For Official Use **C(2013)79**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **20-Jun-2013**

English - Or. English

COUNCIL

C(2013)79
For Official Use

Council

REVISION OF THE RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA [C(80)58/FINAL]

(Note by the Secretary-General)

Anne Carblanc, Head of the Information, Communications and Consumer Policy Division: anne.carblanc@oecd.org; +33 1 4524 9334
Michael Donohue: Senior Policy Analyst, michael.donohue@oecd.org; + 33 1 4524 1479

JT03342203

English - Or. English

1. In 1980, the Council adopted a Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL] ("1980 Guidelines") to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. The 1980 Guidelines represent the first internationally agreed-upon set of privacy principles and have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, changes in personal data usage, as well as new approaches to privacy protection, have left the 1980 Guidelines in need of updating in a number of important respects. This document proposes revisions to this landmark OECD instrument.

2. The review of the 1980 Guidelines arose out of the 2008 Declaration for the Future of the Internet Economy [C(2008)99], which called for the OECD to assess the application of the Guidelines in light of the changing environment. Preparations for the review were conducted during 2010-11 in the context of the 30th anniversary of the Privacy Guidelines, during which the OECD organised a series of events and produced a report on "The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines."[1]

3. In 2011, the OECD Working Party on Information Security and Privacy (WPISP) agreed on Terms of Reference for the review. The Terms of Reference highlight that, as compared with the situation 30 years ago, there has been a profound change of scale in terms of the role of personal data in our economies, societies, and daily lives. The environment in which the traditional privacy principles are now implemented has undergone significant changes, for example, in:

- The ***volume*** of personal data being collected, used and stored;
- The ***range of analytics*** involving personal data, providing insights into individual and group trends, movements, interests, and activities;
- The ***value*** of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- The extent of ***threats*** to privacy;
- The ***number and variety of actors*** capable of either putting privacy at risk or protecting privacy;
- The ***frequency and complexity of interactions*** involving personal data that individuals are expected to understand and negotiate;
- The ***global availability*** of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

4. In accordance with the Terms of Reference, the WPISP convened a multi-stakeholder group of experts from governments, privacy enforcement authorities, academia, business, civil society and the Internet technical community ("Expert Group"). This Expert Group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. On the basis of the work by the Expert Group, proposed revisions were developed by the WPISP. With some adjustments to address outstanding concerns, these revisions were approved, by the Committee for Information, Computer and Communications Policy (ICCP) at its meeting on 11-12 April, for submission to Council.[2]

5. The proposed revisions to the 1980 Guidelines introduce a number of new concepts, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other proposed revisions expand or update existing provisions of the Guidelines such as those related to the accountability of data controllers, transborder data flows and

1 See www.oecd.org/sti/privacyanniversary.

2 See DSTI/ICCP/M(2013)1.

privacy enforcement and international co-operation. A "track changes" version showing the differences between the proposed revisions and the original 1980 version of the Guidelines is available on the Council Extranet.

6. While discussions did take place on whether some of the core principles and terms should be changed, it was decided in the end to leave intact the eight “basic principles of national application” as reflected in Part Two of the 1980 Guidelines, as well as the definitions of key terms like “data controller” and “personal data”.

7. In addition to these proposed modifications to the Guidelines, a new Supplementary Explanatory Memorandum has been prepared to provide context and rationale for the revisions. It is intended to supplement – not replace – the original Explanatory Memorandum,[3] which remains relevant to interpreting the aspects of the 1980 Guidelines that remain unchanged. The Supplementary Explanatory Memorandum was likewise approved by the ICCP for submission to Council and is attached as Appendix II, with a view to Council declassification.

Proposed Action

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

THE COUNCIL

a) noted document C(2013)79;

b) adopted the revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, as set out in Appendix I to document C(2013)79;

c) agreed to declassify the Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, as set out in Appendix II to document C(2013)79;

d) recalled that the participation of non-Members in OECD bodies is governed by the Resolution of the Council on Partnerships in OECD Bodies [C(2012)100/FINAL].

[3] See http://oe.cd/1980privacymemo.

APPENDIX I

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

[C(80)58/FINAL, as amended on […] [C(2013)79]

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

HAVING REGARD to the *Ministerial Declaration on the Protection of Privacy on Global Networks* [Annex 1 to C(98)177]; the *Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks* [C(2002)131/FINAL], the *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* [C(2007)67], the *Declaration for the Future of the Internet Economy (The Seoul Declaration)* [C(2008)99], the *Recommendation of the Council on Principles for Internet Policy Making* [C(2011)154], the *Recommendation of the Council on the Protection of Children Online* [C(2011)155] and the *Recommendation of the Council on Regulatory Policy and Governance* [C(2012)37];

RECOGNISING that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information;

RECOGNISING that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks;

RECOGNISING that the continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities;

RECOGNISING the importance of risk assessment in the development of policies and safeguards to protect privacy;

RECOGNISING the challenges to the security of personal data in an open, interconnected environment in which personal data is increasingly a valuable asset;

DETERMINED to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them;

On the proposal of the Committee for Information, Computer and Communications Policy:

I. **RECOMMENDS** that Member countries:

- Demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government;

- Implement the Guidelines contained in the Annex to this Recommendation, and of which they form an integral part, through processes that include all relevant stakeholders;

- Disseminate this Recommendation throughout the public and private sectors;

II. **INVITES** non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders.

III. **INSTRUCTS** the Committee for Information, Computer and Communication Policy to monitor the implementation of this Recommendation, review that information, and report to the Council within five years of its adoption and thereafter as appropriate.

This Recommendation revises the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58/FINAL].

ANNEX

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

    a) "data controller" means 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;

    b) "personal data" means any information relating to an identified or identifiable individual (data subject);

    c) "laws protecting privacy" means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines;

    d) "privacy enforcement authority" means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings;

    e) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.

3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:

    a) as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or

    b) in a manner which unduly limits the freedom of expression.

4. Exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy ("*ordre public*"), should be:

    a) as few as possible, and

    b) made known to the public.

5. In the particular case of federal countries the observance of these Guidelines may be affected by the division of powers in the federation.

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. 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.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

    a) with the consent of the data subject; or
    b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. Individuals should have the right:

    a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

    b) to have communicated to them, data relating to them

        i. within a reasonable time;

        ii. at a charge, if any, that is not excessive;

        iii. in a reasonable manner; and

        iv. in a form that is readily intelligible to them;

    c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

    d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. IMPLEMENTING ACCOUNTABILITY

15. A data controller should:

    a) Have in place a privacy management programme that:

        i. gives effect to these Guidelines for all personal data under its control;

        ii. is tailored to the structure, scale, volume and sensitivity of its operations;

        iii. provides for appropriate safeguards based on privacy risk assessment;

        iv. is integrated into its governance structure and establishes internal oversight mechanisms;

        v. includes plans for responding to inquiries and incidents;

        vi. is updated in light of ongoing monitoring and periodic assessment;

    b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and

    c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

PART FOUR. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

PART FIVE. NATIONAL IMPLEMENTATION

19. In implementing these Guidelines, Member countries should:

    a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;

    b) adopt laws protecting privacy;

    c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;

    d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

    e) provide for reasonable means for individuals to exercise their rights;

    f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;

    g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy;

    h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and

    i) ensure that there is no unfair discrimination against data subjects.

PART SIX. INTERNATIONAL CO-OPERATION AND INTEROPERABILITY

20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.

21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.

22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

23. Member countries should make public the details of their observance of these Guidelines.

APPENDIX II

SUPPLEMENTARY EXPLANATORY MEMORANDUM TO THE REVISED RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

INTRODUCTION

In 1980, the OECD adopted the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("1980 Guidelines") to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. The 1980 Guidelines, which contained the first internationally agreed-upon set of privacy principles, have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, changes in personal data usage, as well as new approaches to privacy protection, have left the 1980 Guidelines in need of updating in a number of important respects. The Honourable Michael Kirby chaired the original OECD expert group that drafted the Guidelines. In reflecting on that achievement on the occasion of the Guideline's 30th anniversary Justice Kirby observed: "In the field of information policy, the technology is such that no international expression of principles can be immune from the forces of change."[1]

Context of the review

Over the last three decades, personal data have come to play an increasingly important role in our economies, societies and everyday lives. Innovations, particularly in information and communication technologies, have impacted business operation, government administration, and the personal activities of individuals. New technologies and responsible data uses are yielding great societal and economic benefits. The volume of personal data being collected, used and stored is vast and continues to grow. Modern communications networks support global accessibility and continuous, multipoint data flows. The potential uses of personal data have increased tremendously as a result of the wide range of analytics that can provide comprehensive insights into individuals' movements, interests, and activities.

At the same time, the abundance and persistence of personal data have elevated the risks to individuals' privacy. Personal data is increasingly used in ways not anticipated at the time of collection. Almost every human activity leaves behind some form of digital data trail, rendering it increasingly easy to monitor individuals' behaviour. Personal data security breaches are common. These increased risks signal the need for more effective safeguards in order to protect privacy.

In recent years, several initiatives have been undertaken to address new and elevated privacy risks, particularly in the context of transborder data flows. The work is ongoing and examples include the European Union's system of Binding Corporate Rules (BCRs)[2]; the global discussion on the commonly accepted elements of privacy accountability[3]; and the Asia Pacific Economic Cooperation's Cross-Border

Privacy Rules System (APEC CBPR).[4] At the OECD, cross-border co-operation among privacy enforcement authorities has been a priority, resulting in the adoption of the 2007 Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (the "2007 Recommendation").[5]

The *Seoul Declaration for the Future of the Internet Economy* (2008) recommended that the OECD assess the application of certain OECD instruments, including the 1980 Guidelines, in light of "changing technologies, markets and user behaviour and the growing importance of digital identities." This Declaration triggered the launch of a formal review of the 1980 Guidelines.

The OECD Recommendation on Principles for Internet Policy Making (2011)[6] called for a strengthening of consistency and effectiveness in privacy protection at a global level. While the OECD Privacy Guidelines have a broader scope than Internet policies, the 2011 Recommendation is nevertheless instructive. The Communiqué attached to the 2011 Recommendation for information purposes explains that current privacy challenges are likely to become more acute "as the economy and society depends more heavily on broadened and innovative uses of personal information that can be more easily gathered, stored, and analysed".[7]

Privacy frameworks around the world are being examined and refined. Three of the primary frameworks with an international dimension (OECD, European Union, and Council of Europe) have been under review simultaneously, and a fourth (APEC) is implementing new cross-border arrangements. Work on domestic privacy frameworks is likewise underway across the globe, from Australia to Brazil to China to the United States. In light of all of these developments, the OECD concluded that it was an appropriate time to engage in a substantive review of the 1980 Guidelines.

Process of the review

Preparations for the review began in 2010, in the context of the 30th anniversary of the 1980 Guidelines. As part of the process, the OECD organised three thematic events. These events addressed (1) the impact of the 1980 Guidelines; (2) the evolving role of the individual; and (3) the economic dimensions of personal data and privacy. It also produced two reports, "The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines"[8], and "Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation".[9]

Building on this preparatory work, the Working Party for Information Security and Privacy (WPISP) developed Terms of Reference[10] to serve as a roadmap for the review. The Terms of Reference articulated a shared view of current issues and approaches, and provided the rationale for further work. In addition to highlighting the changes in the environment, the Terms of Reference identified those elements which Member countries considered essential to improving the effectiveness of privacy protections.

A Volunteer Group of Privacy Experts ("Expert Group") was formed to assist the WPISP in the review process. This group included experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community. Participants also included representatives of the Council of Europe and the European Union, as well as experts active in APEC. This multi-stakeholder group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene served as the Rapporteur to the group. The Expert Group collaborated through a series of meetings and a virtual workspace during 2011 and 2012. During these meetings, the Expert Group focused on three main themes identified by the Terms of Reference, namely: (1) the roles and responsibilities of key actors; (2) geographic restrictions on transborder data flows; and (3) proactive implementation and enforcement.

The approach that emerged from the work of the Expert Group suggested that, although the environment for privacy and transborder data flows has changed significantly, an update to the 1980 Guidelines was preferred rather than a fundamental rethinking of its core principles. The Expert Group took the view that the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained. The Expert Group introduced a number of new concepts to the OECD privacy framework, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other aspects of the 1980 Guidelines were expanded or updated, such as accountability, transborder data flows and privacy enforcement.

The 1980 Guidelines were accompanied by an Explanatory Memorandum, which described the environment that led to their development, as well as their underlying rationale. The Explanatory Memorandum provides insight into the competing priorities of the time, as well as a detailed interpretation of various provisions in the 1980 Guidelines, some of which have not been modified (in particular those of Part Two). These insights remain relevant today. This Supplementary Explanatory Memorandum has been prepared as part of the review process to complement the revised Guidelines. It is intended to supplement – not replace – the original Explanatory Memorandum. Where there have been changes to the 1980 Guidelines, this Supplementary Explanatory Memorandum sheds light on the rationale and context of these changes to help understand and interpret them.

REVISIONS TO THE GUIDELINES

Privacy management programmes

Part Two of the 1980 Guidelines sets forth the principle of accountability, which places the onus on the data controller to comply "with measures that give effect to the rest of the principles". Recognition of the importance of the accountability principle has increased over time. Domestic privacy laws have come to introduce a variety of mechanisms designed to promote the accountability of both public and private data controllers. Obligations of transparency towards individuals and privacy enforcement authorities are clear examples of such mechanisms.

In recent years, the principle of accountability received renewed attention as a means to promote and define organisational responsibility for privacy protection. Building on this experience, the new Part Three of the Guidelines ("Implementing Accountability") introduces the concept of a privacy management programme and articulates its essential elements.

Paragraph 15(a)(i) specifies that a data controller's privacy management programme should give effect to the Guidelines "for all personal data under its control". The term "control" refers back to the definition of a "data controller", as defined in paragraph 1(a). This formulation emphasises that a privacy management programme should not only address the data controller's own operations, but all operations for which it may be accountable - regardless of to whom data is transferred. For example, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf. Safeguards may also be necessary in relationships with other data controllers, particularly where the responsibility for giving effect to the Guidelines is shared. Appropriate safeguards may include: provisions in contracts that address compliance with the data controller's privacy policies and practices; protocols for notifying the data controller in the event of a

security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits.

Paragraph 15(a)(i) refers only to the Guidelines as a source of rules or principles to be implemented through a privacy management programme. In practice, privacy management programmes may need to reflect other sources as well; including domestic law, international obligations, self-regulatory programmes, or contractual provisions.

Paragraph 15(a)(ii) underlines the need for flexibility when putting in place a privacy management programme. For example, large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment. At the same time, paragraph 15(a)(ii) also provides that privacy management programmes should be adapted to the volume and sensitivity of the controller's operations. Programmes for data controllers that deal with large volumes of personal data will need to be more comprehensive than those of data controllers who handle only limited amounts of personal data. The sensitivity of the data controller's operations may also impact the nature of a privacy management programme, as even a very small data controller may handle extremely sensitive personal data.

A recurring element in the discussions about privacy management programmes was the need for such programmes to develop appropriate safeguards based on privacy risk assessment. Paragraph 15(a)(iii) contemplates that the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals' privacy. This process is sometimes accomplished by conducting a "privacy impact assessment" before a new programme or service is introduced or where the context of the data use changes significantly. "Risk" is intended to be a broad concept, taking into account a wide range of possible harms to individuals. A privacy management programme can also assist in the practical implementation of concepts such as "privacy by design", whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.

Paragraph 15(a)(iv) indicates that privacy management programmes should be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms. Obtaining support and commitment from senior management is a key factor in ensuring the successful implementation of a privacy management programme. Ensuring the availability of sufficient resources and staff, as well as training programmes, may also improve the effectiveness of the programme. Privacy officers may play an important role in designing and implementing a privacy management programme.

Paragraph 15(a)(v) provides that a privacy management programme should also include plans for responding to incidents and inquiries. The increasing frequency of security breaches affecting personal data demonstrates the importance of developing an incident response plan, which includes breach notification (see below). To support the "Individual Participation Principle" in Part Two, data controllers should also be able to provide timely response to inquiries (either in the form of complaints or requests for information) by data subjects. Finally, paragraph 15(a)(vi) stipulates that privacy management programmes should be routinely reviewed and updated to ensure that they remain appropriate to the current risk environment.

Paragraph 15(b) provides that a data controller should be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines. Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of non-compliance,

enhances the accountability of data controllers. The assessment of the programme may be carried out directly by the privacy enforcement authority or by an agent on its behalf.

Paragraph 15(b) includes the terms "appropriate" and "competent" to highlight that data controllers should be prepared to demonstrate their privacy management programmes at the request of a privacy enforcement authority provided that this authority has jurisdiction over the data controller. The Guidelines do not address legal issues related to jurisdiction, competence and conflicts of law.

A privacy management programme may also be demonstrated to an entity which is responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to Guidelines. Such arrangements may involve seal programmes or certification schemes, and may also concern transborder flows of personal data. In this regard it can be noted that paragraph 21 encourages the development of international arrangements that give practical effect to the Guidelines. The European Union's Binding Corporate Rules (BCRs) and the APEC Cross-border Privacy Rules System provide two models for developing such an arrangement.

Data security breach notification

The "Security Safeguards Principle" of Part Two states that "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data." Numerous high-profile data breaches have demonstrated that personal data security continues to be a challenge.

Data breaches can result, for example, from actions by careless employees who fail to follow proper procedures; hackers who gain access to inadequately protected databases; or opportunistic thieves who steal unsecured portable devices. However, the underlying causes – lack of employee training and awareness, out-of-date security safeguards, inadequate rules governing access to personal data, over-collection of data and undefined retention periods, or a lack of adequate oversight – can often be attributed to the data controller.

The potential harm to individuals from the misuse of their personal data, whether accidentally lost or purposefully stolen, may be significant. Organisations experiencing a breach often incur significant costs responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also be significant. A loss of trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals.

Breach notification laws requiring data controllers to inform individuals and/or authorities when a security breach has occurred have been passed or proposed in many countries. These laws are usually justified on the grounds that data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause to their reputation. Requiring notification may enable individuals to take measures to protect themselves against the consequences of identity theft or other harms. Notification requirements may also provide privacy enforcement authorities or other authorities with information to determine whether to investigate the incident or take other action. Ideally, breach notification laws also help to create an incentive for data controllers to adopt appropriate security safeguards for the personal data they hold.

In addition to contributing to data security, data breach notification enhances other basic principles set forth in Part Two of the Guidelines, including accountability, individual participation and openness. Furthermore, mandatory security breach notification may improve the evidence base for privacy and information security policies by generating information about the number, severity and causes of security breaches.

Security breaches not only raise privacy concerns, but also intersect with other issues, including criminal law enforcement and cybersecurity. When an organisation suffers a security breach, particularly one resulting from an external attack, notification of the breach to authorities other than privacy enforcement authorities (*e.g.*, computer incident response teams, criminal law enforcement entities, other entities responsible for cybersecurity oversight) may be appropriate or required.

Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. Additionally, excessive notification to data subjects may cause them to disregard notices. Accordingly, the new provision that has been added to the Guidelines [paragraph 15(c)] reflects a risk-based approach to notification. Notice to an authority is called for where there is a "significant security breach affecting personal data", a concept intended to capture a breach that puts privacy and individual liberties at risk. Where such a breach is also likely to adversely affect individuals, notification to individuals would be appropriate as well. To determine whether individuals are likely to be "adversely affected" by a breach, the term "adverse effect" should be interpreted broadly to include factors other than just financial loss. Notification requirements should be flexible to allow for prevention and mitigation of further damage. There may be circumstances where notification to data subjects would be inappropriate, for example when it would increase the risk to data subjects or impede a law enforcement investigation.

Existing breach notification laws differ in terms of the thresholds for notification, the parties to be notified, the timing of the notification, as well as the role of privacy enforcement and other authorities. Further experience may be needed to determine which modalities of breach notification are most effective in practice.

Security breaches may affect the personal data of individuals residing in different jurisdictions. When designing, implementing or revising breach notification requirements, special consideration may be given to the interests of affected individuals who may live outside their jurisdiction. In particular, the notification of privacy enforcement authorities in other jurisdictions where a significant number of individuals are known or likely to have been affected, can be beneficial. Cross-border enforcement cooperation mechanisms are one way to foster arrangements that might support or disseminate breach notifications of importance to multiple jurisdictions. Such arrangements may also help to address issues arising from conflicting legal requirements.

Privacy enforcement authorities

Neither the 1980 Guidelines nor the 2007 Recommendation explicitly call for the establishment of privacy enforcement authorities, although the latter instrument assumes their existence and recommends their endowment with effective powers and authority. The revised Guidelines define and make explicit the need to establish and maintain "privacy enforcement authorities". They also incorporate a definition of "laws protecting privacy", to refer to "national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines". Both definitions mirror those agreed in the 2007 Recommendation.

The definitions of "laws protecting privacy" and "privacy enforcement authorities" allow for flexibility in application. "Laws protecting privacy" can refer not only to horizontal privacy laws that are common in Member countries, but also to sectoral privacy legislation (*e.g.* credit reporting or telecommunications laws) or other types of legislation that contain provisions which protect personal data so as to give effect to the Guidelines in practice (*e.g.* consumer protection laws). Likewise, a "privacy enforcement authority" refers not only to those public sector entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, provided they

have the powers to conduct investigations or bring proceedings in the context of enforcing "laws protecting privacy".

A new provision in Part Five ("National Implementation") calls on Member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an "objective, impartial and consistent basis" [paragraph 19(c)]. This formulation has been adapted from the 2012 OECD Recommendation on Regulatory Policy and Governance.[11] In the context of the Guidelines, it refers to the need for privacy enforcement authorities to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy. There exist a variety of mechanisms across Member countries for ensuring the necessary impartiality of privacy enforcement authorities in the exercise of their privacy protection functions. Paragraph 19(c) focuses on the practical impact of such mechanisms, which should ensure that these authorities can take decisions free from influences that could compromise their professional judgment, objectivity or integrity.

In some countries, the term "privacy enforcement authority" can also refer to a group of bodies that collectively enforce laws protecting privacy. For example, oversight of public sector data controllers may involve multiple bodies from different branches of government, who may also have the authority to issues guidelines or other data usage requirements. The "governance, resources, and technical expertise" called for in paragraph 19(c) may not, in such a case, be embodied in a single entity, but rather be found in the enforcement system as a whole.

The 2007 Recommendation underlined the need for privacy enforcement authorities to be endowed with the resources and authority necessary to (a) deter and sanction violations of laws protecting privacy; (b) permit effective investigations, including the ability to obtain access to relevant information, relating to possible violations of laws protecting privacy; and (c) permit corrective action to be taken against data controllers engaged in violations of laws protecting privacy. The resources of privacy enforcement authorities should be commensurate with the scale and complexity of data processing operations subject to their oversight. The new provision also calls for empowering privacy enforcement authorities with sufficient technical expertise, which has become crucial in light of the increasing complexity of data uses. This reinforces the emerging trend within privacy enforcement authorities to retain staff with a technical background.

Transborder flows of personal data

When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices. Services, such as "cloud computing", allow organisations and individuals to access data that may be stored anywhere in the world.

The 1980 Guidelines presumed that data flows should generally be allowed, but recognised the ability of governments to restrict them in certain circumstances, namely where the receiving country "does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation." Since then, Member countries have instituted a range of mechanisms to ensure the protection of individuals in the context of transborder data flows. Some of these mechanisms include a country-specific assessment, such as the "adequacy model" adopted within the European Union. Other mechanisms are not based on a country-specific assessment, but are instead based on the safeguards put in place by data controllers. Such mechanisms include, for example, Binding Corporate Rules, model contracts, and Cross-Border Privacy Rules.

The revisions reflected in Part Four attempt to simplify and consolidate the OECD approach to transborder flows of personal data. It begins by recalling that a data controller remains accountable for personal data under its control without regard to the location of the data [paragraph 16]. This paragraph restates the basic principle of accountability contained in Part Two in the context of transborder data flows. Transborder flows of personal data, to Member countries or non-Member countries, present risks, which data controllers must address. Some data flows may require close attention because of the sensitivity of the data or because the receiving jurisdiction may lack either the willingness or capacity to enforce privacy safeguards.

Without precluding the application of paragraph 6, paragraph 17 specifies two circumstances in which a Member country should refrain from imposing restrictions on transborder flows of personal data. Paragraph 17(a) retains the general approach from the 1980 Guidelines, by providing that Member countries should refrain from restricting transborder data flows between itself and another country where the other country substantially observes these Guidelines. Paragraph 17(b) discourages restrictions where sufficient safeguards exist to ensure a continuing level of protection consistent with these Guidelines. It gives recognition to the measures which a data controller can put in place to ensure a continuing level of protection, which may result from a combination of measures, such as technical and organisational security safeguards, contracts, complaint handling processes, audits, etc. However, the measures provided by the data controller need to be sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective. Paragraph 17(b) therefore includes as a consideration the availability of effective enforcement mechanisms which support measures adopted by the data controller. Such enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as cross-border co-operation among privacy enforcement authorities.

Paragraphs 16 and 17 operate independently. The existence or absence of country restrictions on data flows adopted pursuant to paragraph 17 does not, as such, affect the operation of the principle embodied by paragraph 16, namely that data controllers remain accountable for personal data under their control, including in the context of transborder flows.

Paragraph 18 updates the language in the 1980 Guidelines to refer to "risk" and "proportionality", indicating that any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (*i.e.* not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data, the purpose and context the processing. In doing so, the text has been made more coherent with other provisions of the Guidelines, which implement a risk-based approach.

Paragraph 6 of the Guidelines acknowledges that Member countries have the ability to supplement the standards set forth by the Guidelines with additional measures necessary for the protection of privacy and individual liberties, which may impact transborder flows of personal data. Such measures should be implemented in a manner that least impacts the free flow of personal data.

National implementation

Regarding national implementation, the 1980 Guidelines focused on the need for "legal, administrative and other procedures or institutions". Although the 1980 Guidelines also highlighted non-regulatory measures, including self-regulation, it was recognised that there is a need for additional measures to help to protect privacy.

Paragraph 19(a) recommends that Member countries develop national privacy strategies that reflect a co-ordinated approach across governmental bodies. Elevating the importance of privacy protection to the

highest levels within government helps improve the effectiveness of privacy protection. A further element of national privacy strategies concerns intra-governmental co-ordination. As highlighted in the OECD Recommendation on Regulatory Policy and Governance, Member countries should promote regulatory coherence between various levels of government. Where governments act as a policy maker for private sector activity, ensuring co-ordination across governmental departments is a necessary part of a national strategy. In addition, with many government departments making use of personal data, another dimension of co-ordination is to ensure a consistent level of protection across governmental bodies. Finally, national privacy strategies also offer a vehicle to ensure compatibility of policy development in related areas (*e.g.* national cybersecurity strategies).

Paragraph 19(g) calls upon Member countries to consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy. While existing initiatives attempt to raise awareness, there is broad recognition that more needs to be done. The Terms of Reference for the review of the Guidelines called for the creation of a culture of privacy among organisations and individuals through implementation of privacy literacy initiatives. Recent OECD instruments in related areas include measures for education and awareness as part of their policy frameworks.[12] Such initiatives should involve a wide range of stakeholders, including governments, privacy enforcement authorities, self-regulatory bodies, civil society organisations, and educators. As children are a particularly vulnerable category of data subjects, Member countries are specifically encouraged to consider privacy literacy initiatives which seek to equip children with the knowledge and skills necessary to stay safe online and use the Internet to their benefit.

Privacy professionals play an increasingly important role in the implementation and administration of privacy management programmes. Several Member countries have already undertaken initiatives to define the competencies of privacy professionals. Credential programmes in data protection and privacy, as well as specialised education and professional development services may contribute to the development of the necessary skills. Paragraph 19(g) explicitly encourages Member countries to consider the adoption of measures to support such skills development.

Technical measures also play an increasingly important role in complementing laws protecting privacy. Paragraph 19(g) encourages measures to foster the development and deployment of privacy-respecting and privacy-enhancing technologies (PETs). For example, Member countries may choose to support the development of technical standards which advance privacy principles. International standardisation initiatives may also advance technical interoperability among PETs, which may in turn help promote wider adoption of these technologies. Accreditation and seal programmes may further foster the adoption of technologies beneficial to privacy. Other measures include the promotion of research and development, exchange of best practices, and the issuance of regulatory guidance.

Paragraph 19(h) invites Member countries to consider the role of actors other than data controllers, "in a manner appropriate to their individual role". When discussing the need for complementary measures, it was recognised that other actors who, while not covered by the concept of data controller, nevertheless play an important role in determining the level of protection of personal data. Over the past few years, individuals have transcended the role of passive "data subjects" to become actively involved in creating, posting and sharing personal data about themselves, friends, relatives and others, over a vast array of information outlets including social networking services, rating systems and geo-location based applications. When discussing this change, it was recognised that not every actor should necessarily be regulated in the same way. For example, individuals acting in the context of their private lives are generally perceived to fall outside the remit of the Guidelines, as relationships among individuals are usually fundamentally different from those between individuals and organisations. Non-legislative measures, including education and awareness raising, were considered more appropriate to address the privacy risks associated with the activities of individuals. Where an individual does cause damage to the

privacy interests of others, tort or civil law may offer a possible remedy, but other measures may need to be considered as well.

International co-operation and interoperability

The OECD Recommendation on Internet Policy Making calls for a strengthening of consistency and effectiveness in privacy protection at a global level. The Communiqué which is annexed to it for information purposes further recognises the objective of governments to pursue global interoperability in this area. The Terms of Reference similarly identified the value of globally interoperable privacy frameworks that ensure effective protection of privacy and support the free flow of personal information around the world. However, as outlined by the G8 Deauville Declaration, we still "face considerable challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data".[13]

Paragraph 21 expresses the general objective of Member countries to improve global interoperability of privacy frameworks through international arrangements that give practical effect to the Guidelines. There exists a range of approaches to interoperability among privacy frameworks. The US-EU Safe Harbour Framework[14], which was adopted under the EU adequacy regime and implemented in 2000, was an early example. Since then, several initiatives have been undertaken to bring together different approaches and systems of protection, including work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region. At the time of publication of these revised Guidelines, the Council of Europe continues its deliberations on the modernisation of Convention 108 on the Automated Processing of Personal Data. Further work is needed at the policy level towards a more seamless approach to global privacy governance.

A strong global network of privacy enforcement authorities working together is a first important step towards global interoperability. In 2005, the OECD revisited the issue of global cooperation among privacy enforcement authorities, resulting in the adoption of a new framework for cross-border co-operation in the form of the 2007 Recommendation. The three-year implementation report for the 2007 Recommendation highlighted the need for further efforts to ensure that privacy enforcement authorities have sufficient powers to administer effective sanctions and resources to accomplish their mission.[15] The Terms of Reference for the review of the Guidelines called for a redoubling of efforts to develop a globally active network of privacy enforcement authorities. Paragraph 20 reiterates the commitment expressed by Member countries in the 2007 Recommendation to enhance co-operation between privacy enforcement authorities. In particular, Member countries are encouraged to address obstacles – be they legal or practical – towards information sharing among privacy enforcement authorities to facilitate coordinated and effective enforcement. Reducing the barriers to information sharing has been a particular concern in this respect.

Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by organisations and ensure that privacy requirements are maintained. It can also enhance individuals' awareness and understanding of their rights in a global environment.

Improving the evidence base for policy making

The OECD Recommendation on Internet Policy Making calls for the development of capacities to bring publicly available, reliable data into the policy-making process. The Communiqué, annexed to it for information, specifically notes the value of internationally comparable metrics.

The evidence base which is currently available for policymaking in the area of privacy is uneven. Household surveys by national statistical agencies provide some insight into privacy issues on the basis of internationally comparable metrics. However, the scope of these surveys, which focus primarily on awareness issues among individuals, is limited. There are gaps, for example, related to the technical or economic dimensions of privacy, as well as the implementation of prevention measures. Privacy enforcement authorities gather considerable data that are made public through annual reports, but not in a format well-suited to international comparisons. For example, progress in understanding complaint data, data breach statistics, and how fines and other sanctions influence data controllers' behaviour could be a potentially rich source of insight for policy makers. The addition of paragraph 22 in Part Six identifies the need for Member countries' support for initiatives to improve the evidence base in this area.

Other Updates

In addition to the substantive changes discussed in the previous section, the revised Guidelines reflect several minor changes which were made either to enhance readability or otherwise update the language of the 1980 Guidelines.

As a general matter, all references to specific parts of the Guidelines, have been replaced by a more generic phrasing ("these Guidelines").

Paragraph 2, which specifies the scope of the Guidelines, now refers to a "risk" rather than "danger" to privacy and individual liberties, reflecting the increased emphasis on risk within the revised Guidelines. This change should not be construed as preventing Member countries from extending the scope of laws protecting privacy or other privacy regimes to all forms of processing of personal data.

Former paragraph 3(b) has been deleted, as the ability for Member countries to exclude from the application of the Guidelines "personal data which do not pose any risk to privacy and individual liberties" is already reflected in paragraph 2.

Former paragraph 3(c) has been deleted, as Member countries have generally extended the scope of their domestic privacy laws to include the processing of personal data in general.

A new paragraph 3(b) has been added, to recognise the potential conflict between the protection of privacy and other fundamental rights arising from the now ubiquitous nature of personal data processing. It is also in line with the Communiqué on Principles for Internet Policy Making[16] which underlines that "[p]rivacy rules should also consider the fundamental rights of others in society including rights to freedom of speech, freedom of the press, and an open and transparent government".

Former paragraphs 15 and 16 of the 1980 Guidelines were removed in the interests of clarity and to avoid repetition, as the commitment of Member countries to the global free flow of information and security is already underlined elsewhere in the Recommendation.

NOTES

1 Remarks from Hon. Michael Kirby on the 30th anniversary of the OECD Privacy Guidelines, http://www.oecd.org/internet/interneteconomy/49710223.pdf.

2 The system of BCRs is being further developed, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

3 See http://www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Summary.pdf.

4 APEC, APEC Cross-border Privacy Rules System – Policies, rules and guidelines, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

5 OECD (2007), Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, http://www.oecd.org/internet/interneteconomy/38770483.pdf.

6 OECD (2011), Council Recommendation on Principles for Internet Policy Making www.oecd.org/internet/interneteconomy/49258588.pdf.

7 OECD (2011), Communiqué on Principles for Internet Policy Making www.oecd.org/internet/interneteconomy/49258588.pdf.

8 OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No.176, http://dx.doi.org/10.1787/5kgf09z90c31-en.

9 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, http://dx.doi.org/10.1787/5kgdpm9wg9xs-en.

10 OECD (2011), "Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/sti/interneteconomy/48975226.pdf

11 OECD (2012), Recommendation of the Council on Regulatory Policy and Governance, www.oecd.org/gov/regulatorypolicy/49990817.pdf.

12 *E.g.,* OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security, www.oecd.org/internet/interneteconomy/15582260.pdf; OECD (2012), Recommendation of the Council on the Protection of Children Online, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False.

13 G8 (2011), Deauville Declaration: Internet, www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html.

[14] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Official Journal of the European Communities, 25 August 2000, L-215, 7-47. See also www.export.gov/safeharbor.

[15] See 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, http://dx.doi.org/10.1787/5kgdpm9wg9xs-en.

[16] OECD (2011), Council Recommendation on Principles for Internet Policy Making www.oecd.org/internet/interneteconomy/49258588.pdf.