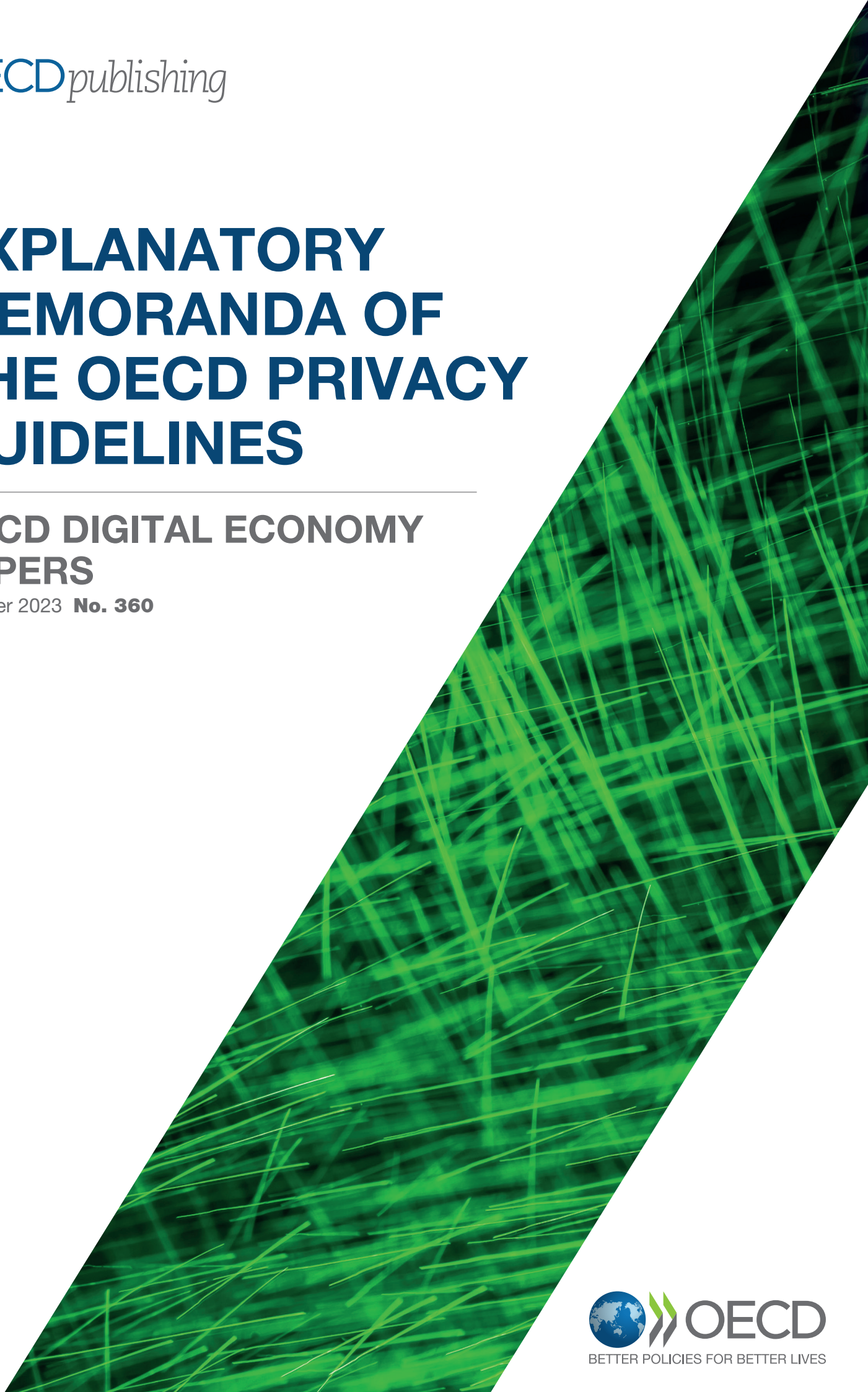
OECD publishing

EXPLANATORY MEMORANDA OF THE OECD PRIVACY GUIDELINES

OECD DIGITAL ECONOMY PAPERS
October 2023 **No. 360**



OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This document reproduces the two existing explanatory memoranda which accompany the OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] (the "OECD Privacy Guidelines") adopted by the Council in 1980 and revised in 2013.

The Explanatory Memorandum was developed alongside the original version of the OECD Privacy Guidelines, which was adopted by the Council on 23 September 1980. The original Explanatory Memorandum is reproduced in Chapter 2 of this document.

In 2013, a supplementary Explanatory Memorandum was developed to provide context and rationale for the revisions to the OECD Privacy Guidelines. It was approved for public release by the OECD Council on 11 July 2013 when it adopted the revised OECD Privacy Guidelines. It is intended to supplement – not replace – the original Explanatory Memorandum, which remains relevant to interpreting the aspects of the OECD Privacy Guidelines that remain unchanged from 1980. The supplementary Explanatory Memorandum is reproduced in Chapter 1 of this document.

This document was prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E. under the reference code::

DSTI/CDEP(2023)21/FINAL

Table of contents

1. Supplementary Explanatory Memorandum to the revised Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)

Foreword

Over many decades the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders.

On 11 July 2013 the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines"). This revision is the first since the original 1980 release of the Guidelines and arises out of a call by Ministers in the 2008 Seoul Declaration for the Future of the Internet Economy to assess the Guidelines in light of "changing technologies, markets and user behaviour, and the growing importance of digital identities".

The OECD Working Party on Information Security and Privacy (WPISP) agreed on Terms of Reference for the review in 2011. The Terms of Reference highlighted 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.

In accordance with the Terms of Reference, the WPISP convened a multistakeholder 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. Omer Tene, consultant to the OECD, served as rapporteur. On the basis of the work by the Expert Group, proposed revisions were developed by the WPISP, approved by the Committee for Information, Computer and Communications Policy (ICCP), before final adoption by the OECD Council.

Two themes run through the updated Guidelines. First is a focus on the practical implementation of privacy protection through an approach grounded in risk management. Second is the need for greater efforts to address the global dimension of privacy through improved interoperability. A number of new concepts are introduced, including:

- ***National privacy strategies*** – While effective laws are essential, the strategic importance of privacy today also requires a multifaceted national strategy co-ordinated at the highest levels of government.
- ***Privacy management programmes*** – These serve as the core operational mechanism through which organisations implement privacy protection.
- ***Data security breach notification*** – This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data.

Other revisions modernise the OECD approach to transborder data flows, detail the key elements of what it means to be an accountable organisation, and strengthen privacy enforcement. As a step in a continuing process, this revision leaves intact the original "Basic Principles" in Part Two of the Guidelines.

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", [OECD, 2007]).

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 (OECD, 2011a) 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" (OECD, 2011b).

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" (OECD, 2011c), and "Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation" (OECD, 2011d).

Building on this preparatory work, the Working Party for Information Security and Privacy (WPISP) developed Terms of Reference (OECD, 2011e) 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 (OECD, 2012a). 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 crossborder 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.[5] 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" (G8, 2011).

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[6], 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.[7] 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 (OECD, 2011g) 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, 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 www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Sum mary.pdf.

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

[5] E.g., OECD (2002), OECD (2012b).

[6] 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.

[7] See OECD (2011f).

References

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

OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security, www.oecd.org/internet/interneteconomy/15582260.pdf

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

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

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

OECD (2011c), "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.

OECD (2011d), "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.

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

OECD (2011f), "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

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

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

OECD (2012b), 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.

2. Original Explanatory Memorandum to the OECD Privacy Guidelines (1980)

Introduction

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.

The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonisation of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions.

The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

I. General background

The problems

The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest

has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

Activities at national level

Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (lois sur la protection des données), whereas in English speaking countries they are usually known as "privacy protection laws". Most of the statutes were enacted after 1973 and this present period may be described as one of continued or even widened legislative activity. Countries which already have statutes in force are turning to new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have bills pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and research papers prepared by public committees or similar bodies, help to clarify the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

The approaches to protection of privacy and individual liberties adopted by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with the initial collection of data and ending with

erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

Differences between national approaches as apparent at present in laws, bills or proposals for legislation refer to aspects such as the scope of legislation, the emphasis placed on different elements of protection, the detailed implementation of the broad principles indicated above, and the machinery of enforcement. Thus, opinions vary with respect to licensing requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing traditional differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

International aspects of privacy and data banks

For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

Relevant international activities

There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).

A number of international agreements deal in a more general way with the issues which are at present under discussion, viz. the protection of privacy and the free dissemination of information. They include the European Convention of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

In 1973 and 1974 the Committee of Ministers of the ***Council of Europe*** adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks and rules of conduct for data processing professionals. The Convention was adopted by the Committee of Ministers on 17th September 1980. It seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

The ***European Community*** has carried out studies concerning the problems of harmonisation of national legislations within the Community, in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

Activities of the OECD

The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, e.g. in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.

A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised (a) the need for generally continuous and uninterrupted flows of information between countries, (b) the legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens, (c) the economic value of information and the importance of protecting “data trade” by accepted rules of fair competition, (d) the needs for security safeguards to minimise violations of proprietary data and misuse of personal information, and (e) the significance of a commitment of countries to a set of core principles for the protection of personal information.

Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonisation of national legislations, without this precluding at a later date the establishment of an international Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by l July 1979.

The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports

containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

a) The specific, sensitive facts issue

The question arose as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (e.g. credit reporting). Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.

b) The ADP issue

The argument that ADP is the main cause for concern is doubtful and, indeed, contested.

c) The legal persons issue

Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.

d) The remedies and sanctions issue

The approaches to control mechanisms vary considerably: for instance, schemes involving supervision and licensing by specially constituted authorities might be compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.

e) The basic machinery or implementation issue

The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level “machinery” questions which should be left to domestic implementation.

f) The choice of law issue

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of transborder data flows. The question arose, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.

g) The exceptions issue

Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?

h) The bias issue

Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organisations; thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a convention which will be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal

data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

II. The guidelines

A. Purpose and scope

General

The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries.

Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;

b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;

c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data,

they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

a) effective national measures for the protection of privacy and individual liberties;

b) avoidance of practices involving unfair discrimination between individuals; and

c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-member countries

The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-member countries and appropriate international organisations.

The broader regulatory perspective

It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments governing such issues as human rights, telecommunications, international trade, copyright, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies. Some Member countries have emphasised the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or

may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

Similarly, it is debatable to what extent people belonging to a particular group (i.e. mentally disabled persons, immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (cf. paragraph 49 below).

Automated and non-automated data

In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and computer networks. The Expert Group has devoted special attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, “mixed” data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

Because of the difficulties mentioned, the Guidelines do not put forward a definition of “automatic data processing” although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes. It should be emphasised that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

B. Detailed comments

General

The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

The list of definitions has been kept short. The term “data controller” is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, viz. (a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes; (b) data processing service bureaux which carry out data processing on behalf of others; (c) telecommunications authorities and similar bodies which act as mere conduits; and (d) “dependent users” who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities. Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

The terms “***personal data***” and “***data subject***” serve to underscore that the Guidelines are concerned with physical persons. The 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. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.

The term “***transborder flows of personal data***” restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated

with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, viz. that data pose a danger to privacy and individual liberties. Such dangers can arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3(b) provides for many “trivial” cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3(c) provides for such a limitation.

Paragraph 4: Exceptions to the Guidelines

To provide formally for exceptions in Guidelines which are part of a non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (e.g. through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret. The formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions – hence the wording that they include national sovereignty, national security and public policy (“ordre public”). Another overriding national concern would be, for instance, the financial interests of the State (“crédit public”). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, e.g. the regulation of certain types of data or activities as compared to regulation of a general nature (“omnibus approach”).

The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection Limitation Principle

As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, viz. (a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no data are intrinsically "private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to:

- data quality aspects (i.e. that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.);

- limits associated with the purpose of the processing of data (i.e. that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose);
- "earmarking" of specially sensitive data according to traditions and attitudes in each Member country;
- limits to data collection activities of certain data controllers;
- civil rights concerns.

The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder ("where appropriate") that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled person, etc.

Paragraph 8: Data Quality Principle

Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose Specification Principle

The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use Limitation Principle

This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can

be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative – see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security Safeguards Principle

Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasised that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has a broad coverage. The cases mentioned in the provision are to some extent overlapping (e.g. access/ disclosure). “Loss” of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. “Modified” should be construed to cover unauthorised input of data, and “use” to cover unauthorised copying.

Paragraph 12: Openness Principle

The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are “readily available” implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual Participation Principle

The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for:

The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data “in a reasonable manner” means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain

copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.

The right to reasons in Paragraph 13(c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, e.g. in order to inform and alert a subject to his rights so that he can exercise them effectively.

The right to challenge in 13(c) and (d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.): such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability Principle

The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, “dependent users” (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. Paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic Principles of International Application

The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other’s interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with security issues in a broad sense and may be said to correspond, at the international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, i.e. effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

For domestic processing **Paragraph 15** has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other’s efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (e.g. access to the addresses of nationals living abroad).

As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to **Paragraph 16**, be uninterrupted and secure, i.e. protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, i.e. data which pass through a Member country without being used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that convention, the members of the International Telecommunications Union, including the OECD Member countries, have agreed, inter alia, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international correspondence. As regards exceptions, the right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws or the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines. In their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

Paragraph 17 reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned – in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

Paragraph 18 attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus not openly announced. However, Paragraph 18 is not intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for intentional data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National Implementation

The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery

is envisaged for putting the Guidelines into effect. The opening sentence shows the different approaches which might be taken by countries, both generally and with respect to control mechanisms (e.g. specially set up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

In Paragraph 19(a) countries are invited to adopt appropriate domestic legislation, the word “appropriate” foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions. Paragraph 19(b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19(c) should be given a broad interpretation; it includes such means as advice from data controllers and the provision of assistance, including legal aid. Paragraph 19(d) permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19(e) dealing with discrimination is directed against unfair practices but leaves open the possibility of “benign discrimination” to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information Exchange and Compatible Procedures

Two major problems are dealt with here, viz. (a) the need to ensure that information can be obtained about rules, regulations, decisions, etc., which implement the Guidelines, and (b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

The importance of the second problem is, generally speaking, proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for co-ordinating special provisions on transborder data flows in domestic laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for Co-operation

The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21(ii), i.e. mutual aid in procedural matters and requests for information, is future-oriented: its practical significance is likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of Laws

The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of

international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.