Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

OECD Legal Instruments

OECD
BETTER POLICIES FOR BETTER LIVES

Please cite this document as:
OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188

Series: OECD Legal Instruments

Date(s)

Adopted on 23/09/1980
Amended on 11/07/2013

Background Information

The Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data was adopted by the OECD Council on 23 September 1980 ("1980 Guidelines"). The 1980 Guidelines were adopted 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. They represent the first internationally agreed-upon set of privacy principles and have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, they were updated on 11 July 2013 due to changes in personal data usage, as well as new approaches to privacy protection. The Recommendation aims to promote and protect the fundamental values of privacy, individual liberties and the global free flow of information to foster the development of economic and social relations among Adherents.

THE COUNCIL,

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

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

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

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

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

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

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

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

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

I. **RECOMMENDS** that Member countries:

- Demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government;
- Implement the Guidelines contained in the Annex to this Recommendation, and of which they form an integral part, through processes that include all relevant stakeholders;
- Disseminate this Recommendation throughout the public and private sectors;

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

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

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

ANNEX

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

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

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

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

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

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

Scope of Guidelines

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

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

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

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

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

   a) as few as possible, and

   b) made known to the public.

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

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

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

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

Purpose Specification Principle

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

Use Limitation Principle

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

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

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

Openness Principle

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

Individual Participation Principle

13. Individuals should have the right:

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

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

   i. within a reasonable time;

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

   iii. in a reasonable manner; and

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

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

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

Accountability Principle

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

PART THREE. IMPLEMENTING ACCOUNTABILITY

15. A data controller should:

a) Have in place a privacy management programme that:

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

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

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

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

v. includes plans for responding to inquiries and incidents;

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

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

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

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

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

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

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

PART FIVE. NATIONAL IMPLEMENTATION

19. In implementing these Guidelines, Member countries should:

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

b) adopt laws protecting privacy;

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

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

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

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

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

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

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

PART SIX. INTERNATIONAL CO OPERATION AND INTEROPERABILITY

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

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

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

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

Adherents*

OECD Members	Non-Members
Australia	
Austria	
Belgium	
Canada	
Chile	
Czech Republic	
Denmark	
Estonia	
Finland	
France	
Germany	
Greece	
Hungary	
Iceland	
Ireland	
Israel	
Italy	
Japan	
Korea	
Latvia	
Luxembourg	
Mexico	
Netherlands	
New Zealand	
Norway	
Poland	
Portugal	
Slovak Republic	
Slovenia	
Spain	
Sweden	
Switzerland	
Turkey	
United Kingdom	
United States	

*Additional information and statements are available in the Compendium of OECD Legal Instruments: http://legalinstruments.oecd.org

About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Legal Instruments

Since the creation of the OECD in 1961, around 450 substantive legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions**: OECD legal instruments which are legally binding on all Members except those which abstain at the time of adoption. While they are not international treaties, they entail the same kind of legal obligations. Adherents are obliged to implement Decisions and must take the measures necessary for such implementation.

- **Recommendations**: OECD legal instruments which are not legally binding but practice accords them great moral force as representing the political will of Adherents. There is an expectation that Adherents will do their utmost to fully implement a Recommendation. Thus, Members which do not intend to do so usually abstain when a Recommendation is adopted, although this is not required in legal terms.

- **Declarations**: OECD legal instruments which are prepared within the Organisation, generally within a subsidiary body. They usually set general principles or long-term goals, have a solemn character and are usually adopted at Ministerial meetings of the Council or of committees of the Organisation.

- **International Agreements**: OECD legal instruments negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangement, Understanding and Others**: several ad hoc substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.