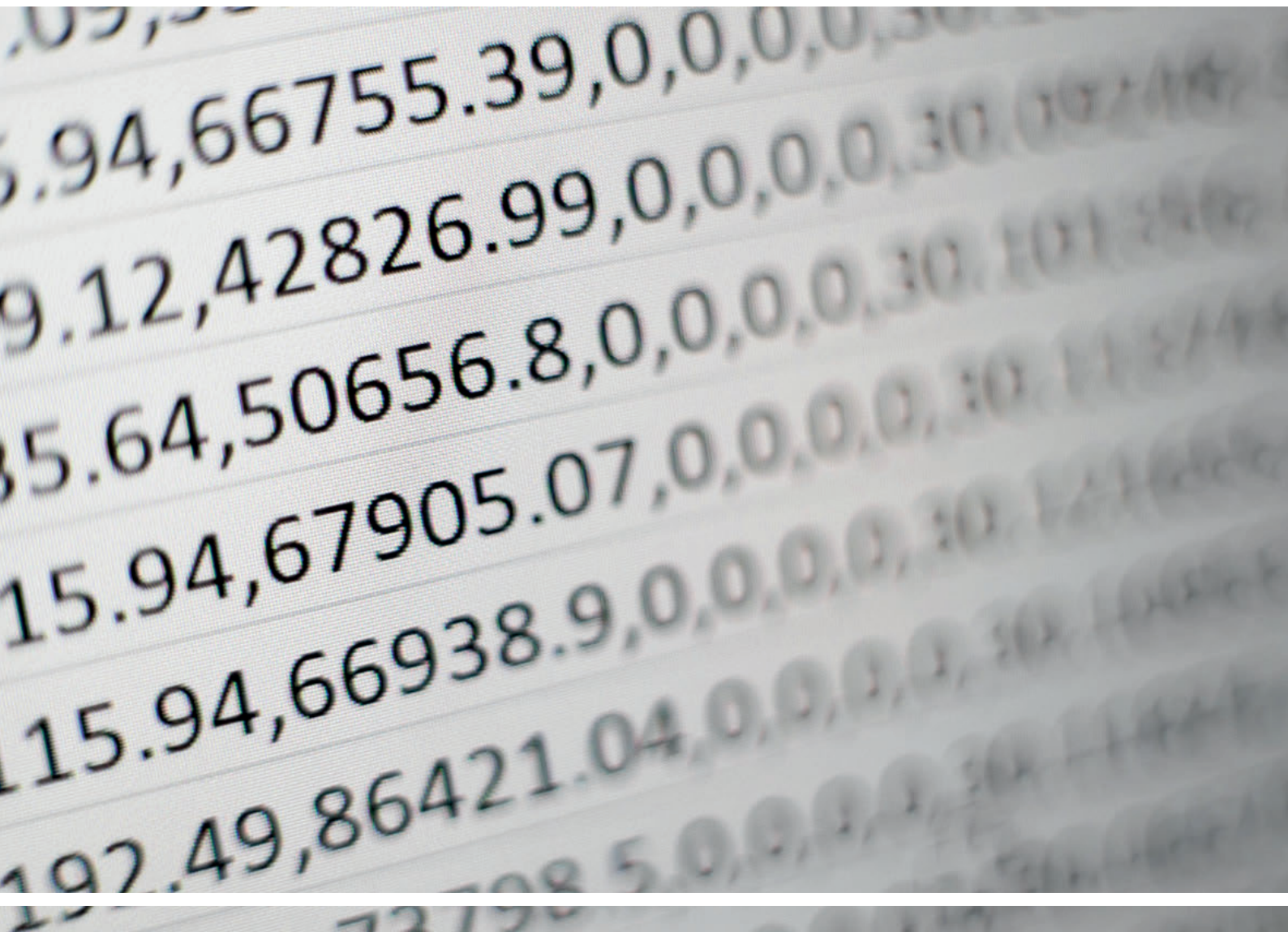
Country	Definition
China <i>Personal Information Protection Law of the People's Republic of China (Art. 4)</i>	'Personal information' refers to various information related to an identified or identifiable natural person recorded electronically or by other means, but does not include anonymized information.
Indonesia <i>Government Regulation No. 71 of 2019 Regarding Implementation of Electronic System and Transaction</i>	Personal data is any data about a person (where person is an individual, whether a citizen, foreign national, or an entity) either identified and/or can be identified separately or in combination with other information either directly or indirectly through electronic and/or non-electronic systems.
Indonesia <i>Minister of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in the Electronic System</i>	Personal data that may identify certain individual directly or indirectly that is stored, maintained which truthfulness and confidentiality thereof secured and protected.
Japan <i>Act on the Protection of Personal Information</i>	Information relating to a living individual which falls under any of the following items: (i) those containing a name, date of birth, or other descriptions, etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same applies in item (ii) of the following paragraph); the same applies hereinafter)) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual); (ii) those containing an individual identification code.
Mexico <i>Federal Law for the Protection of Personal Data in Possession of Individuals (Art.3 V)</i>	Any information concerning an identified or identifiable individual.
Mexico <i>General Law for the Protection of Personal Data in Possession of Obligated Entities (Art.3 XXI)</i>	Any information concerning an identified or identifiable natural person. An individual is deemed to be identifiable when his/her identity may be directly or indirectly determined from any information.
Russian Federation <i>Federal Law No. 152-FZ on Personal Data 2006 (Personal Data Protection Act, Art.3)</i>	Personal data is any information directly or indirectly related to an identified or identifiable individual (data subject).
Saudi Arabia <i>Personal Data Protection Law</i>	Any piece of data, whatever its source or format, that identifies, or makes it possible to identify, a natural person directly or indirectly, e.g. name, personal ID number, addresses, contact numbers, license numbers, records, personal property details, bank account numbers, credit cards, moving or still pictures images of an individual, and other information of a personal nature.

Country	Definition
Republic of Korea <i>Personal Information Protection Act (Art.2(1))</i>	<p>The term “personal information” means any of the following information relating to a living individual:</p> <p>(a) Information that identifies a particular individual by his or her full name, resident registration number, image, etc.;</p> <p>(b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured;</p> <p>(c) Information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (hereinafter referred to as “pseudonymized information”).</p>
Singapore <i>Personal Data Protection Act 2012 (Sec.2)</i>	<p>“Personal data” means data, whether true or not, about an individual who can be identified —</p> <p>(a) from that data; or</p> <p>(b) from that data and other information to which the organisation has or is likely to have access;</p>
Türkiye <i>Personal Data Protection Law</i>	<p>‘Personal data’ means any information relating to an identified or identifiable natural person.</p>
United Kingdom of Great Britain and Northern Ireland <i>GDPR and Data Protection Act 2018</i>	<p>‘Personal data’ means any information relating to an identified or identifiable living individual. “Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.</p>
United States of America <i>The Privacy Act of 1974, 5 United States Code § 552a</i>	<p>Records maintained on individuals.</p> <p>The term ‘record’ means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.</p>
United States of America <i>Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, Breach Notification, and Enforcement Rules (§ 160.103)</i>	<p>Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:</p> <p>(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and</p> <p>(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and</p> <p>(i) That identifies the individual; or</p> <p>(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.</p>
European Union <i>General Data Protection Regulation 2016/679 (Art 4 (1)) and other regulations/directives linked to personal data</i>	<p>‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>

Annex table 2: Sensitive data definitions

Country	Definition
Argentina <i>Law n° 25.326 on Personal Data Protection (Art. 2)</i>	Sensitive data: Personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral convictions, trade union membership and information concerning health or sex life.
Australia <i>Privacy Act</i>	Sensitive information means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
Brazil <i>General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, Art. 5 II)</i>	Sensitive personal data: personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political, organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person.
Mexico <i>Federal Law for the Protection of Personal Data in Possession of Individuals; General Law for the Protection of Personal Data in Possession of Obligated Entities</i>	Sensitive personal data: Those personal data that affect the most intimate sphere of their owner, or whose improper use may give rise to discrimination or entail a serious risk for the owner. In particular, sensitive data are considered to be those that may reveal aspects such as racial or ethnic origin, present and future state of health, genetic information, religious, philosophical and moral beliefs, trade union membership, political opinions, sexual preference.
Saudi Arabia <i>Personal Data protection law</i>	Personal data that reveals an individual's ethnic or tribal origin, political opinions, religious or philosophical beliefs, or trade union membership. Sensitive data also includes criminal and security data, biometric data for the purpose of uniquely identifying a natural person, genetic data, credit data, health data, location data, and data revealing that an individual is of unknown parent(s).
Republic of Korea <i>Personal Information Protection Act</i>	A personal information controller shall not process any information prescribed by Presidential Decree (hereinafter referred to as "sensitive information"), including ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject.
Türkiye <i>Personal Data Protection Law</i>	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data are deemed to be special categories of personal data.

Country	Definition
<p>United Kingdom of Great Britain and Northern Ireland</p> <p><i>GDPR and Data Protection Act 2018</i></p>	<p>In this section, “sensitive processing” means— (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; (c) the processing of data concerning health; (d) the processing of data concerning an individual’s sex life or sexual orientation. Criminal records are also included under this definition.</p>
<p>European Union</p> <p><i>European Union Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)</i></p>	<p>This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (‘sensitive data’)</p>



Annex table 3: Overview of submissions categorized by data type

Personal data

Personal data/information protection

- Argentina: Law n° 25.326 on Personal Data Protection
- Argentina: Provision n°60 / 2016 of the Agency for Access to Public Information
- Cambodia*: Draft data protection law
- Canada: Personal Information Protection and Electronic Documents Act
- China: Personal Information Protection Law of the People's Republic of China
- Indonesia: Minister of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in the Electronic System
- Japan: Act on the Protection of Personal Information
- Mexico: Federal Law for the Protection of Personal Data in Possession of Individuals + Regulation
- Mexico: General Guidelines on Personal Data Protection for the Public Sector
- Mexico: General Law for the Protection of Personal Data in Possession of Obligated Entities
- Republic of Korea: Personal Information Protection Act
- Russian Federation: Federal Law No. 152-FZ on Personal Data 2006 (Personal Data Protection Act)
- Saudi Arabia: Personal Data Protection Law
- Singapore: Personal Data Protection Act 2012
- Türkiye: Personal Data Protection Law
- United Arab Emirates: Federal Decree Law No. 45 Of 2021 On Personal Data Protection
- United Kingdom: Data Protection Act 2018
- United Kingdom: Privacy and Electronic Communications (European Commission Directive) Regulations 2003
- European Union: Directive (European Union) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
- European Union: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- European Union: Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data
- European Union: Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

General Data Protection Law/Regulation

- Brazil: General Data Protection Law (Lei Geral de Proteção de Dados Pessoais)
- of such data, and repealing Directive 95/46/EC
- United Kingdom: United Kingdom General Data Protection Regulation and Data Protection Act 2018
- European Union: Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement

Privacy Law/Act

- Australia: Privacy Act 1988
- Canada: Privacy Act
- United States: Privacy Act of 1974, 5 United States Code § 552a
- European Union: Directive 2002/58/EC on privacy and electronic communications

Electronic communications

- Türkiye: By-Law on the Processing of Personal Data and the Protection of Confidentiality in the Electronic Communications Sector
- Türkiye: Electronic Communications Law No. 5809

- United States: Stored Communications Act
- Canada: Personal Information Protection and Electronic Documents Act
- Indonesia: Regulation No. 20 of 2016 on Personal Data Protection in the Electronic System
- United Kingdom: Privacy and Electronic Communications Regulations 2003
- European Union: Directive 2002/58/EC on privacy and electronic communications

Financial transaction related

- Cambodia: Law on taxation
- Türkiye: Banking Law No. 5411
- Türkiye: Law on Approval of the Multilateral Convention on Mutual Administrative Assistance in Tax Matters (MAC) No. 7018
- Türkiye: Tax Procedure Law No. 213

Health

- Russian Federation: Federal Law No. 323 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation
- United States: Confidentiality of Substance Use Disorder Patient Records
- United States: Health Insurance Portability and Accountability Act of 1996 Privacy, Security, Breach Notification, and Enforcement Rules

Public sector

- Türkiye: Statistics law of Türkiye
- Mexico: General Law for the Protection of Personal Data in Possession of Obligated Entities
- Mexico: General Guidelines on Personal Data Protection for the Public Sector
- European Union: Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data

Other

- Cambodia: Law on consumer protection
- Russian Federation: Civil Aviation Code (Article 85.1)
- United States: Children's Online Privacy Protection Act

Non-personal data

Geospatial

- Indonesia: Government Regulation No. 45 of 2021 on Implementation of Geospatial Information
- Republic of Korea: Act on the Establishment and Management of Spatial Data

Trade secrets/Intellectual Property

- United States: Copyright Law
- United States: Economic Espionage Act
- European Union: Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
- European Union: Directive 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

Trade

- Indonesia: Government regulation No. 5 of 2020 on Trade Information System (derivative from Law No.7 of 2014 on Trade, amended by Law No. 11 of 2020 on Job Creation)

Cybersecurity

- European Union: ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Regulation 2019/881)

Other

- European Union: Framework for the free flow of non-personal data in the European Union (Regulation 2018/1807)

All data

Cybersecurity

- Cambodia*: Draft cybersecurity law
- China: Data Security Law
- Saudi Arabia: Critical systems cybersecurity controls
- Saudi Arabia: Essential cybersecurity controls
- United States: Federal Information Security Modernization Act

Databases/information systems/cloud computing

- Minimum information security requirements for cloud computing for public administration
 - » Brazil: Normative Instruction GSI/PR Nº 5 - Provides for the minimum information security requirements for the use of cloud computing solutions by bodies and entities of the federal public administration.
 - » Republic of Korea: Standards for Cloud Computing Service Information Protection
 - » European Union: Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
- Saudi Arabia: Cloud computing regulatory framework
- Saudi Arabia: Cloud first policy
- Saudi Arabia: IoT regulatory framework
- Türkiye: Communiqué on management of information systems
- European Union*: Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act)

Data governance

- Argentina: Provision nº60 / 2016 of the Agency for Access to Public Information
- Brazil: Open data policy
- Cambodia*: Draft data governance policy
- Japan: Basic Act on the Advancement of Public and Private Sector Data Utilization
- Saudi Arabia: Data Classification Policy
- United States: Open Government Data Act
- European Union*: Regulation on harmonised rules on fair access to and use of data (Data Act)
- European Union: Regulation (European Union) 2022/868 on European data governance and amending Regulation (European Union) 2018/1724 (Data Governance Act)
- European Union: A European strategy for data

Health

- Indonesia: Government Regulation No. 46 of 2014 on Health Information System
- European Union*: European Health Data Space

Security/Law Enforcement

- United States: Clarifying Lawful Overseas Use of Data (CLOUD) Act
- United States: Judicial Redress Act (link to criminal offenses)
- United States: The Wiretap Act

(Public) Procurement

- Cambodia: Law on public procurement
- United States: Procurement Law - 10 United States Code 3771, 130, 3013; related procurement regulations

Competition

- European Union*: Single Market For Digital Services
- European Union*: Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)
- European Union: Directive 2019/790 on copyright and related rights in the Digital Single Market

Telecommunications/Electronic Information

- Cambodia: Law on telecommunications
- Indonesia: Law No. 11 of 2008 on Electronic Information and Transaction as lastly amended by Law No. 19 of 2016 (Law 11/2008) + Regulation No. 71 of 2019
- Russian Federation: Federal Law No. 149-FZ on Information, Information Technologies and Data Protection 2006 (Data Protection Act)

- United States: The Stored Communications Act, 18 United States Code § 2701 et. seq.

Public sector

- Cambodia: Digital government policy
- Türkiye: Regulation on the Services of State archive

Other

- Cambodia: Digital Economy and society policy framework
- Cambodia: Draft digital development policy
- Cambodia: Law on e-commerce
- United States: Commodity Exchange Act

Note: The categorization in this table is predominantly descriptive to highlight clusters of topics addressed by the laws and regulations nor are the categories exclusive. Some laws and regulations are listed multiple times as they fall into several categories.

*indicate drafts and proposals.

Source: UNCTAD based on G20 member States and invited guests' submissions.



Recent UNCTAD publications on E-commerce and the Digital Economy

Digital Economy Report (formerly Information Economy Report)

Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow, UNCTAD/DER/2021, 2021.

Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries, UNCTAD/DER/2019, 2019.

Information Economy Report 2017: Digitalization, Trade and Development, UNCTAD/IER/2017, 2017.

Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries, UNCTAD/IER/2015, 2015.

Other Research Studies

Digital Economy Report Pacific Edition 2022: Towards value creation and inclusive-ness, UNCTAD/DTL/ECDE/2022/4, 2023.

E-commerce and the digital economy in LDCs: At breaking point in COVID-19 times, UNCTAD/DTL/STICT/2022/1, 2022.

COVID-19 and e-commerce: a global review, UNCTAD/DTL/STICT/2020/13, 2021.

What is at stake for developing countries in trade negotiations on e-commerce? The case of the joint statement initiative, UNCTAD/DITC/TNCD/2020/5, 2021.

UNGIS Dialogue on the Role of Digitalization in the Decade of Action: Accelerating the achievement of the SDGs through better collaboration in the UN System, UNCTAD/DTL/STICT/INF/2020/3, 2020.

COVID-19 and e-commerce: impact on businesses and policy responses, UNCTAD/DTL/STICT/2020/12, 2020.

eTrade Readiness Assessments

Fast-tracking implementation of eTrade Readiness Assessments – Second edition, UNCTAD/DTL/STICT/2022/5, 2022.

Tunisia: eTrade Readiness Assessment, UNCTAD/DTL/STICT/2022/3, 2022.

Côte d'Ivoire: eTrade Readiness Assessment, UNCTAD/DTL/STICT/2020/11, 2021.

Fast-tracking implementation of eTrade Readiness Assessments, UNCTAD/DTL/STICT/2020/9, 2020.

Member States of the West African Economic and Monetary Union eTrade Readiness Assessment, UNCTAD/DTL/STICT/2020/10, 2020.

United Republic of Tanzania: Rapid eTrade Readiness Assessment, UNCTAD/DTL/STICT/2020/2, 2020.

Kiribati: Rapid eTrade Readiness Assessment, UNCTAD/DTL/STICT/2019/15, 2019.

Afghanistan: Rapid eTrade Readiness Assessment, UNCTAD/DTL/STICT/2019/5, 2019.

Bangladesh: Rapid eTrade Readiness Assessment, UNCTAD/DTL/STICT/2019/6, 2019.

Zambia: Rapid eTrade Readiness Assessment, UNCTAD/DTL/STICT/2018/10, 2018.

Uganda: Rapid eTrade Readiness Assessment, UNCTAD/DTL/STICT/2018/9, 2018.

E-commerce and Law Reform

Data protection regulations and international data flows: Implications for trade and development, UNCTAD/DTL/STICT/2016/1, 2016.

Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations, UNCTAD/DTL/STICT/2013/1, 2013.

Measuring E-commerce and the Digital Economy

Impacts of the covid-19 pandemic on trade in the digital economy, UNCTAD Technical Notes on ICT for Development No. 19, TN/UNCTAD/ICT4D/19, 2021.

Manual for the Production of Statistics on the Digital Economy 2020, UNCTAD/DTL/STICT/2021/2, 2021.

