29 CREATING A LEVEL PLAYING FIELD FOR DATA PROTECTION

Michael Pisa, Center for Global Development
Ugonma Nwankwo, Center for Global Development
Pam Dixon, World Privacy Forum

ABSTRACT

To build trust in digital tools and systems – and the governments and companies which use them – data laws and regulations need to be well designed, tailored to local realities, and enforced effectively and consistently. Early evidence suggests that in many countries, the regulations and governance systems meant to protect against misuses of personal data fail to meet these standards, potentially undermining public confidence in the advantages of digital transformation. At the global level, low- and middle-income countries have largely been excluded from debates on data policies and have little leverage to influence how cross-border data flows are managed. Development actors should support efforts to strengthen implementation of existing data protection standards, and harmonise those standards while recognising developing countries' different needs and resources, and better measure the impact of data protection laws on economic and digital development.

Key messages

- Over the last decade, the adoption of data protection laws has accelerated dramatically in low- and middle-income countries and has been catalysed by growing concerns about data misuse.
- Despite these trends, questions remain about the impacts of weak implementation of data protection frameworks on economic, social and human rights outcomes.
- Development actors can support better data protection with initiatives to harmonise national data policies through inclusive global and regional processes and supporting low- and middle-income countries' efforts to build up regulatory and enforcement capacity.
- International actors should promote an approach to cross-border data flows that ensures data protection while allowing governments to design frameworks that meet their own needs, priorities and capacities.

As data and digital tools assume an ever-larger role in all aspects of daily life, it is increasingly important to have clear and effective rules that govern how different actors can use personal data throughout its life cycle and across different data ecosystems. A key challenge for governments is establishing rules that protect citizens from harm yet do not stifle useful innovation.

For many national governments, establishing a data protection regime is a foundational step in developing a broader approach to modern digital governance. The choices that policy makers make when creating and implementing data protection laws set a trajectory for how a government and its citizens will engage with digital ecosystems and data. These choices, therefore, have direct consequences for economic development.

Data protection laws and regulations can help build trust in digital tools and systems that promise greater efficiency and value by establishing rights that protect citizens against the misuse of their personal data and obligations that require organisations to use data in a fair, transparent and accountable manner. In theory, this greater trust should translate into greater acceptance of services that rely on data sharing and data use, leading to more investment in the resources and expertise needed to fuel a country's digital transformation (World Bank, 2021[1]; World Economic Forum, 2019[2]; Chakravorti and Chaturvedi, 2017[3]). However, early evidence suggests that in many countries that have enacted data protection laws, enforcement is weak, regulatory authorities lack independence and policies are poorly designed. The absence of harmonised and inclusive global data protection standards exacerbates the challenges, especially for low- and middle-income countries that have had little input into data policy debates. This includes discussions on designing legal frameworks for cross-border data sharing, which, at the global level, have largely been limited to G20 countries.

Over the last two years, a series of roundtables and interviews with experts working at the intersection of data policy and development were held, to better understand the relationship between data protection frameworks and economic outcomes, particularly in low- and middle-income countries. These experts welcomed the growing number of countries that have enacted data protection regimes in recent years, but also raised concerns about the effectiveness of these regimes in practice, the challenges resource-constrained governments face in implementing them and the potential negative consequences of poor implementation.

Too much, too little or poorly focused data regulation may hamper development

Data protection rules that are poorly designed or inadequately enforced can hinder

economic development through different channels that can be roughly categorised as under-regulation, over-regulation and regulating the wrong things in the wrong way.

- **Under-regulation:** Even when data protection laws exist "on the books", they often fail to translate into "law on the ground" (Pisa et al., 2020[4]). This weakens the level of protection provided and undermines trust in data use and sharing that data protection laws are meant to instil. It also contributes to regulatory uncertainty, which can hinder useful data innovation by both the public and private sectors (Mungan, 2019[5]) and the economic growth that could result.
- **Over-regulation:** As is the case in other sectors, over-regulation – in the form of high compliance costs that bear little relation to improvements in desired policy outcomes – has the potential to slow innovation by creating an unnecessary disincentive to investment. These costs are especially damaging to small- and medium-sized enterprises, which typically lack the well-resourced legal teams needed to navigate complex compliance requirements (Digital Competition Expert Panel, 2019[6]; Voss, 2021[7]).
- **Regulating the wrong things in the wrong way:** Several theorists have argued that current approaches to data protection place too much emphasis on protecting against individual harms and not enough on collective harms, putting data protection at odds with the growing reliance on machine learning algorithms that extract insights from collective data (Tisné, 2020[8]; Moerel and Prins, 2016[9]). Overemphasis on protecting against individual harms is mirrored by overreliance on informed consent as the primary basis for data processing, which often places an unreasonable burden on individuals and is meaningless in situations where they lack a basic understanding of how their data will be used (Medine and Murthy, 2020[10]; Selinger and Hartzog, 2020[11]).

Early evidence suggests that in many countries that have enacted data protection laws, enforcement is weak, regulatory authorities lack independence and policies are poorly designed

By undermining people's trust in how their data are used and raising hurdles to responsible innovation, each of these regulatory channels seem likely to lead to less investment in digital tools and data-driven services. But empirical evidence is lacking. Developing a better understanding of the causal pathways through which data regulations can affect a country's digital and economic development is crucial to designing effective policies. For example, firm-level surveys could help identify the degree to which high compliance costs or regulatory uncertainty may curtail investment.

Resources to enforce increasingly complex data protection laws vary widely

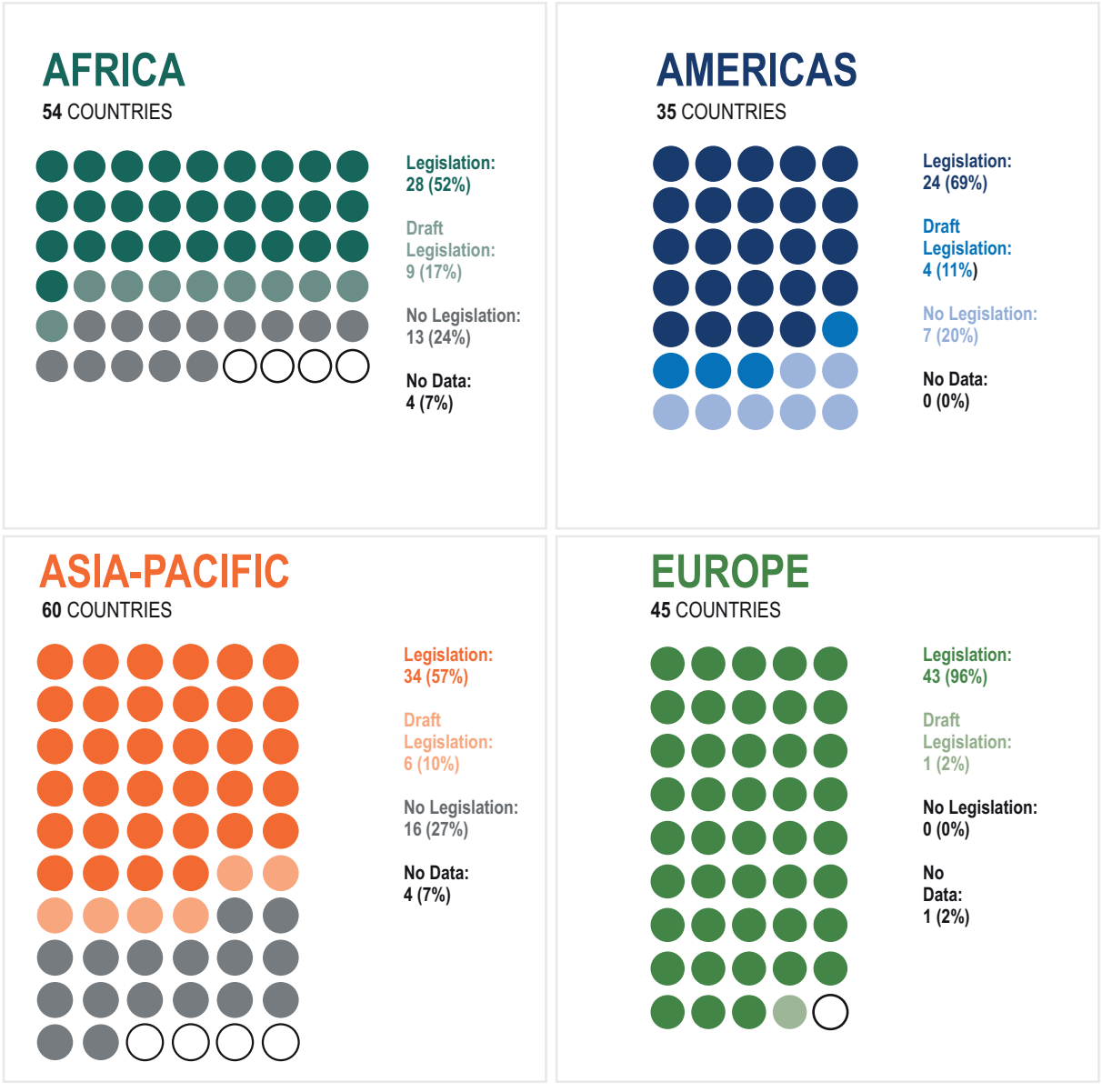
Modern approaches to data protection can be traced back to the establishment of the Fair Information Practices in the United States in the 1970s and the OECD's codification of and expansion on those principles in its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, published in 1980. The following years brought a slow and steady diffusion of national data protection frameworks, mostly in wealthier countries, based and building on these principles (Gellman, 2014[12]).

Over the last two decades, however, the number of countries that adopted data protection legislation has significantly

increased. Since 2010, 64 countries – most of which are in Africa, Asia and Latin America and over 70% of which are categorised as lower middle-income countries – have enacted new data protection laws, bringing the total with such laws in place up to 146 (Figure 29.1).

Several factors are driving the recent rapid spread of national data protection frameworks, among them growing awareness of the risks of data misuse; the desire to create an enabling framework for responsible data use and sharing; the need to meet requirements of international development partners; and, perhaps most importantly, the catalytic effect of the European Union (EU) General Data Protection Regulation (GDPR), which was enacted in 2016 and came into effect in 2018. Of the more than 60 countries that have enacted new data protections laws over the last decade, almost all modelled their approach in full or in part on the GDPR and

Figure 29.1. Country data protection laws by region



Source: UNCTAD (n.d.[13]), Data protection and privacy legislation worldwide website, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

its predecessor, the 1995 EU Data Protection Directive (DPD).

The GDPR sets out a more rigorous model for protecting the privacy of individual data than had previously existed, altering the global data protection landscape and establishing the EU as the global leader in the field. The regulation provides mechanisms that strengthen individual control over how data are used, increased the accountability of data controllers, and raised the stakes of non-compliance through greater fines and penalties. In contrast, the United States, home to the world's largest tech firms, has taken a sectoral and relatively hands-off approach to regulating the use of personal data.

The influence of the GDPR and the DPD also reflects the extraterritorial scope of the EU's adequacy framework,[1] which calls on the European Commission to determine whether non-EU countries "offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union (European Parliament, 2016[14]), in particular where personal data are processed in one or several specific sectors" as a basis for transferring data. Because companies based in countries that receive a favourable adequacy determination face lower barriers to doing business with EU citizens, achieving adequacy confers a significant competitive advantage in the global digital economy. A study published before the United Kingdom achieved GDPR adequacy, for instance, estimated that not receiving it would cost UK firms between GBP 1 billion and GBP 1.6 billion due to the additional compliance obligations (McCann, Patel and Ruiz, 2020[15]).

Although a growing number of countries have incorporated elements of the GDPR into law, early and anecdotal evidence suggests that most of them struggle to implement it effectively due to its breadth and complexity (Voss, 2021[7]). Even EU member states, which had roughly 25 years of practice implementing a similar framework under the DPD, have struggled to implement the updated law (European Commission, 2020[16]). The challenge is much greater for countries that face severe resource constraints, have a smaller pool of experts to draw from and have less experience implementing a comprehensive data protection framework.

Data protection authorities, the institutions responsible for interpreting and enforcing data protection laws in most countries that have comprehensive data protection frameworks, often lack functional independence from the executive branch or other ministries, particularly in lower income countries, which makes it difficult for them to resist political influence or to hold other government actors accountable (Davis, 2021[17]). There also are wide disparities in the level of human and financial resources available to data protection authorities across regions and economic classifications (Figure 29.2) (Fazlioglu, 2018[18]).

Acknowledging the difficulties of implementing the GDPR framework is not an endorsement of either watering down existing rules or taking an entirely different approach. In fact, the experts who participated in the roundtables were nearly unanimous in their support of the principles that underlie the GDPR and in their belief that countries should take a comprehensive and rights-based approach to personal data protection (as opposed to a sectoral approach or one that seeks to achieve an economic balance of interests) (Pisa and Nwankwo, 2021[19]).

Several experts did, however, express frustration with how current arrangements for governing cross-border data flows have, in their view, unduly restricted domestic policy choices. This includes the GDPR adequacy process, which they regarded as excessively opaque and driven by political and economic considerations rather than the fitness of a country's data protection regime that leave countries with smaller markets less likely to receive an adequacy determination (Pisa and Nwankwo, 2021[19]).

Lack of co-ordination on data regulations at the global and regional levels further

Figure 29.2. Regional disparities in staffing and budget for data protection regulation

REGION	MEDIAN PER-COUNTRY DPA BUDGET	MEDIAN PER-COUNTRY DPA STAFF
North America	USD 58 million	647
Asia/Oceania	USD 6.9 million	77
Europe	USD 2.2 million	34
Africa/Middle East	USD 500 000	14
Central and South America	USD 400 000	13
OECD		
Member	USD 6 million	50
Non-member	USD 500 000	17

Note: DPA: data protection authority.
Source: Fazlioglu (2018[18]), *How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population*, https://iapp.org/media/pdf/resource_center/DPA-Budget-Staffing-Whitepaper-FINAL.pdf.

disadvantages low- and middle-income countries which, on their own, lack the economic leverage needed to influence both the practices of big tech companies that dominate global data flows and the terms on which cross-border data flows are governed in bilateral agreements with wealthier countries.

What the international community can do to strengthen data policies

The international development community and high-income countries can promote a more level playing field for data protection policies and help low- and middle-income countries advance on their path of digital transformation in five main ways:

1. **Devote more resources to strengthening domestic data governance and protection regimes in line with countries' needs and capacities.** Development organisations should work with partner countries to make sure their data governance and protection frameworks can support digital transformation. Improving how these frameworks are implemented and enforced should be a key focus of funding vehicles to support more and better data use, such as the World Bank's recently announced Global Data Facility (Hammer et al., 2021[20]).
2. **Promote a common, transparent, and flexible approach to establishing the legality of cross-border data flows.** As more countries establish their own mechanisms for determining the legality of cross-border data flows, there is a danger that a proliferation of national data protection adequacy regimes could further fragment the global digital economy. As a first step, jurisdictions should be transparent about how they reach adequacy decisions. Beyond this, countries should agree to a set of standards to govern cross-border data flows that are strong enough to ensure high-quality data protection but flexible enough to allow governments to design frameworks that meet their own needs, priorities and capacities. The Council of Europe's Convention 108+ (Council of Europe, 2018[21]), which is the only legally binding multilateral instrument on the protection

of privacy and personal data, provides a model of such an outcomes-based yet flexible arrangement, but governments are more likely to ratify a framework whose design they have provided input to.

3. **Foster global and regional initiatives to harmonise national data policies with genuine input from low- and middle-income countries.** If developing countries have a voice in shaping the data policy standards they are expected to meet, they are more likely to implement them. New institutions may be required to ensure standard-setting processes are inclusive as "existing institutional frameworks at the international level are not fit for purpose to address the specific characteristics and needs of global data governance" (UNCTAD, 2021[22]).
4. **Identify and develop better data policy metrics.** Currently, most cross-country measures about data protection policy focus solely on legislation (Greenleaf, 2019[23]; Chen, 2020[24]; UNCTAD, n.d.[13]). New metrics are needed to better understand the relationship between data protection policies and economic outcomes, including on how well or poorly data protection measures are implemented, the effect of these measures on data protection, investment outcomes, and the value created by key data ecosystems, cross-border data flows and data-driven innovation more broadly.
5. **Encourage the development of approaches that move beyond consent as the primary basis for protecting personal data.** Relying on individual consent places an unreasonable and unworkable burden on individuals. Additionally, in complex data ecosystems, obtaining consent is not always possible. Policy makers should therefore consider ways to support testing and measuring the effectiveness of different models of personal data protection and enforcement, including, for example, legitimate purposes tests, data fiduciaries and trusts, and participatory data stewardship (Medine and Murthy, 2020[10]; Ada Lovelace Institute, 2021[25]; Hardinges et al., 2019[26]; Wylie and McDonald, 2018[27]; Moerel and Prins, 2016[9]).

REFERENCES

Ada Lovelace Institute (2021), *Participatory Data Stewardship: A Framework for Involving People in the Use of Data*, Ada Lovelace Institute, London, https://www.adalovelaceinstitute.org/report/participatory-data-stewardship (accessed on 3 November 2021). [25]

Chakravorti, B. and R. Chaturvedi (2017), *Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World*, The Fletcher School, Tufts University, Medford, MA, https://sites.tufts.edu/digitalplanet/files/2020/03/Digital_Planet_2017_FINAL.pdf. [3]

Chen, R. (2020), "Mapping data governance legal frameworks around the world: Findings from the Global Data Regulation Diagnostic", *Policy Research Working Paper*, No. 9615, World Bank, Washington, DC, https://openknowledge.worldbank.org/handle/10986/35410 (accessed on 13 September 2021). [24]

Council of Europe (2018), *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, Council of Europe, Strasbourg, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf. [21]

Davis, T. (2021), *Data Protection in Africa: A Look at OGP Member Progress*, Open Government Partnership, Washington, DC, https://www.opengovpartnership.org/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf. [17]

Digital Competition Expert Panel (2019), *Unlocking Digital Competition*, Digital Competition Expert Panel, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [6]

European Commission (2020), *Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation*, COM/2020/264 final, European Commission, Brussels, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264 (accessed on 3 November 2021). [16]

European Parliament (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, Official Journal of the European Union, L 119, 4.5.2016, pp. 1-88, https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 17 November 2021). [14]

Fazlioglu, M. (2018), *How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population*, International Association of Privacy Professionals, Portsmouth, NH, https://iapp.org/media/pdf/resource_center/DPA-Budget-Staffing-Whitepaper-FINAL.pdf. [18]

Gellman, R. (2014), "Willis Ware's lasting contribution to privacy: Fair information practices", *IEEE Security & Privacy*, Vol. 12/4, pp. 51-54, http://dx.doi.org/10.1109/msp.2014.82. [12]

Greenleaf, G. (2019), "Global tables of data privacy laws and bills (6th Ed January 2019)", *Privacy Laws & Business International Report*, Supplement to No. 157, https://ssrn.com/abstract=3380794 (accessed on 3 November 2021). [23]

Hammer, C. et al. (2021), "Putting data and innovation to work for the SDGs: The Data Innovation Fund", *World Bank Data Blog*, https://blogs.worldbank.org/opendata/putting-data-and-innovation-work-sdgs-data-innovation-fund (accessed on 3 November 2021). [20]

Hardinges, J. et al. (2019), *Data Trusts: Lessons from Three Pilots*, Open Data Institute, London, https://theodi.org/article/odi-data-trusts-report (accessed on 3 November 2021). [26]

McCann, D., O. Patel and J. Ruiz (2020), *The Cost of Data Inadequacy*, New Economics Foundation/UCL Europe Institute, London, https://neweconomics.org/2020/11/the-cost-of-data-inadequacy (accessed on 3 November 2021). [15]

Medine, D. and G. Murthy (2020), *Making Data Work for the Poor: New Approaches to Data Protection and Privacy*, Consultative Group to Assist the Poor, Washington, DC, https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf. [10]

Moerel, L. and C. Prins (2016), "Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of big data and the Internet of Things", *Cybersecurity*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 (accessed on 3 November 2021). [9]

Mungan, M. (2019), *Seven Costs of Data Regulation Uncertainty*, Data Catalyst, Washington, DC, https://datacatalyst.org/reports/seven-costs-of-data-regulation-uncertainty (accessed on 3 November 2021). [5]

Pisa, M. et al. (2020), "Governing data for development: Trends, challenges, and opportunities", *CDG Policy Paper*, No. 190, Center for Global Development, Washington, DC, https://www.cgdev.org/sites/default/files/governing-data-development-trends-challenges-and-opportunities.pdf. [4]

Pisa, M. and U. Nwankwo (2021), *Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development*, Center for Global Development, Washington, DC, https://www.cgdev.org/publication/are-current-models-data-protection-fit-purpose-understanding-consequences-economic (accessed on 3 November 2021). [19]

Selinger, E. and W. Hartzog (2020), "The inconsentability of facial surveillance", *Loyola Law Review*, Vol. 66/101, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557508 (accessed on 3 November 2021). [11]

Tisné, M. (2020), *The Data Delusion: Protecting Individual Data is Not Enough When the Harm is Collective*, edited by Marietje Schaake, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf. [8]

UNCTAD (2021), *Digital Economy Report 2021 – Cross-border Data Flows and Development: For Whom the Data Flow*, United Nations Conference on Trade and Development, Geneva, https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf. [22]

UNCTAD (n.d.), "Data protection and privacy legislation worldwide", web page, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed on 17 November 2021). [13]

Voss, A. (2021), *Fixing the GDPR: Towards Version 2.0*, epp group in the European Parliament, https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf. [7]

World Bank (2021), *World Development Report 2021: Data for Better Lives*, World Bank, Washington, DC, https://doi.org/10.1596/978-1-4648-1600-0 (accessed on 3 November 2021). [1]

World Economic Forum (2019), *Data Collaboration for the Common Good: Enabling Trust and Innovation Through Public-Private Partnerships*, World Economic Forum, Geneva, https://www3.weforum.org/docs/WEF_Data_Collaboration_for_the_Common_Good.pdf. [2]

Wylie, B. and S. McDonald (2018), "What Is a data trust?", Centre for International Governance, Waterloo, Ontario, https://www.cigionline.org/articles/what-data-trust (accessed on 3 November 2021). [27]

NOTE

1. The EU adequacy process, which is detailed in Article 44 of the GDPR, grants the European Commission the power to determine whether a non-EU country offers levels of data protection that are "essentially equivalent" to that within the EU. If a third country is deemed adequate, personal data can flow from the EU to the third country without the need for additional safeguards. When assessing for adequacy in a third country, the Commission considers several factors, including: the rule of law; respect for human rights and fundamental freedoms; the effective functioning of one or more independent supervisory authorities; and international commitments the third country has entered into. In the absence of an adequacy decision, the data controller or processor should take measures to compensate for the lack of data protection in the third country through binding corporate rules or standard contractual clauses.

From:

Development Co-operation Report 2021

Shaping a Just Digital Transformation

Access the complete publication at:
https://doi.org/10.1787/ce08832f-en

Please cite this chapter as:

Pisa, Michael, Ugonma Nwankwo and Pam Dixon (2021), "Creating a level playing field for data protection", in OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/63ebb18e-en