Organisation for Economic Co-operation and Development

C(2021)42

For Official Use English - Or. English

17 March 2021

COUNCIL

Council

REPORT ON THE IMPLEMENTATION OF THE RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

(Note by the Secretary-General)

JT03473010

1. This document presents, in its Annex, a report by the Committee on Digital Economy Policy (CDEP), developed through its Working Party on Data Governance and Privacy (DGP), on the implementation, dissemination and continued relevance of the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] (hereafter, the "Recommendation") and conclusions on whether the instrument requires revision or further actions to support its dissemination and implementation.

Background

2. The Council adopted the Recommendation on 23 September 1980 to address concerns arising from the increased use of personal data and the risk to economies resulting from restrictions to the flow of information across borders [C(80)58/FINAL; C/M(80)17/PROV]. The Guidelines governing the protection of privacy and transborder flows of personal data (hereafter the "Privacy Guidelines"), set out in the Annex to the Recommendation, represented the first internationally agreed set of privacy principles applicable to the protection of personal data, whether in the public or private sectors. In the four decades since their adoption, the Privacy Guidelines have significantly influenced legislation and policy in Member and non-Member countries having adhered to the Recommendation (hereafter "Adherents")[1] and beyond.

3. Initiated in 2010, the first review of the Recommendation and the Privacy Guidelines culminated in a revision of the Recommendation and the Privacy Guidelines, adopted by the Council on 11 July 2013 [C(2013)79, C/M(2013)15/REV1]. The 2013 revision reaffirmed the validity and pertinence of the eight "basic principles of national application" in Part Two of the Privacy Guidelines (hereafter "the basic principles"), namely collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The 2013 revision also introduced a number of new concepts, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other revisions expanded or updated existing provisions of the Privacy Guidelines, for instance those related to the accountability of data controllers, transborder data flows and privacy enforcement and international co-operation. A new Supplementary Explanatory Memorandum was also developed to provide context and rationale for the revision. It was intended to supplement – not replace – the original Explanatory Memorandum, which remains relevant for interpreting the aspects of the Privacy Guidelines that were not revised (OECD, 2013, p. 5[1]) .

4. In paragraph III of the Recommendation (as revised in 2013), the Council instructed the Committee for Information, Computer and Communication Policy (now the Committee on Digital Economy Policy, CDEP) to "monitor the implementation of the [revised] Recommendation, review that information, and report to the Council within five years of [its] adoption and thereafter as appropriate". This Report sets out the results of this review, including information on progress made across Adherents in the implementation and dissemination of the Recommendation, as well as considerations with respect to its continued relevance and whether it needs revision. It also recommends further actions to support the Recommendation's implementation, dissemination and continued relevance in

[1] To date the Recommendation has no non-Member adherents.

light of ongoing changes, in particular relating to emerging technologies and regulatory developments.

Methodology

5. The former Working Party on Security and Privacy in the Digital Economy ("SPDE" – now replaced by the DGP and the Working Party on Security in the Digital Economy (SDE)) adopted the methodology and process for the review of the implementation of the Privacy Guidelines at its November 2018 meeting [DSTI/CDEP/SPDE(2018)8; DSTI/CDEP/SPDE/M(2018)2].

6. The Report is based on: (i) the responses of 28 Adherents[2] and three non-OECD Member Participants in the CDEP (referred to together hereafter as "Respondents")[3] to a questionnaire shared by the Secretariat in 2019 on national and international developments and on the relevance of the Privacy Guidelines; (ii) thematic expert roundtables dedicated to exploring the main challenges for privacy and personal data protection in the current digital environment; (iii) focused thematic reports, including on data localisation and transparency reporting; (iv) input from relevant work streams, notably the work on artificial intelligence, enhanced access to and sharing of data, data portability and personal data breach notification; and (v) discussions in conference calls, workshops, and comments by an ad hoc informal advisory group of experts (the Privacy Guidelines Expert Group, hereafter "PGEG"), consisting of over 60 experts from governments, business, civil society, and academia, co-chaired by Ms. Jennifer Stoddart (former Privacy Commissioner of Canada and current strategic advisor at Fasken) and Mr. Gwendal Le Grand (Deputy-Secretary General of the Commission nationale de l'informatique et des libertés, "CNIL").

Process

7. Noting the instruction to review and report set out in paragraph III of the Recommendation, the CDEP, in its 2016 Standard-setting Action Plan, included monitoring the implementation of the Recommendation as the appropriate action [DSTI/CDEP(2016)8]. Subsequently, at its November 2018 meeting, the former SPDE discussed the purpose of this review, noting that it should "examine what measures have been and are being taken by governments to implement [the Privacy Guidelines], with a view to identifying good practices and providing governments with tools for implementation" [DSTI/CDEP/SPDE(2018)8].

8. A first draft of this report was discussed in the DGP in its November 2019 [DSTI/CDEP/DGP(2019)1, DSTI/CDEP/DGP/M(2020)1]. Comments from the discussion and received in writing thereafter were integrated into a revised draft, which was in turn discussed in the DGP's April 2020 meeting [DSTI/CDEP/DGP(2019)1/REV1, DSTI/CDEP/DGP/M(2020)3].

9. Following the integration of comments received from DGP delegates in the April 2020 meeting and in writing, as well as input received from the PGEG, a further revised

[2] Australia, Canada , Chile, Colombia, Denmark, Estonia, Finland, France, Germany, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Switzerland, Turkey, the United Kingdom, and the United States.

[3] Brazil, Singapore and Thailand.

version of the Report was discussed by the DGP at its meeting of 17 November 2020, and by the CDEP at its meeting on 30 November 2020 [DSTI/CDEP/DGP(2019)1/REV2]. Delegates also submitted further written comments following these meetings, which were incorporated together with comments coming out of the discussions themselves. CDEP approved the Report by written procedure on 12 March 2021 [DSTI/CDEP/DGP(2019)1/REV3], for transmission to Council.

10. The Council is now invited to note and declassify the final Report, as set out in the Annex. Thereafter, a link to the Report will be included in the public webpage of the Recommendation on the online Compendium of OECD legal instruments. Further, the implementation section of the report will be excerpted and published along with related working documents separately online.

Dissemination

11. Under Paragraph I of the Recommendation, the Council instructed Adherents to "[d]isseminate [it] throughout the public and private sectors".

12. The Privacy Guidelines are recognised as the global minimum standard for privacy and data protection and are consistently featured in timelines and histories of the development of data protection and privacy laws. Adherents repeatedly refer to them as forming the bedrock of their own national frameworks. They are widely recognised also as forming the basis of other data protection frameworks such as the APEC Privacy Framework, expanding their reach beyond OECD membership.

13. In addition to dissemination efforts by Adherents, the OECD Secretariat actively promotes the Recommendation and the Privacy Guidelines at events attended by governments, privacy enforcement authorities, the private sector, civil society, academia and other stakeholders including meetings of the G20, the Global Privacy Assembly ("GPA", previously known as the International Conference of Data Protection and Privacy Commissioners); the Computers, Privacy and Data Protection conference (CPDP); and the Asia Pacific Privacy Authorities (APPA) Forum.

14. The COVID-19 pandemic has further highlighted the importance of the Privacy Guidelines, and the OECD has drawn attention to their importance in this context, for instance through :

- policy notes on the Digital Hub on Tackling the Coronavirus (COVID-19) in relation to contact tracing, privacy, data protection, security, and consumer-facing issues[4]; and
- two virtual workshops on the data governance and privacy challenges associated with COVID-19 with the support of the GPA.

15. The first workshop, on 15 April 2020, attracted more than 260 high-level international representatives active in implementing data protection and privacy approaches as part of the global COVID-19 pandemic response. These ranged from GPA member authorities, data protection and privacy experts, to representatives of civil society

[4] Available at <http://www.oecd.org/coronavirus/en/>. Relevant policy notes include OECD, "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics" (2020); OECD, "Ensuring data privacy as we battle COVID-19" (2020); OECD, "Combatting COVID-19 disinformation on online platforms" (2020); and OECD, "Dealing with digital security risk during the Coronavirus (COVID-19) crisis" (2020).

stakeholders, government and technologists leading the charge in developing mobile applications to address the crisis. The workshop represented one of the first international forums through which this community engaged collectively with policy makers and experts to address the privacy challenges raised by the current crisis, including with common guidance and common messages upholding the Privacy Guidelines as minimum standards for data protection and privacy.

16. A follow-up workshop with more than 170 participants from governments, data protection authorities, the private sector, academia, civil society, and international organisations was held on 16 September 2020, again with the support of the GPA. The workshop provided a forum for all stakeholders to anticipate future challenges and to discuss how to deal with them.

17. The Secretariat and Adherents will continue to raise awareness of the Recommendation and the importance of respecting data protection and privacy principles, during the COVID-19 crisis and beyond.

Summary and conclusions

18. This review confirms the continuing importance of the Privacy Guidelines as an international reference on minimum standards for privacy and personal data protection that Adherents implement in practice through legislation, enforcement and policy measures. Framed in concise and technology-neutral language, the principle-based approach of the Privacy Guidelines is widely recognised not only as a solid foundation for building effective protection and trust for individuals, but also for developing common international approaches to transborder data flows.

19. The COVID-19 crisis has highlighted the role that digital technologies and data could play in helping economies weather the pandemic, and has put into sharp focus the continued relevance of the Privacy Guidelines' basic principles, which give Adherents a clear indication of the standard level of protections expected by the global community. These are principles concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The unprecedented efforts to monitor individuals' compliance with lockdown and quarantine provisions, and to track, trace and contain the spread of the pandemic have, however, also brought renewed attention to the societal impacts of the collection and processing of mass amounts of personal data and the relationship between the protection of privacy and individual liberties, fundamental values and democracy. This monitoring has intensified calls for the OECD to champion a holistic approach to privacy and data protection practices, that is an approach that takes into account multiple societal objectives including the collective and ethical dimensions of personal data processing.

20. In the implementation of the Recommendation during the past few years, common approaches have surfaced. In particular, and as reflected in the questionnaire, all Respondents have: enacted privacy and data protection legislation; established (or are in the process of establishing) Privacy Enforcement Authorities; participated in international fora for cross-border privacy enforcement co-operation; and adopted a range of approaches to enable transborder flows of personal data.

21. Most Respondents report having reformed existing laws consistent with the strengthened aspects of the Privacy Guidelines. One notable example is data breach notification laws, covering both notice to an authority and affected individuals. All Respondents also deploy a range of complementary policy measures to promote the

implementation of the different parts of the Privacy Guidelines (education and awareness raising, skills development, and the promotion of technical measures), indicating rising awareness that privacy laws are necessary but not sufficient.

22. Notwithstanding this progress, the analysis of the implementation of the Recommendation across Adherents has identified a number of significant challenges in implementing the Privacy Guidelines, especially against the backdrop of technological developments which continue to evolve and to create tensions with established legal norms. Since the 2013 review of the Privacy Guidelines, personal data have come to play an even more important role in our economies, societies and everyday lives. Close to real-time collection and analysis of large volumes of data, generated from a myriad of devices, transactions, production and communication processes coupled with the increasing use of artificial intelligence (AI) are accelerating knowledge and value creation across society. These trends in data collection, analysis and use are transforming business models and organisational practice across all sectors of our economies. They also pose challenges to the implementation of current privacy legislation, to enforcement, to accountability models and to existing frameworks for transborder data flows. Several of these issues require further exploration to ensure the Recommendation and the Privacy Guidelines remain relevant in the context of changing technological conditions and regulatory developments.

23. Adherents overwhelmingly indicated that in addressing such issues, revisions of the Privacy Guidelines themselves are not necessary at this time, and recommended to focus on the development of further implementation guidance and, possibly, revisions to the Supplementary Explanatory Memorandum.

24. Respondents specifically noted three areas where additional guidance and/or revisions to the Supplementary Explanatory Memorandum were considered necessary. The first relates to the need for further guidance on the implementation of the accountability principle set out in Part Three of the Privacy Guidelines, and for information on best practices as to how to strengthen the role of enforcement and of Privacy Enforcement Authorities. The original interpretation of accountability, namely, compliance with legal obligations, was also identified as requiring evolution in the context of emerging technologies, such that organisations would be required to proactively act as responsible and ethical stewards of personal information. Further clarification on the role of all actors handling personal data was also identified as potentially important, including to ensure that data processors and controllers understand their respective obligations and can minimise risks to individuals and organisations (including legal and reputational risks).

25. The second relates to data localisation, an issue that has gained prominence since 2013 and may directly and significantly impact transborder data flows. Adherents indicated that they would benefit from concrete further guidance on the implementation of paragraph 16 of Part Four, which states that a data controller remains accountable for personal data under its control without regard to the location of the data; and from a review of current practice in the proportionality assessment articulated in paragraph 18 of Part Four. Respondents also indicated that it would be important and urgent to further examine good practices among Adherents concerning ‘guarantees’ or ‘restraints’ on government access to data held by the private sector to ensure trust in data flows. This work would provide an opportunity for Adherents to converge around the circumstances in which government access to privately-held data is appropriate, in stark contrast to access practices of some authoritarian regimes.

26. Third, although the Privacy Guidelines already provide for many protections for data subjects under the individual participation principle, additional work is needed to

clarify the application of the Privacy Guidelines to specific developments in the privacy and personal data protection sphere. These include in particular work to strengthen data subject rights (such as the right to data portability, right to correction and erasure, right to object to automated decision making) for which no clear direction has as yet emerged as to what changes or additional guidance, may be needed for such rights to be adequately addressed by the Privacy Guidelines.

27. Further analytical work was also recommended in areas such as regulatory sandboxes, certification schemes for business, transparency reporting, and privacy enhancing technologies. Specifically, Adherents and experts agreed that a greater understanding of the benefits and risks of regulatory sandboxes aided by a common terminology and set of use cases would likely prove useful for any future developments.

28. It is therefore proposed that the CDEP, through the DGP, explore these issues further and develop additional guidance on the implementation of the Recommendation and Privacy Guidelines, as well as draft amendments to the Supplementary Explanatory Memorandum where appropriate. Further, it is proposed that the DGP report to the CDEP on specific developments in this regard by the end of 2021. More broadly, it is proposed that the CDEP, through the DGP, continue to review the implementation, dissemination and continued relevance of the Recommendation and report thereon to the Council in five years.

Proposed Action

29. In the light of the preceding, the Secretary-General invites the Council to adopt the following draft conclusions:

THE COUNCIL

a) noted document C(2021)42, in particular the report set out in its Annex, and agreed to its declassification;

b) encouraged Adherents to the Recommendation to continue their efforts to implement and disseminate the Recommendation and to address the main findings and challenges identified in the summary and conclusions section of the report;

c) invited the Committee on Digital Economy Policy, through the Working Party on Data Governance and Privacy, to:

i. support further dissemination and implementation of the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data;

ii. support Adherents in addressing the findings and challenges identified in the summary and conclusions section of the report;

iii. report to the Council in five years on the implementation, dissemination and continued relevance of the Recommendation.

ANNEX. REPORT ON THE IMPLEMENTATION OF THE RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

Table of Contents

Tables

Figures

Boxes

1. Background

1. The Council adopted the Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] on 23 September 1980 [C(80)58/FINAL; C/M(80)17/PROV] (hereafter, the "Recommendation") and it was revised on 11 July 2013 [C(2013)79 C/M(2013)15/REV1].

2. The Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereafter, the "Privacy Guidelines"), set out in the Annex to the Recommendation and forming an integral part of it, were the first internationally agreed upon set of privacy principles applicable to the protection of personal data, whether in the public or private sectors.

3. Recognising the common interest in promoting and protecting both privacy and global free flow of information, they aim to further advance the free flow of information and "avoid the creation of unjustified obstacles". The Privacy Guidelines are intended as minimum standards for adoption in domestic legislation regarding the protection of personal data and set out eight "basic principles of national application" in Part Two (hereafter "basic principles"). These are: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The validity and pertinence of these basic principles was reaffirmed in context of the 2013 revision.

4. Part Three of the Privacy Guidelines, which was added in the 2013 revision, provides guidance on the implementation of the accountability principle. The Privacy Guidelines further include a section on international application and legitimate restrictions on the free flow of personal data (Part Four), a section on means for national implementation of the basic principles (Part Five), and a section on international co-operation and interoperability (Part Six) (OECD, 1980[2]). They were deliberately drafted in technology-neutral language so as to be adaptable to technological and societal changes (OECD, 2013, p. 19[1]).

5. In addition, a new Supplementary Explanatory Memorandum was developed during the 2013 revision to provide context and rationale for the revision. It was intended to supplement – not replace – the original Explanatory Memorandum, which remains relevant for interpreting the aspects of the Privacy Guidelines that were not revised (OECD, 2013, p. 5[1]).

6. The 2013 revision identified profound changes of scale in terms of the role of personal data in economies, societies and daily lives since the Privacy Guidelines' adoption in 1980. It further outlined and foresaw some of the major challenges that today's digital environment is posing for protecting privacy under existing approaches. As reported at the 44th meeting of the former Working Party on Security and Privacy in the Digital Economy (SPDE – " – now replaced by the Working Party on Data Governance and Privacy in the Digital economy (DGP) and the Working Party on Security in the Digital Economy (SDE)) in November 2018 [DSTI/CDEP/SPDE(2018)8], these trends and challenges concern, among others, technological developments such as advanced analytics, artificial intelligence (AI) and the Internet of Things (IoT), increased global data flows, changes in data collecting and sharing practices of organisations and individuals, evolving regulatory frameworks, and intensified security risks. While raising the value and potential benefits of personal data, for example through its secondary use to serve public interest purposes (e.g. the development of national statistics, the development and monitoring of public policies, the tackling of health care and scientific challenges of societal importance), or by driving data-driven innovation and new business models, these trends and challenges also raise questions as to users' consent to, or awareness of, the way their data is being collected and used. The increase in value of personal data as well as the increase of risks and questions associated with their gathering and processing underpins the importance of trust as the foundation of today's digital economy. These

developments set the background for the current review of the implementation of the Privacy Guidelines.

7. In paragraph III of the Recommendation as revised, the Council instructed the Committee for Information, Computer and Communication Policy (now the Committee on Digital Economy Policy, CDEP) to "monitor the implementation of the [revised] Recommendation, review that information, and report to the Council within five years of [its] adoption and thereafter as appropriate". This draft Report sets out the results of this review. It examines the ways in which the Privacy Guidelines are currently being implemented, identifies gaps and outlines possible next steps. The following section describes the methodology for the review. Section 3 explains the process for the draft report's development. Section 4 addresses dissemination. Section 5 provides the main findings, organised according to the Parts of the Privacy Guidelines. Section 6 concludes and proposes next steps.

2. Methodology

8. The methodology for the review of the implementation of the Privacy Guidelines was agreed by the SPDE [DSTI/CDEP/SPDE(2018)8; DSTI/CDEP/SPDE/M(2018)2] in November 2018. It included the following elements:

1. An online survey among Members and non-Members having adhered to the Recommendation (hereafter "Adherents")[5] on national and international developments (regulatory, policies, and technological) and on the relevance of the Privacy Guidelines ("privacy questionnaire") [DSTI/CDEP/SPDE(2019)5]. The survey was circulated in April 2019 to all Adherents to the Recommendation as well as non-OECD Member Participants in the CDEP. Thirty one countries responded to the survey : 28 Adherents (Australia, Canada[6], Chile, Colombia, Denmark, Estonia, Finland, France, Germany, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Switzerland, Turkey, the United Kingdom and the United States) and three non-OECD Members Participants in the CDEP (Brazil, Singapore and Thailand) (hereafter, "respondents" or "responding countries").[7]
2. Thematic roundtables and workshops dedicated to exploring the main challenges for privacy and personal data protection in the current digital environment: Mechanisms for Privacy Interoperability (May 2018 [DSTI/CDEP/SPDE(2018)5/REV2]); Organisational Accountability jointly organised with the Centre for Information Policy Leadership (May 2019 [DSTI/CDEP/SPDE(2019)9]) ; Emerging Enforcement Challenges (November

[5] To date, the Recommendation has no non-Member Adherents.

[6] Canada responded to the survey twice – once for its public sector privacy laws, and once for its private sector privacy laws. Unless specified otherwise, we refer to the latter response when including Canada in the country statistics below.

[7] Unless otherwise specified, the questionnaire allowed countries to select multiple answers for each of the multiple choice questions.

2019) [DSTI/CDEP/DGP(2020)5 ; DSTI/CDEP/DGP/M(2020)2] jointly organised with the UK Information Commissioner's Office and the Electronic Privacy Information Center (EPIC); a virtual scoping Expert Consultation on Unlimited Government Access to Personal Data held by the Private Sector (7 July 2020); a virtual Business at OECD Roundtable on Regulatory Sandboxes (23 September 2020); and a virtual Roundtable jointly organised with Japan's Personal Information Protection Commission (PPC) on Data Localisation and Trusted Government Access to Personal Data held by the Private Sector (5-6 October 2020) [DSTI/CDEP(2020)19];

3. Focused thematic reports, including "Towards National Privacy Strategies" [DSTI/CDEP/SPDE(2018)17], "Data Localisation Trends and Challenges: Considerations for the Review of the OECD Privacy Guidelines" [DSTI/CDEP/DGP(2020)7], and "Transparency Reporting: Considerations for the Review of the OECD Privacy Guidelines" [DSTI/CDEP/DGP(2020)8 and DSTI/CDEP/DGP(2020)8/ANN]; and

4. Input from relevant work streams, notably the work on AI, enhancing access to and sharing of data (OECD, 2019[3]), data portability [DSTI/CDEP/DGP(2019)2], and personal data breach notification [DSTI/CDEP/DGP(2020)1].

9. The review process benefitted from ongoing expert input from an informal ad hoc group of experts (the Privacy Guidelines Expert Group – "PGEG"), consisting of over 60 experts from governments, business, civil society and academia. Over multiple conference calls, workshops and through written comments, the group – co-chaired by Ms. Jennifer Stoddart (former Privacy Commissioner of Canada and current strategic advisor at Fasken) and Mr. Gwendal Le Grand (Deputy-Secretary General of the Commission nationale de l'informatique et des libertés, "CNIL") – provided input into the main challenges in current day privacy and personal data protection, the selection of topics for the Roundtables and Workshops and the selection of questions for inclusion in the privacy questionnaire.

3. Process

10. Noting the instruction to review and report contained in paragraph III of the Recommendation, the CDEP included monitoring the implementation of the Recommendation as the appropriate action in its 2016 Standard-setting Action Plan [DSTI/CDEP(2016)8]. Subsequently, at its November 2018 meeting, the former SPDE discussed the purpose of this review, noting that it should "examine what measures have been and are being taken by governments to implement [the Privacy Guidelines], with a view to identifying good practices and providing governments with tools for implementation" [DSTI/CDEP/SPDE(2018)8].

11. This Report has undergone an extensive fact gathering and inclusive horizontal consultative process designed to ensure all Adherents and experts had the opportunity to comment on its findings and conclusions. PGEG experts provided input through conference calls, roundtables and workshops. A first draft of this report was presented and discussed at the first meeting of the DGP in November 2019 [DSTI/CDEP/DGP(2019)1, DSTI/CDEP/DGP/M(2020)1]. Comments received were integrated into a second draft, presented to and discussed with the DGP at its second virtual meeting in April 2020 [DSTI/CDEP/DGP(2019)1/REV1,

DSTI/CDEP/DGP/M(2020)3]. Thereafter, PGEG experts were invited to provide further comments through roundtables and workshops. All comments received were integrated and a revised third version of the draft report was discussed by the DGP at its virtual meeting of 17 November 2020 and by the CDEP at its meeting on 30 November 2020 [DSTI/CDEP/DGP(2019)1/REV2]. Following the implementation of the final comments received, the Report was transmitted to and approved by the CDEP by written procedure on 12 March 2020 [DSTI/CDEP/DGP(2019)1/REV3], for transmission to the Council to be noted and declassified.

12. Following the report's declassification by the Council, a link to the report will be included in the public webpage of the Recommendation on the online Compendium of OECD legal instruments. Furthermore, the implementation section of the report will be excerpted and published along with related working documents separately online.

4. Dissemination

13. Under Paragraph I the Recommendation, the Council instructed Adherents to "[d]isseminate [it] throughout the public and private sectors". Since their adoption the Privacy Guidelines are regarded as the global minimum standard for privacy and data protection. The Privacy Guidelines are consistently featured in timelines and histories of the development of data protection and privacy laws. Adherents repeatedly refer to them as forming the bedrock of their own national frameworks, and the Privacy Guidelines are widely recognised as forming the basis of other data protection frameworks such as the APEC Privacy Framework, expanding their reach beyond Adherents.

14. The OECD Secretariat actively promotes the Recommendation and Privacy Guidelines at events attended by governments, data protection authorities, the private sector, civil society, academia and other stakeholders. Such events include meetings of the G20, the Global Privacy Assembly (GPA, previously known as the International Conference of Data Protection and Privacy Commissioners); the Computers, Privacy and Data Protection (CPDP) conference; and the Asia Pacific Privacy Authorities (APPA) Forum.

15. Recently, the OECD has reiterated the importance of the Privacy Guidelines in the context of the COVID-19 pandemic through the publication of policy notes on the Digital Hub on Tackling the Coronavirus (COVID-19) in relation to contact tracing, privacy, data protection, security and consumer-facing issues.[8]

16. Over 2020, with the support of the Global Privacy Assembly, the OECD hosted two virtual workshops on the data governance and privacy challenges associated with COVID-19. The first, on 15 April 2020, attracted more than 260 high-level international representatives active in implementing data protection and privacy approaches as part of the global COVID-19 pandemic response. These ranged from GPA member authorities, data protection and privacy experts, to

[8] Available at <http://www.oecd.org/coronavirus/en/>. Relevant policy notes include OECD, "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics" (2020); OECD, "Ensuring data privacy as we battle COVID-19" (2020); OECD, "Combatting COVID-19 disinformation on online platforms" (2020); and OECD, "Dealing with digital security risk during the Coronavirus (COVID-19) crisis" (2020).

representatives of civil society stakeholders, government and technologists leading the charge on development of mobile applications to address the crisis. The workshop represented one of the first international forums through which this community engaged collectively with policy makers and experts to address the privacy challenges raised by the current crisis, including with common guidance and common messages upholding the Privacy Guidelines as minimum standards for data protection and privacy.

17. On 16 September 2020, the OECD and the Global Privacy Assembly held a follow-up workshop, with more than 170 participants in attendance representing governments, data protection authorities, the private sector, academia, civil society, and international organisations. It was designed as an opportunity to share lessons learned as countries entered different stages of the pandemic. The workshop provided a forum for all stakeholders to anticipate future challenges and to discuss how to deal with them.

18. The OECD Secretariat and Adherents will continue to raise awareness of the Recommendation and the importance of respecting data protection and privacy principles, during the recovery from the COVID-19 crisis and beyond.

5. Implementation

19. The Recommendation calls on adhering countries to demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest level of government; to implement the Privacy Guidelines set out in the Annex of the Recommendation through processes that include all relevant stakeholders; and to disseminate the Recommendation in the public and private sectors.

20. Key current challenges to personal data protection, in general, as well as specific challenges in the implementation of the Privacy Guidelines were discussed with experts and delegates in the initial stages of the review.

21. Some of the issues raised correspond directly to sections of the Privacy Guidelines, namely, accountability (Part Three), transborder data flows (Part Four), and implementation and enforcement (Part Five). Others concern the potential implications of emerging technologies and data-intensive business models (and their societal impact) as well as changing public attitudes towards privacy and personal data protection. In particular, the PGEG discussed how increasing amounts of data fall within the scope of "personal data" (Part One), the role of consent and new data subject rights (e.g., data portability) in the new data ecosystem (of relevance to Part Two). They also extend to issues of international co-operation and interoperability (Part Six).

5.1. Definitions, scope and basic principles

22. This section is based on responses to the survey, as well as discussions at the roundtables on Mechanisms for Privacy Interoperability [DSTI/CDEP/SPDE(2018)5/REV2], Organisational Accountability [DSTI/CDEP/SPDE(2019)9] , Enforcement Challenges [DSTI/CDEP/DGP(2020)5], Regulatory Sandboxes and Data Localisation and Trusted Government Access to Personal Data held by the Private Sector [DSTI/CDEP(2020)19]. It also benefited from input from the PGEG and was further informed by input from other, relevant work streams (including the OECD's work on AI, data portability, and on enhanced access to and sharing of data) and the consultation process leading towards the 2013 revision of the Privacy Guidelines.

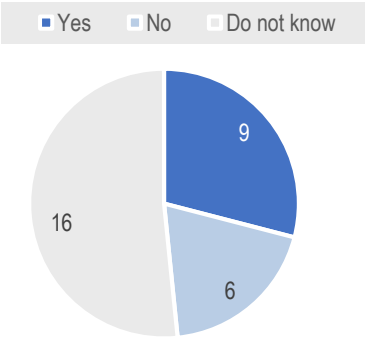
23. This section considers Parts One and Two of the Privacy Guidelines. Part One defines key terms and determines the scope of the Privacy Guidelines. Part Two contains the basic principles

of national application: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. A comprehensive review of both Parts took place in the context of the 2013 revision. Revisions were made at that time, including to modernise the wording, enhance clarity, and introduce new or expanded terms to keep abreast of technological, social and other changes. However, as is explained further below, the 2013 revision of the Privacy Guidelines concluded that, although there are questions regarding their implementation in today's digital environment, the basic principles remain valid and useful to guide personal data protection [DSTI/CDEP/SPDE(2018)8] (OECD, 2013[1]).

5.1.1. Part One: definitions and scope

24. Five terms are defined in Part One of the Privacy Guidelines. Three of them, "data controller", "personal data" and "transborder flows of personal data", were defined in the original text of the Privacy Guidelines as adopted in 1980 (hereafter "the 1980 Privacy Guidelines"). The definitions of two additional terms, "laws protecting privacy" and "privacy enforcement authority" (PEA), were added in 2013, in tandem with respective additions in Part Five, calling for the adoption of such laws and the establishment of these authorities (see section 3.4.1 below). Respondents to the privacy questionnaire were asked about the need for possible changes or additions to these existing definitions. Nine responding countries made some suggestions for the inclusion of new definitions. The proposed new definitions included "data processor", "agent", "subcontractor", "anonymity", "pseudonymity", and "consent". With the exception of "agent" and "consent", none of these terms appear in the main body of the Privacy Guidelines. 16 Respondents indicated that they did not know whether additional definitions are necessary (see Figure 1). This section of the report focuses on the definitions of "personal data" and "data controller" which became the focus of discussions at the expert consultation on Organisational Accountability [DSTI/CDEP/SPDE(2019)9] .

Figure 1. Responding countries that consider that changes need to be made to the definitions in the Privacy Guidelines or new ones should be added



Source: Privacy Guidelines questionnaire.

Considerations made on the term "personal data"

25. The Privacy Guidelines define *"personal data"* as "any information relating to an identified or identifiable individual (data subject)". This definition is well-aligned with that of other regulatory frameworks such as the European Union's General Data Protection Regulation (hereafter "GDPR") (European Union, 2016[4]), the 1985 Council of Europe (hereafter "COE") *Convention for the Protection of Individuals with regard to Automatic Processing of Personal*

Data[9] ("Convention 108") (Council of Europe, 1981[5]), and the revised *Asia-Pacific Economic Cooperation* (hereafter "APEC") *Privacy Framework*.[10] While Respondents and experts generally deemed this definition appropriate challenges in its practical implementation remain. In particular, technological advances are rapidly expanding the methods and ease with which individuals may be identified by their data or re-identified from apparently anonymised data, thereby expanding the scope of instances where individuals may be "identifiable". The term "identifiable" in the definition extends the meaning of personal data not just to data that presently identifies an individual but also to data that could potentially identify an individual under future circumstances. In other words, it encompasses data that are currently unidentified, but which may identify individuals when combined with other data or subjected to advanced analytical processing techniques. Technological developments create increasing difficulties in determining (and continually re-determining) what data should be considered "personal" in a given situation. On the other hand, there might be other useful limiting factors (such as time, costs) to take into consideration when interpreting this notion of "identifiable". Additionally, experts noted that personal data is not just data that is provided by the data subject – it is increasingly also data that is observed, derived or inferred (OECD, 2019, pp. 29-31[3]). Feedback from experts and adhering countries indicates that redefining the concept of personal data in the Privacy Guidelines, particularly in terms of what constitutes "identifiable" data, is however not an option. Revising it may run counter to efforts to ensure the interoperability of global privacy frameworks. Instead, further guidance may be needed on available technical and organisational safeguards. Responding countries and experts pointed to the need for an in depth examination of opportunities and barriers in the use of emerging new privacy enhancing technologies (PETs) such as pseudonymisation (coding) and privacy by design and default in the context of emerging technologies such as AI. A number of possible barriers to the implementation or adoption of PETs, for example, include lack of awareness about the existence of these tools, poor usability, and a lack of incentives for organisations to offer or implement these tools. Additional work is needed to assess the relative strengths and weaknesses of PETs, develop new PETs or improve the effectiveness of existing ones, and better understand the barriers to their deployment and adoption, including their application to transborder data flows.

Considerations made on the term "data controller"

26. A *"data controller,"* under the Privacy Guidelines, is "a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf." Similar definitions appear in other frameworks such as the GDPR, Convention 108+ and the APEC Privacy Framework. Over 84% of responding countries to the privacy questionnaire define "data controller" in their privacy legislation. Responding countries considered the definition in the Privacy Guidelines to be valid and useful. Notwithstanding, some experts and delegates (at

[9] In October 2018, a Protocol to amend Convention 108 opened for signature. The amendments pursued two main objectives: to modernise it to ensure its applicability to new information and communication technologies, and to strengthen its effective implementation (Council of Europe, 2018[12]). The Convention as amended by the Protocol is referred to as "Convention 108+".

[10] The APEC Privacy Framework arose from the discussions of the APEC Electronic Commerce Steering Group during the Data Privacy Workshop held in Thailand in February 2003, and was adopted by APEC during its 2004 summit in Santiago. In conjunction with the APEC Cross-Border Privacy Rules, it is a set of principles and implementation guidelines created to establish minimum standards of privacy protections in participating nations.The APEC Privacy Framework was updated in 2015 to draw upon concepts introduced in the 2013 revision of the Privacy Guidelines.

the consultation on Organisational Accountability and in written comments), explicitly raised the question as to whether it would be desirable to include an additional definition of "data processor", a question which had already been discussed during the 2013 review. The Privacy Framework acknowledges that the traditional concept of a data controller may not encompass all actors that have a role to play in data protection when it comes to allocating responsibilities (OECD, 2013[1]). The current definition of "data controller" therefore recognises that a controller may have an agent acting to collect, store, process or disseminate data on its behalf[11], and – as a minimum standard (see paragraph 6 of the Privacy Guidelines) – retains flexibility with regard to the allocation of responsibilities to other actors in accordance to their roles. The possible responsibility of other actors, such as data processors, was made explicit in the original explanatory memorandum, which provides that nothing in the Privacy Guidelines prevents others from also being accountable (OECD, 2013[1]). It was further reinforced in the 2013 revision with the addition under Part Five (National Implementation) of paragraph 19 h), which calls on countries to "*consider the role of actors other than data controllers, in a manner appropriate to their individual role*", in implementing the Privacy Guidelines.

27. The potential responsibility of data processors, as well as that of other actors, is thus already covered in the Privacy Guidelines. Unless the concept of a data processor is to be mentioned explicitly in the Privacy Guidelines (which may be the subject of further discussion between adhering countries and experts), it is unnecessary to include its definition in Part One. However, there may be scope to explore and further explain data processors' responsibilities in the explanatory memorandum or in further guidance, for example by proposing ways for allocating responsibilities to data processors and distinguishing their responsibilities from those of data controllers. Several countries indicated their support for this approach in written feedback on previous drafts of this report.

Terms for which further clarification is desirable

28. A few other terms were suggested for possible inclusion in the definitions section of the Privacy Guidelines. One responding country commented that it may be useful to define other actors, such as "agents", "supervisory authorities", and "data subcontractors" (with one country indicating that they would be more likely to use term 'service providers' over 'data subcontractors) . It should be noted that with the exception of the term "agent", these terms are not used in the body of the Recommendation. Nonetheless, it was strongly suggested at least by one responding country that there may be scope to introduce the notion of the data subcontractor, particularly in view of how the current digital ecosystem operates, and to clarify these actors' responsibilities in the explanatory memorandum or in further guidance.

29. It was also suggested that "anonymity" and "pseudonymity" be defined in the Privacy Guidelines. Relevantly, the original Explanatory Memorandum states that "[t]he precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country" (OECD, 1980[2]). The 2013 review re-examined difficulties with these concepts and concluded with similar sentiments, recognising that "practical limits of pseudonymisation and anonymisation are clearly being tested" (OECD, 2013[1]). Nevertheless, it was determined that there was no demand to introduce these concepts into the body of the Privacy Guidelines, so

[11] The Recommendation defines "data controller" to mean "a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

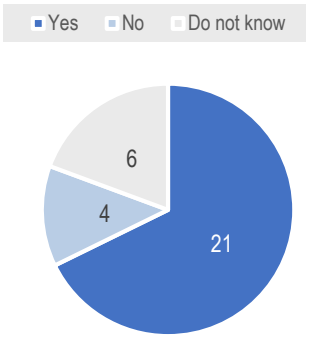
definitions were not necessary. A few years later, the OECD Health Ministers welcomed the Recommendation of the OECD Council on Health Data Governance, which relevantly includes a definition of "de-identification" and "re-identification" (OECD, 2019[6]).[12] It may be the case that these definitions and associated commentary prove useful to countries seeking additional guidance on such concepts for policymaking.

30. With regard to the *scope* of the Privacy Guidelines, it was generally considered by responding countries in their responses to the privacy questionnaire, and by consulted experts, that it remains useful and appropriate. No specific suggestions were made for its revision.

5.1.2. Part Two: basic principles of national implementation

31. In response to the questionnaire, 21 responding countries (68% of responding countries) considered that the Privacy Guidelines are a useful standard or reference point in national policy making, six responding countries indicated that they do not know (19%), and four responding countries said the Privacy Guidelines are not their main reference point (13%) (see Figure 2). Responding countries that answered affirmatively were asked to provide examples of the impact of the Privacy Guidelines on policymaking in their country. Many explained that their laws were originally modelled off, and still reflect, the Privacy Guidelines. Feedback was also received that, from a PEA perspective, the Privacy Guidelines continue to be relevant as a "unifying regime for encouraging co-operation among member countries and [a] set of benchmark norms for non-member countries that encourage uniformity and better data privacy across the globe." Other responding countries saw the Privacy Guidelines as a possible "bridge" between countries that have adopted GDPR and similar data protection laws and those that have not. Four responding countries (Iceland, Lithuania, Norway and Switzerland) explained that the GDPR and Convention 108+ are their current standard reference point for privacy.

Figure 2. The majority of responding countries consider the Privacy Guidelines to be a useful standard or reference point in national privacy policy making



Source: 2019 Privacy Guidelines questionnaire.

32. Very few responding countries suggested modification to the wording of the basic principles (with another few strongly of the opinion that they should not be amended). In relation

[12] The Recommendation defines "de-identification" to mean "a process by which a set of personal health data is altered, so that the resulting information cannot be readily associated with particular individuals. De-identified data are not anonymous data. "Re-identification" means a process by which information is attributed to de-identified data in order to identify the individual to whom the de-identified data relate."

to the use limitation principle and the security safeguards principle, one responding country felt that there is a need for guidance to assist in their comprehension, particularly in relation to the accepted exceptions to the former, which could be considered for inclusion in the Explanatory Memorandum.

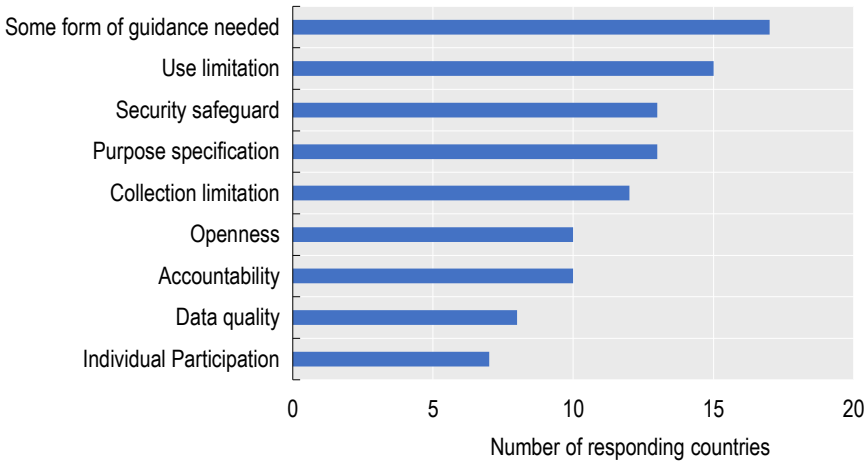
33. In a similar vein, experts consulted through the PGEG expressed the view that, on balance, the eight basic principles in Part Two remain generally sound and should be maintained in their current form (OECD, 2013[1]). There appeared to be overwhelming consensus among delegates and experts, including during roundtable discussions, that the basic principles continue to provide useful guidance on minimum internationally agreed standards for personal data protection, and that the principles themselves did not require revision. Nevertheless, experts and some responding countries noted areas for further discussion, including on data retention periods and regarding transparency. One responding country considered in particular that a data retention principle would be a logical consequence of the purpose specification principle since there would no longer be a basis for storing or processing data once all purposes are exhausted.

34. The 2013 report for the review of the Privacy Guidelines suggests that there was debate on the issue and notes that while indeed many privacy regimes do include a data retention principle, time limits for retention or requirements for erasure vary significantly (depending also on whether the data is collected for research, medical care or other specific purposes).These "lower level machinery questions..should (thus) be left to domestic implementation". Nonetheless, it also warns that"[t]he implications of data persistence are significant – whether it is the effect on an individual's reputation, the unanticipated and unauthorised uses of data, or the threats from breaches or malware to increasing amounts data that is stored indeterminately." (OECD, 2013, p. 115[1]).

35. Additionally, responding countries mentioned that there are areas where the principles come under pressure. Of the responding countries that considered that there is a need for additional guidance in relation to Part Two of the Privacy Guidelines, almost all suggested data use limitation. This was followed by security safeguards, purpose specification and collection limitation (see Figure 3). Just under half of the respondents considered that no implementation guidance is needed.

36. Responding countries generally suggested that guidance would be helpful in relation to the application of the principles to new technologies and accountability (discussed further below). Some countries saw a need for additional information on practical guidance. One country explained that to remain relevant, the implementation of the Privacy Guidelines needs to recognise growing global opposition to the mass collection of personal data for commercial and political purposes.

Figure 3. Responding countries that consider that there is a need for additional guidance in relation to Part Two of the Privacy Guidelines



Source: 2019 Privacy Guidelines questionnaire.

37. In particular two main issues emerged from discussions with adhering countries and experts in the PGEG and in roundtables: the extent to which individuals' rights and controls over their own personal data are adequately reflected in the basic principles; and the application of the basic principles to emerging technologies.

Enhancing data subjects' agency and control over their personal data

38. As to the first issue, adhering countries and experts recognised that there is an increasing amount of international attention on ensuring that data subjects can exert greater agency and control over their personal data. This is reflected in the GDPR, which entered into force in May 2018 and has a significant emphasis on ensuring greater data subject rights.

39. It is no longer possible for individuals to participate in the digital environment without providing data to third parties that may, in and of themselves be personal, or that, when combined with other data and analysed, may reveal sensitive personal information. For example, pervasive data collection, sharing, aggregation, and use today allows companies with the aid of advanced analytics to develop detailed profiles of their customers' health status, psychologies and willingness to pay. In addition, in the context of new and emerging technologies (such as Artificial Intelligence and the Internet of Things), privacy regimes cannot rely exclusively on individual choice and consent. In 2019, for example, 86% of the population in the European Union felt they did not have complete control over the information they provide (e.g. the ability to correct, change or delete this information) compared to 67% in 2015 (European Commission, 2015[7]; European Commission, 2019[8]).

40. As the processing of personal data becomes more complex and has more unanticipated uses, as is particularly true in the case of AI, it may become less transparent to users and more difficult to understand. The same is true for IoT devices, where their ubiquity and discreteness sometimes mask the fact that personal data is constantly collected, often without an easily accessible interface for user interaction and control (e.g., to set personal data gathering preferences). 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, and multiple requests to "accept", "agree" or "set preferences" at every mouse click, individuals are unable to exert meaningful choice or consent or to simply grasp the nature of the use of their personal data. The choice is even less meaningful when users must accept the "terms of use" as they are in order to use the service. Added to this, the protection of their personal data is not always the immediate concern of data subjects and nor are they always able or willing to comprehend the different consents they give when faced with the need or desire for prompt access to a particular product or service.[13]

41. These trends, in addition to the increased number of recent large scale personal data breaches, have brought about significant challenges to individuals' understanding of the risks to their privacy and hesitation in engaging with services and products that collect and use their personal data. For this reason, additional protections must be layered on top of notice and consent, and there should be greater focus on the uses of data.

42. Adhering countries as well as experts consulted in the PGEG, in roundtables, and in subsequent written comments recognised that the Privacy Guidelines already incorporate many protections and key rights for data subjects. For instance, the collection limitation principle (paragraph 7) provides that there "should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." Further, the purpose specification principle and the use limitation principle (paragraphs 9 and 10, respectively) provide that personal data should not be used for a purpose other than that for which it was collected, unless the data subject consents or if it is by the authority of law. The original Explanatory Memorandum explains that the knowledge or consent of the individual is essential for personal data collection (with knowledge being the minimum requirement). It also recognises that, for practical reasons, consent cannot always be obtained – hence the inclusion of the words "where appropriate" in the collection limitation principle (OECD, 2013[1]). It may thus be concluded that the basic principles adequately acknowledge the difficulties associated with obtaining informed, specific, explicit and truly voluntary consent from data subjects. However, responding countries and experts noted continued challenges in the implementation of the principles of collection limitation and purpose specification, suggesting the need for good practice. Responding countries agreed there is a need for more guidance, including a review of emerging practices and use case scenarios (e.g. when consent should be employed and when it may not be a useful or meaningful way of ensuring privacy; consent in the context of AI and IoT ; consent in the context of cross-border data transfers).

43. Under paragraph 13 (a) the individual participation principle provides that individuals "should have the right to obtain from a data controller, or otherwise, confirmation of whether the controller has data relating to them [and] under 13 (b) to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them". Under 13(c) the individual should have the right to be given reasons for, and be able to challenge, a decision made by the controller, or otherwise, to decline such a request. Under 13 (d) the individual should also be able to "challenge data relating to them and, if the challenge is successful to have that data erased, rectified, completed or amended."

44. The data subject rights contained in the Privacy Guidelines represent a subset of rights contained in other recent legal frameworks such as the GDPR. Experts noted that the GDPR grants

[13] See further Office of the Privacy Commissioner of Canada, *Consent and Privacy: A discussion paper exploring potential enhancements to consent under the* Personal Information Protection and Electronic Documents Act (2016), available at <https://www.priv.gc.ca/media/1806/consent_201605_e.pdf>.

data subjects rights akin to the OECD individual participation principle but extends them with an explicit right to be forgotten and to be informed, an explicit right to data portability, and the right to object to automated decisions (GDPR, Articles 17, 20 and 22 respectively). So, too, it requires data controllers to provide data subjects with concise, transparent, intelligible and easily accessible information regarding data collection and processing (Articles 12-14).

45. It could be argued that the individual participation principle under Part Two of the Privacy Guidelines addresses the right to be informed under principle 13 a) (with the right to obtain confirmation of whether or not the data controller has personal data relating to the individual), the right to data portability under principle 13 b) (with the right to to have communicated data relating to them) and the right to be forgotten under principle 13 d) (with the right to have the data erased); and that the OECD (2019[9]) Recommendation on Artificial Intelligence [OECD/LEGAL/0449], which contains the OECD Principles on AI, complements the Privacy Guidelines by addressing the right of an individual to object to automated decisions.[14]

46. In respect to data portability, however, initial findings of OECD work on data portability[15] strongly suggest that data portability is only partly enshrined in the individual participation principle described above. Data portability encompasses the transfer of personal data in a structured, commonly used machine-readable format to both (i) the data subject him or herself, and (ii) to a third party data controller of his or her choice. It could be argued that in the age of big data the transfer of personal data in a structured, commonly used machine-readable format constitutes "a reasonable manner" and "readily intelligible" form according to principle 13 b) iii and iv of the Privacy Guidelines. However, the transfer to a third party data controller is not covered by the individual participation principle of the Privacy Guidelines.

47. Furthemore, OECD work on data portability shows that data portability is motivated by other additional considerations beyond those related to privacy and data protection. Besides *(i)* enhancing 'informational self-determination', the rationale most in accordance with the individual participation principle, other major rationales for data portability include: *(ii)* increasing competition and choice, *(iii)* encouraging innovation; and *(iv)* facilitating data sharing and data flows. These other considerations have been as important, if not more important, for the establishment of some data portability initiatives in adhering countries such as the 'My Data' initiatives of the United States initiated in 2010, the 'Midata' data portability initiative of the United Kingdom in 2011, and Australia's Consumer Data Right (CDR), which contrary to the 'Right to Data Portability' (Art. 20) of the EU GDPR are not grounded in privacy and data protection regulation. A similar statement can be made in respect to some of the sector specific data portability initiatives such as regulations on open banking and on access to in-vehicle data.

48. Last, but not least, OECD work shows that data portability itself raises important privacy and data protection issues. For instance, data portability can affect the privacy of third parties. In particular, when an individual opts to download his or her data from a data controller, or requests that it be shared with a different controller, the first controller must determine (within the

[14] More information about the Recommendation and the Principles can be found at https://www.oecd.org/going-digital/ai/principles/. A particular focus of the Recommendation is the development of metrics to measure AI research, development and deployment, and to gather the evidence base to assess progress in its implementation. The online OECD.AI Policy Observatory (https://oecd.ai/), launched in February 2020, aims to facilitate this by providing evidence and guidance on AI metrics, policies and practices to help implement the Principles, and constitute a hub to facilitate dialogue and share best practices on AI policies.

[15] The Secretariat is currently developing an analytical report on data portability with an aim to publish it in early 2021 [DSTI/CDEP/DGP(2019)2].

parameters set by the law and regulatory guidance) what constitutes the requesting party's personal data and the point at which it implicates or becomes someone else's. Data portability also raises liability challenges if there is a security failure or privacy breach. It may be the case that effective portability frameworks hold participants liable for their own conduct, but not the conduct of other participants, in accordance with existing legal frameworks. Furthermore, there is a strong probability that data portability initiatives may span multiple regulators.[16] Governments implementing data portability schemes, therefore, should be wary of this and plan which regulator will have primary oversight of the initiative to ensure efficiency, streamlined processes and beneficial consumer outcomes. All these challenges call for more policy guidance on data portability and show a need for good practices to ensure effective privacy protection when data is ported.

Implementation of the basic principles to emerging technologies

49. The second major area of focus that arose from the discussions among adhering countries and experts in the DGP and PGEG on the basic principles in Part Two of the Privacy Guidelines concerns their implementation in the context of emerging technologies, such as AI and the IoT. Responding countries considered this a priority area, with all but four replying that catching up with technological developments was one of the main challenges to their current regulatory framework and ranking AI as the main challenge to privacy and personal data protection (see also section 5.4.3 below). Adhering countries' and experts' discussions sought to take account of societal implications of the use of these technologies on personal data. Some experts noted that while the basic principles focus on the impact on the individual, the collective societal impacts of the use of mass amounts of personal data processed by emerging technologies should also be taken into account (see also the sections below). With respect to the implementation of the basic principles in the context of AI, it should be noted that whilst these principles remain relevant, further guidance could be developed as to how to implement them. The need to address the potential for bias and other harmful consequences from personal data processing without hindering innovation and preventing the beneficial uses of these technologies was noted. It could be argued that this concern is already partly addressed under provision 13(d) whereby the individual should have the right to "challenge data relating to them …and to have the data erased, rectified, completed or amended". The technology-netural approach of the Privacy Guidelines appears to be a solid foundation for building effective protection and trust in this matter.

50. Building on previous OECD work on data-driven innovation and how policy-makers might maximise the benefits of new technologies whilst mitigating associated economic and societal risks (OECD, 2015[10]), the 18 November 2019 expert consultation further explored the impact of emerging technologies (particularly AI) on the application of the basic principles. One of the dominant themes in the discussions was the importance of "explainability" of AI algorithms to ensure accuracy, fairness and accountability. Experts noted that the rise of AI has also seen an attendant rise in demand for large datasets, and that this is critical to build accurate AI but increases privacy-related risks. Experts also noted that most AI guidelines refer to privacy in general terms

[16] The Australian Consumer Data Right in the banking sector, for example, falls within the ambit of banking and privacy regulators, including the Australian Prudential Regulation Authority (APRA, the prudential regulator of the Australian financial services industry), the Australian Securities and Investments Commission (ASIC, which regulates the conduct of financial service and consumer credit providers), the Reserve Bank of Australia (RBA, the primary regulator of the payments system) and the Australian Competition and Consumer Commission (ACCC, which regulates competition), and the Office of the Australian Information Commissioner (OAIC, which protects the privacy of individuals and handles privacy complaints).

but do not establish an explicit connection between the capabilities of AI and the nature of AI-specific privacy challenges. This could have the effect of shifting the focus away from privacy when it comes to AI, and greater guidance may be needed to ensure that current AI guidelines sufficiently address privacy-related concerns. Adhering countries generally agreed with the experts but did not consider that the basic principles of the Privacy Guidelines should be amended specifically to account for AI. To this end, countries noted that the Privacy Guidelines' technology-neutral language was key to their adaptability and that these important matters related specifically to AI could be addressed in the forthcoming mechanisms and guidance related to the recently adopted OECD Recommendation on Artificial Intelligence [OECD/LEGAL/0449; DSTI/CDEP(2019)4/REV1].

5.1.3. Conclusions and proposed next steps

51. Consultations identified profound changes of scale regarding the role of personal data in economies, societies and daily lives since the Privacy Guidelines original adoption in 1980. Nevertheless, the eight basic principles remain remarkably adaptive to these changes and developments in technologies, due to their concise and technology-neutral language, and status as minimum standards for adoption in domestic legislation. Adhering countries emphasised the importance of maintaining this technical neutrality in any future changes to the Guidelines or the Explanatory Memorandum.

52. Nevertheless, technological developments and the intensification of data collection, storage and processing put pressure on the basic principles and scope of the Privacy Guidelines. The determination of what constitutes personal data may warrant further guidance in the supplementary Explanatory Memorandum, along with more detailed explanation as to the roles and responsibilities of data processors and other actors involved in data protection. Further discussions might usefully be had to assess whether additional safeguards – such as limitations on data retention, the right to object to automated decisions, and the right to information – are necessary (for example as further guidance in the supplementary Explanatory Memorandum) to strengthen the Privacy Guidelines. In the context of data subjects' rights, outcomes from the related work on data portability suggests the need for more policy guidance on data portability as well as for good practices to ensure effective privacy protection when data is ported. A suggestion was also made by adhering countries to integrate more fully the work at the OECD on Enhancing Access to and Sharing of Data ("EASD") in revisions to the supplementary Explanatory Memorandum.

53. In addition, it may also be useful to draw lessons learned from the recent discussions on responses to the COVID-19 pandemic where certain basic principles seemed to arise frequently such as necessity, use limitation, proportionality. Finally, there was consensus that future work should examine new and emerging privacy enhancing technologies and other technical measures to enhance privacy and personal data protection and their impact on the types of "identifiable" data.

5.2. Part Three: implementing accountability

54. This section is based on responses to the privacy questionnaire and the expert consultation on Organisational Accountability, co-organised with the Centre for Information Policy Leadership (CIPL), on 6 May 2019 [DSTI/CDEP/SPDE(2019)9]. It is further informed by the outcomes of two side events that took place in Tirana, Albania, on 24 October 2019 at the International Conference of Data Protection and Privacy Commissioners (ICDPPC, now the Global Privacy Assembly) and by work of the DGP on data breach notification reporting, including a respective questionnaire [DSTI/CDEP/SPDE(2019)6] and by the CDEP on online platforms (OECD, 2019[11]).

5.2.1. Background

55. The accountability principle is one of the original eight basic principles. It provides that "[a] data controller should be accountable for complying with measures which give effect to the principles stated above" (OECD, 1980[2]) (see paragraph 26 above for the definition of data controller). The Explanatory Memorandum to the original 1980 Privacy Guidelines further provides that the data controller must be accountable for complying with privacy protection rules and decisions, irrespective of whether the data processing is carried out on their behalf by another party (OECD, 2013[1]).

56. The 2013 revision of the Privacy Guidelines included a new Part Three, "Implementing accountability", which fleshes out the elements required of data controllers to implement the accountability principle, notably introducing the concept of "privacy management programmes". Under the revised Privacy Guidelines, privacy management programmes are the primary operational vehicle through which an organisation is expected to give practical effect to the basic principles contained in Part Two of the Privacy Guidelines. Specifically, the added section provides that a data controller should give effect to the Privacy Guidelines for all personal data under its control by implementing a privacy management programme that is tailored to the structure, scale, volume and sensitivity of its operations and that provides appropriate safeguards based on privacy risk assessment including plans for responding to inquiries and incidents. In addition, the data controller should be prepared to demonstrate its privacy management programme and provide notice, as appropriate, to authorities and data subjects where there has been a significant security breach affecting personal data. The revised Guidelines also specify that a data controller is accountable for personal data under its control irrespective of the location of the data (see also section 5.3.1 below).

57. The supplementary Explanatory Memorandum to the revised Privacy Guidelines provides further guidance on privacy management programmes, for instance by listing examples of "appropriate safeguards" a data controller can put in place (e.g., contractual provisions, employee training and education, and audits) and underpinning the importance of risk assessments, which may be achieved through a privacy impact assessment, in this process (OECD, 2013[1]).

5.2.2. Implementation findings

58. The components of accountability, its objectives, and its potential benefits and shortcomings were discussed extensively at the aforementioned expert consultation on 6 May 2019 [DSTI/CDEP/SPDE(2019)9]. The consultation was conducted over three roundtables: i) state of the play of organisational accountability; ii) accountability 2.0; and iii) accountability in the Privacy Guidelines: addressing the gaps. The first roundtable focused on understanding the term and examining its implementation in practice, with examples from PEAs and organisations. The second roundtable introduced the concept of "accountability 2.0" which aims to incorporate ethical notions of data use (ethics by design) to ensure that data serves all stakeholders and explored changes to accountability models in response to emerging technologies, to ensure trusted, advanced data processing activities. Finally, the third roundtable sought to identify possible gaps in the Privacy Guidelines' approach to accountability, in light of the preceding sessions, and ways to address them. The interventions primarily concerned two themes: understanding accountability, and the role of enforcement. With regard to the former, participants discussed different models and features of accountability, questioning the existence of a common understanding of accountability, especially across languages and legal systems or different business models and scales. Accountability should apply equally to both public and private entities, and to both data controllers and processors. The ability to scale down accountability to small and medium enterprises (SMEs) in practice was questioned. Unlike larger organisations, SMEs are not used to implementing

accountability programmes and may not be equipped with the necessary resources and understanding to do so, which may necessitate further guidelines, for examples to appropriately define risks and harms. While the notion of risk-management seemed prevalent, experts noted that there was no agreement on how risks should be defined and assessed and through what mechanisms, and asked whether the OECD, as well as civil society, might provide useful additional guidance in this context.

59. The trust deficit today is higher than ever, current experience with accountability, in both public and private sectors, has led to the understanding that accountability requires a robust oversight regime to work well in practice. Participants to the roundtables, adhering countries and experts consulted in the PGEG noted that an internationally agreed approach to accountability is needed to raise the bar and drive up standards internationally. In addition enforcement cooperation has a crucial role in giving it effect.

60. The Global Privacy Assembly (former ICDPPC) in October 2019 featured two side-events dedicated to accountability that were co-hosted with the OECD, the Centre for Information Policy Leadership (CIPL) and Information Accountability Foundation (IAF). The first event, "What is Accountability? Addressing the Confusion, Finding Consensus", examined the concept of organisational accountability. The panellists explained that accountability, despite differing views as to its precise meaning, can facilitate transparency, social responsibility and trust in organisations, as well as productive conversations with regulators and stakeholders. The second side-event, "Accountability 2.0 - Data Stewardship and Beneficial AI", focused on Accountability 2.0. Panellists described that the 1980 interpretation of accountability – namely, compliance with legal obligations – has evolved to require organisations to proactively act as responsible and ethical stewards of personal information. Accountability 2.0 requires corporate commitment to internal and external data protection policies, mechanisms to implement privacy-by-design, internal monitoring of those mechanisms, individual data subject participation and a readiness to demonstrate compliance (or implement remedial measures) when required by the regulator. The discussions revealed a general consensus that the meaning of accountability and what it requires has developed considerably since 1980. However, much more work can be done to harmonise different definitions of accountability and imbed comprehensive accountability frameworks in organisations.

Implementation findings from survey responses

61. As noted in the preceding section, in the May 2019 expert consultation on accountability, participants identified existing gaps in the understanding of accountability and of the role of enforcement, and underscored the need for international guidance on accountability. In particular, they highlighted recent accountability failures and different – language- and culture-dependent – interpretations of the term. They further questioned the possibility to scale down accountability to SMEs, the role of incentives other than enforcement, and the subjects and objects of the accountability obligation.

62. These gaps are also demonstrated by the findings of the questionnaire, where 39% of respondents replied that they were applying "incentives for data controllers' accountability" as part of their policy measures to further privacy and data protection by small businesses. In addition 17 responding countries (or 58%) considered that there is scope to expand the Explanatory Memorandum concerning Part Three (implementing accountability).

63. Specifically, clarificationis needed, for example, regarding the practical mechanisms to implement and enforce accountability , the potential role of data ethics, in particular in the context of emerging technologies (including ethics by design); the concept of information fiduciaries; the role of organisational codes of conduct. One country added, similarly to the comments made by

some of the experts in the organisational accountability consultation, that the Privacy Guidelines should specify to whom data controllers are accountable (such as to PEAs, data subjects, boards and shareholders) and that data controllers should designate one or more individuals to be responsible for ensuring that the organisation complies with data protection laws and regulations. One country added that the Explanatory Memorandum should specify that privacy management programmes should be implemented by the top level of management in organisations, to emphasise their relative importance in the organisation's governance structure.

Notification of security breaches affecting personal data

64. An important aspect of accountability concerns personal data breach notifications (paragraph 15 c) of the Privacy Guidelines).

65. The OECD has a separate but related work stream on promoting comparability in personal data breach notification reporting, which is part of a broader project aimed at improving the evidence base for security and privacy policy making (DSTI/CDEP/SPDE(2017)1). This work has been carried out since 2017 under the supervision of an international Expert Group, drawing from the Working Party on Security and Privacy in the Digital Economy (SPDE) and the Working Party on Measurement and Analysis of the Digital Economy (MADE). The work involved a feasibility study on whether PEAs collect or may be able to collect the proposed set of data. A questionnaire was circulated to PEAs in June 2019 with the support of the ICDPPC (now the Global Privacy Assembly), the Asia Pacific Privacy Authorities (APPA) and the European Data Protection Board (EDPS) (DSTI/CDEP/DGP(2020)1). By 14 February 2020, 35 countries had responded to the questionnaire, consisting of 20 European Union (EU) countries and 15 non-EU countries. Responses were sought in the United States at State level as the regulation of data breach notification is mostly local. Responses were received from 23 US States and one US Territory. The survey results show that there is a general trend towards mandatory PDBN reporting. All countries applying the GDPR, six countries not applying the GDPR, and 16 US States answered they have introduced mandatory PDBN reporting. All remaining five non-GDPR countries responded they expected to introduce such a law within the next two years. While many countries are introducing mandatory PDBN reporting, there are, however, significant differences across countries in the way regulation is framed and implemented.

5.2.3. Conclusions and proposed next steps

66. The responses to the questionnaire and the expert consultation clearly suggest that responding countries consider accountability to have an important role in personal data protection in general, and in the Privacy Guidelines in particular. In this context, it should be noted that only 4 responding countries replied that they did not consider the language of Part Three of the Privacy Guidelines (implementing accountability) to be appropriate and corresponding to their objectives. The findings further suggest that countries increasingly put in place measures, notably transparency reporting and guidance and mandatory personal data breach notifications, to promote the implementation of accountability by organisations. Examples of organisations not complying with accountability requirements in domestic data privacy laws are not indicative of broader failings of accountability.

67. Based on the evidence to date, it appears therefore that the accountability principle remains an important pillar of the Privacy Guidelines but there exists some confusion as to its meaning and what it requires. The move towards what has been referred to by some academics and civil society as "Accountability 2.0" entails more than just legal compliance and avoiding risk to customers. Rather, it is about data stewardship and organisations being responsive, creating value for individuals and society as well as for one's own organisation; it is about greater transparency and

corporate responsibility as well as making responsible data use a competitive advantage for business.[17]

68. Responding countries agreed on the need to clarify the application of the accountability principle and further guide its implementation with best practice on how to strengthen the role of enforcement and of PEAs. It is therefore proposed that the DGP consider revising corresponding sections of the supplementary Explanatory Memorandum to clarify some of the issues raised above, and/or consider developing additional implementation guidance on accountability for both PEAs and organisations drawing also on ongoing work on data ethics. Such clarifications and guidance could stress the need for enhanced control and enforcement of the accountability principle, and contribute to effective implementation of accountability and to the dissemination of the Privacy Guidelines. To this end, proposals for draft revisions of the supplementary Explanatory Memorandum and the scope of additional accountability implementation guidance could be developed over the course of 2021.

5.3. Part Four: basic principles of international application: free flow and legitimate restrictions

69. This section is based primarily on responses to the privacy questionnaire. It also draws on the roundtable on interoperability work conducted by the OECD on data portability, data localisation and on trusted government access to data held by the private sector.

5.3.1. Background

70. The significance of transborder data flows has been recognised in the OECD since at least 1969 when it retained a group of experts to study different aspects of privacy. In the decade that followed, the OECD dedicated research and a number of seminars and symposiums to develop knowledge of the importance of data flows, implications for privacy, and the need to harmonise countries' approaches to data transfers to promote growth. The subsequent 1980 Privacy Guidelines sought to strike a balance between protecting privacy and encouraging the free flow of information necessary for the facilitation of trade and the global economy. The 1980 Privacy Guidelines presumed that free transfers of personal data should generally be allowed, but recognised that they could be restricted when the receiving country "does not yet substantially observe these Privacy Guidelines or where the re-export of such data would circumvent its domestic privacy legislation" (paragraph 17 of the 1980 Privacy Guidelines) (OECD, 2013[1]).

71. As part of the 2013 revision of the Privacy Guidelines, the Part on free flow and legitimate restrictions was revised. This revision was prompted by recognition that advances in technology

[17] See further, for example, Christopher Docksey, "Keynote on Accountability At the 41st Conference of Data Protection and Privacy Commissioners", speech given on 24 October 2019 in Tirana, Albania, available at <http://informationaccountability.org/christopher-docksey-keynote-on-accountability-at-the-41st-conference-of-data-protection-and-privacy-commissioners-24-october-2019-in-tirana-albania/>; Centre for Information Policy Leadership, "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" (July 2018), available at <http://bit.ly/2koS7IT>; GPEN Sweep 2018, 'Privacy Accountability', Office of the Privacy Commissioner, New Zealand and Information Commissioner's Office, UK (October 2018), available at <https://ico.org.uk/media/about-theico/documents/2614435/gpen-sweep-2018-international-report.pdf>; and Information Accountability Foundation, *Ethical Accountability Framework for Hong Kong China: A Report prepared for the Office of the Privacy Commissioner for Personal Data* (October 2018), available at <https://iapp.org/media/pdf/resource_center/Ethical_Accountability_Framework_HongKong.pdf>.

and changes in organisational practices have significantly increased the frequency and volume of transborder data flows. Transfers have become a continuous, multipoint global flow, regulated by a variety of different national and regional regulatory approaches. The 2013 revision also recognised that individuals are playing an increasingly important role in generating transborder data flows, although they may be unaware of where their data are stored and transferred. Overall, the amendments sought to simplify and consolidate the OECD's approach to free data flows. This was considered to be especially important given the variety of ways in which countries had instituted mechanisms to protect privacy in the context of transborder data flows (OECD, 2013[1]).

72. Given these considerations (and in addition to the pre-conditions for transborder data flows, namely substantial observance of the Privacy Guidelines and enforcement mechanisms), a new paragraph 16 in the revised Part (Four) now provides that a "data controller remains accountable for personal data under its control" irrespective of where the data are located. Paragraph 17 of the Privacy Guidelines provides that a Member country should refrain from restricting transfers between itself and another country when the other country "substantially observes" the Privacy Guidelines (a retention of the 1980 wording) or has "sufficient safeguards" consistent with the Privacy Guidelines in place to protect the data. The addition of the sufficient safeguards wording was intended to promote transborder data flows by acknowledging the measures a data controller can take to ensure the continuing protection of the data when accompanied by effective enforcement mechanisms (OECD, 2013[1]). Paragraph 18 of the revised Privacy Guidelines provides that any restrictions to free data flows should be proportionate to the risks presented, taking into account the sensitivity of the data and the purpose and context of the processing. In parallel, paragraph 6, which provides that the Privacy Guidelines may be supplemented by "additional measures for the protection of privacy and individual liberties", was amended in 2013 to clarify that such measures may impact transborder flows of personal data.

73. Since the adoption of the 1980 Privacy Guidelines, similar provisions for permitting or encouraging transborder personal data flows when privacy is protected have been incorporated in other international instruments. Convention 108+, for example, 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 (Art. 14(1), subject to limited exceptions). The Convention further provides that transfers to recipients in states not party to the Convention may generally only take place when there is an appropriate level of protection (Art. 14(2), with some exceptions in (4)) (Council of Europe, 2018[12]). Similarly, the 2005 *APEC Privacy Framework*, revised in 2015, was drafted with the objective of protecting information privacy while maintaining information flows among economies in the Asia-Pacific region and their trading partners (Preamble, paragraph 1). It provides that APEC member economies should take all reasonable and appropriate measures to remove unnecessary barriers to data flows and avoid the creation of such barriers (paragraph 30).

74. At a national level, an increasing number of countries around the world are putting in place modern data protection systems that combine openness for international data flows with the highest level of privacy and data protection for individuals. The entry into force of the GDPR on 25 May 2018 introduced updated rules governing the global free flow of personal data regarding data subjects who are in the European Union. Chapter V of the GDPR ensures that personal data protections travel with data originating from EU Member states when data are transferred abroad. This is made possible through the use of different tools (some of which pre-dated the GDPR), ranging from "adequacy decisions" in respect of recipients[18] or when "appropriate safeguards" are in place

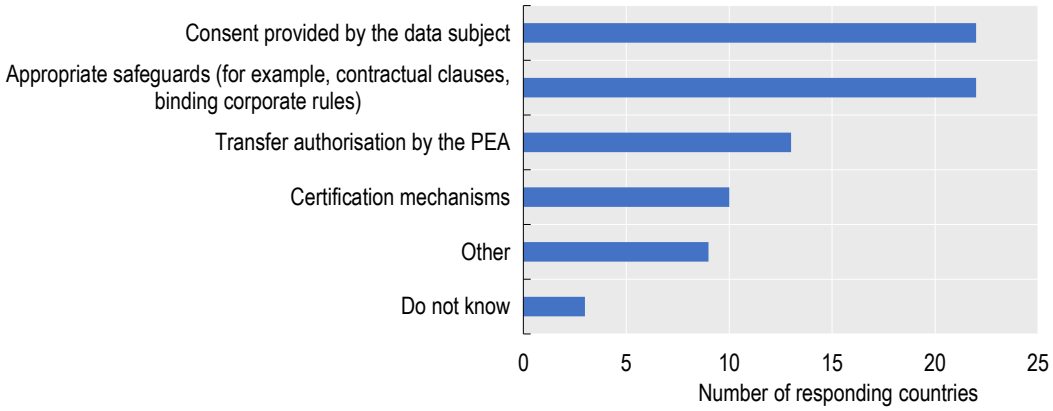
[18] Article 45 of the GDPR gives the European Commission power to make an adequacy decision, which indicates that the non-European Union Member state will "ensure an adequate level of protection" of the personal data.

for the data (such as model clauses, binding corporate rules, codes of conduct and certification) (Arts. 45-46). Within the EU, the GDPR aims to ensure a consistent and an equivalent high level of protection and remove obstacles to the free flows of data within the Union (Recital 10) (European Union, 2016[4]).

5.3.2. Implementation findings

75. The essence of Part Four, then, is enabling the flow of personal data across borders and delineating legitimate restrictions on those flows. In this respect, the majority of responding countries to the privacy questionnaire (over 84%) are parties to at least one *multilateral agreement* or legal framework that defines legitimate restrictions on transborder flows of personal data. Those agreements and frameworks included the GDPR (18 respondents), Convention 108 (19 responding countries), the Privacy Shield (17 respondents), and the APEC Privacy Framework (7 responding countries). Other prevalent mechanisms for enabling transborder personal data flows (8 responding countries) included consent provided by the data subject and "appropriate safeguards" (for example, contractual clauses, binding corporate rules[19]) (see Figure 4 below).

Figure 4. Mechanisms in place for enabling personal data flows to other countries (not covered in multilateral agreements)



Source: 2019 Privacy Guidelines questionnaire.

76. Over 80% of responding countries to the questionnaire said that they have provisions in their *privacy and personal data legislation* restricting transborder data flows. Some of them explained they have enacted their own frameworks regulating data flows, some of which are still evolving. Some responding countries (36% of respondents) added that they have provisions in their regulatory framework concerning data localisation. In some of them, only specific types of personal data (for example, health records, national archives or data relevant to national security) were subject to a localisation requirement.

77. Additionally, in the case of 13 respondents, organisations are required to report on transborder flows of personal data. The content of these requirements, however, varies. For example, organisations in one responding country must report all data transfers (regardless of where the data are being transferred). Another responding country answered that there are

[19] Binding corporate rules are legally binding rules that specify how personal data must be transferred between a group of undertakings or a group of enterprises engaged in a joint economic activity. They are generally intended to protect privacy and other rights of the data subjects that are the subject of the transfers.

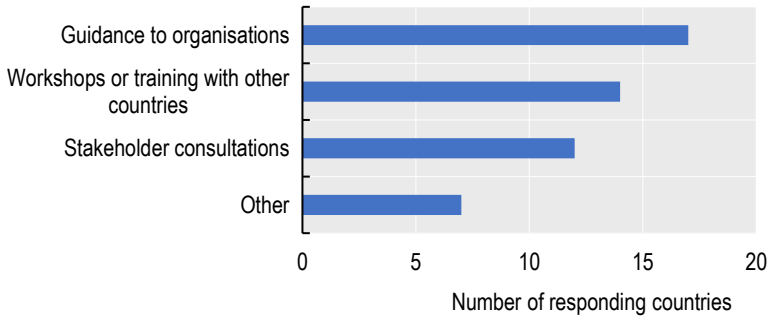
requirements for federal government Privacy Impact Assessments for public sector data transfers, and yet another noted the requirement to report on the transfer of passenger name record data between itself and the European Union.

78. Two responding countries answered that organisations subject to the GDPR must seek authorisation for "bespoke" (individualised) data protection contracts, although these are rarely used since the European Commission has approved "Standard Contractual Clauses" (SCC).

79. It should be noted that the questionnaire was circulated prior to the Court of Justice of the European Union (CJEU) Schrems II decision of July 16, 2020 (case C-311/18). In its judgement the CJEU invalidated the EU-U.S. Privacy Shield framework, however concluded that EU organizations can continue relying on SCCs but have an obligation to take a proactive role in assessing on a case by case basis prior to any transfer, whether or not their counterparts in third countries will be able to comply with the SCC. In other words EU organizations that currently rely on SCCs will need to consider whether, having regard to the nature of the personal data, the purposes and context of the processing, and the country of destination, they can comply with their obligations under EU law, or if the laws of any third country conflict with such obligations. , Should they not be able to comply, organizations should consider what additional safeguards may need to be implemented.

80. The questionnaire also sought information about *policy measures* governments or PEAs apply to promote transborder data flows. Respondents offered a variety of responses, including stakeholder consultations, workshops, advisory guidelines and participation in international fora (see Figure 5). One responding country explained that organisations in its jurisdiction have a "right of inquiry" whereby they can present an inquiry to the data protection authority when an aspect of the law pertaining to data flows is unclear (including the application of that law). The authority has 15 business days to respond. Another responding country said that it had arranged for a seminar to be held for all non-EU countries on binding corporate rules. However, only four responding countries reported that there were mechanisms in place to measure the prevalence and success of their policy measures to promote transborder data flows. Those mechanisms included a regulation whereby the PEA must monitor the implementation of the free data flows regulation, consultations with data subjects, records of the number of certified enterprises, and records of website traffic and queries received through various channels.

Figure 5. Policy measures to promote transborder data flows, international privacy enforcement co-operation, or interoperability



Source: 2019 Privacy Guidelines questionnaire.

81. Also of note to findings about the implementation of the Privacy Guidelines are various trade agreements, to the extent they include provisions promoting the free flow of personal data or prohibiting data localisation. The existence of such trade agreements contributes to the complexity

of the legal landscape in which countries, organisations and other bodies are transferring personal data across borders. One country noted the importance of the G20 Leader's Declaration made in Osaka in June 2019, which says that trust is an important pre-condition of data flows, and that data protection and security are important for ensuring trust. Another country noted the importance of the "Horizontal Provisions of the European Union on cross-border data flows and for data protection" in the context of trade discussions, which "recognise that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade" (Art B(1)). Experts suggested a role for the DGP in collating relevant provisions in trade agreements that purport to shape the use and/or free flows of personal data.

82. Box 1 below describes some examples of how countries are implementing paragraph 16 of the Privacy Guidelines, regarding the continuous accountability of data controllers for personal data under their control without regard to the location of the data.

Box 1. Implementation of paragraph 16 regarding the continuous accountability of data controllers
Select Examples

Responses to the questionnaire provided examples on how countries are implementing paragraph 16 of the Privacy Guidelines, which require that data controllers remain accountable for personal data under their control without regard to the location of the data.

The *Australian* Privacy Principles (in the *Privacy Act 1988*) generally require transferring entities to ensure that an overseas recipient will handle an individual's personal information in accordance with these Privacy Principles; the entity is accountable if the overseas recipient mishandles the information.

The *GDPR* requires that personal data is only transferred to third countries under certain conditions pertaining to data protection, with a view to ensure that the protection guaranteed in the EU is not undermined when the data "travels abroad". The responsibilities of data controllers are not limited in the GDPR by the location of the data, and data controllers can be held liable for damages caused by processes infringing the Regulation irrespective of where the data are located, unless the controller can establish that they are in no way responsible for the damage (Art 44, 82(2)-(3)) (European Union, 2016[4]).

The *EU-U.S. Privacy Shield* provided that to (onward) transfer personal data (received from the EU) to a third party acting as an agent or controller, organisations had to "take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organisation's obligations under the Principles" (Art 3(b)). Under the Privacy Shield, an organisation was responsible for personal information that it received and subsequently transferred to a third party acting as an agent or controller on its behalf, and remained liable if that agent processed the information in a manner inconsistent with the *Privacy Shield's* privacy principles unless it could prove that it was not responsible for the event giving rise to the damage (Art 7(d)) (International Trade Administration (US), n.d.[13]). The Privacy Shield was invalidated by the Court of Justice of the European Union in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case C-311/18) ("Schrems II").

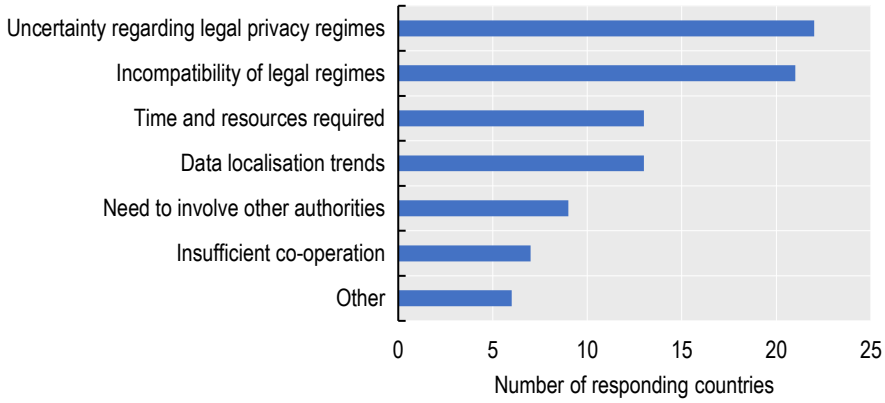
In the *United States*, the Federal Trade Commission investigated and settled a case against GMR Transcription Services, a company that provides medical transcription services, for inadequate data security measures that unfairly exposed the personal information of thousands of consumers on the open Internet having made it publicly available on a major

search engine. In particular, in outsourcing services, GMR did not require its contractor typists to implement security measures, such as installing anti-virus software or requiring authentication for data access requests. The files were transmitted in clear and readable text on a server that was configured so that they could be accessed online by anyone without authentication. The settlement agreement required GMR to implement a comprehensive information security program and submit to regular evaluation amongst other things (Federal Trade Commission (US), 2014[14]).

5.3.3. Challenges

83. In identifying the main challenges to transborder data flows, respondents to the Privacy Guidelines Questionnaire most often noted "uncertainty regarding legal privacy regimes", followed by "incompatibility of legal regimes" (see Figure 6). Time and resources required to enable transborder data flows, and recent trends in favour of data localisation, were other popular responses given by countries. In the April 2020 DGP virtual meeting, it was noted that the survey answer "incompatibility of legal regimes" is unclear and needs further unpacking, especially in the context of interoperability, enforcement and transborder data flows. In particular, it is not clear which legal regimes were being referred to (and in particular whether they are the regimes of adherents or non-adherents to the Privacy Guidelines), and where that incompatibility lies. This ambiguity should be noted in any conclusions drawn from this question of the survey. Further work may be useful to elucidate what respondents meant in selecting this answer in the survey.

Figure 6. Main challenges to transborder data flows



Source: 2019 Privacy Guidelines questionnaire.

84. There was a strong consensus among experts and delegates that there is an important role for the OECD to play in facilitating the free flow of data while maintaining personal data protection and international co-operation. In considering the OECD's role in the context of transborder personal data flows, international privacy enforcement co-operation and interoperability, many responding countries said in their responses to the privacy questionnaire that they considered the DGP's role to include identifying and sharing good practice, evidence gathering and knowledge sharing. Some explained that the Privacy Guidelines are an important international standard or benchmark that have been useful in guiding countries' development of national privacy legislation that is harmonious with other jurisdictions. The harmony across jurisdictions was said to encourage co-operation and better data privacy practices across the globe. One responding country explained

that it considered the OECD's role to involve setting standards for data governance to facilitate transborder data flows with trust. Another responding country urged further research work to be done by the OECD on the value of cross-border data flows and the economic impacts of barriers to data flows.

85. Overall, 20 responding countries (65%) considered the language of Part Four to be appropriate and corresponding to the objectives of the Privacy Guidelines. Four responding countries said the language of Part Four was not appropriate or did not correspond to its objectives. A number of issues were identified by those countries as useful for inclusion in Part Four, namely data localisation; government access to personal data held by the private sector; law enforcement access to data; principles for onward data transfers; and stronger language to ensure that, when data are transferred, adequate safeguards are put in place both by the exporters and the importers so as to ensure the continuing level of protection after the transfers. One responding country suggested modifying the "scope of application of the law to investigate and sanction extraterritorial violations of [its] law" as a way forward. Some respondents (48%) further considered that there was scope to expand the Explanatory Memorandum concerning Part Four of the Privacy Guidelines, in particular to take account of emerging trends in data localisation and barriers to transborder data flows. In general, adhering countries considered that the issue of data localisation has gained prominence since the 2013 review, and that there is a lack of consensus regarding appropriate localisation requirements. One country suggested that it may be useful to develop different data categories to provide guidance on the different types of data that can flow across borders and those likely to be of concern to governments due to the sensitivity of the data (for example, national defence, military data). A suggestion was also made to assist in the strengthening of co-operation between authorities, recognising that different personal data protection schemes exist (and perhaps discussing how interoperability is developing among privacy frameworks). Finally, one country suggested expanding the Explanatory Memorandum to address how appropriate safeguards can be implemented to ensure that domestic privacy legislation and data subject rights (including the right of redress) are not circumvented by transborder data flows.

86. At its meeting in November 2019, the DGP discussed the ongoing review and the interim report. Countries agreed with a proposal brought by Japan for the DGP to conduct further research into emerging barriers to data flows and data privacy protection before the final submission of the report [DSTI/CDEP/DGP/M(2020)1]. Two emerging barriers were proposed for additional research: data localisation and "unlimited" government access to personal data held by the private sector (UGA).

87. In relation to UGA, Japan's proposal noted that "unlimited government access to personal data held by the private sector not only affects privacy but also organisations. Organisations will hesitate to transfer personal data to countries with such government access, as this has the potential to hinder their accountability efforts and may lead to non-compliance with privacy laws or invasions of privacy of their customers." The proposal was made in the context of the G20 Osaka Track focus on data free flow with trust, first espoused by former Prime Minister Shinzo Abe in a speech at the World Economic Forum's annual meeting in Davos, Switzerland, in January 2019.

88. The two issues were the subject of further scoping exercises by the secretariat, by way of reports prepared by external expert consultants. On data localisation, to inform discussions, Professor Dan Jerker B. Svantesson was engaged to draft a focused research report on the trends and challenges of data localisation [DSTI/CDEP/DGP(2020)7/REV1]. The foundation of the report was a 2015 paper written by Professor Christopher Kuner, "The Governance of Globalized Data Flows – Current Trends and Future Challenges" [DSTI/ICCP/REG(2015)3]. To progress the work on UGA, the transparency reports produced by companies on government requests for access to personal data held by them were examined with a viewto providing a snapshot as to the nature and

frequency of government requests and understanding (if possible) the extent to which governments are obtaining access to personal data held by the private sector. The findings of these two reports are summarised in Box 2 and 3 respectively below.

Box 2. Analytical Report on the Trends and Challenges of Data Localisation

This report mainly focuses on data localisation requirements providing an overview of the phenomenon of data localisation, its characteristics, uses and the concerns to which it may give rise. It does not attempt to address holistically all aspects of data localisation. In particular, it does not attempt to thoroughly engage with the trade dimension of data localisation, including approaches taken in regional trade agreements and at the World Trade Organisation.

In the report, 'data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.

The report's review of trends within, and attitudes towards, data localisation amongst countries, consumers, industry and the expert community, highlights a complex situation in which data localisation is both seen as useful and as a significant threat and obstacle. Importantly, some forms of data localisation are largely uncontroversial, while other forms are generally seen as problematic, although there is still insufficient evidence on the economic impacts.

The report emphasises the need to recognise that data localisation has the potential to directly and significantly impact cross-border data flows, but suggests that, generally, the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation measures.

Further, the report asserts that, whether a specific requirement is classed as a data localisation measure is not, on its own, determinative for whether such a requirement is incompatible with the Privacy Guidelines. More specifically, the report sets out a number of recommendations arguing that, in the context of the Privacy Guidelines, the proportionality test articulated in paragraph 18 should be considered a key mechanism for the evaluation of data localisation measures. In this context, the report suggests that the OECD should initiate work to map out what guidance or good practice for the application of the proportionality assessment articulated in paragraph 18 of the Privacy Guidelines, can be gained from sources such as national laws, in international law and e.g. in EU law, WTO jurisprudence, academic literature and various trade agreements.

The report also emphasises that where a legal or administrative requirement is found to constitute a data localisation measure, and it amounts to a restriction to transborder flows of personal data under paragraph 18 of the Privacy Guidelines, the assessment of whether it is proportionate (under that same paragraph) to the risks presented, ought to take into account multiple factors such as : a) the sensitivity of the data; b) the purpose and context of the processing; c) the extent to which it is demonstrated that the data localisation measure effectively achieves the goals for which it was introduced; d) whether there are any less restrictive measure that could be enacted; e) the direct and indirect, domestic and international, implications of the measures; f) evidence of intent where it is possible to establish; g) the implications likely to arise if also other countries adopt the same measure ('scalability' as a consideration in the assessment of proportionality).

Box 3. Report on Current Practices in Transparency Reporting

This report, prepared by Dr. José Tomas Llanos, consultant to the OECD, analysed current practices in transparency reporting from a sample of 20 Internet-based companies and, on the basis of this information, identifies commonalities and trends, offers insights and highlights best practices capable of improving the comparability and informative value of transparency reports [DSTI/CDEP/DGP(2020)8/REV1].

Results from the study indicate that the information publicly available in the transparency reports does not allow for a comprehensive analysis of the reasons why governments request access to personal data from the private sector.

Dr Llanos presented an overview of the draft report at the April 2020 DGP meeting [DSTI/CDEP/DGP/M(2020)3]. The draft was then circulated to the DGP delegates for comment in July 2020 and its recommendations further discussed at the virtual Roundtable on Data Localisation and Trusted Government Access to Data, on 5-6 October, 2020. Experts and delegates agreed that companies' transparency reporting practices have limited informative value, particularly insofar as they are currently too heterogeneous, the data is based on self-reporting, and it is not independently obtained or verifiable. Thus, it is difficult to draw reliable inferences about the extent to which governments are requesting and obtaining access to personal data. Guidance based on common high level principles (e.g. accountability, transparency, reliability, comparability, accessibility) is needed. Governments have, however, a key role to play in providing comprehensive information on the reasons, authorities, limits, and frequency of government's access to personal data. Such information is critical to evaluating both the effectiveness and the need for various types of government surveillance activities.

The report also highlights the relevance of the accountability principle of the Privacy Guidelines and of paragraph 16 in the context of data localisation and recommends that the review of the OECD Privacy Guidelines engages with the potential compliance and enforcement issues that data localisation may cause.

Finally, the report recommends that, either the Guidelines or the Explanatory Memorandum be revised to directly address data localisation and provide a clear definition.

Outcomes of the expert consultation, workshop and survey

89. Cognisant of the limitations of the work done on transparency reporting and the proposal by some countries to address government access to data more broadly within the scope of the review of the Privacy Guidelines, the Secretariat held an Expert Consultation on 7 July 2020 and a two-day Workshop on 5-6 October.

90. In July 2020, the OECD Secretariat also circulated a brief, voluntary survey to adhering countries. The survey included questions to clarify countries' understanding of the term "unlimited" and identify common limitations and safeguards to government access to private sector data reflecting shared values.

91. The survey itself was voluntary, and responded to by 17 adhering countries. Questions were asked regarding: (i) terminology, and whether or not 'unlimited' appropriately encompasses

the issue; (ii) whether there are legislative standards for governmental access; (iii) whether access should be necessary and proportionate to achieve a legitimate aim; (iv) transparency (to the public in general regarding how the government may access private sector data; and individual notice to those directly affected); (v) independent oversight; (vi) statutory limitations on use/retention of data; (vii) judicial redress; and (viii) standards for transparency reporting by the private sector.

92. The survey results suggest commonalities surrounding: (i) standards for governmental access established in legislation; (ii) legislation or jurisprudence requiring government access to be necessary and proportionate to achieve a legitimate aim (including for national security and law enforcement purposes); (iii) transparency to the public regarding when and how the government can access personal data held by the private sector; (iv) government access authorised by an independent judiciary or authority whose activities are governed by the rule of law (with possible exception for emergency circumstances); (v) government access overseen by at least one legitimate and independent body/authority/regulator; (vi) judicial redress for individuals when there has been a violation of the established standards in a democratic society.

93. It is noted that this survey was conducted as a means of supporting and informing the discussions at the October roundtable, and a more comprehensive survey may be needed to support any future analytical work. Accordingly, the above elements are considered non-exhaustive, and aim to provide a starting point for discussions.

94. In their responses to the survey and at the October 2020 Roundtable DGP delegates agreed that unlimited government access in this context means "unconstrained" or "disproportionate" access by the government to data held by the private sector. Delegates agreed at the October 2020 Workshop that "unlimited" government access to personal data held by the private sector is an impediment to transborder data flows and an urgent and important issue that must be addressed. There was consensus that the OECD is a good place to address this issue but many countries voiced concern that the DGP does not have the necessary expert representation (national security and law enforcement agencies) to address the matter as holistically as might be necessary. Delegates acknowledged that the DGP's mandate could limit the scope of further work, which would therefore benefit from cross-disciplinary collaboration.

95. Suggestions were also made to clarify the intention behind using the language of "unlimited" government access and shift the tone to reflect the shared values and practices by highlighting trust in government access to data, and frame the proposal under the revised title of "Trusted Government Access to Private Sector Data". The stated advantage of this framing is that it incorporates both rule of law and the transparency and oversight, thereby ensuring that the government acts in accordance with what the law provides. Some adhering countries also suggested to frame the proposal under the title of "Principles on Government Access to Personal Data held by the Private Sector" or "Trusted Access by Governments to Personal Data" to avoid questions of terminology.

96. In subsequent discussions, delegates indicated that it would be most productive for this work to address what adhering countries have in common, particularly best practices in national laws and regulations concerning 'guarantees' or 'restraints' on government access, in harmony with the basic principles in the Privacy Guidelines. It was noted that relevant stakeholders from national law enforcement and intelligence agencies also need to be involved, in order to have meaningful discussions of how individual privacy interests relating to government access are protected in countries with democratic legal systems based on the rule of law and constitutional protections of individual rights.

97. Adhering countries view this as an opportunity to unite around principles defining in what circumstances and within what constraints and safeguards government access to data is legitimate,

necessary and proportionate, in stark contrast to unlimited access practices of some authoritarian regimes. Given the importance of the subject and its scope beyond the mandate of the DGP, requiring consultation with other bodies such as the Working Party on Security in the Digital Economy (SDE) and other stakeholders within government such as law enforcement and national security agencies, delegates requested that the matter be formally raised at the CDEP. In particular, delegates proposed that CDEP consider leading the drafting and adoption of a high-level statement or a set of principles that may be adopted as an OECD Recommendation regarding when government access to personal data held by the private sector is appropriate.

98. Accordingly, in November 2020, the issue was raised at the CDEP. On 22 December 2020, the Committee issued a statement reflecting its views, concerns and future plans with regard to government access to personal data held by the private sector.[20] In particular it decided to "*conduct further work to deepen the understanding of approaches in OECD countries*" and to examine "*the possibility of developing as a matter of priority, an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector*". The work will seek to "*elaborate a set of common and coherent good practices and legal guarantees from across OECD countries for best reconciling law enforcement and national security needs for data with protection of individual rights*".

99. It is envisioned that these principles and practices will address the legitimate public purposes that may justify government access to personal data held by the private sector and the relevant safeguards for reconciling those needs with protection of individual rights. Such safeguards and their application would facilitate the promotion and protection of data free flow with trust.

100. The Committee agreed to convene a drafting group composed of nominated government representatives and experts, including from law enforcement and national security agencies to support this work.

101. Additionally, adhering countries agreed that there is a need for additional commentary to the Supplementary Explanatory Memorandum of the Privacy Guidelines on the importance of common approaches regarding government access to personal data held by the private sector which can eventually cross-reference any principles or high level statement agreed by CDEP.

5.3.4. Conclusions and proposed next steps

102. The responses to the questionnaire suggest that, overall, responding countries implement Part Four of the Privacy Guidelines by generally enabling the free flow of personal data across borders when there are safeguards in place to protect the privacy of persons whose personal data are being transferred. A majority of responding countries had in place some restrictions on transborder data flows, either in their domestic legislation or in multilateral agreements that they are parties to. Responding countries also had in place various mechanisms to promote transborder flows, including consultations, workshops and participation in international fora (including the entering into of trade agreements).

103. Responding countries indicated that the challenges to transborder data flows primarily concerned divergence of legal privacy regimes, and the possible incompatibility of those regimes, followed by the time and resources required. This divergence can be partly attributed to the fact that many countries are in the process of updating their national privacy legislation (see also sections below). As is discussed above, responding countries also considered that trends in data localisation have increased since the 2013 revision, that unlimited government access to personal

[20] https://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm

data is an urgent and important issue that the OECD should address, and that these trends have an impact on transborder data flows. Privacy and data protection frameworks may be undermined by a lack of transparency in government actions and a lack of common approaches to government access to data.

104. In the face of these uncertainties, responding countries saw an important role for the DGP in evidence gathering and for identifying and sharing good practice. The Privacy Guidelines were generally viewed as a useful global benchmark on which countries could continue to base their own national legislation. It was recommended that future work should include expanding the Explanatory Memorandum in respect of Part Four to address barriers to transborder data flows from the increasing trends in data localisation and unlimited government access to personal data, setting out good practice drawing also on the work on enhancing access to and sharing of data. On data localisation, the DGP could usefully map out guidance on the implementation of paragraph 16 of the Privacy Guidelines and review current practice in the application of the proportionality assessment articulated in paragraph 18. Further work could also support the development of principles to unite adhering countries as to the constraints and safeguards on government access to data they have in common, based on existing good practice.

5.4. Part Five: national implementation

105. This section is based mainly on responses to the questionnaire and the expert consultation on enforcement and implementation in the context of emerging technologies that took place on 18 November 2019.

5.4.1. Background

106. As noted in the original Explanatory Memorandum, the implementation of the Privacy Guidelines is "left in the first place to national governments". Part Five is the operative heart of the Privacy Guidelines in the domestic context. It provides the general framework to guide governments' national implementation, taking into account differences of governance culture between countries. Most of the elements of this framework were included already in the 1980 Privacy Guidelines (then under Part Four), notably the adoption of laws protecting privacy and application of sanctions in case of failure to comply, measures aimed at businesses (support for self-regulation) and measures aimed at individuals (provision of remedies and means for exercising their rights, and ensuring there is no discrimination against data subjects).

107. The 2013 revision of the Privacy Guidelines included the addition of key elements (as well as some revisions in the existing ones), such as development of national privacy strategies, establishment of privacy enforcement authorities, and complementary measures, including technical measures. Considered as a whole, these elements attempt to "establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect" (original Explanatory Memorandum) (OECD, 2013[1]).

5.4.2. Implementation findings

108. All respondents to the privacy questionnaire have implemented national measures for privacy and personal data protection in accordance with Part Five of the Privacy Guidelines.

General measures

109. The prevalence of national privacy strategies (paragraph 19 a) of the Privacy Guidelines) and their components were explored in depth in a dedicated report [DSTI/CDEP/SPDE(2018)17]. This report, based primarily on the replies to the privacy questionnaire for the 2017 edition of the

Digital Economy Outlook (DEO), concluded that most countries did not have national privacy strategies, and also understood the term in different ways, but did have in place some of their basic elements (OECD, 2017[15]). The findings from the privacy questionnaire for the current review underscore these findings, focusing on the element of whole-of-government approach. The responses suggest that just under half of the respondents have a national privacy strategy or whole-of-government approach to privacy.

110. Only seven responding countries positively stated they have a national privacy strategy, while other countries noted alternative means of whole-of-government co-ordination, such as through legislation, the PEA or other dedicated entity or forum, or other policy instruments. Additional co-ordination mechanisms described by respondents were, for example, a joint statement by PEAs in the country to improve co-ordination in complaint handling and enforcement and model clauses for ordinances on the protection of personal information.

111. With regard to "laws protecting privacy" (paragraph 19 b of the Privacy Guidelines), the picture is more encouraging, with all respondents having in place some form of legislation for privacy and personal data protection. In their responses to the questionnaire eighteen of the adhering countries and one non-adhering country[21] reported that their main privacy legislation had been updated after 2013 (the year the Privacy Guidelines were revised). In ten countries (including one non-adhering country), the privacy legislation was (at the time of responding to the questionnaire) under revision, reflecting countries' attempts to adapt their national legislative frameworks to developments in the privacy landscape. Eight countries (including one non-adhering country) reported that there are plans for the revision of their privacy and data protection legislation.

112. In enacting privacy legislation, responding countries clearly take into account developments on the international level, with all but one country taking into account at least one of the available international instruments (the OECD Privacy Guidelines, GDPR, the APEC Privacy Framework or Convention 108+) in recent revisions to their privacy legislation (since 2013, and including ongoing or planned revisions).

Establishment of Privacy Enforcement Authorities

113. Paragraph 19 c) of the Privacy Guidelines refers to the establishment of PEAs. All but two[22] responding (non-adherent) countries report having established PEAs. Five countries (Australia, Canada, Germany, Mexico, and Switzerland) reported having local, provincial, state or regional PEAs in addition to a national or federal PEA. As an illustration, in the United States, the Federal Trade Commission (FTC) and several other agencies enforce laws protecting privacy. In addition to the FTC, multiple federal agencies including the U.S. Department of Health and Human Services, the Consumer Financial Protection Bureau, and the Federal Communications Commission enforce various privacy laws tailored to specific types and uses of information, such as to health information, financial information, educational records, and governmental use of personal data. States have their own laws with their own enforcement authority. Further, state attorneys general can enforce some Federal laws protecting privacy, such as the Children Online Privacy Protection Act. In all but two countries (including one non-adhering country), the PEAs oversee both private and public sectors.

[21] Brazil adopted its first general data protection law in 2018.

[22] In both cases, a national Data Protection Authority was constituted in a recently adopted law, but has not yet been established for one case.

114. Paragraph 19 c) also recommends that Member countries should "maintain PEAs with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis". This formulation, in the context of the Privacy Guidelines, refers to the need for a PEA to be free from instructions (i.e., maintain autonomy), bias or conflicts of interest when enforcing laws protecting privacy, in other words to have regulatory independence.

115. Several elements are necessary to ensure regulatory independence, in particular having autonomy with regard to both recruitment and budget. PEAs require sufficient financial and personnel resources to do their job properly and resist political influence. A lack of sufficient financial resources may seriously impede the PEA's ability to ensure fulfilment of their mandate.

116. At EU level, PEAs independence is enshrined in Article 8 (3) of the Charter of Fundamental Rights of the European Union (adopted in 2000, legally binding as EU Primary law with the entry into force of the Lisbon Treaty in 2009), which asserts that the rules laid down by the Charter "shall be subject to control by an independent authority". Independence of PEAs at EU level is also enshrined in Article 16 (2) of the Treaty on the Functioning of the European Union, which states that "the European Parliament and the Council (…) shall lay down the rules relating to the protection of individuals with regard to the processing of personal data" and that "compliance with these rules shall be subject to the control of independent authorities."

117. In the COE context, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) itself did not originally provide for the setting up of national supervisory authorities. The 2001 Additional Protocol to Convention 108, however, enhanced the data protection guarantees by setting up supervisory authorities that "shall exercise their functions in complete independence".

118. According to the Additional Protocol to Convention 108 (in para 17) "a number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions. These could include the composition of the authority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority or the adoption of decisions without being subject to external orders or injunctions." [23]

119. The procedures in place to govern the recruitment and dismissal of staff members should thus also come under scrutiny, with indirect influence able to be exerted through the recruitment process.

120. Any assessment made of what constitutes "sufficient", for the purposes of assessing the adequacy of financial and personnel resources has to be made with reference to the duties, tasks and powers of the PEAs and this is particularly complex.

121. The 2019 questionnaire on data breach notification practices [DSTI/CDEP/SPDE(2019)6] included questions on the funding sources of the respondent authorities and their composition. Out of 30 responding countries (excluding the US), 20 reported that they were entirely funded by government grants. The remaining countries reporting mixed funding explained that other sources come from chargeable services, registration or licensing fees, fines and penalties. The UK

[23] Building on Article 1 of the additional protocol, the modernised Convention 108 complements the catalogue of the authorities' powers with a provision that, in addition to their powers to intervene, investigate, engage in legal proceedings or bring to the attention of the judicial authorities violations of data protection provisions, the authorities also have a duty to raise awareness, provide information and educate all players involved (data subjects, controllers, processors etc.). It also allows the authorities to take decisions and impose sanctions.

Information Commissioner Office is for example primarily funded by registration or licensing, fees which account for around 85% to 90% of the ICO's annual budget. The responses provided indicate that the majority of PEAs are involved to some degree in the process of drafting their budget, but their ability to influence the amount of funds that they receive appears limited.

122. Over 61% of the responding countries indicated having other supervisory authorities with privacy and personal data related enforcement responsibilities, for example for specific sectors, and all countries reported that their PEAs collaborate with other authorities, notably those addressing consumer protection and digital or cyber security issues.

123. Finally, in terms of implementing sanctions, remedies and other enforcement mechanisms (paragraph 19 f) of the Privacy Guidelines), only 2 responding countries stated that their PEA or other authorities did not have any of these in cases of failure to comply with privacy and data protection laws. Monetary sanctions, enforcement notices, enforcement of corrective action, and restriction of data processing are at the top of list of measures applied (see Box 4 for select examples).

Box 4. Enforcement of sanctions and remedies by PEAs – select examples

Australia's PEA, the Office of the Australian Information Commissioner, has a range of enforcement powers, including:

- accepting an enforceable undertaking;
- bringing proceedings to enforce an enforceable undertaking;
- making a determination;
- bringing proceedings to enforce a determination;
- reporting to the relevant Minister in certain circumstances following an investigation, monitoring activity or assessment;
- seeking an injunction including before, during or after an investigation or the exercise of another regulatory power; and
- applying to the court for a civil penalty order for a breach of a civil penalty provision.

The *Canadian* Office of the Privacy Commissioner (OPC) has a number of enforcement tools with regard to the private sector, including:

- investigating complaints filed by individuals or initiated by the Commissioner;
- appearing before the Federal Court regarding matters raised by a complainant who has applied for a hearing, or on behalf of the complainant;
- making public any information that comes to light in the performance of the Privacy Commissioner's duties, if the Commissioner considers it to be in the public interest;
- auditing an organisation's privacy management practices;
- referring an organization to the Attorney General of Canada who can pursue a matter before the Courts for certain offences, including for wilfully not reporting a privacy breach to the OPC. The Federal Court may issue fines as appropriate; and

- entering into compliance agreements.

With regard to the public sector, the Commissioner can conduct investigations into complaints arising from, and reviews into, the personal information handling practices of government institutions; he/she can also make findings and recommendations where appropriate.

The OPC does not have order-making powers with respect to either law.

In the *United States*, the Federal Trade Commission (FTC) can seek redress for consumers, disgorgement of ill-gotten gains, the rescission of contracts or other equitable remedies, and can halt unfair or deceptive practices. Further, the FTC can seek civil penalties for violations of its orders or rules. This includes civil penalties for violations of the Fair Credit Reporting Act or the Children's Online Privacy Protection Act.

Finally, *France's* CNIL has the following enforcement powers:

- issue a warning;
- send the company formal notice;
- temporarily or definitively restrict a processing operation;
- suspend data flows;
- order them to comply with data subjects requests;
- requests to exercise their rights;
- order to rectify, limit or erase data;
- issue an administrative fine of up to €20 million, or – for companies – up to 4% of their global yearly turnover. These financial sanctions can be made public; and
- in cases of immediate and grave violations on fundamental rights and freedoms, the CNIL's Chair can refer a request to the competent jurisdiction to order any necessary security measures. It can also denounce any violations of the French Data Protection Act to the State Prosecutor.

Measures addressed to specific stakeholders

124. Part Five of the Privacy Guidelines provides for measures aimed at the business community (paragraphs 19 d) and g)) and at individuals (paragraphs 19 e), f), g) and i)), including technical measures (highlighted specifically in paragraph 19 g)). As the responses to the privacy questionnaire suggest, all but two respondents apply measures addressed at these groups to promote privacy and personal data protection. Some of these initiatives were described in detail in the national privacy strategies report [DSTI/CDEP/SPDE(2018)17].

125. Additionally Paragraph 19 h) of the Privacy Guidelines refers to the role of actors other than data controllers. In this context, 84% of the respondents include in their legislation a definition of "data processors" and of "data controllers", which suggests they recognise that in the ever complex data ecosystem, these actors may bear certain responsibilities for privacy and personal data protection.

126. Responding countries deploy an array of policy measures to promote privacy and data protection by *businesses*, prominently good practice guidelines and public awareness campaigns (education and awareness raising are mentioned explicitly in paragraph 19 g) of the Privacy

Guidelines). Specifically, over 83% of the responding countries, the PEAs have issued guidance or official position papers in relation to privacy or data protection impact assessments (16 countries), consent forms (13 countries), guidance to consumers regarding redress on possible privacy violations (13 countries), targeted advertising and AI (11 countries each). One country mentioned specifically guidance aimed at SMEs and sectoral guidance. Nevertheless, incentives for self-regulation by businesses, highlighted specifically in paragraph 19 d) of the Privacy Guidelines, are reported only by 39% of the respondents.[24] Certification schemes were mentioned by just less than half of the respondents as a means they employ to further privacy and data protection by businesses (see Box 5 for select examples).

Box 5. Privacy and data protection certification schemes

Certification schemes are a means for organisations to demonstrate their – or their services' or products' – compliance with specific standards. They can facilitate the work of PEAs and empower users to make better-informed choices; in this way, they can also serve as a competitive advantage for businesses. Different models of certification schemes exist, varying in scope and in operation.

In *New Zealand*, the Privacy Commissioner awards the "Privacy Trust Mark" to a good or service that warrants recognition for excellence in privacy, recognising the growing importance, and difficulty, for consumers to identify products that are outstanding in the way they handle personal information and manage privacy considerations. The trust mark identifies such products and services (not agencies or organisations), based on set criteria and submitted applications (New Zealand, Office of the Privacy Commissioner, 2013[16]).

Mexico operates a certification and accreditation scheme, by which the Ministry of Economy approves accreditation entities, which in their turn accredit certification bodies to certify individuals and organisations who are in charge of personal data processing (Mexico, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, n.d.[17]).

In *Singapore*, the Infocomm Media Development Authority (IMDA) launched its "Data Protection Trustmark Certification", a voluntary enterprise-wide certification for organisations to demonstrate their accountable data protection practices and their compliance with Singapore's Privacy and Data Protection Act (PDPA) (Singapore, IMDA, 2019[18]).

127. Other measures related to the business sector mentioned by respondents were privacy compliance assessments or audits carried out by the PEA as an educational process to raise awareness, self-assessment tools provided by the PEA to organisations, operating an enquiries or reporting line, convening multi-stakeholder dialogues on specific issues, holding workshops, briefing sessions and town-hall meetings, and offering training and educational resources on the PEA website.

128. In terms of determining the impact or success of the measures deployed, only four of the respondents reported having in place mechanisms to this end. Such mechanisms included quarterly

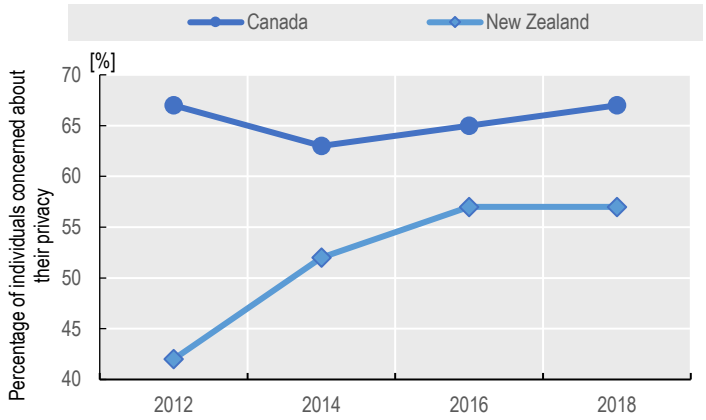
[24] Notwithstanding, in some countries sectoral authorities encourage privacy promoting self-regulation or industry standards in the relevant industries. This is the case, for example, with the Canadian Radio-television and Communications Commission.

statistics on specific policies, regular surveys, and analysis of web traffic (including of social media awareness-raising campaigns).

129. All but one responding country reported that they implement measures to enhance *individuals'* understanding and control over their personal data. Primarily, these measures concern education and awareness raising campaigns (paragraph 19 g) of the Privacy Guidelines), for example through the PEA website, social media, online trainings and educational material, responses to public inquiries, dedicated sessions or workshops and general campaigns (such as the APEC countries "privacy awareness week"). In this context, 42% of the respondents noted that their PEAs issued guidance to consumers regarding redress for possible privacy violations. While establishing awareness and understanding of privacy are the first step, as described in more detail in the National Privacy Strategies report [DSTI/CDEP/SPDE(2018)17], responding countries also implement measures to empower individuals and enhance their control over their personal data, for example by simplifying complaint procedures or by facilitating access to personal data in government services. These measures relate to both "means for individuals to exercise their rights" and "remedies in case of failure to comply with laws protecting privacy" (paragraphs 19 e) and f) of the Privacy Guidelines, respectively) (see also the discussion of data subjects' rights in section 3.1.2 above).

130. In terms of the effectiveness of the measures applied, 14 responding countries reported that they conduct surveys or otherwise regularly gather and analyse data on public perceptions of privacy (see, for example, Figure 7).

Figure 7. Sample of PEA public surveys



Source: Canada: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#fig03; New Zealand: https://www.privacy.org.nz/news-and-publications/surveys/privacy-survey-2018/.

131. 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, with a quarter of respondents not having in place guidance or other means to encourage the adoption of technical measures for privacy protection (for example, anonymization, cryptography, de-identification, differential privacy and pseudonymisation). Generally speaking, implementation at national level concerns guidance, recommendation or reports by the PEA on the application of privacy enhancing technologies, primarily pseudonymisation and anonymisation. One country mentioned a blog that their PEA maintains, where they issue a number of posts on

technical measures to protect privacy, including information on the basics of cryptography and artificial intelligence. Four responding countries reported that they are monitoring the success of these measures, through reports, surveys, audits and administrative fines.

132. Finally, while not explicitly mentioned in the Privacy Guidelines, the combination of emerging technologies (such as AI, big data analytics, blockchain, IoT) and personal data may have implications on *society as a whole,* for example in the context of targeted misinformation through social media campaigns. There seems to be growing awareness of countries to this issue, with 71% of respondents reporting having in place measures to address potential societal harms of such use of personal data, notably in the form of awareness campaigns (half of all respondents) and in the context of political campaigns (one third of all respondents; see Box 6).

Box 6. Use of personal data in political campaigns

The rise of the Internet has created new, and at times unregulated avenues for political parties to promote their platforms. Compounded with the prevalence of social media and increasing personal data collection and processing, an opportunity was created for political parties, and other advertisers, to target their advertising campaigns to specific audiences, based on demographic and other characteristics. The ability to – in some instances covertly – designate certain messages to select audiences raises unprecedented questions of autonomy, public deliberation and transparency (Council of Europe, 2017[19]).

Aware of these developments, countries have begun taking action, notably by examining the way political campaigns can and do use personal data, and by setting regulations or guidance in this context. The United Kingdom Information Commissioner's Office's (ICO) 2018 report, *Democracy Disrupted? Personal Information and Political Influence*, for example, determined that political parties "are increasingly using personal information and sophisticated data analytics techniques to target voters" and that there is a "significant shortfall in transparency and provision of fair processing information" that could compromise the integrity of the elections themselves. The report provided recommendations and concrete steps that political parties were required to take, with mandatory follow up audits by the ICO (Information Commissioner's Office (UK), 2018[20]). The report is complemented by guidance to both individuals and organisations on the use of personal data in political campaigns (Information Commissioner's Office (UK), n.d.[21]; Information Commissioner's Office (UK), 2018[22]).

Norway's data protection authority undertook a similar exercise, where it explored the way its different parties were using "digital targeting of political messages". The 2019 report, *Digital Targeting of Political Messages in Norway*, concluded that while targeted messaging can have beneficial impacts such as providing voters with more relevant information and increasing their political engagement, it bears risks to the individual – such as privacy, manipulation and discrimination – and also to the legitimacy of the democratic process. Based on its findings, the report provided six recommendations for political parties to consider when using digital targeting technology (Norwegian Data Protection Authority, 2019[23]).

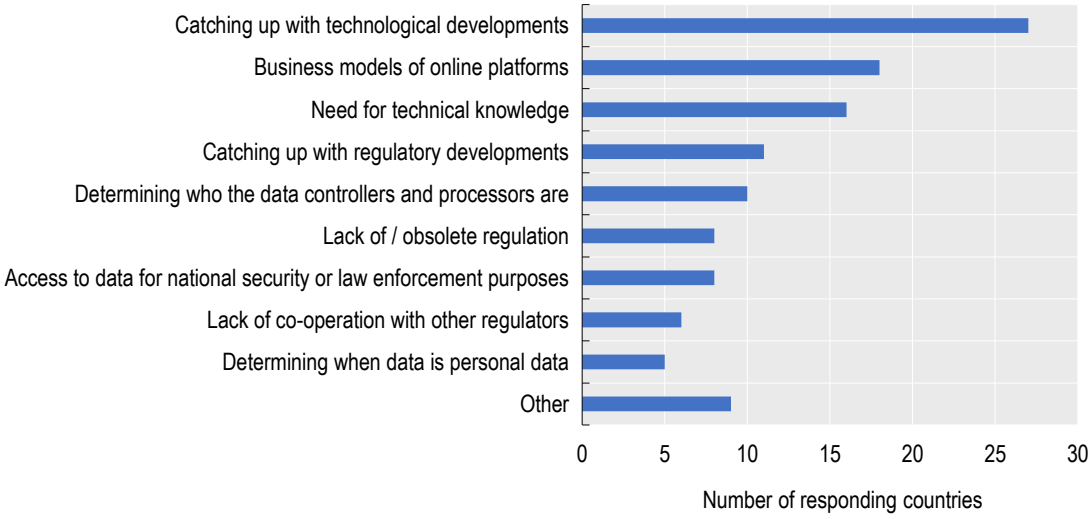
5.4.3. Challenges

133. As described in the process paper [DSTI/CDEP/SPDE(2018)8], a prominent challenge in implementing the Privacy Guidelines, including at a national level, relates to technological developments that have reshaped the privacy landscape. With dramatic changes in the volume,

velocity and variety of personal data collection and use ("big data"), enabling and also triggered by technological improvements, the role of personal data in economies and societies has transformed, challenging our understanding of personal data and how they are and should be collected, processed and protected.

134. This notion is reflected in the responses to the privacy questionnaire, with 87% of respondents listing "catching up with technological developments" as a challenge to their current regulatory framework. Related challenges of "business models of online platforms" and "need for technical knowledge" came next in line in respondents' selections (see Figure 8). Other challenges mentioned by responding countries were barriers to data sharing, including a lack of a whole-of-government approach and inconsistencies between national and sub-national legal frameworks, barriers to transborder flows of personal data (see section 3.3.3 above), intra-regional coordination, and adjusting the regulatory framework to SMEs without compromising privacy protections. One responding country also mentioned the low level of compliance with legal frameworks as one of the main challenges, perhaps due to a variety of factors including lack of knowledge/uncertainty, poor implementation, outdated policies, incompatible business models and strategies, and lack of private sector commitment.

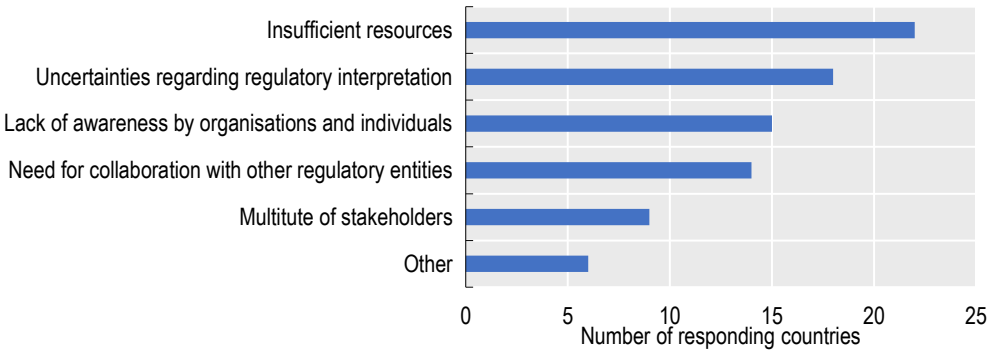
Figure 8. Main challenges to regulatory frameworks



Source: 2019 Privacy Guidelines questionnaire.

135. When asked about enforcement challenges, responding countries most often cited insufficient resources, followed by uncertainty in interpreting regulatory frameworks (which is also linked to its application to technological developments) (see Figure 9). Nearly 45% of the respondents considered the need for collaboration with other regulatory authorities, such as competition or consumer protection, as an enforcement challenge, notwithstanding the fact that all of them reported that such collaboration was taking place in practice (see paragraph 113 above). One responding country also mentioned the inability of its PEA to issue binding orders as an enforcement challenge, noting that it was the PEA's position that investigative powers alone were insufficient and needed to be complemented by powers to issue binding orders and fines. The implications of technological developments are present in the enforcement context as well, as noted by one country, which reported that the resources needed include qualified "technical staff, to understand and operate in the changing technological environment".

Figure 9. Enforcement challenges

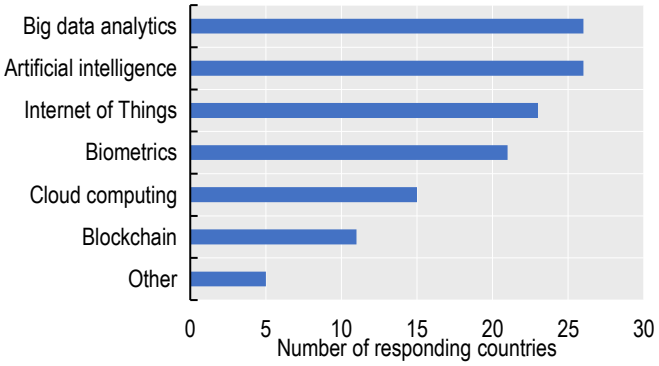


Source: 2019 Privacy Guidelines questionnaire.

136. Given the prominence of technological developments and the challenges they pose to national implementation of the Privacy Guidelines and of privacy and personal data protections in general, the privacy questionnaire included a dedicated section to this issue, to better understand responding countries' perceptions and inform the future work of the OECD in this regard. In their responses, over 80% of countries mentioned AI and big data analytics as the technologies that pose the main challenges for privacy and personal data protection, followed closely by the Internet of Things (IoT) and biometrics (see Figure 10) as well as facial recognition and financial technologies ("fintech", including new payment methods such as Libra). When asked about the nature of the challenges of emerging technologies, ethical issues, including bias and discrimination,[25] emerged as a main concern for all but two respondents. 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 main concerns (68% and 77% of respondents, respectively). In their comments by written procedure, responding countries added concerns including increasing incentives for hackers to steal personal data (due to their greater value), a lack of public understanding of how much personal data are gathered and how they are used, personalised pricing, state surveillance, and technical aspects, such as anonymisation and re-identification, algorithmic transparency and data portability.

[25] Discrimination is mentioned in Part Five of the Privacy Guidelines, paragraph 19 i): "ensure that there is no unfair discrimination against data subjects".

Figure 10. Emerging technologies that pose the main challenges for privacy and personal data protection



Source: 2019 Privacy Guidelines Questionnaire.

Responses to challenges posed by technology

The need for regulatory innovation

137. When asked about the possibility of current privacy and personal data legislation to address the challenges identified, respondents most often referred to the principle-based nature and technological neutrality of their legislation. Other responses concerned sector specific rules, a risk-based approach and data protection impact assessments, and regular reviews and revisions. Notwithstanding, responding countries noted that understanding how current laws apply to emerging technologies, such as AI, and their impact on consumers, remains a challenge.

138. Responding countries are already responding to these challenges, including through revising their current privacy regulatory framework or developing dedicated regulation. Just over half of the respondents reported having in place or under development additional laws or regulations, or plans to revise the existing privacy legislation, to strengthen privacy and personal data protection in the context of social media and online platforms (10 respondents), of emerging technologies[26] (such as AI, big data analytics and IoT) (9 respondents), and of targeted advertising or pricing (9 respondents). Another possible response to challenges posed by technology concerns enhancing enforcement efforts, for example by expanding the roles, responsibilities and authority of the PEA. In this respect, two countries reported recent legislative changes to expand or streamline the mandate of their PEAs, and two other countries reported on draft legislation to enhance the powers of their PEAs by expanding the enforcement means at their disposal. Twelve responding countries said that they have developed incentives for self-regulation to further privacy and data protection by businesses.

139. Furthermore, responding countries are employing, developing or considering the development of a range of policy measures for *regulatory innovation* in the context of emerging technologies, most commonly regulatory sandboxes and experimentation (Australia, Israel, Norway, Singapore, Thailand and the United Kingdom). Other measures reported include development of international standards for specific technologies (such as blockchain), a Digital Charter, a privacy research grants programme, and AI auditing framework.

[26] Data portability and re-identification are some areas mentioned specifically by countries where revisions were necessary to strengthen privacy and personal data protection against the backdrop of emerging technologies.

140. Given the prominence of regulatory sandboxes, and the widespread interest in the topic from countries, in September 2020 the Secretariat co-hosted a Workshop on the topic with *Business at the OECD* (BIAC). A Regulatory Sandbox was defined as a controlled environment wherein for some predetermined amount of time and for a defined use case, a close collaboration between firms and a regulator enables firms to test new data uses, technologies and applications while receiving regulatory guidance. Companies that participate in the Sandbox benefit from an understanding about the approach a regulator will take to assess whether privacy by design and other regulatory requirements have been effectively implemented. At the same time, Regulatory Sandboxes enable regulators and governments to understand the implications of different policy choices and respond to uncertainties introduced by new technologies, new data uses, and rapid innovation. They enable regulators to consider the practical application of the law in new or novel use cases where norms of compliance may not yet be established and crystalize their positions on new technology and data uses.

141. Presentations demonstrated however the risk of divergent understandings of the approach and its applications. To be successful, regulatory sandboxes need to afford companies with the appropriate level of regulatory forbearance to allow them to experiment in the Sandbox without fear of exposure to an enforcement action. Regulators will thus need to determine what legal assurances are appropriate, and how those assurances can be articulated to companies clearly. At the same time, the sandbox does not provide regulatory forbearance once the sandbox ends and/or for other activities. A goal of the regulatory sandbox for privacy is to develop guidance, not provide the suspension of legal requirements.

142. Regulators also need clearly articulated criteria to evaluate participant applications and determine what projects are appropriate for the sandbox as well as criteria against which the findings of the regulatory sandbox should be clearly articulated and to determine when broad publication is appropriate, and what steps should be taken to protect confidentiality and intellectual property interests.

143. Finally, regulators and companies participating in the sandbox will require guidance about how to address cross-jurisdictional issues that may arise in, for example, a sandbox project that involves more than one regulatory regime, e.g., data protection regulations and telecommunications law; or data protection law and financial services regulation. A framework may also be needed to assist in creating and running sandboxes that involve the use of data that is transferred and shared across borders. Such a multinational instrument would articulate the role of PEAs, and establish measures to be taken to promote cooperation between authorities in administering the sandbox and extracting benefits.

144. Responding countries generally agreed that a greater understanding of the benefits and risks of regulatory sandboxes – aided by a common terminology and use cases – would likely prove useful for any future developments.

The policy perspective

145. In addition to regulatory reforms and regulatory innovation, countries are addressing challenges posed by emerging technologies through policy responses, primarily by (i) the development of new frameworks; (ii) the creation of new bodies or institutions; and (iii) guidance on specific technologies.

i. New frameworks. 13 countries reported that they are addressing, or are planning to address, technological challenges through the establishment of new data governance frameworks, for example by setting additional norms on the management of the availability, accessibility, usability, quality, interoperability,

and ownership of the data collected, processed and stored. 9 of those 13 countries have or are developing sector-specific data strategies or a national data strategy. However, it would appear that respondents had different perceptions of what data governance frameworks encompass, ranging from more limited scope (for example, the "notifiable data breach scheme" introduced in Australia in 2018) or technology-specific (see Table 1 on AI frameworks), to broader ones (the United Kingdom's "National Data Strategy", Turkey's planned national data strategy, Japan's "Tech Strategy to Grasp the Future", Canada's Digital Charter, and ASEAN's Framework on Digital Data Governance reported by Singapore).

Table 1. Some Responding Countries' AI frameworks

Country	Name	Status
Australia	AI: Australia's Ethics Framework	Being implemented
Brazil	National AI Strategy	Planned
Canada	Directive on automated-decision making	Effective April 1, 2019, with compliance required by no later than April 1, 2020[27]
Chile	National Policy on AI	Planned
Estonia	Action plan for implementing AI in public services	Approved
Finland	Ethical Guidelines for AI	Planned
Israel	National AI plan	Planned
Japan	Principles for human-centric AI society	Adopted
Norway	National strategy on AI	In progress (to be published by the end of 2019)
Singapore	Model AI Governance Framework	Published in January 2019 (for voluntary adoption by industry)
Slovenia	National AI Strategy	Planned
Thailand	Ethical issues in AI	Early stages
United Kingdom	Accountability Framework for AI Audits	Accountability framework for AI audits
United States	Accelerating America's leadership in artificial intelligence	Signed in February 2019

Note: A general overview of countries' AI policies and initiatives can be found in chapter five of the OECD publication *AI in Society* (OECD, 2019[24]). The OECD AI Policy Observatory (OECD.AI, launched in February 2020) hosts a database of national AI strategies and policies.
Source: 2019 Privacy Guidelines questionnaire.

ii. New bodies or institutions. Just over a quarter of the respondents reported having established new institutions, bodies or centres to address the privacy and data protection challenges posed by technology. Australia recently appointed an (interim) National Data Commissioner, supported by a National Data Advisory Council, to develop "new data sharing and release legislation [to] improve the sharing, use and reuse of public sector data" (Australian Government, Office of the National Data Commissioner, 2019[25]). The United Kingdom recently established a Centre for Data Ethics and Innovation to identify ethical issues raised by emerging

[27] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

technologies, agree on best practices around data use, and develop potential new regulations to "build trust and enable innovation in data-driven technologies" (Department for Digital, Culture, Media & Sport (UK), 2018[26]).[28] 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. Turkey and the Slovak Republic have further established hubs for digital innovation and transformation. Finally, while not a new body, in 2017, New Zealand appointed its Chief Statistician as the Government Chief Data Steward.

iii. Guidance on specific technologies. As is stated above, the majority of the responding countries reported having issued guidance on technology related aspects of privacy and personal data protection, such as privacy or data protection impact assessments, targeted advertising, AI, IoT and app development. Other areas for guidance mentioned by certain countries were data analytics, connected cars, data protection by design, direct-to-consumer genetic testing, smart cities and drones, blockchain and data sharing. Singapore is currently in the process of developing a self-assessment guide for organisation, to complement its Model AI Governance Framework.

iv. Guidance on compliance with privacy legislation generally. The results of the questionnaire demonstrate that countries have put considerable resources into the development of guidance to individuals and organisations. There was considerable overlap, particularly on the rights of data subjects, how to comply with the GDPR provisions (particularly in relation to transborder data flows and the requirement for appropriate safeguards and essentially equivalent levels of protection, obtaining valid consent, and conducting data protection impact assessments), how to deal with a data breach (including mandatory reporting), and guides for IT security.

v. Additional policy measures. Finally, some responding countries reported the use or development of complementary policy measures to address the challenges posed by emerging technologies, including with a view to integrate ethical considerations in the context of privacy and personal data protection. For example, at least two countries reported on research strategies; in one responding country, the PEA developed a technology strategy to enhance its technological understanding and ensure it is effectively communicated; and another responding country uses mandatory privacy impact assessment to evaluate privacy risks in emerging technologies used by government agencies. Some countries reported using or planning to use multi-stakeholder dialogues on new digital technologies and their implications on privacy issues to identify best practices. One responding country indicated having a Memorandum of Understanding on co-operation and exchange of information between authorities on financial information and technologies. Finally, another country said that it was engaging in an exercise to map government information and reported having established a policy on the accessibility of public databases and the transfer of information between government ministries.

[28] Perhaps with a greater focus on privacy and data protection, it should be noted that, in October 2018, the United Kingdom ICO has created the Technology Policy and Innovation Directorate, which is tasked with identifying, understanding and addressing emerging technologies with privacy implications.

5.4.4. Conclusions and proposed next steps

146. The responses to the questionnaire suggest that overall, responding countries implement Part Five of the Privacy Guidelines (national implementation), notably by having in place legislation, enforcement authorities that (in most cases) can apply sanctions and provide remedies, and relevant policy measures for privacy and personal data protection. The implementation of the Privacy Guidelines is left in the first place to national governments, which means that there are a range of approaches to ensuring privacy protections that are consistent with the Privacy Guidelines. However, mechanisms for measurement and assessment of existing policy measures are generally lacking. Equally lacking is robust information on the governance and resourcing of PEAs.

147. On the basis of the available information, implementation gaps exist, mostly with respect to the existence of national privacy strategies co-ordinated at the highest levels of government.

148. Responding countries reported challenges in both regulation (catching up with regulatory developments) and enforcement (notably insufficient resources), but by and large the main challenge identified by responding countries on both counts was adjustments necessary in light of emerging technologies. Responding countries are already moving ahead to meet these challenges, in updating or planning to update their laws, in creating new frameworks and in some cases new institutions, and in guidance and other policy measures. These relatively recent developments would need to be assessed in due course.

149. Responding countries are also employing, developing or considering the development of a range of policy measures for regulatory innovation or experimentation in the context of emerging technologies, most commonly regulatory sandboxes. Regulatory sandboxes enable regulators and governments to understand the implications of different policy choices and respond to uncertainties introduced by new technologies, new data uses, and rapid innovation. They enable regulators to consider the practical application of the law in new or novel use cases where norms of compliance may not yet be established and crystalize their positions on new technology and data uses. Responding countries generally agreed, however, that a greater understanding of the benefits and risks of regulatory sandboxes – aided by a common terminology and use cases – would likely prove useful for any future developments.

150. These results indicate that the measures listed in Part Five are generally sound and remain relevant (with only three countries considering that the language of this Part should better correspond to its objectives).

151. Nevertheless, there may be a role for the DGP in contributing to the development of necessary additional guidance for the implementation of the Privacy Guidelines in the context of emerging technologies, including based on use-case scenarios, and in providing a forum for countries to share their best practices and learn from each other. This work could usefully leverage and synergise parallel work under the newly established OECD ONE AI Community aimed at implementing the 2019 OECD Recommendation on AI.

5.5. Part Six: international co-operation and interoperability

152. This section is based on responses to the questionnaire. It is also based on the two expert consultations: Mechanisms for Privacy Interoperability on 15 May 2018 [DSTI/CDEP/SPDE(2018)5/REV2] and Addressing Emerging Enforcement Challenges on 18 November 2019 [DSTI/CDEP/DGP(2020)5].

5.5.1. Background

153. Part Five of the 1980 Privacy Guidelines, "International Co-operation", focused on co-operation between countries in the context of transborder flows of personal data. It provided that countries should make the relevant procedures simple, compatible, and known to other countries; that they should establish procedures to facilitate exchange of information and mutual assistance in investigations; and that they should work towards developing principles to govern the applicable law in these cases. The Explanatory Memorandum for the 1980 Privacy Guidelines explains that there existed a "need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements." The memorandum foresaw that international data networks and the complications associated with them would become more numerous, and explained that provisions on mutual assistance were drafted to alleviate some of these complications (OECD, 2013[1]).

154. Since 1980, the OECD has continued to dedicate specific work to this area, including by the development of relevant standards to facilitate international co-operation. In 2007, the Council adopted the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy [OECD/LEGAL/0352] (Cross-border Co-operation Recommendation), which aimed to foster co-operation among PEAs to better protect data and enable cross-border data flows. In particular, this Recommendation focused on the authority and enforcement activities of PEAs and suggested particular steps countries could take to improve the ability of PEAs to co-operate with each other, other authorities and stakeholders; to act in a timely manner against privacy law violations; and to provide mutual assistance in procedural, investigative and other matters. The Cross-border Co-operation Recommendation highlighted that information sharing between PEAs is essential to co-operation.

155. The international co-operation section of the Privacy Guidelines was revised in 2013. Now in Part Six, renamed "international co-operation and interoperability", the new provisions call for countries to (i) take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among PEAs; (ii) encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to the Guidelines; and (iii) encourage the development of internationally comparable metrics to inform privacy and data flows policy. The notion that countries should make public information concerning their compliance with the Privacy Guidelines was retained.

156. The reference to interoperability was added in the 2013 revision due to the proliferation of international privacy frameworks. Those frameworks, noted in the supplementary Explanatory Memorandum as including the US-EU Safe Harbour Framework,[29] the EU Binding Corporate Rules, and the APEC Cross-Border Privacy Rules System, adopt different approaches and systems of protection (see also section 5.1.1 above). The revisions to the Privacy Guidelines sought to encourage a more harmonious approach to global privacy governance, with the added benefits that global interoperability can help simplify compliance by organisations and enhance individuals' understanding of their rights in a global environment (OECD, 2013[1]).

157. In May 2018, the SPDE hosted a roundtable on mechanisms for privacy interoperability. The need to re-visit the importance of co-operation and interoperability was prompted by recent

[29] The US-EU Safe Harbour Framework (Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC) was adopted under the EU adequacy regime and implemented in 2000. It preceded the US-EU Privacy Shield agreement. The US-EU Safe Harbour Framework was invalidated by the CJEU in 2015 ("Schrems I"), as was the US-EU Privacy Shield in 2020 ("Schrems II")

technological trends such as the development of AI and IoT, as well as the commercialisation of personal data transfers and related transactions. The roundtable was held to inform the SPDE about current policy developments fostering interoperability among privacy frameworks, and asked questions such as how we can enhance global interoperability among privacy frameworks, how national privacy strategies help foster international co-operation, and what role the OECD and the Privacy Guidelines can play in fostering interoperability.

158. In the discussion, "interoperability" was defined by some as the ability of various privacy regimes, or legal frameworks, to work together to facilitate transborder data flows while ensuring the consistent protection of these data [DSTI/CDEP/SPDE(2018)5/REV2]. Panellists articulated the objectives of interoperability as allowing transborder data flows with an appropriate baseline privacy protection; creating legal and regulatory certainty as to applicable privacy requirements; and maintaining consumers' trust in technology and business.

5.5.2. Implementation findings

Cross-border enforcement co-operation

159. The Privacy Guidelines provide that adhering countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, including by sharing relevant information. In line with this, approximately two-thirds of responding countries to the questionnaire said that their PEA had sought assistance from, or referred a privacy violation complaint to, a PEA in another country and/or vice versa (23 responding countries said their PEA sought assistance from/referred a violation to another country and 22 responding countries said another PEA sought assistance from/referred to them). Responses indicated the existence of joint cross-border investigations, such as between Australia and Canada in relation to a data hack and threatened exposure of the accounts of approximately 36 million adult dating user accounts (Australian Government, Office of the Australian Information Commissioner, 2016[27]). Israel provided specific examples of co-operation with PEAs from the European Union in relation to a company then-registered in Israel that was allegedly violating their privacy legislation. Korea, too, referred to its co-operation with the Irish PEA and the UK ICO in relation to the Facebook/Cambridge Analytica matter (the website domain being hosted in Korea).

160. Within the European Union, co-operation is mandated under Chapter 7 of the GDPR. Specifically, co-operation is mandated between the lead supervisory authority and the other supervisory authorities concerned (including by exchanging all relevant information with each other), and free mutual assistance must be provided to the extent it is appropriate (Articles 60, 61) (European Union, 2016[4]). However, one country within the European Union responded that while they had participated in several instances of international co-operation, the lack of an operational binding international agreement complicated procedures and some requests could not be granted. One country also explained that some challenges stem from uncertainty on the part of PEAs in the European Union regarding the limits on their ability to share information with PEAs outside the Union.

161. Adhering countries are also adopting other, additional measures to facilitate cross-border enforcement co-operation. Japan, for example, has built privacy co-operation and collaboration into its legal regime. Article 6 of the Act on the Protection of Personal Information ("APPI") provides that the government shall take necessary legislative and other action so as to take discreet action to protect personal information, and shall "take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning

personal information through fostering cooperation with an international organization and other international framework"[30] (European Union, 2019[28]).

162. Additionally, responding countries to the questionnaire reported their participation in international fora to advance co-operation in *transborder enforcement* of privacy laws. Participation in the Global Privacy Enforcement Network ("GPEN", a network for privacy enforcement co-operation created by the OECD in 2010) was the most popular (18 responding countries), followed by the ICDPPC[31] Enforcement Cooperation Arrangement (11 responding countries) and the APEC Privacy Cross-border Privacy Enforcement Arrangement (CPEA) (8 responding countries) (although the total number of participants in both initiatives which extend beyond the OECD area is much higher).

163. The European Data Protection Board (EDPB) was often mentioned by respondents within the EU as a body established to facilitate regulatory co-operation within the Union and as a means to promote privacy consistency. The EDPB is an EU body, tasked with ensuring the consistent application of EU legislation in the field of data protection. Within the Union, where integration is very advanced, co-operation has been made compulsory, under the aegis of the EDPB. The GDPR also provides for specific co-operation mechanisms, including between supervisory authorities.

164. At the November 2019 roundtable discussion on emerging enforcement challenges, experts emphasised the importance of cross-border international collaboration, particularly in order to facilitate the free flow of data with trust. Many of the aforementioned collaboration and co-operation mechanisms were proposed as good practices, including information sharing, joined investigations and conducting co-ordinated compliance actions. Experts suggested that effective international collaboration can allow PEAs to overcome the challenges of regulating in an environment involving such rapid innovation. However, representatives from the PEAs explained the main difficulties to achieving this as being lack of resources, expertise and legal powers to audit and enforce privacy regulations. A few PEA representatives expressed a need for regulators to have a better understanding of how new technologies, including AI, work.

Promoting interoperability

165. The responses to the privacy questionnaire demonstrate that responding countries participate in a variety of regional and international fora to promote *privacy interoperability*, with all respondents bar one participating in at least one. The country that was the exception said that it will consider participation once it has established its PEA (although it already sends delegates to particular privacy steering groups). Again, participation in the ICDPPC (now the Global Privacy Assembly) was the most common fora (26 respondents), followed by Asia Pacific Privacy Authorities (APPA), GPEN and APEC.

5.5.3. Challenges

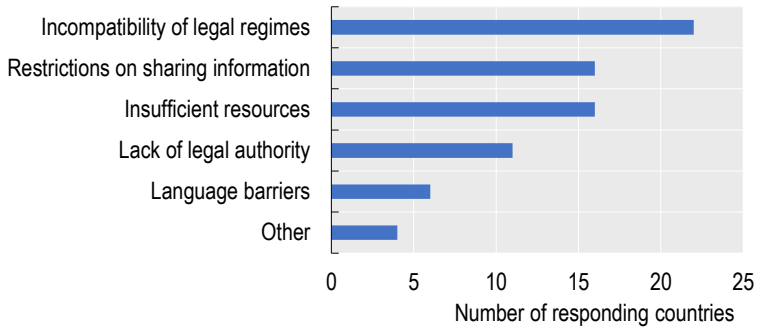
166. The main challenge to cross-border enforcement co-operation, according to the countries'survey responses, is incompatibility of legal regimes although speakers at the roundtable discussions referred to an increase in joint international investigations. Almost three quarters of respondents considered incompatibility to be one of the main reasons that enforcement co-operation has not improved (see Figure 11). Further work may be warranted to identify evidence

[30] This provision authorised the Japanese PEA to establish stricter regulations for the use and processing of personal data concerning citizens within the European Union, and contributed to Japan's ability to benefit from a GDPR adequacy decision.

[31] Now the Global Privacy Assembly

of this lack of compatibility. After incompatibility, insufficiency of resources and restrictions on sharing information were the most common responses to the question.

Figure 11. Main challenges to cross-border enforcement co-operation



Source: 2019 Privacy Guidelines questionnaire.

167. These findings are consistent with the findings of the 2017 DEO, which revealed that governments ranked potential incompatibilities of legal regimes as a major challenge to be addressed through enhanced international co-operation. In spite of these challenges, the DEO also showed that countries have in place initiatives for international co-operation: 76% of responding countries could, at that time, name at least one initiative through which they co-operate internationally and/or facilitate cross-border privacy enforcement (OECD, 2017[15]). Responding countries' willingness to engage in such co-operation initiatives was echoed in the May 2018 Interoperability Roundtable, where participants provided specific examples of co-operation in interoperability mechanisms, including the GDPR and the EDPB, APEC and its CBPR system, efforts towards the development of a BCR/CBPR referential as a possible basis for certification (initiated pre-GDPR to facilitate co-operation between the European authorities and members of APEC), and bilateral discussions between countries and between countries and international frameworks [DSTI/CDEP/SPDE(2018)5/REV2].

168. A 2011 monitoring report of the implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy noted an assessment of particular cases and suggested that "cross-border co-operation appears to remain more the exception than the rule" but there were some success stories particularly between EU member states. The report noted, though, that there were problems obtaining good quantitative data about the volume and nature of cross-border complaints (OECD, 2011[29]).[32] Notwithstanding the challenges identified, the current findings are encouraging: only four countries reported that there has been an instance when their PEA declined another country's request for assistance. In explaining their position, one country said that their PEA is not always able to provide the full assistance requested but will generally endeavour to assist within the scope of their legal abilities, including by exploring bilateral memorandums of understanding as necessary. Four countries reported having experienced disagreements with other countries concerning co-operation, and another country indicated that it would have liked to discuss broader regulatory solutions and

[32] In particular, the implementation report recommended that countries renew their enforcement co-operation efforts, including by additional efforts to (i) designate a point of contact; (ii) share technical expertise and investigative methodologies; (iii) share information on enforcement outcomes, possibly in a common format for ease of comparison; (iv) consult with other law enforcement authorities and stakeholders; and (v) consider joining regional or global enforcement arrangements or enter into effective memorandums of understanding with other authorities.

preliminary elements of investigations before other countries took action. Countries did not otherwise elaborate on the nature of the disagreements they had experienced.

169. When asked whether the language of Part Six is appropriate and corresponds to the objectives of the Privacy Guidelines, 68% of responding countries replied affirmatively. One responding country explained that the language of Part Six should identify specific ways of addressing interoperability, such as through mutual recognition of certification frameworks, comparable protection afforded by legal frameworks, or "trust marks". Another country suggested that revisions were necessary to take account of recent regulatory trends such as data localisation and government access. Two responding countries suggested that guidance as to cross-border co-operation and how interoperability is developing among different privacy frameworks should be included in the Explanatory Memorandum. Additionally, some responding countries suggested that the issue should be examined in the context of the next review of the implementation of the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.

5.5.4. Conclusions and proposed next steps

170. International co-operation and interoperability are increasingly important, particularly in light of the increased frequency and volume of transborder data flows and influence of regional data protection frameworks. Responses to the privacy questionnaire indicate that there is a widespread appreciation of the importance of enforcement co-operation and interoperability, that countries are participating in a variety of regional and international fora to promote privacy interoperability, and that they co-operate and share information on privacy enforcement (particularly in terms of seeking assistance with privacy violations). However, uncertainties around the compatibility of legal privacy regimes appear to be one of the main reasons that enforcement co-operation has not improved. Insufficient resources for enforcement is also a challenge most countries are dealing with when it comes to co-operation and cross-border enforcement.

171. Building on the interoperability roundtable, next steps may include sharing best practices for enhancing cross-border co-ordination (particularly regarding joint investigations, sharing intelligence, and international assistance with privacy violations, leveraging existing work wherever possible and the next review of the implementation of the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy); revising the Explanatory Memorandum to address the challenges of data localisation and, possibly, trusted access by government to personal data held by the private sector; identifying specific ways to deepen the convergence between existing data protection frameworks and the Privacy Guidelines; and developing internationally comparable metrics for data localisation to support evidence-based policy. Further work may involve measuring the cost of lack of compatibility of privacy frameworks globally, and include , for example, research onpossible unintended consequences of uncoordinated regional efforts (such as voluntary avoiding provision of services or access from specified locations, to avoid the costs of compliance with privacy legislation), and on differences and commonalities among data protection and privacy systems with a focus on data localisation requirements , policies and regulation of transborder data flows.

6. Summary and main conclusions

172. The review of initiatives and practices by adhering and responding countries documented in this draft Report sought to examine the implementation of the Recommendation and the Privacy Guidelines and identify gaps and actions that may need to be considered to facilitate alignment and ensure the Recommendation remains relevant in today's digital environment.

173. The responses to the privacy questionnaire, dedicated expert consultations, analytical work and the guidance of the PGEG, presented in detail in the previous sections, demonstrate the continuing relevance of the Privacy Guidelines as an international reference in privacy policy making and for building effective protection and trust in transborder data flows. Framed in concise and technology neutral language, the principle-based approach of the Privacy Guidelines has contributed to their widely recognised international relevance and lasting impact.

174. While questions were raised as to the application of, in particular, some of the basic principles (in Part Two) in the context of emerging technologies and to possible adjustments of the more operative parts of the Privacy Guidelines, responding countries generally considered that the provisions and language of the Privacy Guidelines remain appropriate and correspond to their objectives.

175. The review of the implementation conducted revealed a number of key findings. In particular it indicated that all responding countries implement the Privacy Guidelines through legislation, enforcement and policy measures. In practice, the analysis of the responses to the privacy questionnaire revealed that all responding countries have in place privacy and data protection legislation, all have established (or are in the process of establishing) Privacy Enforcement Authorities, participate in international fora for cross-border privacy enforcement co-operation, and all have some form of mechanism governing transborder flows of personal data. Notably, most responding countries report reform of existing laws consistent with the strengthened aspects of the 2013 Privacy Guidelines, for example the enactment of data breach notification laws, the establishment of PEAs, and the development of complementary policy measures to promote the implementation of the different parts of the Privacy Guidelines (e.g., on education and awareness raising, skills development, and the promotion of technical measures).

176. Notwithstanding the above progress, the analysis of the implementation of the Recommendation across Adherents identified a number of issues (summarised below) which need to be considered and could be further scoped and examined in the context of the programme of work for the biennium 2021-22. Emerging technologies (particularly AI) , the volume of personal data being collected and used, the range of analytics they are subject to, the number of actors involved and the global availability of personal data all pose challenges to the implementation of current privacy legislation, to enforcement, to accountability models and to existing frameworks for transborder data flows. Accordingly, as part of the programme of work for the biennium 2021-22 several of these issues could be further explored to ensure the Recommendation and the Privacy Guidelines remain relevant in the context of changing technological and regulatory conditions.

177. Responding countries overwhelmingly indicated that in addressing such issues, revisions of the Privacy Guidelines themselves are not necessary at this time, and recommended to focus on the development of further implementation guidance and, possibly, revisions to the Supplementary Explanatory Memorandum. In particular, responding countries indicated support for:

- Revisions to the Supplementary Explanatory Memorandum to clarify and guide the implementation of the Privacy Guidelines;
- The development of further implementation guidance on specific Parts of the Privacy Guidelines, where deemed useful (for example, on implementing accountability in Part Three);
- Further analytical work through dedicated research papers and expert consultations in areas such as regulatory sandboxes, data localisation, government access to data held by the private sector, and privacy enhancing technologies;

- Cross-cutting work to identify intersections between privacy, consumer and competition policy, and stronger co-operation between different types of regulators, as well as on cross-border co-operation in the enforcement of laws protecting privacy; and
- Contributions to cross-cutting analytical work (e.g. implementation guidance on the AI Recommendation).

178. Throughout the review process, responding countries and experts also repeatedly referred to the important role of the OECD as a forum for sharing knowledge and expertise and in providing the analytical and evidence base for addressing emerging issues. They also stressed the importance of other OECD work and instruments that complement the Privacy Guidelines, such as the Recommendation on Artificial Intelligence [OECD/LEGAL/0449], the forthcoming Recommendation on Enhancing Access to and Sharing of Data, work on data portability and data ethics and work on data localisation in the context of trade. The relevance of this work and other OECD instruments to the Privacy Guidelines review suggests the importance of adhering countries adopting a holistic approach to privacy and data protection practices that takes into account multiple societal objectives.

6.1. Part Two: basic principles of national implementation

179. As discussed in this draft Report, responding countries overwhelmingly took the view that the eight basic principles in Part Two remain generally sound and do not require revision. Nevertheless, survey responses demonstrate that in the context of new technological developments such as AI and IoT the principles of collection limitation, purpose specification, data use limitation, and security safeguards, come under pressure. Almost all responding countries suggested that further guidance on the application of these principles would be helpful in relation to emerging technologies and accountability (discussed further below).

180. Additionally, although the Privacy Guidelines already provide many protections for data subjects under the individual participation principle, responding countries recommended further work to clarify the application of the Privacy Guidelines to specific developments in the privacy and personal data protection sphere. These include in particular efforts to strengthen data subject rights (such as the right to data portability, right to correction and erasure, right to object to automated decision making) for which no clear direction has as yet emerged as to what changes or additional guidance may be needed for such rights to be adequately addressed by the Privacy Guidelines.

6.2. Part Three: Implementing Accountability

181. A vast majority of responding countries consider accountability to have an important role in personal data protection. The accountability principle remains an important pillar of the Privacy Guidelines. It can facilitate transparency, social responsibility and trust in organisations, as well as productive conversations with regulators and stakeholders. The review did, however, identify gaps in the understanding of accountability and revealed a general consensus that to work well in practice, it requires a robust oversight regime. The original interpretation of accountability – namely, compliance with legal obligations – remains essential. However, it was identified as in need of evolution in the context of emerging technologies, including requirements for organisations to act proactively as responsible and ethical stewards of personal information. Guidance will need to be developed by policy makers in supporting them to do so, taking into account the differing levels of technological sophistication and understanding as well as resources.

182. Responding countries and experts agreed on the need to further clarify the application of the accountability principle and further guide its implementation with best practice on how to strengthen the role of enforcement. Further clarification of the role of all actors handling personal data, including to ensure that data processors and controllers understand their respective obligations and can minimise their risks (including legal and reputational risks) was also recommended.

6.3. Part Four: free flow and legitimate restrictions

183. Responding countries agreed that there was scope to expand the Supplementary Explanatory Memorandum concerning Part Four of the Privacy Guidelines to address the issue of data localisation which has gained prominence since 2013 and is viewed as having a growing impact on transborder data flows. Based on expert consultations, it was suggested that the OECD could promote a common definition of the term and map out guidance on the application of paragraph 16 of Part Four, which states that a data controller remains accountable for personal data under its control without regard to the location of the data. It could also review current practice in the proportionality assessment articulated in paragraph 18 of Part Four, and further examine the potential compliance and enforcement issues that data localisation may raise.

184. The review also indicated that it would be important and urgent for the OECD to examine good practices among adhering countries concerning 'guarantees' or 'restraints' on access by governments to personal data held by the private sector to ensure trust in data flows. Adhering countries agreed on the need for additional commentary to the Supplementary Explanatory Memorandum on the importance of these common approaches. Adhering countries see this work as an opportunity to unite member countries regarding the circumstances in which government access to privately-held data is appropriate, in stark contrast to unlimited data access practices of some authoritarian regimes. In November 2020 the CDEP decided to conduct further work to examine the possibility of developing "*an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector*". The work will seek to "*elaborate a set of common and coherent good practices and legal guarantees from across OECD countries for best reconciling law enforcement and national security needs for data with protection of individual rights*".

185. As such, it is likely that any additional commentary to the Supplementary Explanatory Memorandum should be informed by the outcome of this work.

6.4. Part Five: national implementation

186. The review identified implementation gaps, mostly with respect to the existence of national privacy strategies. The findings suggest that just under half of the responding countries have a national privacy strategy or whole-of-government approach to privacy. Only seven responding countries positively stated they have a national privacy strategy, while others noted alternative means of whole-of-government co-ordination, such as through legislation, a dedicated entity or forum, or other policy instruments.

187. Additionally, responding countries reported challenges in both regulation (catching up with regulatory developments) and enforcement (notably insufficient resources) but the main challenge identified by countries on both accounts was adjustments necessary in light of emerging technologies. Responding countries are already moving ahead to meet these challenges, in updating or planning to update their laws, in creating new frameworks and in some cases new institutions, and in guidance and other policy measures.

188. Responding countries are also employing, developing or considering the development of a range of policy measures for regulatory innovation or experimentation in the context of emerging technologies, most commonly regulatory sandboxes. Regulatory sandboxes enable regulators and governments to understand the implications of different policy choices and respond to uncertainties introduced by new technologies, new data uses, and rapid innovation. They enable regulators to consider the practical application of the law in new or novel use cases where norms of compliance may not yet be established and crystalize their positions on new technology and data uses. Responding countries generally agreed that a greater understanding of the benefits and risks of regulatory sandboxes – aided by a common terminology and use cases – would likely prove useful for any future developments.

189. Responding countries also agreed that further guidance is needed on available technical and organisational safeguards. Specifically responding countries and experts pointed to the need for an in depth examination of opportunities and barriers in the use of emerging new privacy enhancing technologies (PETs), including their application to transborder data flows.

190. Finally, while adhering countries deploy an array of policy measures to promote privacy and data protection by businesses, incentives for self-regulation and certification schemes , which are considered promising means to further privacy and data protection by businesses as well as interoperability, were mentioned by less than half of the responding countries.

6.5. Part Six: international co-operation and interoperability

191. International co-operation and interoperability are increasingly important, particularly in light of the increased frequency and volume of transborder data flows and influence of regional data protection frameworks. The review indicates that there is a widespread appreciation of the importance of enforcement cooperation and interoperability, that countries are participating in a variety of regional and international fora to promote privacy interoperability, and that they cooperate and share information on privacy enforcement (particularly in terms of seeking assistance with privacy violations). However, uncertainties around the compatibility of legal privacy regimes appear to be one of the main reasons for enforcement cooperation barriers. Insufficient resources for enforcement is also a challenge most countries are dealing with when it comes to cooperation and cross-border enforcement. The review highlighted the need for further work to identify intersections between privacy, consumer and competition policy, and stronger co-operation between the different regulatory agencies.

6.6. Next steps

192. In light of the foregoing, it is proposed that the CDEP, through the DGP, explore the issues and challenges set out in the summary and conclusions section above, as well as in the challenges, and conclusions and proposed next steps sections at the end of each section of the report, and develop practical guidance on the implementation of the Recommendation and the Privacy Guidelines as well as draft amendments to the Supplementary Explanatory Memorandum where appropriate. Further, it is proposed that the DGP report to the CDEP on specific developments in this regard by the end of 2021

193. More broadly, it is proposed that the CDEP, through the DGP, continue to review the implementation, dissemination, and continued relevance of the Recommendation and Privacy Guidelines and report thereon to the Council in five years.

References

Australian Government, Office of the Australian Information Commissioner (2016), *Ashley Madison joint investigaiton*, https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/ashley-madison-joint-investigation. [27]

Australian Government, Office of the National Data Commissioner (2019), *About*, https://www.datacommissioner.gov.au/about. [25]

Council of Europe (2018), *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS No. 223. [12]

Council of Europe (2017), *Study on the use of internet in electoral campaigns*, https://rm.coe.int/study-use-of-internet-in-electoral-campaigns/1680776163. [19]

Council of Europe (1981), *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS No. 108. [5]

Department for Digital, Culture, Media & Sport (UK) (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. [26]

European Commission (2019), *Special Eurobarometer 487a: The General Data Protection Regulation*, https://ec.europa.eu/commfrontoffice/publicopinionmobile/index.cfm/Survey/getSurveyDetail/surveyKy/2222. [8]

European Commission (2015), "Data protection", *Special Eurobarometer 431*, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf. [7]

European Union (2019), *Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan [...]*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=EN. [28]

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*, O.J. (L 119) 32. [4]

Federal Trade Commission (US) (2014), *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it (accessed on 16 January 2020). [14]

Information Commissioner's Office (UK) (2018), *Democracy Disrupted? Personal information and political influence*, https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf. [20]

Information Commissioner's Office (UK) (2018), *Guidance on political campaigning*, https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf. [22]

Information Commissioner's Office (UK) (n.d.), *Political campaigning practices: direct marketing*, https://ico.org.uk/your-data-matters/be-data-aware/political-campaigning-practices-direct-marketing. [21]

International Trade Administration (US) (n.d.), *Privacy Shield Overview*, https://www.privacyshield.gov/Program-Overview. [13]

Mexico, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (n.d.), *Certification*, http://rea.inai.org.mx/_catalogs/masterpage/Sec1_5.aspx. [17]

New Zealand, Office of the Privacy Commissioner (2013), *Applying for the privacy trust mark*, https://privacy.org.nz/privacy-for-agencies/applying-for-a-privacy-trust-mark/. [16]

Norwegian Data Protection Authority (2019), *Digital targeting of political messages in Norway*, https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/pa-parti-med-teknologien---engelsk.pdf. [23]

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en. [11]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://dx.doi.org/10.1787/eedfee77-en. [24]

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), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [9]

OECD (2019), *Recommendation of the Council on Health Data Governance*, *OECD/LEGAL/0433*. [6]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264276284-en. [15]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, https://dx.doi.org/10.1787/9789264229358-en. [10]

OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220, OECD Publishing, Paris, https://dx.doi.org/10.1787/5k486qtxldmq-en. [30]

OECD (2013), *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines*, OECD Publishing, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [1]

OECD (2011), "Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", *OECD Digital Economy Papers*, No. 178, OECD Publishing, Paris, https://dx.doi.org/10.1787/5kgdpm9wg9xs-en. [29]

OECD (1980), "OECD Privacy Guidelines", *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [2]

Singapore, IMDA (2019), *Data Protection Trustmark Certification*, https://www2.imda.gov.sg/dptm. [18]