

Chapter 6

PRIVACY AND DATA PROTECTION

KEY FINDINGS

- All 29 countries that responded to the OECD's 2019 Privacy Guidelines Questionnaire have in place some form of legislation for privacy and personal data protection. Of these, 17 reported their main privacy legislation was adopted after 2013. In addition, 10 countries reported they are revising their privacy and data protection legislation, and eight countries reported plans for revisions.
- Timely, secure and reliable data access and sharing – within and outside borders – is critical to understanding COVID-19 and its spread, enhance government policies and foster global co-operation in the development and distribution of a vaccine.
- Global sharing and collaboration of research data have reached unprecedented levels. Clinical, and epidemiological and laboratory data about COVID-19, are today widely available. Similar efforts may also be needed for other types of data.
- Many governments have passed or are about to pass laws specifying how data collection will be restricted to a certain population, for what time and for what purpose.
- Privacy frameworks generally facilitate data sharing in the interests of national and public security, including public health and welfare. However, countries have not always embraced these frameworks.
- Privacy enforcement authorities across much of the OECD have endorsed a pragmatic and contextual approach to data sharing, including discretion in enforcement. Many jurisdictions are also issuing guidance on the collection, processing and sharing of personal data to support COVID-19 contact tracing and other response measures. Use of privacy-enhancing solutions such as homomorphic encryption and data sandboxes may add protection.

Introduction

In recent years, the generation and sharing of personal data have increased. This has been driven by, and in turn contributed to, changes in organisational practices and the data-sharing behaviours of individuals. This chapter delves into recent trends and challenges in privacy and personal data protection, and analyses evolving national and international regulatory and policy responses.

With the rapid emergence of data-rich technologies such as artificial intelligence (AI), the Internet of Things (IoT) and big data analytics, it is increasingly clear that trust remains a critical factor in the digital transformation of economies and societies (OECD, 2015^[1]). Individuals and organisations must feel confident their privacy is respected to take advantage of the benefits arising from technological developments.

However, fuelled by high-profile data breaches such as in Cambridge Analytica, individuals are increasingly concerned about digital risks. This is particularly true with respect to the expanded uses of their personal data. These concerns can pose a serious barrier to the adoption of digital technologies and applications (OECD, 2017^[2]).

There is strong evidence that governments are responding to the challenges. Over the past two years, countries around the world have developed significant regulations. In particular, the number of international, regional and national privacy and data protection frameworks enacted or amended since 2013 has increased substantially. All 29 countries that responded to the OECD's 2019 Privacy Guidelines Questionnaire have in place some form of legislation for privacy and personal data protection. Of these, 17 reported their main privacy legislation was adopted after 2013. In addition, 10 countries reported they are revising their privacy and data protection legislation, and eight countries reported plans for revisions. Countries consider that catching up with technological developments – particularly AI and big data analytics – is the biggest challenge they face with regard to those frameworks.

Countries' attention is now shifting towards strengthening compliance with, and enforcement of, privacy and data protection frameworks. In particular, governments are investing in policy measures

to enhance awareness of the frameworks and what they require of organisations that collect, process and share personal data. There is also growing emphasis on promoting the accountability of data controllers, and engaging in international enforcement co-operation.

Recent legal and policy responses recognise that children are particularly vulnerable in the digital environment. As such, they merit special protection in regard to their privacy and personal data. The disproportionate risk faced by children in the digital environment will likely only become more evident with time, and policy makers will have to respond accordingly.

The proliferation of frameworks presents its own challenges, such as the uncertainty that occurs when frameworks conflict. However, clear rules, guidance and levels of compliance could markedly improve overall trust in the digital economy. Efforts to increase the interoperability of privacy frameworks will likely be a positive step to enhance trust in data flows and ensure benefits from technological developments.

The COVID-19 crisis has been an important reminder of why such data flows are critical. Timely, secure and reliable data access and sharing – within and outside borders – can help understand the virus and its spread, enhance government policies and foster global co-operation in the development and distribution of a vaccine.

Data, privacy and the fight against the COVID-19 pandemic

At the time of publication, the gravity of COVID-19 had taken form in the collective minds of governments and policy makers, businesses and individuals. Timely, secure and reliable data access and sharing – within and outside borders – is critical to understanding the virus and its spread. It can also improve the effectiveness of government policies and foster global co-operation in the race to develop and distribute a vaccine. In particular, lessons from previous outbreaks have underscored the importance of data concerning the spread of virus infections. This includes the location and number of new confirmed cases, rates of recoveries and deaths, and the source of new cases (international arrivals or community transmission).

Knowing how a virus mutates as it moves through a population is also vital. Such information can help policy makers understand possible changes in disease severity or transmissibility, its amenity to diagnosis and its responsiveness to vaccine. In addition, accurate information on population movements helps monitor the progression of an outbreak and predict its spread, set priorities for interventions and design effective containment strategies. Armed with these data, governments are rapidly introducing a wide range of measures to contain outbreaks, protect the vulnerable and limit community transmission.

In the current global health emergency, scientific discovery has progressed much more rapidly than before. Barely a month after the first patient was admitted into Wuhan hospital, researchers shared the full genome of COVID-19 as an open-access publication. Full viral genome sequences were released through public access platforms, leading to polymerase chain reaction assay protocols. These made it possible to accurately diagnose infections early during the pandemic.

Global sharing and collaboration of research data have reached unprecedented levels. Clinical, and epidemiological and laboratory data about COVID-19 are widely available. However, similar efforts may also be needed for other types of data.

Privacy frameworks generally facilitate data sharing in the interests of national and public security, including public health and welfare. These include the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines).

More recent OECD work suggests countries have not always taken up these frameworks. Few countries have policy initiatives to facilitate data sharing within the private sector. Even fewer have data governance frameworks to support such extraordinary data collection and sharing measures in ways that are fast, secure, trustworthy, scalable and in compliance with the relevant privacy and data protection regulations (OECD, 2019_[3]).

Many countries have recently sought advice from privacy enforcement authorities (PEAs), private-sector law firms, civil society, academics and other actors. They want to ensure their actions are necessary and proportionate, and that they fully understand their potential implications. Many governments have passed or are about to pass laws specifying how data collection will be restricted to a certain population, for what time and for what purpose.

PEAs across many OECD countries have generally endorsed a pragmatic and contextual approach, including discretion in enforcement. They point out that respect for fundamental data protection and privacy principles does not stand in the way of necessary and proportionate frontline responses to COVID-19.

Additionally, PEAs in many jurisdictions are issuing advisory guidance on the collection, processing and sharing of personal data to support COVID-19 contact tracing and other response measures. Much of this guidance relates to how privacy-by-design features can be incorporated into “track and trace” applications to ensure that personal data collected are protected.

The European Data Protection Board and the Council of Europe have released similar statements. These explain that the General Data Protection Regulation (GDPR) and Convention 108 do not hinder measures taken in the fight against the pandemic. Further, they require that emergency restrictions on freedoms be proportionate and limited to the emergency period (Council of Europe, 2020^[4]; EDPB, 2020^[5]). Indeed, many data governance and privacy frameworks expressly permit data processing for legitimate public interests, including public health, provided necessary safeguards are maintained.

The use of privacy-enhancing solutions may add protection (OECD, 2019^[3]). These can include homomorphic encryption, which allows processing of encrypted data without revealing its embedded information. They also include data sandboxes that grant access to highly sensitive (personal) data within a restricted digital and/or physical environment to trusted users.

Technological developments and implications for privacy

The advancement of computing capabilities and the increased availability of storage have fuelled widespread adoption of Internet and personal computing devices. This, in turn, has increased the creation of data and the possibility for its analysis. Data have never been so prevalent: the volume of data produced globally is forecast to grow from 33 to 175 zettabytes over 2018-25, a compounded annual growth rate of 61% (European Commission, 2020^[6]).

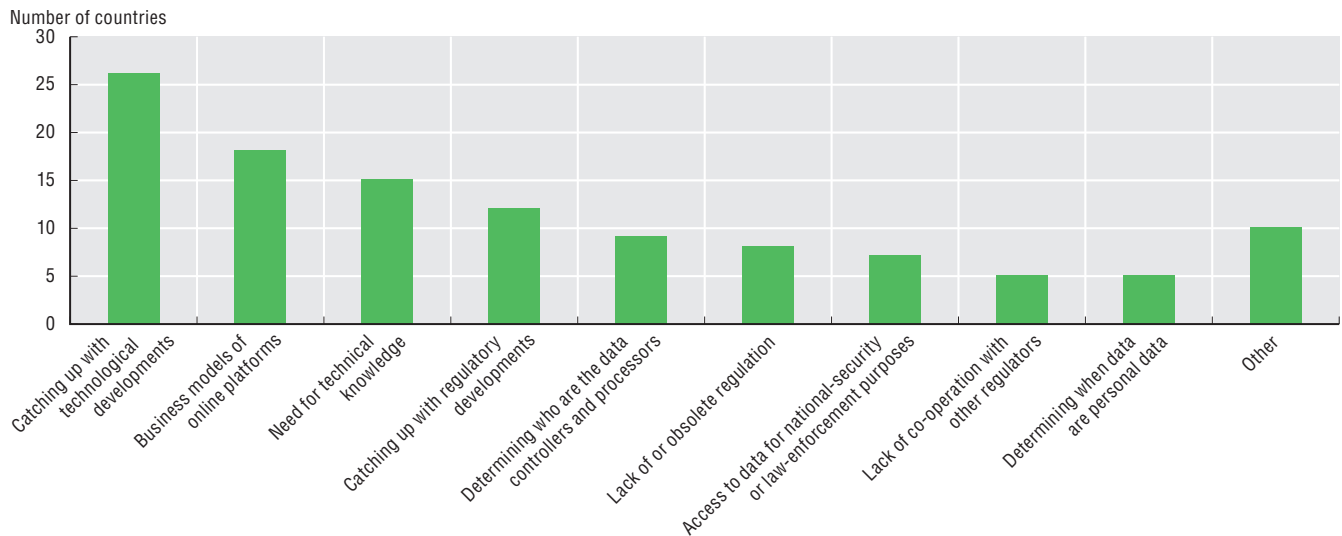
Increasingly, organisations and individuals are using third-party cloud-based data storage services that may be located outside their country. Data processing and analytical software have also become increasingly powerful, sophisticated, ubiquitous and inexpensive, making information easily searchable, linkable and traceable. This means that personal data are both more valuable and more likely to have unanticipated uses, increasing the incentive to collect and store them. Emerging technologies, particularly AI and IoT, are a compelling demonstration of these interdependencies. They are generally based on the abundance of data, and the gathering, linking and processing of that data, which increases their value.

This increase in the generation and sharing of personal data has been driven by, and in turn contributed to, related changes in organisations’ practices and individuals’ data-sharing behaviours. Individuals, knowingly or not, share more personal data today than ever. For their part, a growing number of entities such as online retailers, Internet service providers, financial service providers and governments is increasingly collecting vast amounts of personal data, usually spanning a wide range of economic and social activities (OECD, 2015^[1]). For an increasing number of companies, the very use of personal data – whether for sale to third parties, advertising or for tailoring their own services – is a core element of their business model. This, in turn, leads to a rise in the value of personal data (“personal data as resource or commodity”). Similarly, the value rises for the generation and processing of data; the use of technologies that link datasets and extract further value from them; and transborder data flows.

Countries consider that catching up with technological developments is the main challenge to their privacy and data protection regulatory frameworks

In 2019, countries reported that catching up with technological developments was the main challenge to their privacy and data protection regulatory framework. They identified related challenges of “business models of online platforms” and the “need for technical knowledge” as the next most pressing challenges (Figure 6.1).

Figure 6.1. Main challenges to regulatory frameworks, 2019

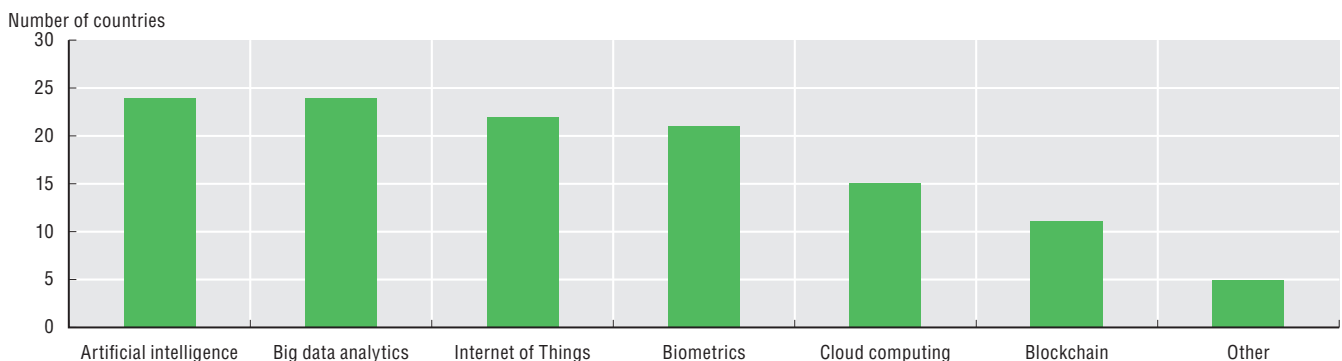


Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink <https://doi.org/10.1787/888934192167>

The 2019 OECD Privacy Guidelines Questionnaire¹ provided much insight into privacy questions. With respect to technological developments posing the biggest challenges to privacy and personal data protection, over 80% of 29 countries mentioned AI and big data analytics, followed closely by the IoT and biometrics (Figure 6.2). Facial recognition and FinTech (particularly new payment methods such as Libra) were mentioned in comments. With respect to challenges related to emerging technologies, all but two respondents noted ethical issues, including bias and discrimination, as a main concern. The increasing risk of re-identification and the use of personal data with societal implications (such as targeted online advertising campaigns) followed as the next most pressing concerns.

Figure 6.2. Emerging technologies that pose the main challenges for privacy and personal data protection, 2019



Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink <https://doi.org/10.1787/888934192186>

Big data analytics and AI pose challenges to privacy frameworks in part because of the wealth of data they generally require. With technological advances to date, they can increasingly identify specific individuals and reveal sensitive personal information (including when paired with other information). This means the data supporting these technologies increasingly fall within the ambit of privacy frameworks. These generally apply to information relating to an identified or identifiable individual (data subject). Applying frameworks to masses of data can become unwieldy without clear guidance, co-operation and communication.

There is a movement underway concerning the development and use of privacy-respecting and privacy-enhancing technologies. These could increase compliance with privacy frameworks and foster trust in digital society, organisations and specific technologies. Numerous privacy-enhancing tools for online and mobile protection exist. These include “small data” AI, anonymisation, anti-tracking, encryption, hashing, secure file sharing and secure communication tools. Efficient privacy-enhancing approaches often combine one or more advanced technologies such as synthetic data, homomorphic encryption, blockchain or differential privacy. Still, more work can be done in several areas. Policy makers need to evaluate the relative strengths and weaknesses of these technologies. They need to develop new ones or improve effectiveness of existing ones. Finally, they need to better understand barriers to their deployment and adoption in the online global marketplace.

Privacy and data protection concerns

The number and severity of data breaches, including high-profile cases, has risen

Technological advancement goes hand in hand with increased global data flows. Data are more valuable (and “big data” especially so), thus increasing incentives to share them, including across borders. Moreover, it is increasingly faster and cheaper to do so. However, as the quantity of data collected and stored increases, so too does the prevalence of data breaches. Such breaches can result from accidents, malicious hacking, unauthorised access or disclosure, phishing and denial-of-service attacks.

Between 2018 and 2019, over 89 000 data breaches were registered in the European Union (EU), representing an increase of 20% from 2015 (EDPB, 2019^[7]). It is likely, however, that the GDPR’s mandatory data breach reporting requirement contributed to this substantial increase.

In recent years, the private sector has been involved in high-profile data breaches. In October 2018, Facebook was fined GBP 500 000, the maximum fine possible by the Information Commissioner’s Office of the United Kingdom. It was charged for “unfairly process[ing] personal data” and “fail[ing] to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data” (Information Commissioner’s Office, 2018^[8]). This incident involved more than 87 million personal records that were unlawfully used by Cambridge Analytica (Granville, 2018^[9]; Graham-Harrison and Cadwalladr, 2018^[10]; Hern and Pegg, 2018^[11]).

Data breaches are not limited to data held by the private sector. In 2015, for example, more than 21 million records stored by the US Office of Personnel Management were stolen, including 5.6 million fingerprints. The same year, a breach in the Japanese Pension Service affected 1.25 million people (Otaka, 2015^[12]).

Data breaches violate the privacy of individuals concerned (leading possibly to identity theft), and can also cause significant economic losses to affected organisations. A 2019 IBM study indicated the cost of a data breach had risen 12% over the previous five years and costs USD 3.92 million on average per organisation. The report also revealed that organisations feel the effects of a data breach for years (IBM Security, 2019^[13]).

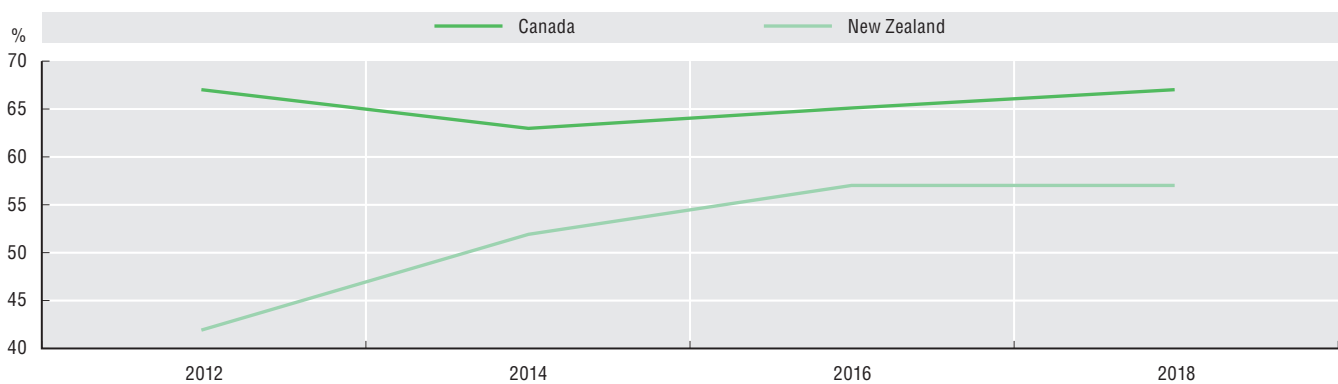
Individuals are increasingly concerned about the use of their personal data

The increasing prevalence and cost of data breaches have contributed to changing public awareness and perceptions of the importance of privacy. Public perception studies in the last few years suggest that individuals are increasingly concerned about the use and protection of their personal data. Indeed, these concerns may prevent many people from going on line.


This trend towards greater concern about use of personal data is particularly apparent in studies that followed the 2018 Cambridge Analytica data breach. Half of the countries responding to the 2019 OECD Privacy Guidelines Questionnaire said they conduct surveys or otherwise regularly gather and analyse data from individuals on their public perception of privacy and personal data mechanisms. Figure 6.3 depicts the findings from surveys in two respondents to the OECD questionnaire. In Canada, the percentage of individuals “extremely concerned” about the protection of their personal privacy grew from 25% to 37% between 2012 and 2018; only 8% of individuals were not concerned at all (OPC, 2019_[14]). In New Zealand, more than half of all New Zealanders are more concerned about their privacy than they were in 2012. Separately, in the United States, most Americans reported they are concerned by how companies and the government use their data (Auxier et al., 2019_[15]). Indeed, 81% of Americans believe their potential risks from data collection by companies outweigh the benefits (Auxier et al. 2019_[15]).

Figure 6.3. Sample of privacy enforcement authority public surveys, 2012-18

Percentage of individuals concerned about protecting personal privacy



Sources: 2018-19 Survey of Canadians on Privacy, www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#fig03; New Zealand Privacy Survey 2018 www.privacy.org.nz/news-and-publications/surveys/privacy-survey-2018 (accessed on 31 March 2020).

StatLink  <https://doi.org/10.1787/888934192205>

In the European Union, in all but four countries at least half of all respondents to a survey were concerned about lacking complete control over information provided on line (European Commission, 2019, p. 40_[17]). In 2019, Eurostat reported that 44% of EU citizens aged 16 to 74 claimed to have limited their private Internet activities in the previous 12 months due to security concerns. The survey asked individuals about potential security-related issues when accessing the Internet on any connected device, such as a desktop, laptop, tablet or smartphone. Due to security concerns, people appeared to have mostly avoided providing personal information to social or professional networking services (25% of those surveyed). These security concerns also reportedly limited or prevented 19% of people from using public Wi-Fi and 17% from downloading software, apps, music, video files, games or other files. Meanwhile, 16% and 13%, respectively, reported avoiding online shopping and Internet banking (IDC and Lisbon Council, 2018_[18]). The results are based on self-reporting and may suffer from various biases.

In Australia, a government survey revealed that 69% of citizens were more concerned about their privacy in 2017 compared to 2012. Most reported concerns about their privacy in the digital environment (Australian Government, 2017_[19]).

The privacy concerns of individuals may be partly related to confusion about their rights and ability to give fully informed, specific consent before their personal data are collected, processed and shared. The processing of personal data is becoming more complex and has more unanticipated uses, particularly in the case of AI. As it does, those activities become less transparent to users and more difficult to understand.

The same is true for IoT devices, whose ubiquity and discreteness can mask how they are constantly gathering data. Indeed, often people have no easy way to set preferences for how these technologies gather personal data. Consent is evidently more difficult to give when personal data can be used in unanticipated ways, or where processing is less transparent and more complex.

In this context, increased disclosure to individuals about an organisation's privacy practices and personal data usage may not always compensate for the information asymmetry. Facing arcane and legalistic explanations, many individuals cannot choose or consent meaningfully or even simply grasp how personal data are used. The choice is even less meaningful when users must accept the "terms of use" to use the service. Added to this, data subjects are not always immediately concerned about protecting their data. Nor are they always willing to make sense of different consents when they need or want to access a particular product or service quickly (consent fatigue). As a result, the problems associated with relying on consent as a legitimate basis for the collection, processing and sharing of personal data will likely become more apparent over the next few years. Policy makers will have to respond accordingly.

There is also increased concern regarding the protection of children's privacy in the digital environment

Due to the increase in time spent in the digital environment and from a wide range of devices, privacy has also become a central issue for children. Children are part of all kinds of databases, and subject to the data economy irrespective of whether they are active users. Their activities are the focus of commercial interests, as well as a multitude of monitoring and data-generating processes.

Children's personal information and their data go beyond what they knowingly share. Information can also be gleaned from their actions or even from disclosures that parents and friends may make on line. These disclosures may follow children into their adulthood. The unlawful collection of data can lead to privacy violations; disclosure or inappropriate use can lead to harmful and (in a number of cases) irreversible consequences for the child.

Children have a fluid understanding of their privacy, which reflects the complexity of the digital ecosystem (OECD, 2019^[20]). As children do not have fully developed cognitive abilities, their lack of experience and limited awareness of privacy risks make it difficult for them to protect their personal data, manage privacy settings and understand complicated privacy policies. As children grow, however, they tend to care a lot more about their privacy than parents or caregivers would assume. Yet, in many cases, children are still generally not consulted on this issue. Evolving trends, such as multiplication of social media accounts, can greatly affect children's privacy. The same is true for technological advancements like AI, IoT, cloud computing and facial recognition. Children's own actions can also influence the privacy of third parties, including in cases when they post pictures or information about other children.

Researchers at the London School of Economics and Political Science noted the importance of distinguishing between three types of data (Livingstone, Stoilova and Nandagiri, 2018^[21]). These can summarise how children of different ages understand the impacts of their online activities on their privacy:

- "Data given": data provided by individuals (about themselves or about others), usually knowingly though not necessarily intentionally while they are on line.
- "Data traces": data left by participation on line (usually without the user's knowledge) and captured via data-tracking technologies such as web, beacons or device browser fingerprinting, cookies, location data and other metadata.
- "Inferred data": data derived from analysing data traces and data given, frequently by algorithms (also referred to as "profiling"). These can also be combined with other data sources (Livingstone, Stoilova and Nandagiri, 2018^[21]).

Research reveals that children are aware they may have contributed data about themselves or about third parties as a result of their actions in the digital environment. However, the extent to which they will understand the consequences for their privacy will depend on their age, maturity and individual circumstances and their understanding of interpersonal relationships (OECD, 2019^[22]).

Children are aware of "data given", particularly in interpersonal contexts. For example, they may share data themselves or are aware that their friends and family do, too. In such cases, children most likely consciously decide whether and with whom they are choosing to share data (Hof, 2017^[23]).

Children are becoming increasingly aware of the commercial uses of "data traces". However, their understanding of "inferred data" and its value to businesses relies on their comprehension of business

models in institutional and commercial contexts (Livingstone, Stoilova and Nandagiri, 2018^[21]). They are rarely educated about such issues.

At the same time, commercial uses of children's data are becoming a more visible concern. The privacy risks of connected smart toys and apps designed for, and targeted towards, children create more opportunities for the collection and use of children's data. In many cases, this type of activity conflicts with measures designed to protect children's privacy (Norwegian Consumer Council, 2017^[24]; Irwin Reyes et al., 2018^[25]).

New regulations under international, regional and national frameworks for cross-border data flows, privacy and personal data protection

Over the past two years, a number of significant regulatory developments have taken place worldwide. On 25 May 2018, for example, the European Union's GDPR entered into force (European Union, 2016^[26]). By replacing the Data Protection Directive (European Union, 1995^[27]), the GDPR introduced new rules governing the collection, processing and free flow of personal data regarding data subjects in the European Union.

The GDPR champions data subject rights. When data originating in EU member states are transferred abroad, the GDPR ensures that personal data protections travel with them. This is made possible through the use of different tools, some of which pre-dated the GDPR. These include "adequacy decisions" in respect of recipients and when "appropriate safeguards" are in place for the data (such as model clauses, binding corporate rules, codes of conduct and certification). The GDPR aims to ensure a consistent and high level of protection and remove obstacles to the free flow of data within the Union (European Union, 2016^[26]).

Further, the Council of Europe has recently engaged in an extensive review and revision of its 1985 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (Council of Europe, 1981^[28]). The Convention generally permits or encourages transborder personal data flows when privacy is protected. It provides that Parties shall not prohibit or limit the transfer of personal data to a recipient who is subject to the jurisdiction of another Party to the Convention. The Convention further provides that transfers to recipients in states not parties to the Convention may generally only take place with an appropriate level of protection (Council of Europe, 1981^[28]). In October 2018, a Protocol to amend Convention 108 opened for signature. The amendments are designed to ensure the Convention applies to new information and communications technologies, and to strengthen its implementation. The modernised instrument, Convention 108+, will enter into force in October 2023.

The OECD is also reviewing implementation of the 2013 revisions to the 1980 OECD Privacy Guidelines (OECD, 2013^[36]). The guidelines are intended as minimum standards for adoption in domestic legislation regarding the protection of personal data, and have influenced legislation and policy in OECD countries and beyond. However, the 2013 review process identified profound changes of scale. These related to the role of personal data in economies, societies and daily lives since 1980. The current review aims to monitor implementation of the 2013 guidelines, identify gaps and suggest possible next steps to ensure the guidelines remain relevant.

More trade agreements and other frameworks that seek to promote trust in transborder flows of personal data have also been approved. These contribute to the complexity of the legal landscape in which countries, organisations and other bodies are transferring personal data across borders. These instruments sit alongside others that continue to shape privacy and global data transfers. The EU-US Privacy Shield Framework, for example, facilitates the transfer of personal data from the European Union to certified companies in the United States to support transatlantic commerce. Other agreements and frameworks include the Asia-Pacific Economic Cooperation (APEC) Privacy Framework,² the African Union Convention on Cyber Security and Personal Data Protection, and the Supplementary Act on Personal Data Protection within the Economic Community of West African States. In addition, the G20 Leader's Declaration in Osaka in June 2019 provides that domestic and international legal frameworks should be respected to facilitate data flows and strengthen consumer and business trust. In this way, it can help industry harness opportunities of the digital economy.

Significant challenges to transborder data flows are associated with recent international and regional developments

Over 86% of respondents to the 2019 OECD Privacy Guidelines Questionnaire are Parties to at least one multilateral agreement or legal framework that defines or overcomes legitimate restrictions on transborder flows of personal data. Those agreements and frameworks included the GDPR, Convention 108, the APEC Privacy Framework and the Privacy Shield. These evolving regulatory developments indicate that countries are adapting to the challenges posed by increased transborder data flows. However, they have also produced a degree of uncertainty as governments, organisations and individuals try to adapt. Countries are reporting that greater privacy interoperability is needed to reap the benefits from technological developments and transborder data flows.

Indeed, in identifying the main challenges to transborder data flows, questionnaire respondents most often noted uncertainty regarding legal privacy regimes. This was followed by incompatibility of legal regimes (Figure 6.4). One country, for example, had challenges stemming from the uncertainty of PEAs in the European Union about sharing information with authorities outside the Union. Other popular responses from countries with respect to challenges include time and resources required to enable transborder data flows and recent trends in favour of data localisation.

Figure 6.4. Main challenges to transborder data flows, 2019



Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink  <https://doi.org/10.1787/888934192224>

National regulatory activity relating to privacy and personal data protection has increased markedly

At a national level, an increasing number of countries around the world (including OECD countries) are putting in place modern data protection frameworks and policies. These combine openness for international data flows with safeguards ensuring the highest level of privacy and data protection for individuals. Many governments have been introducing and modifying data-related policies. They aim to adapt policies to the digital age, place conditions on the transfer of data across borders or require that data be stored locally (OECD, 2019^[29]).

Additionally, all 29 countries that responded to the OECD's 2019 Privacy Guidelines Questionnaire have some form of legislation for privacy and personal data protection. Of these, 17 reported adopting their main privacy legislation after 2013. Ten countries reported they are revising their privacy and data protection legislation, while eight reported plans for revisions. This activity reflects countries' attempts to adapt their national legislative frameworks to developments in the privacy landscape.

In enacting or revising privacy legislation, all countries but one clearly consider regulatory developments at the international level. This includes the OECD Privacy Guidelines, GDPR, APEC Privacy Framework or the Council of Europe's Convention 108. Notwithstanding, countries noted the challenge of understanding how privacy laws apply to emerging technologies, such as AI, and their impact on consumers. To deal with these challenges, countries are developing **dedicated regulation and guidance**.

Table 6.1. Amendments to countries' privacy and data protection legislation

Country	Revised since 2013	Under revision (Nov 2019-Feb 2020)	Planned revision
Australia	x	x	x
Brazil	✓	x	x
Canada (public sector)	✓	x	✓
Canada (private sector)	x	✓	x
Chile	x	✓	x
Colombia	x	x	x
Denmark	✓	x	x
Estonia	x	x	x
Finland	✓	x	x
France	✓	x	x
Iceland	✓	x	x
Israel	x	✓	✓
Italy	✓	x	x
Japan	✓	x	x
Korea	✓	✓	x
Latvia	✓	Do not know	Do not know
Lithuania	✓	✓	✓
Luxembourg	✓	x	x
Mexico	x	x	Do not know
New Zealand	x	✓	✓
Norway	✓	x	x
Portugal	✓	x	✓
Singapore	x	✓	✓
Slovak Republic	x	x	Do not know
Slovenia	x	✓	x
Switzerland	x	✓	✓
Thailand	x	x	x
Turkey	✓	x	x
United Kingdom	✓	x	x
United States	x	✓	✓

Source: 2019 OECD Privacy Guidelines Questionnaire.

Just over half of the respondents to the 2019 OECD Privacy Guidelines Questionnaire reported additional laws or regulations in place or under development, or plan to revise privacy legislation. Other key actions reported were strengthening privacy and personal data protection in the context of social media and online platforms (eight respondents), emerging technologies (seven respondents) and targeted advertising or pricing (seven respondents).

Countries are also employing, developing or considering the development of measures for **regulatory innovation** in the context of emerging technologies. Most commonly (25%), they are using regulatory sandboxes and experimentation. Other measures reported include development of **international standards** for specific technologies (such as blockchain), a Digital Charter, a privacy research grants programme and an AI auditing framework.

Some national privacy developments are particularly notable. The California Consumer Privacy Act (CCPA), enacted in 2018 and effective since 1 January 2020, creates new consumer rights for the collection, processing, retention and sharing of personal data (OAG, 2020^[30]). It has prompted a fundamental re-thinking of privacy rights in the United States, which does not have comprehensive or overarching federal privacy law. Businesses subject to the CCPA are bound by strict new requirements. For example,

they are obliged to provide notice to consumers at or before data collection, respond to consumer requests, disclose financial incentives offered in exchange for personal information and maintain detailed records.

Brazil also enacted a General Data Protection Law in 2018 (*Lei Geral de Proteção de Dados Pessoais, LGPD*). Initially developed by the Ministry of Justice and Public Security, the LGPD underwent extensive public consultation with stakeholders from civil society, academia and the business community over seven years. The law creates a new framework for online and offline personal data applicable to the public and private sectors. It has a strong focus on individual rights, including the right to access data, rectification, explanation and data portability. However, it was also designed to create greater consistency and uniformity regarding data protection and data processing. To that end, it covers international data transfers and mandatory data breach notification requirements. Like the GDPR, the law has extraterritorial reach. As such, organisations based outside of Brazil must comply with the law if they are processing the personal data of Brazilian citizens.

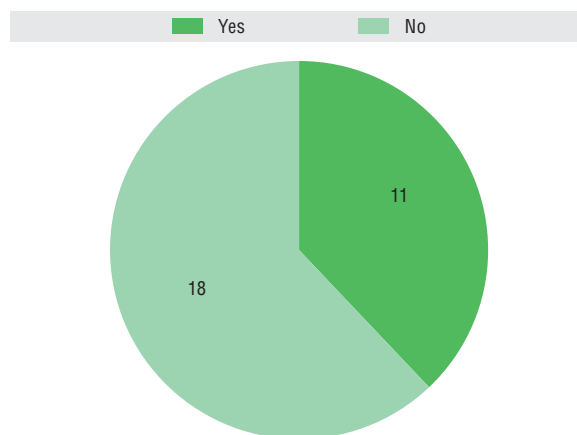
In India, long-awaited national data protection legislation is before parliament. Like the GDPR, it aims to protect the privacy of individuals relating to their personal data. It also confers certain rights on data subjects, including the right to be forgotten and the right to data portability. It also creates rules for cross-border transfers and establishes a Data Protection Authority of India. Yet the legislation has been criticised for exempting government agencies. In an example of data localisation, it also requires sensitive personal information to be stored on servers located in India.

Countries tend to have provisions in their national legislation regulating the free flow of data

Responses to the 2019 OECD Privacy Guidelines Questionnaire suggest that countries generally enable the free flow of personal data across borders when safeguards protect the privacy of persons whose personal data are being transferred. Countries also reported having various mechanisms to promote transborder flows. These include consultations, workshops and participation in international fora (such as entering into trade agreements).

Nevertheless, over 73% of respondents said provisions in their privacy and personal data legislation restrict transborder data flows. Some countries were referring to the GDPR, which has strengthened the rules governing transfers of personal data regarding data subjects who are in the European Union. Others have enacted their own frameworks to regulate data flows, some of which are still evolving. Some 40% of respondents added they have provisions in their regulatory framework concerning data localisation (Figure 6.5). In some of these countries, only specific types of personal data were subject to a localisation requirement. These include, for example, health records, national archives or data relevant to national security.

Figure 6.5. Countries with provisions requiring some form of data localisation in their regulatory framework, 2019



Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink  <https://doi.org/10.1787/888934192243>

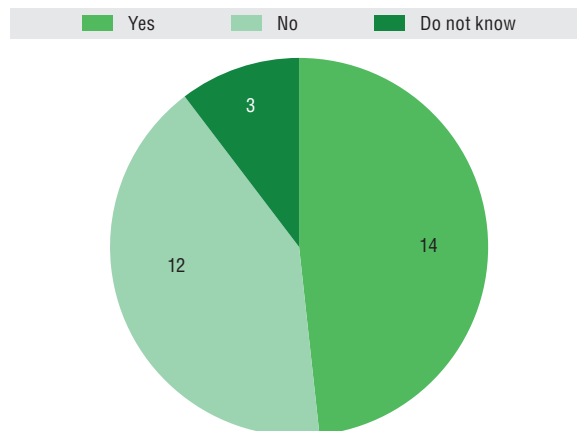
Additionally, in the case of 11 respondents, organisations are required to report on transborder flows of personal data. The content of these requirements, however, varies. For example, organisations in one country must report all data transfers (regardless of where the data are being transferred). Organisations subject to the GDPR, conversely, must report to and obtain permission from supervisory authorities for data transfers to non-EU countries under certain circumstances. It is an additional burden for data controllers to demonstrate compliance with data protection rules. The authorisation for personal data transfers abroad depends on different factors such as reciprocity, national personal data protection law limitations (including non-EU countries) and so on.

Yet few countries have a national privacy strategy or whole-of-government approach to privacy

The 2013 revision of the OECD Privacy Guidelines (OECD, 2013^[36]) calls on governments to “develop national privacy strategies that reflect a co-ordinated approach across governmental bodies.” The importance of such strategies has also been stressed in the 2016 OECD Ministerial Declaration on the Digital Economy (Cancún Declaration) and in the Digital Economy Ministerial Declaration of the G20 Ministerial adopted in April 2017. The prevalence of national privacy strategies and their components was explored in depth in OECD (2018^[37]), which concludes that most countries did not have national privacy strategies. However, countries also understood the term in different ways, and did have some basic elements in place (OECD, 2017^[2]).

The findings from the 2019 OECD Privacy Guidelines Questionnaire underscore these findings, focusing on the whole-of-government approach. Just under half of the 29 respondents reported a national privacy strategy or whole-of-government approach to privacy (Figure 6.6). Of those countries, only four positively stated they have a national privacy strategy. Other countries noted alternative means of whole-of-government co-ordination, such as through legislation, the privacy enforcement authority or other dedicated entity or forum, or other policy instruments. Respondents also described several other co-ordination mechanisms. These included a joint statement of PEAs in the country to improve co-ordination of complaint handling and enforcement, as well as model clauses for ordinances on the protection of personal information.

Figure 6.6. Countries with a national strategy for privacy or a whole-of-government approach to it, 2019



Note: Of the countries that responded “yes”, four had a national strategy for privacy and the remaining ten adopted a whole-of-government approach to privacy.

Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink  <https://doi.org/10.1787/888934192262>

Countries are adopting policy measures tailored to specific emerging technologies

Legislation and regulation are often the primary response to privacy and data protection in emerging technologies. However, with the progressive digitalisation of the economy and society, legal protection is increasingly recognised as only one element in the toolkit. Policy measures are also needed ranging from education and innovation to self-regulation. In addition to regulatory reforms and innovation,

countries are thus developing new data governance frameworks, creating new bodies or institutions, and offering guidance on specific technologies.

- **New frameworks.** Twelve countries responding to the 2019 OECD Privacy Guidelines questionnaire reported they are addressing, or are planning to address, technological challenges through new national data governance frameworks. For example, they are setting additional norms on the management of the availability, accessibility, usability, quality, interoperability and ownership of the data collected, processed and stored. Nine of those 12 countries have or are developing sector-specific data strategies or a national data strategy. Respondents had different perceptions of what data governance frameworks encompass. Some had a more limited scope, such as Notifiable Data Breach schemes and frameworks for specific technologies including AI.³ Others had more holistic approaches such as national data strategies and Digital Charters.
- **New bodies or institutions.** Just over a quarter of the respondents reported establishing new institutions, bodies or centres to address the privacy and data protection challenges posed by technology. For example, the United Kingdom recently established a Centre for Data Ethics and Innovation. It identifies ethical issues raised by emerging technologies, agrees on best practices around data use and develops potential new regulations to “build trust and enable innovation in data-driven technologies” (UK Department for Digital, Culture, Media & Sport, 2018_[31]). Singapore, Canada and Slovenia have recently established AI advisory councils, research centres or institutes to advise their governments on issues that arise from AI and may require policy intervention.
- **Guidance on specific technologies.** Most respondents reported having issued guidance on technology-related aspects of privacy and personal data protection. This included privacy or data protection impact assessments, targeted advertising, AI, IoT and app development. Certain countries also mentioned areas for guidance such as data analytics, connected cars, data protection by design, direct-to-consumer genetic testing, smart cities and drones, blockchain and data sharing.

Countries are protecting children’s privacy in the digital environment through legislation and policy

Data protection and privacy legislation provides for a variety of ways to protect individuals’ – including children’s – right to privacy. Countries are striving to provide additional and complementary policy responses to enhance the protection of children’s privacy (OECD, 2019_[22]). At the domestic level, in response to a 2017 OECD survey, almost all countries reported their privacy laws include specific provisions regarding the protection of children.

The entry into force of the GDPR is an important development for children’s privacy at the international and regional level. It recognises that children merit special protection in regard to their personal data, particularly in relation to marketing and the collection of data. The GDPR states that children should be able to understand any communication and information addressed to them. It also grants data subjects the right to request erasure of their personal data (the “right to be forgotten”). This can be an especially important right for children, given their digital identity is increasingly cultivated from a very young age.

The European Union’s Audio-visual Media Services Directive, amended in 2018, provides special protection for children in the processing of their data. It states that the personal data of minors generated by media service providers should not be processed for commercial purposes. This includes uses such as profiling, marketing and behaviourally targeted advertising.

The Council of Europe recently approved guidelines to respect, protect and fulfil the rights of the child in the digital environment. They also guide member states on the data protection and privacy of children. In addition, they underline that the protective responsibility of actors is tied to how children themselves can manage and protect their own privacy (Council of Europe, 2018_[32]).

OECD countries differ in approaches to notice and consent for the collection, processing and sharing of children’s personal data. In most countries, a data processor has to obtain parental consent before processing a child’s data, although the age of legal obligation for parental consent varies (OECD, 2019_[22]). According to the GDPR, the processing of personal data of a child under the age of 16 is lawful “only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.” In the United States, the Children’s Online Privacy Protection Act prevents the collection, use or disclosure of personal information of children under the age of 13 without parental consent.

Ongoing efforts to strengthen compliance with, and enforcement of, privacy and data protection frameworks

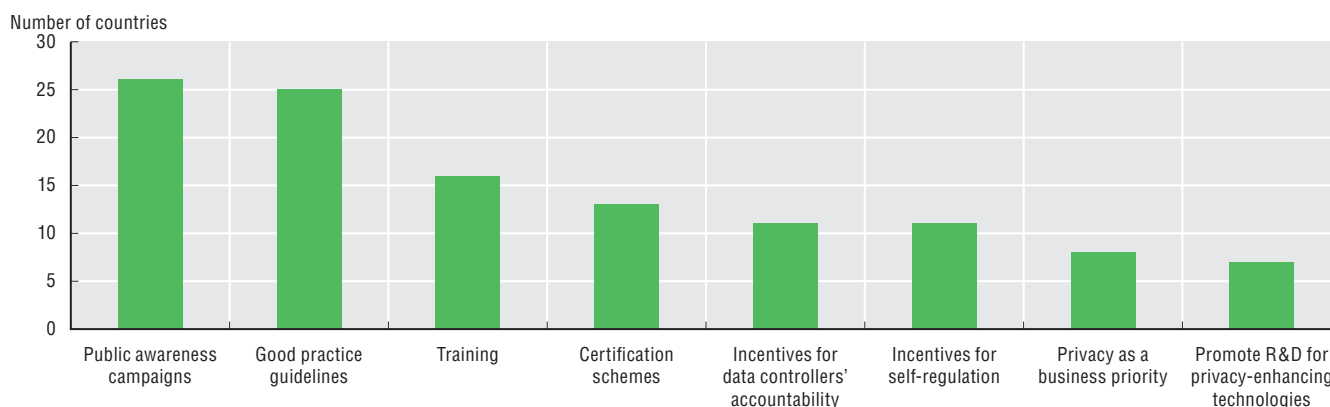
As more privacy and data protection frameworks are enacted, attention has begun to shift to enhancing compliance with those frameworks, including by strengthening enforcement. In particular, governments are investing in policy measures to enhance awareness of requirements in privacy and data protection frameworks. There is also a strong emphasis on promoting data controllers' accountability, along with engaging in international enforcement co-operation. These are discussed in turn below.

Raising awareness

The vast majority of countries implement measures to enhance individuals' awareness and understanding of their personal data rights. Results from the 2019 OECD Privacy Guidelines Questionnaire indicate that measures include education and awareness-raising campaigns, online trainings, social media, educational material, dedicated sessions or workshops and general campaigns. A large majority of countries also conducted education programmes and informed the public on the role of the PEA. And over a third of countries said their PEAs issued guidance to consumers regarding redress for possible privacy violations.

Countries also reported deploying an array of policy measures to promote businesses' awareness of and compliance with privacy and data protection frameworks. These are primarily public awareness campaigns and good practice guidelines (Figure 6.7).

Figure 6.7. Policy measures by governments or PEAs to further privacy and data protection by businesses, 2019



Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink  <https://doi.org/10.1787/888934192281>

In more than 82% of responding countries, PEAs have issued guidance or official position papers in relation to privacy or data protection impact assessments (15 countries), consent forms (12 countries), guidance to consumers for redress on possible privacy violations (11 countries), targeted advertising and AI (9 countries each). In addition, 38% of responding countries are implementing incentives for self-regulation by businesses. Only four respondents reported having mechanisms to assess the impact or success of the measures deployed. Such mechanisms include quarterly statistics on specific policies, regular surveys and analysis of web traffic (including of social media awareness-raising campaigns).

The Privacy Guidelines mention in particular “the promotion of technical measures which help to protect privacy” as one means of national implementation (paragraph 19 g). Here, the picture is mixed. A quarter of respondents have no guidance or other means to encourage adoption of technical measures for privacy protection. These could include anonymisation, cryptography, de-identification, differential privacy and pseudonymisation. Generally, national implementation involves guidance, recommendations or reports by PEAs on the application of privacy-enhancing technologies, primarily pseudonymisation and anonymisation.

Respondents mentioned several other measures related to the business sector. PEAs conducted privacy compliance assessments or audits to raise awareness, provided self-assessment tools to organisations and offered training and educational resources on their websites. Respondents also operated an

6. PRIVACY AND DATA PROTECTION

enquiries or reporting line. They convened multi-stakeholder dialogues on specific issues and held workshops, briefing sessions and town-hall meetings. Almost half of responding countries mentioned certification schemes to further privacy and data protection by businesses.

Promoting accountability

As mentioned above, countries and PEAs are increasingly looking towards data controllers' accountability to promote compliance with privacy and data protection frameworks. Accountability was one of eight basic principles in the original 1980 Privacy Guidelines. It requires data controllers to be accountable for complying with privacy protection rules and decisions, irrespective of whether another party processes the data on their behalf. Still, nothing in the Privacy Guidelines prevents others from also being accountable (OECD, 2013^[33]).

Unlike in 1980, accountability is no longer synonymous with compliance with legal obligations. Accountability now entails a risk-based approach to privacy and implementing a comprehensive privacy management programme. The 2013 revision of the Privacy Guidelines (OECD, 2013^[36]) introduced this concept along with other safeguards to comply with privacy best practices. Countries consider accountability to have an important role in personal data protection, and this will only continue to grow as accountability can aid enforcement.

Nonetheless, the exact meaning and requirements of accountability are unclear. There is growing consensus that accountability should also be about organisations being responsive. It should create value for individuals and society, as well as for one's own organisation. The concept of "accountability 2.0" or "ethical accountability" has recently emerged. This reflects the need for data controllers to be aware of and accountable for the broader social implications of data processing.⁴

Policy measures are being adopted to promote accountability

In their responses to the 2019 OECD Privacy Guidelines Questionnaire, 38% of countries said they were applying "incentives for data controllers' accountability" as part of their policy measures to further privacy and data protection by businesses. These included measures on transparency reporting and enforcement of personal data breach notifications. Answers also referred to accountability and good practice guides. These focused on data protection-management programmes and on managing data breaches (including a focus on small and medium-sized enterprises or on specific sectors). In addition, respondents mentioned software to promote data protection impact assessments. Some countries expressed a need for further clarity on other areas. They sought guidance on practical mechanisms to implement accountability, including to whom data controllers are accountable. They also noted the need for more information on the impact of emerging technologies on organisational accountability.

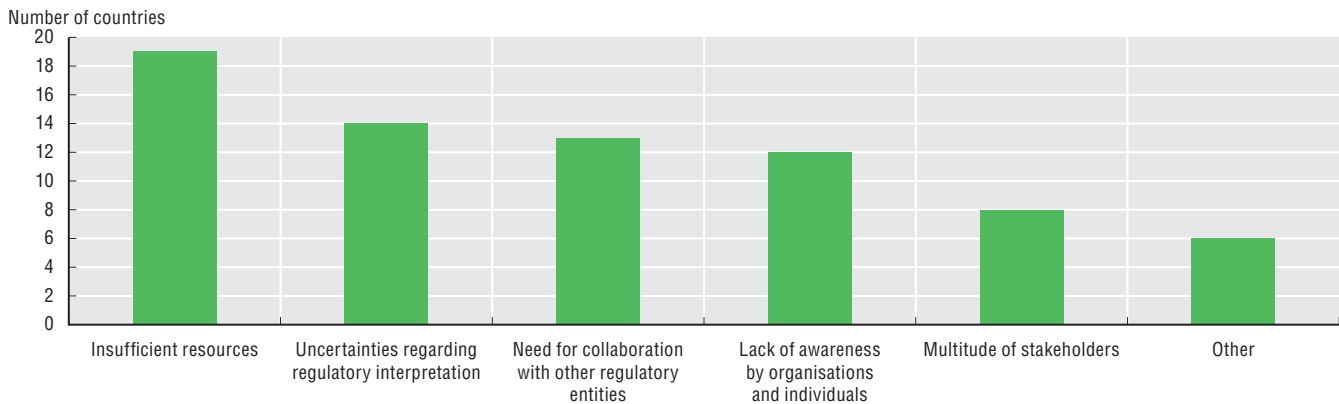
Personal data breach notification (PDBN) is another important aspect of accountability. In a 2019 OECD survey of PEAs, many countries said they had introduced mechanisms for mandatory PDBN reporting. Of the 35 respondent authorities, all EU authorities answered they have mandatory PDBN reporting to one or more authorities (compulsory under the GDPR). Half of the non-EU/GDPR countries have introduced mandatory PDBN reporting to the authority, while four said they expected to introduce such a law within the next two years. For example, through the Notifiable Data Breach scheme in Australia, entities are legally obliged to carry out an assessment whenever they suspect a data breach. They are also required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) (OAIC, 2019^[34]).

Enforcement

All but two respondents to the 2019 OECD Privacy Guidelines Questionnaire reported having established PEAs, generally to oversee both the private and public sectors. Two countries from outside the OECD reported passing relevant legislation, but had not yet established a national PEA. All countries reported their PEAs collaborate with other authorities, notably those addressing consumer protection and digital or cybersecurity issues. And all but one country have given their PEA and other enforcement authorities key powers. These are the ability to implement sanctions; award remedies; and employ other enforcement mechanisms in cases of failure to comply with privacy and data protection laws. Countries generally apply monetary sanctions and enforcement notices, as well as enforce corrective action and restrict data processing.

When asked about enforcement challenges, countries most often cited insufficient resources, followed by uncertainty in interpreting regulatory frameworks (Figure 6.8). Nearly 45% of respondents considered the need for collaboration with other regulatory authorities, such as competition or consumer protection, as an enforcement challenge. At the same time, all reported that such collaboration was taking place.

Figure 6.8. Main challenges to enforcement, 2019



Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink  <https://doi.org/10.1787/888934192300>

A related challenge involves increasing complexities associated with the types of actors involved in data collection, processing and use. The traditional concepts of a data controller and processor may not encompass all actors that play a role in data protection. In particular, national legislation and other frameworks are increasingly allocating responsibilities among data processors, data controllers, agents, supervisory authorities and other actors.

Policy makers need to strike a fine balance between flexibility and accountability. On the one hand, they need to remain flexible in terms of allocating responsibilities to other actors in accordance to their roles. On the other, they must ensure all actors are held to account in their collection, processing and use of personal data. The responsibility of actors other than data controllers will likely continue to be an open question in 2020 and beyond.

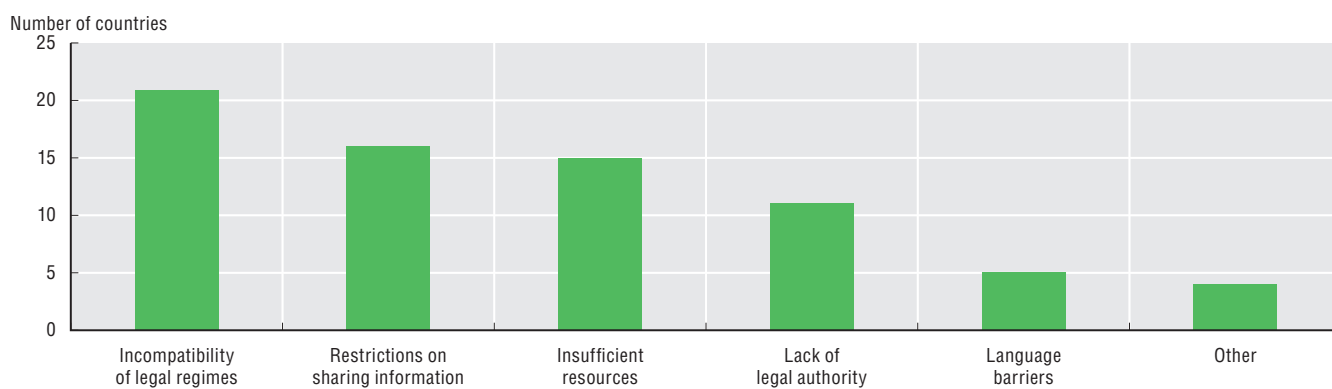
International enforcement co-operation

There is increasing emphasis on international enforcement co-operation, particularly in light of the increased frequency and volume of transborder data flows and influence of regional data protection frameworks. With one exception, all respondents to the 2019 OECD Privacy Guidelines Questionnaire participate in regional and international fora to facilitate co-operation and share information on privacy enforcement (particularly to seek assistance with privacy violations). Participation in the Global Privacy Enforcement Network⁵ was the most popular response. This was followed by the International Conference of Data Protection and Privacy Commissioners (now the Global Privacy Assembly) Enforcement Cooperation Arrangement and the APEC Privacy Cross-border Privacy Enforcement Arrangement.

Despite progress, countries also consider that incompatibility of legal privacy regimes is one of the main reasons that enforcement co-operation has not improved (Figure 6.9). Most countries are also dealing with restrictions on sharing information and insufficient resources for enforcement.

Approximately two-thirds of countries responding to the questionnaire said their PEA had sought assistance from, or referred a privacy violation complaint to, a PEA in another country and/or vice versa. Only four countries reported their PEA had declined another country's request for assistance. One country explained that its PEA cannot always provide the full assistance requested but will generally try to assist within the scope of its legal abilities.

Figure 6.9. Main challenges to cross-border enforcement co-operation, 2019



Source: 2019 OECD Privacy Guidelines Questionnaire.

StatLink  <https://doi.org/10.1787/888934192319>

References

- Australian Government (2017), *Information about the Data Integration Partnership for Australia*, Department of the Prime Minister and Cabinet, Data and Digital Branch, <http://www.pmc.gov.au/sites/default/files/publications/DIPA-information.pdf>. [19]
- Auxier, B. et al. (2019), *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over their Personal Information*, Pew Research Center, Internet & Tech, 15 November, <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>. [15]
- Burns, T. (ed.) (2019), *Educating 21st Century Children: Emotional well-being in the digital age*, Educational Research and Education, OECD Publishing, Paris, <https://doi.org/10.1787/b7f33425-en>. [22]
- Centre for Information Policy Leadership (2018), *The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society*, July, <http://bit.ly/2koS7IT>. [39]
- Council of Europe (2020), *Joint Statement by Alessandra Pierucci and Jean-Philippe Walter on the Right to Data Protection in the Context of the COVID-19 Pandemic*, Council of Europe, Strasbourg, <https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter>. [4]
- Council of Europe (2018), *Guidelines to Respect, Protect and Fulfil the Rights of Children in the Digital Environment*, Council of Europe, Strasbourg, <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html>. [32]
- Council of Europe (1981), *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS No. 108, Council of Europe, Strasbourg. [28]
- Docksey, C. (2019), “Keynote on accountability”, 41st Conference of Data Protection and Privacy Commissioners, Tirana, 24 October. [38]
- EDPB (2020), *Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak*, adopted on 19 March, European Data Protection Board, Brussels, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. [5]
- EDPB (2019), *1 Year GDPR - Taking Stock*, European Data Protection Board, Brussels, 22 May, https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en. [7]
- European Commission (2020), *A European Strategy for Data*, European Commission, Brussels, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. [6]
- European Commission (2019), *Study on Broadband Coverage in Europe 2018*, European Commission, Brussels, <https://ec.europa.eu/digital-single-market/en/news/study-broadband-coverage-europe-2018> (accessed on 21 October 2020). [17]
- European Union (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 (GDPR)*, O.J. (L 119) 32, European Union, Brussels, <http://data.europa.eu/eli/reg/2016/679/oj>. [26]
- European Union (1995), *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, O.J. (L 281), European Union, Brussels. [27]
- GPEN (2018), *GPEN Sweep 2018: Privacy Accountability*, Office of the Privacy Commissioner, New Zealand and Information Commissioner's Office, United Kingdom, October, <https://ico.org.uk/media/about-theico/documents/2614435/gpen-sweep-2018-international-report.pdf> (accessed on 28 October 2020). [40]
- Graham-Harrison, E. and C. Cadwalladr (2018), “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, *The Guardian*, 17 March, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (accessed 21 October 2020). [10]
- Granville, K. (2018), “Facebook and Cambridge Analytica: What you need to know as fallout widens”, *The New York Times*, 19 March, <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> (accessed 21 October 2020). [9]
- Hern, A. and D. Pegg (2018), “Facebook fined for data breaches in Cambridge Analytica scandal”, *The Guardian*, 11 July, <https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal>. [11]
- Hof, S. (2017), “I agree...or do I? - A rights based analysis of the law on children’s consent in the digital world”, *Wisconsin International Law Journal*, Vol. 34, https://openaccess.leidenuniv.nl/bitstream/handle/1887/58542/S_van_der_Hof_-_I_AGREE._._._OR_DO_Ioe1oe.pdf?sequence=1. [23]

6. PRIVACY AND DATA PROTECTION

References and Notes

- IBM Security (2019), *Cost of a Data Breach Report*, IBM, Armonk, New York, <https://databreachcalculator.mybluemix.net/>. [13]
- IDC and Lisbon Council (2018), *Updating the European Data Market Monitoring Tool*, https://datalandscape.eu/sites/default/files/report/EDM_D2.1_1stReport-FactsFigures_revised_21.03.2018.pdf (accessed 21 October 2020). [18]
- Information Commissioner's Office (2018), *Monetary Penalty Notice to Facebook Ireland Ltd*, 24 October, Information Commissioner's Office, Wilmslow, United Kingdom, <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>. [8]
- Irwin Reyes et al. (2018), "Won't somebody think of the children?": Examining COPPA compliance at scale", *Proceedings on Privacy Enhancing Technologies*, Vol. 3, pp. 63-83, <https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf>. [25]
- Livingstone, S., M. Stoilova and R. Nandagiri (2018), "Conceptualising privacy online: What do, and what should, children understand?", LSE blog, <https://blogs.lse.ac.uk/medialse/2018/09/07/conceptualising-privacy-online-what-do-and-what-should-children-understand/>. [21]
- Norwegian Consumer Council (2017), "Significant security flaws in smartwatches for children", *Forbrukerradet*, 18 October, <https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/>. [24]
- OAG (2020), "California Consumer Privacy Act (CCPA)", webpage, <https://oag.ca.gov/privacy/ccpa> (accessed on 21 October 2020). [30]
- OAIC (2019), *Notifiable Data Breaches Scheme 12-month Insights Report*, Office of the Australian Information Commissioner, Sydney, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/>. [34]
- OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/eedfee77-en>. [35]
- OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/276aaca8-en>. [3]
- OECD (2019), "Protection of Children in a Connected World", OECD– University of Zurich Expert Consultation 15-16 October, University of Zurich, internal document. [20]
- OECD (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, <https://doi.org/10.1787/b2023a47-en>. [29]
- OECD (2018), *Towards National Privacy Strategies (NPS)*, Final report, internal document, OECD, Paris. [37]
- OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264276284-en>. [2]
- OECD (2015), "Assessing government initiatives on public sector information: A review of the OECD Council Recommendation", *OECD Digital Economy Papers*, No. 248, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5js04dr9l47j-en>. [1]
- OECD (2013), *The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines*, OECD, Paris, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [33]
- OECD (2013), *OECD Privacy Framework*, OECD Publishing, Paris, www.oecd.org/internet/ieconomy/privacy-guidelines.htm. [36]
- OPC (2019), *2018-2019 Survey of Canadians on Privacy*, Office of the Privacy Commissioner of Canada, Ottawa, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#fig03. [14]
- Otaka, T. (2015), "Japan Pension Service hack used classic attack method", *The Japan Times*, 2 June. [12]
- UK Department for Digital, Culture, Media & Sport (2018), *Centre for Data Ethics and Innovation Consultation - Consultation Outcome*, <https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation>. [31]

Notes

1. This questionnaire was conducted as part of the current review of the implementation of the OECD Privacy Guidelines. It asked countries questions pertaining to national and international privacy and data protection developments (regulations, policies and technology) and on the relevance of the guidelines. Twenty-nine countries responded by the due date, 14 February 2020: 26 OECD countries (Australia, Canada, Chile, Colombia, Denmark, Estonia, Finland, France, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, New Zealand, Norway, Portugal, the Slovak Republic, Slovenia, Switzerland, Turkey, the United Kingdom and the United States) and three partner economies (Brazil, Singapore and Thailand).
2. The 2005 APEC Privacy Framework, revised in 2015, was drafted to protect information privacy, while maintaining information flows among economies in the Asia-Pacific region and their trading partners. It provides that member economies should take all reasonable and appropriate measures to remove unnecessary barriers to data flows and avoid the creation of such barriers.
3. Chapter 5 of OECD (2019^[35]) provides a general overview of countries' AI policies and initiatives. The OECD AI Policy Observatory (OECD.AI, launched in February 2020) hosts a database of national AI strategies and policies.
4. See further, for example, Docksey, C. (2019^[38]); Centre for Information Policy Leadership (2018^[39]); and GPEN (2018^[40]).
5. The Global Privacy Enforcement Network (GPEN) is an informal group that facilitates co-operation and the sharing of information between privacy enforcement authorities. Created by the OECD in 2010, the GPEN has 50 members that navigate the practical aspects of privacy enforcement co-operation. This includes issues in relation to cross-border investigations, joint enforcement and awareness campaigns and effective communication between the public and private sectors.



From:
OECD Digital Economy Outlook 2020

Access the complete publication at:

<https://doi.org/10.1787/bb167041-en>

Please cite this chapter as:

OECD (2020), "Privacy and data protection", in *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/153ac49f-en>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.