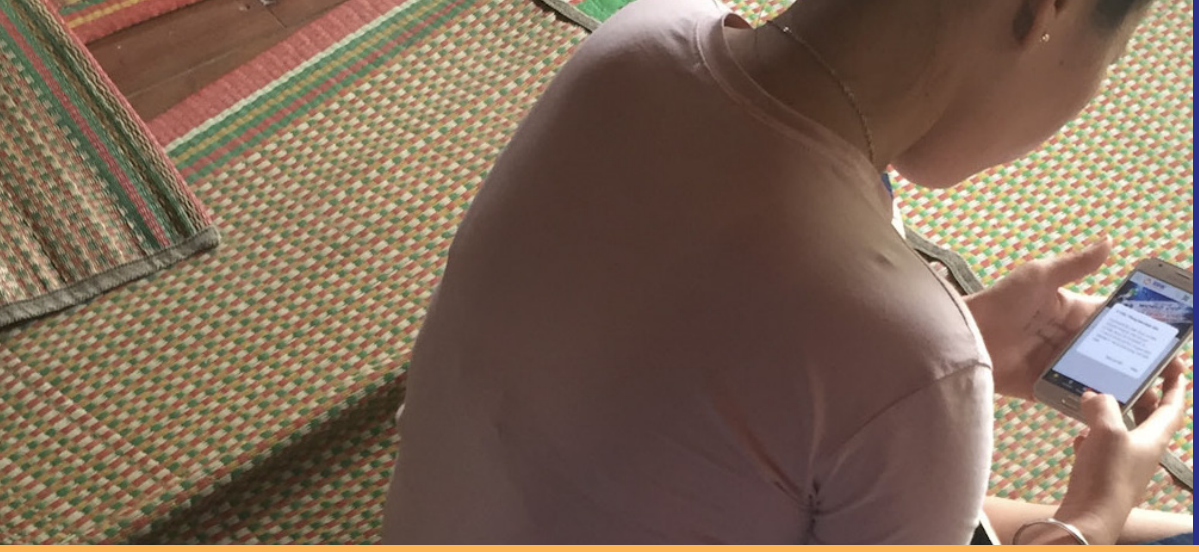

# The role of data protection in the digital economy

Governments, organizations and individuals increasingly generate, collect and process personal data. A strong data protection framework helps foster consumer trust and increased use of digital tools, which in turn can incentivize investment, competition and innovation in the digital economy.

The brief, written in close collaboration with Macmillan Keck, seeks to identify specific attributes of a data protection framework that can help policymakers and regulators build a digital economy that includes — and serves — everyone.

BRIEF

November 2021

Macmillan Keck

Seharish Gillani,
Ahmed Dermish, and
Jeremiah Grossman
of the UNCDF
Policy Accelerator

## Summary

Governments, organizations and individuals increasingly generate, collect and process personal data.

Data protection seeks to balance the benefits and the risks of personal data processing[1] so that individuals have confidence that their data is collected and stored safely and used solely for legitimate purposes.

Data protection laws typically require personal data processing to be lawful, limited, transparent, accurate and secure. They often seek to protect individuals' privacy[2] and grant some control over how personal data about them is processed. They also typically establish institutions with powers to conduct investigations and enforce obligations.

A strong data protection framework provides certainty which may encourage investment, competition and innovation in the digital economy and uptake of digital government and private sector services.

## Considerations while reading this brief

1. Which challenges related to data protection and the digital economy are most prominent in your market, both 1) in general and 2) for underserved groups such as women and low-income people?

2. Do data protection regulations in your country address:
   - **Digitization:** The application of data protection regulation to the digital economy?
   - **Inclusivity:** The specific data protection challenges faced by women, low-income people, and/or other marginalized groups?

3. Which entities are responsible for regulation of data protection? Are responsibilities clear, and are mechanisms in place to avoid regulatory arbitrage? If not, how could this be improved?

## Why we need data protection

### *Data for development*

Digital technologies and data are potential enablers of development in health, education, agriculture, food security, financial services, manufacturing, trade and infrastructure, and the digital economy itself. They can transform public and private services, inform policy decisions, and improve the monitoring of progress and impact. For example:

- An online e-participation platform in Morocco allows citizens to submit and vote on ideas and provide feedback on proposed legislation to improve public services;[3]
- Digital financial service providers analyze data about potential customers to market digital payment services to them, profile their risk levels for credit, manage identity and detect suspicious transactions;
- Digital identification systems collect and exchange personal data to authenticate people, reducing fraud and barriers to accessing services;
- Data about individuals' use of financial services worldwide is distilled to produce the Global Findex, which enables countries and other stakeholders such as[4,5] to track progress and develop policy towards;[6] and
- Gender-disaggregated data is an essential component to bridging the financial inclusion gender gap.

While more effective collection, organization, analysis, storage, and transfer of data (the lifecycle that comprises data ***processing***) may improve its productive use, measures should be taken to ensure consumer data protection and privacy. Governments, organizations, and individuals increasingly generate, collect, and depend on data about people. 64.2 zettabytes (or 64.2 trillion gigabytes) of data were created or replicated globally in 2020 alone, and it is estimated that this amount will grow at a compound annual growth rate of 23 percent through.[7] Much of this data is[8] to be ***personal data***, meaning it relates to or can be used to identify individual persons, referred to as ***data subjects.***

### *Risk and trust*

The generation and processing of vast amounts of personal data involves risks. Personal data can be lost, stolen, disclosed without consent, or misused. This can result in identity theft,[9] unwanted or embarrassing disclosures,[10] loss of important information,[11] or unwelcome marketing or solicitation.[12] Personal data can also be used for government[13] or corporate surveillance,[14] as well as discriminatory treatment of vulnerable individuals and communities.[15]

Individuals may be unaware of how data about them may be used or to which entities such data may be transferred, and their trust should not be taken for granted. As individuals become more aware of risks relating to their personal data, they may avoid or limit using digital services, potentially impeding efforts for economic development and inclusion.

Recent studies show that in in both higher- and lower-income countries consumers value protection of their personal data. A majority of low-income customers in Kenya were willing to pay a premium for greater protection of their personal data in digital loan services, and customers in India were likely.[16] Similarly,[17] women can have different data privacy concerns and be more privacy conscious as a result of their vulnerability to reputational harm.

Recent research suggest women's concern parallel the challenges and threats they encounter in their physical lives, such as location tracking and sexual harassment.[18] Relatedly, an important deterrent for women from using DFS is the fact that they have to share personal information, such as mobile numbers with agents who might misuse it.[19] Concerns about their data and security can lead women to curtail their use of different services and self-censored their behavior. Women might also lack knowledge of how to safeguard their personal data and rely on male family members and more educated people for advice on how to protect their photos, social media messages, etc.[20] Policymakers must take into account these concerns unique to women when drafting a data protection and privacy framework.

### *International trends*

Data protection is increasingly mandated in national laws and regional laws and agreements across higher and lower income countries. As of April 2020, 66 percent of countries had adopted data protection and privacy legislation.[21] A widely cited example is Europe's General Data Protection Regulation 2016 (GDPR). Such laws typically seek to balance the benefits and the risks of personal data processing so that individuals have confidence that personal data relating to them are collected and stored safely and used solely for legitimate purposes.

## Who must comply with data protection

Data protection frameworks designed in the GDPR tradition impose obligations on two principal actors:

- *Controllers* are those persons or entities that determine the purpose of and means for processing personal information. For example, a bank collecting personal information about account holders would be a controller.
- *Processors* are those persons or entities that carry out processing of personal data at the direction of or on behalf of a controller. For example, the entity that operates the software that the bank uses to access and store its records would be the processor.

The European Commission's examples of controllers and processors provide some further context for this distinction. It is worth noting that controllers may process their own data, but processors are always acting on behalf of a controller.

## The key elements of data protection

### *Lawfulness of processing*

Data protection frameworks typically require that processing of personal data be carried out ***lawfully***, meaning that the basis for processing is expressly authorized by law.

The ***consent*** of the data subject is frequently relied upon as a lawful basis. Consent should be voluntary, freely given, and evidenced by an affirmative action of the data subject, so it should not be enough to give the data subject pre-checked boxes or default settings. Consent is also typically considered narrowly. For example, consent given for collection and storage of personal medical records cannot be viewed as consent to generation and receipt of unrelated marketing emails.

Consent has some weaknesses as a means of legitimizing data processing. Individuals cannot realistically read all of the disclosures made by controllers, and they may not understand the implications

of consenting to personal data processing. People may also give consent because the only alternative is to forego the service, meaning they may not have any real choice. Nevertheless, consent remains the only basis for processing in which the data subject has some control over processing of his or her personal data, and efforts are being made to enable consent to be more meaningful, so it remains an important feature of a data protection framework.

Another commonly used lawful basis for processing personal data is the ***legitimate interests*** of the controller or third party. This is the most flexible of the lawful bases and can apply to virtually any type of processing for any reasonable purpose. However, it requires the controller to weigh these interests against the interests and fundamental rights and freedoms of the data subject using a three-part test:[22]

1. **Purpose:** Is there a legitimate interest behind the processing?
2. **Necessity:** If so, is the proposed processing necessary for that purpose?
3. **Balancing:** Is this legitimate interest overridden by the data subject's interests or fundamental rights and freedoms?

Other lawful bases for processing on which controllers rely include (among others) when processing is:

- Necessary to perform a contract with the data subject (for example, to provide a product suited to his or her needs);
- Necessary to satisfy a legal obligation of the controller (for example, if a telecommunications company is required to keep records of customers' services for billing purposes);
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (for example, the administration of justice); or
- Essential to the life of the data subject or a third party (for example, to inform the doctor of a medical condition in an emergency).

Often processing is lawful because it is expressly authorized in a particular law separate from the data protection framework, such as the collection of personal data by a national ID system under a national ID law.

### *Data minimization*

The theme of ***data minimization*** runs through many elements of data protection. It involves minimizing the processing of personal data to only that which is necessary in relation to the purposes for which they are processed.[23]

A data protection framework will typically require that any collection of personal data be carried out for a specific and express purpose which must be "lawful" or "legitimate." This ***purpose specification*** requirement limits further processing of data beyond this specified purpose. This limitation guards against "function creep," where personal data originally collected for one purpose is used for other purposes. For example, a superstore with a pharmacy should not use data about the prescription medicines of customers to market unrelated sporting goods products to those customers.

Once a purpose has been specified, many frameworks require that processing of personal data be limited only to what is necessary to achieve the specified purpose, sometimes referred to as the ***proportionality principle***. However, some frameworks do not go quite this far, requiring only that

processing not be "excessive" or merely that it be "relevant" to the specified purpose.[24] For example, an employer might need to retain detailed medical information on employees engaged in hazardous factory work in case of an accident, but might not require such data from its administrative staff in an office situated elsewhere.[25]

***Data retention limitations*** also minimize processing by requiring controllers and processors to retain personal data only for as long as is needed to fulfil the specified purpose. This reduces risks of data breaches and unauthorized onwards sharing that arise from unnecessary storage. For example, the EU requires that banks store customer data for five years and allows member states to extend this to up to 10 years.[26] By contrast, an employment agency should not retain CVs of persons seeking employment for decades, as this is not proportionate to the purpose of finding employment for these persons in the short and medium term.[27]

Some frameworks require that data processing systems incorporate ***privacy by design*** or ***privacy by default***. These terms refer to the implementation of administrative and technical measures that apply data minimization principles in the architecture and processes of the data system. For example, a hospital's patient records can be pseudonymized when stored or otherwise processed in order to reduce risk of disclosure in case of a data breach.

### *Transparency*

Data protection frameworks typically require that data processing be fair and transparent, requiring mandatory disclosures to data subjects when data about them is collected, regardless of the legal basis for such collection and processing. Some frameworks require such disclosures to be made to the data subject even if the personal data is obtained from a third party or from publicly available sources. These must typically disclose the identity of the controller, the purpose of collecting the personal data, any third parties to whom it may be disclosed, and individual rights available to the data subject. Fair and transparent notification requirements are closely related to consumer protection.

### *Data quality*

Data protection frameworks also typically require that controllers actively maintain the ***quality*** of the personal data they are processing. This may create an affirmative obligation to ensure that personal data is and remains accurate, complete, and up-to-date.

### *Direct marketing*

Data protection frameworks often incorporate ***limitations on direct marketing activities*** targeting data subjects by controllers. Some frameworks prohibit direct marketing activities unless a data subject has expressly opted in, with some exceptions for existing customer relationships.[28] Others only provide that a data subject may object or opt out.[29]

### *Data security*

Data protection frameworks typically require controllers and processors to assess and maintain security in their data systems, including disclosing data breaches to the data protection authority and in some situations to the relevant data subjects.

### *Cross-border data flows*

Efficient and innovative use of data may involve transferring data across country borders. This may be necessary, for example, for provision of cross-border digital services and electronic commerce, operation of international supply chains, customer

relations management by international service providers, access to better or lower cost data processing, or pooling of data for better analytics.

On the other hand, it is difficult to monitor and enforce data protection requirements if data leaves the country. Many data protection frameworks therefore impose conditions and restrictions on transfer of data outside the jurisdiction.

### *Sensitive personal data*

Some data is viewed as ***sensitive personal data***, such as personal attributes about an individual's body and behaviors (biometrics, health status, sexuality), lineage (race, ethnicity), or spiritual beliefs, philosophy and opinions (religion, political beliefs). These data are typically given enhanced protections because they may be embarrassing or uncomfortable to the data subject if disclosed, or risk being used for undesirable profiling or discriminatory treatment adverse to members of a potentially vulnerable group. The enhanced protections typically involve heightened requirements to obtain the data subject's consent to data processing and tighter restrictions on transfer of such data abroad.

### *Individual rights*

In an increasing number of jurisdictions, the principles of data protection are not merely reflected in obligations of controllers and processors but are implemented in enforceable rights of data subjects. These rights give data subjects a degree of control over how personal data about them is processed and are generally supposed to be exercisable at no or nominal cost. These rights are similar to other rights afforded to consumers generally under consumer protection frameworks.

Individual rights usually include a ***right to verify whether one's personal data is being processed*** by a controller and, relatedly, a ***right to access and review*** a copy of that personal data. Individuals may then have a ***right to rectify*** any out-of-date, misleading and incomplete personal data they identify. The right to verify, review, and rectify personal data an organization holds about a person would be important, for example, where data is used to assess eligibility for a loan and incorrect data might harm his or her prospects.

Under some frameworks, data subjects are granted a ***right to deletion*** of personal data held by a controller. When provided, this right typically can only be exercised when personal data was obtained unlawfully, the controller no longer has a valid basis to retain the data, or retention of the data is no longer necessary (i.e., the right implements the principles on lawful basis of processing and data minimization discussed above). For example, a utility company may require the residential address of a subscriber, but there may no longer be a legal basis to retain that personal data once the subscriber deactivates the service. In that case, the subscriber would be justified in requesting deletion of the personal data.

Some frameworks include a ***right to data portability:*** the ability to easily move, copy, or transfer personal data from one controller to another. Portability is intended to reduce the risk that the data subject is locked into a particular service or service provider because the provider has accumulated useful or necessary personal data. It thus lowers barriers to switching to another service provider. For example, if an individual tracks her or his physical activity data using a wearable device linked to an app, the individual should be able to transfer that data to a competing app.

Some countries are introducing data portability requirements in financial services. Many digital credit services make credit decisions based on linked mobile money transaction histories. A right to data portability would allow such customers of one mobile money service to use their transaction histories with an unrelated digital credit service. This can be especially relevant for women who are less likely than men to have physical assets they can use as loan collateral, but who can leverage their digital transaction history as an alternative source to prove their creditworthiness.[30]

Some personal data processing incorporates computer algorithms that sort and analyze data to make decisions about data subjects. These decisions can be subject to errors and bias resulting from training data that is erroneous, out-of-date or biased; erroneous data about the data subject; or errors or biases in the algorithms themselves. Some decisions that rely on ***profiling*** based on factors such as race, ethnicity, or religion would be unlawfully discriminatory if the decision were made by a person. To address these risks, many frameworks provide data subjects with a ***right not to be subject to decisions based solely on automated processing*** of personal data that result in legal consequences for the data subject. Examples include automatic refusal of loans submitted via online applications and electronic recruitment practices that are concluded without human intervention.

Data protection frameworks typically provide data subjects with a ***right to object to processing*** of personal data.[31] When such an objection is validly made, the controller will typically need to cease any such processing.

## What data protection covers

### *Geographic connections*

There are practical and legal limits to applying domestic law outside the jurisdiction. Data protection laws typically require a minimum level of connection to the territory. In many countries, the law only applies when controllers and/or processors are established in the territory, processing takes place within the territory, or data subjects are targeted or monitored within the territory. Applicability based solely on the location of the data subject is often considered an overreach.

For example, a foreign data controller operating a website but having no connection to the territory or desire to engage its residents would not want to become subject to local data protection obligations just because a resident happens to browse that website unbeknownst to the data controller. Accordingly, some jurisdictions apply their data protection frameworks to foreign data controllers only when the controller engages in some active targeting of, marketing to, or monitoring of residents of that jurisdiction.

### *Scope of processing activities*

Given the breadth of the concepts of "personal data" and "processing", data protection could be interpreted to apply to a vast range of human activities. Many frameworks explicitly exempt the processing of personal data for ***personal, household, family or recreational affairs.*** Processing of personal data for the purposes of activities such as organizing amateur sport teams or planning family reunions is not likely to cause harm and regulating such processing would be a massive intrusion into the private lives of individuals.

Some activities are not subject to data protection law because they offer societal benefits that should be permitted, subject to some protections. Examples are processing data for ***journalistic, artistic or literary purposes.*** Government processing of personal data for purposes of ***national or public security, law enforcement,*** or other ***sensitive government functions*** may also be excluded, though usually with safeguards to mitigate abuse.

### *Anonymization*

Where personal data can be ***anonymized*** so that it is more difficult or impossible to identify the individual to whom they relate, the rationale for protecting such data greatly diminishes and they may be processed without being subject to data protection requirements. Anonymization requires that all linkages to the data subject are permanently and irrevocably removed. By contrast, data that are merely ***de-identified***, meaning for example that identifying information is replaced with coded information which could be de-coded to re-identify the individual, would not qualify as anonymized. However, anonymization is a dynamic field where the threshold keeps getting higher as new technologies find new ways to link anonymized data to the data subject.

## Institutions that support data protection

### *Data protection authorities*

Data protection frameworks typically designate an agency to serve as a ***data protection authority*** or in a similar capacity. Many frameworks require that a data protection authority be ***independent*** to prevent capture by political or commercial influences. This is all the more important as public bodies collect, use, and record extensive personal data about the population when providing public services to them. Such authorities' functions and powers vary in different jurisdictions. They generally include monitoring compliance, receiving complaints and conducting investigations, serving enforcement notices, imposing administrative fines, issuing or advising on the issuance of regulations, engaging in public outreach efforts, and advising legislators and policy makers on data protection issues. An authority is typically funded through a combination of allocations made by the legislature and proceeds from fees or fines.

Some frameworks require controllers, and even processors, to register with a data protection authority to strengthen the authority's information about data activities and enable it to charge fees. To avoid administrative burdens, usually this ***registration requirement*** only applies when certain thresholds are met or processing involves particularly sensitive matters.

Data protection frameworks typically allow for ***appeals or judicial review*** of adverse decisions of a data protection authority. Sometimes appeals are made to an ad hoc appeals body as an intermediary step, other times directly to a court.

### *Penalties and remedies*

The effectiveness of obligations and protections in a data protection framework depend on a credible threat of consequences for violations. Many frameworks empower a data protection authority to impose ***administrative fines*** on controllers and processors for violations. The amounts of fines are often limited by a monetary cap or a percentage of an entity's annual turnover (either domestic or worldwide) or both. Some frameworks

permit individuals to bring direct ***civil claims*** in domestic courts against controllers and processors for damages resulting from violations. Some frameworks provide for ***criminal penalties*** consisting of fines and/or imprisonment and are applicable to individuals such as directors, officers, and managers of legal entities. Criminal penalties are more common in jurisdictions that have weaker confidence in the effectiveness of administrative fines and civil claims.

### *Civil society, education and culture*

In addition to a legal framework, civil society engagement, education and professionalization are often vital to effect change in understanding and conduct across public bodies and commercial and non-profit organizations.

For example, the Nubian Rights Forum in Kenya has pressed for data protection laws to protect data used in proposed digital identification systems.[32] Some jurisdictions, such as the EU, have created a specific professional category of ***data protection officers*** (DPOs) that organizations of a particular scale or nature are required to engage. DPOs have certain responsibilities, perform various functions, and are expected to be suitably trained and to register with data protection authorities. These and similar requirements promote the development of a community of knowledgeable professionals with shared understanding and approaches, integrated into public and private institutions.

## How data protection supports the digital economy

### *Growth in the digital economy*

Increased trust in the digital realm is vital to uptake and usage of digital services. Providers also need certainty about the rules of the game. The implementation of a data protection framework may be a valuable precondition for investment in data-intensive businesses. For example, immediately after Kenya's 2019 Data Protection Act was signed into law, Amazon Web Services announced new investments in the country, including establishing part of its data cloud infrastructure in Nairobi. The company reportedly characterized the new law as paving the way for the investment, noting that it had been awaiting such a law for seven years.[33]

### *Confidence in government services*

A data protection framework can also increase confidence that government uses of personal data will not result in unwarranted surveillance, profiling, or other discrimination. For example, national ID systems implemented in some developing countries have been heavily criticized when they were implemented without a robust data protection framework. In India,[34] Jamaica,[35] and Kenya,[36] recent court decisions even invalidated or limited the adoption of national ID systems, largely because of insufficient protection of personal data. Concerns about data protection underlie lack of take-up of contact tracing applications in the recent Covid-19 pandemic. For example, a recent study showed that in countries where individuals tend to distrust their governments, they have been more hesitant to download and use contact-tracing apps.[37]

## Emerging issues

***Artificial intelligence*** (AI) refers to computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

*Machine learning* refers to the ability of such systems to progressively improve their own performance by analyzing large volumes of data, rather than through human programming.

These technologies present opportunities for development of the digital economy, such as through improved credit scoring that supports financial inclusion, or better fraud detection. However, these systems use vast amounts of data, and it may be difficult or impossible to know what data is being processed, how it is being processed, or how decisions are generated about individuals. These systems thus present challenges for many of the key protections of data protection frameworks.

For example, Amazon found that its AI-based automated hiring software was unintentionally favoring male candidates. The software was "trained" on resumes of past applicants, which were predominantly male, leading it to penalize female candidates.[38] Potential solutions to these sorts of issues include addressing the type of training data used and ensuring there is a "human in the loop" when decisions are made.[39]

*Facial recognition technology* (FRT) refers to computer systems that can process images of human faces to identify, authenticate, or categorize an individual. While presenting opportunities for digital identification and verification that may support development of the digital economy, FRT raises many data protection challenges.

First, cameras have become increasingly ubiquitous through government surveillance, private-sector security systems, and consumer products such as smart doorbells and smartphones. Individuals expose their face whenever they are in public, opening themselves up to surveillance and processing of their personal information, often without their consent.

Second, by its nature, FRT can discern sensitive personal information of individuals, including gender, race, ethnicity, and health status (as well as data that is not sensitive, such as location).

Finally, FRT is not always accurate, particularly when identifying faces of certain population groups, potentially resulting in misidentification that can have legal consequences for individuals.

For example, a recent study showed that facial recognition technologies identify lighter-skin men with almost no error but had an error rate of nearly 35 percent when identifying darker-skin female faces.[40,41]

## Additional resources

### *Data Protection Model Frameworks*

- EU General Data Protection Regulation
- APEC Privacy Framework
- OECD Privacy Framework
- IAPP Glossary of Terms

### *Resources for further reading*

- Convention 108+ for the Protection of Individuals with regard to the Processing of Personal Data, 2018
- UNSDG Data Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda, 2017
- Big data, artificial intelligence, machine learning and data protection, 2016
- Privacy and Freedom of Expression in the Age of Artificial Intelligence, 2018

### *Organizations*

- International Association of Privacy Professionals (IAPP)
- European Commission (data protection resources page)
- Center for Information Policy Leadership
- Future of Privacy Forum
- ICO: Information Commissioner's Office (UK)
- Electronic Privacy Information Center (EPIC)
- Privacy International
- Center for Democracy & Technology
- Center for Data Innovation
- Electronic Frontier Foundation

## Notes

[1] The term 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, Article 4 GDPR

[2] The terms "data protection" and "data privacy" are sometimes used interchangeably, but can have different meanings depending on the legal tradition. For simplicity, one can think of data privacy as motivated by notions of dignity, liberty and autonomy. It concerns limitations on the communication of data about individuals to others, and may seek to enable individuals to determine the timing, manner and extent of such communication. A large part of data protection, which governs the collection, use, sharing and storage of personal data, concerns ensuring data privacy. However, as set out below, data protection policies also address data security (see discussion of data security below and [the briefing paper on cybersecurity and data security]) and consumer protection (see the discussion of individual rights in this briefing paper and [the briefing paper on consumer protection]).

[3] See e-Government Program, Kingdom of Morocco, e-Participation Platform: FIKRA, available at: http://www.egov.ma/en/e-participation-platform-fikra.

[4] See the World Bank Universal Financial Access by 2020, available at: https://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020.

[5] See the United Nations' Sustainable Development Goals (SDG Target 8.10), available at: https://sdg-tracker.org/economic-growth.

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

[7] Data Creation and Replication Will Grow at a Faster Rate Than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts, Business Wire, 24 March 2021, www.businesswire.com/news/home/20210324005175/en/Data-Creation-and-Replication-Will-Grow-at-a-Faster-Rate-Than-Installed-Storage-Capacity-According-to-the-IDC-Global-DataSphere-and-StorageSphere-Forecasts.

[8] Susan Aaronson, 2018, Data is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows, Working Papers 2018-10, The George Washington University Institute for International Economic Policy, available at: https://www.cigionline.org/sites/default/files/documents/paper%20no.197_0.pdf.

[9] For example, in 2020 the US Federal Trade Commission received 1.4 million reports of identity theft through its IdentityTheft.gov website, about twice as many as in 2019. "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020," Federal Trade Commission (4 February 2021). Available at https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

[10] For example, in 2015 AshleyMadison.com, a dating website for married individuals seeking covert extramarital affairs, was hacked. Personal data from 36 million customers was disclosed, including names, addresses and phone numbers. See, e.g., "Ashley Madison settles with FTC over data security," Federal Trade Commission (14 December 2016). Available at https://www.ftc.gov/news-events/blogs/business-blog/2016/12/ashley-madison-settles-ftc-over-data-security.

[11] For example, in 2020 560 US healthcare facilities fell victim to ransomware attacks. One Colorado hospital was unwilling to pay the ransom and was unable to recover a significant number of patient medical records. "Another banner year for cybercriminals," EMSISOFT Blog (18 January 2021). Available at https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/. Jerich, Kat, "Ransomware attack leaves 5 years of patient records inaccessible at Colo. Hospital," HealthcareITNews (16 June 2020). Available at https://www.healthcareitnews.com/news/ransomware-attack-leaves-5-years-patient-records-inaccessible-co-hospital.

[12] For example, the UK's Information Commissioner's Office found that the country's three major credit ratings agencies were all "using personal data collected for credit referencing purposes for direct marketing purposes" contrary to the requirements of the GDPR. Investigation into data protection compliance in the direct marketing data brokering sector, Information Commissioner's Office (October 2020). Available at https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf.

[13] For example, disclosures of classified documents by Edward Snowden in 2013 revealed massive government surveillance programs, including that (1) the US National Security Agency (NSA) was requiring telecommunications company Verizon to hand over metadata on millions of American citizens' phone calls; (2) the NSA had direct access to the servers of some of the biggest technology companies including Apple, Facebook, Google, Microsoft, Skype, Yahoo, and YouTube; and (3) similar types of government surveillance were undertaken by other developed country governments. Lyon, David, "Surveillance, Snowden, and Big Data: Capacities, consequences, critique," Big Data & Society, July-December 2014: 1-13. Available at https://journals.sagepub.com/doi/10.1177/2053951714541861.

[14] See, e.g., Christl, Wolfie, "Corporate Surveillance in Everyday Life, How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions," Cracked Labs (2017). Available at https://crackedlabs.org/en/corporate-surveillance.

[15] See, e.g., Favaretto, Maddalena et al., "Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review," Journal of Big Data 6:12 (2019). Available at https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0177-4.

[16] Fernandez Vidal, Maria, Data Privacy Concerns Influence Financial Behaviors in India, Kenya, CGAP, 29 September 2020, available at: www.cgap.org/blog/data-privacy-concerns-influence-financial-behaviors-india-kenya.

[17] See PWC, "Four steps to gaining consumer trust in your tech," PWC website. Available at https://www.pwc.com/us/en/tech-effect/cybersecurity/trusted-tech.html.

[18] Collins, Daryl, and Derry Moore. "Gender And Digital Worldviews: Divergent User Perspectives On Data Collection And Use | Center For Financial Inclusion". Centerforfinancialinclusion.Org, Last modified 2021. https://www.centerforfinancialinclusion.org/gender-and-digital-worldviews-divergent-user-perspectives-on-data-collection-and-use.

[19] "LESSONS ON ENHANCING WOMEN'S FINANCIAL INCLUSION USING DIGITAL FINANCIAL SERVICES (DFS)", 2021. https://www.afi-global.org/sites/default/files/publications/2020-05/AFI_WFI_DFS_SR_AW_digital.pdf.

[20] Berg, Leandro. "Privacy On The Line". Dalberg, Last modified 2017. https://dalberg.com/our-ideas/privacy-line/.

[21] See United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide, available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[22] See Information Commissioner's Office, What is the 'legitimate interests' basis? (accessed 6 October 2021).

[23] "Data Protection Glossary". EUROPEAN DATA PROTECTION SUPERVISOR. Accessed 16 December 2021. https://edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=The%20principle%20of%20%E2%80%9Cdata%20minimisation,necessary%20to%20fulfil%20that%20purpose.

[24] For example, EU's GDPR and Kenya's Data Protection Act, 2019 both limit processing of personal data to "what is necessary" in relation to the purposes for which the data is processed. By contrast, South Africa's Protection of Personal Information Act 2013 and Malaysia's Personal Data Protection Act, 2010 impose an arguably lower standard requiring that processing of personal data be "not excessive" given the purpose for which data is processed.

[25] Derived from an example provided by the UK's Information Communication's Office website, "Principle (c): Data minimisation." Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

[26] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Art. 40.

[27] Derived from an example provided by the European Commission website, "For how long can data be kept and is it necessary to update it?" Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en.

[28] For example, Section 69 of South Africa's Protection of Personal Information Act 2013.

[29] For example, Section 41 of Malaysia's Personal Data Protection Act, 2010.

[30] "ADVANCING WOMEN'S DIGITAL FINANCIAL INCLUSION". G20 Global Partnership for Financial Inclusion, 2020. https://www.gpfi.org/sites/gpfi/files/sites/default/files/saudig20_women.pdf.

[31] "Art. 21 GDPR – Right To Object - General Data Protection Regulation (GDPR)". General Data Protection Regulation (GDPR). Accessed 16 December 2021. https://gdpr-info.eu/art-21-gdpr/.

[32] Nubian Rights Forum, Kenya Human Rights Commission and Kenya National Commission on Human Rights v The Hon. Attorney General and Others [2020] at eKLR http://kenyalaw.org/caselaw/cases/view/189189/

[33] Oblultsa, G and Miriri, D., Kenya passes data protection law crucial for tech investments, Reuters, 8 November 2019, available at https://www.reuters.com/article/us-kenya-dataprotection/kenya-passes-data-protection-law-crucial-for-tech-investments-idUSKBN1XI1O1

[34] Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aug. 24, 2017).

[35] Robinson v. Att'y Gen. of Jamaica [2019] JMFC Full 04 (Sup. Ct. Jamaica Apr. 12, 2019) https://supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica.

[36] Nubian Rights et al. v Attorney General of Kenya (High Ct. Kenya Apr. 1, 2019).

[37] M. Bano, D. Zowghi and C. Arora, Requirements, Politics, or Individualism: What Drives the Success of COVID-19 Contact-Tracing Apps?, in IEEE Software, vol. 38, no. 1, pp. 7-12, Jan.-Feb. 2021, doi: 10.1109/MS.2020.3029311.

[38] Dastin J, "Amazon scraps secret AI recruiting tool bias against women", Reuters, 10 October 2018, available at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[39] Center for Information Policy Leadership, Artificial Intelligence and Data Protection in Tension, 2018; Center for Democracy & Technology, AI & Machine Learning, 2020.

[40] Joy Buolamwini, Timnit Gebru, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.

[41] National Conference of State Legislatures, Facial Recognition Gaining Measured Acceptance, 2020; Roussi, Antoaneta, Resisting the rise of facial recognition, 2020; How should we regulate facial-recognition technology?, Nature, 2019; Wiewiórowski, Wojciech, Facial recognition: A solution in search of a problem?, European Data Protection Supervisor, 2019.

## About UNCDF

The UN Capital Development Fund makes public and private finance work for the poor in the world's 46 least developed countries (LDCs). UNCDF offers "last mile" finance models that unlock public and private resources, especially at the domestic level, to reduce poverty and support local economic development. UNCDF pursues innovative financing solutions through: (1) financial inclusion, which expands the opportunities for individuals, households, and small and medium-sized enterprises to participate in the local economy, while also providing differentiated products for women and men so they can climb out of poverty and manage their financial lives; (2) local development finance, which shows how fiscal decentralization, innovative municipal finance, and structured project finance can drive public and private funding that underpins local economic expansion, women's economic empowerment, climate adaptation, and sustainable development; and (3) a least developed countries investment platform that deploys a tailored set of financial instruments to a growing pipeline of impactful projects in the "missing middle."

The UNCDF Policy Accelerator works with governments to help them create policies and regulations that include everyone in the digital economy, shares practical tools and guides based on our technical assistance model and our go-to resources, and provides scholarships to policymakers and regulators to study with our world-class partner organisations.

## About Macmillan Keck

Macmillan Keck Attorneys & Solicitors advises clients on strategy, advocacy, deals, controversies and reforms in the digital economy. The firm's clients include telecom operators, digital financial service providers, online health and education providers, other digital content, application and service providers, governments and sector and competition regulatory authorities, and international organisations. The firm has successfully completed numerous complex projects across a majority of countries in every continent.

## Disclaimer



*This publication was last reviewed in November 2021.*


**policy.accelerator@uncdf.org**

**policyaccelerator.uncdf.org | uncdf.org**

FIND US