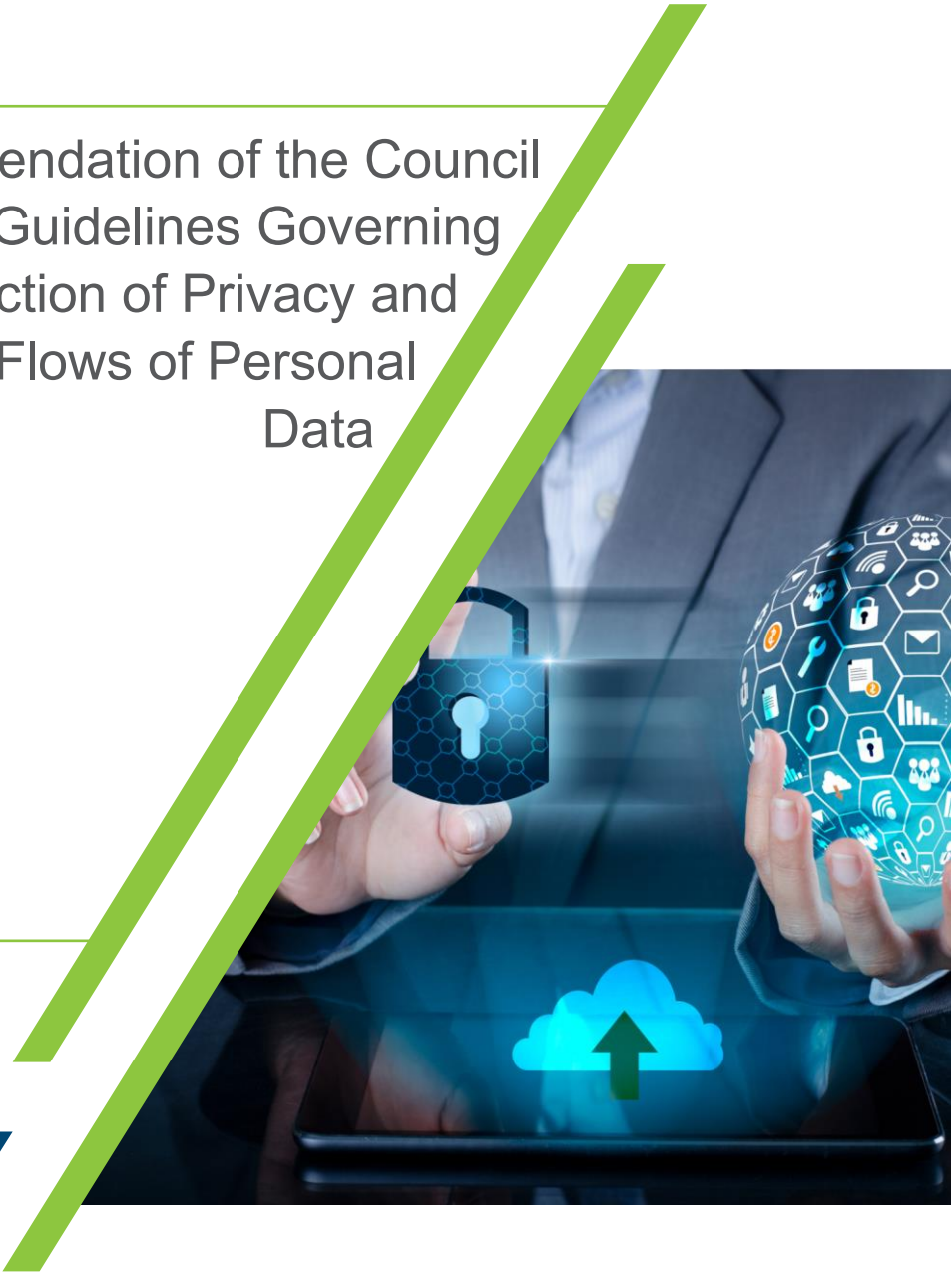




Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data



**OECD Legal
Instruments**

This document is published under the responsibility of the Secretary-General of the OECD. It reproduces an OECD Legal Instrument and may contain additional material. The opinions expressed and arguments employed in the additional material do not necessarily reflect the official views of OECD Member countries.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

For access to the official and up-to-date texts of OECD Legal Instruments, as well as other related information, please consult the Compendium of OECD Legal Instruments at <http://legalinstruments.oecd.org>.

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

Photo credit: © sarayut_sy/shutterstock.com

© OECD 2024

This document is provided free of charge. It may be reproduced and distributed free of charge without requiring any further permissions, as long as it is not altered in any way. It may not be sold.

This document is available in the two OECD official languages (English and French). It may be translated into other languages, as long as the translation is labelled "unofficial translation" and includes the following disclaimer: *"This translation has been prepared by [NAME OF TRANSLATION AUTHOR] for informational purpose only and its accuracy cannot be guaranteed by the OECD. The only official versions are the English and French texts available on the OECD website <http://legalinstruments.oecd.org>"*

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, and revised on 11 July 2013, on the proposal of the Committee for Information, Computer and Communication Policy (now the Committee on Digital Economy Policy - CDEP). It recommends that Adherents implement the Guidelines contained in the Annex to the Recommendation, and of which they form an integral part (commonly referred to as the 'OECD Privacy Guidelines').

The OECD Privacy Guidelines represent the first internationally agreed-upon set of privacy principles, developed to address concerns arising out of increased use of personal data for the protection of privacy and individual liberties (often merged as privacy for ease of use in common language), and the resulting risk to global economies from restrictions to the flow of personal data across borders. Since their adoption, they have influenced legislation and policy in OECD countries and beyond.

OECD's work on privacy and cross border data flows

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 with trust across borders for many decades. The OECD Privacy Guidelines are the cornerstone of this work, and are considered the global minimum standard for privacy and data protection. They are framed in concise, technology-neutral language, and have proven remarkably adaptable to technological and societal changes.

The OECD, through the CDEP and its Working Party on Data Governance and Privacy (DGP), works with countries and experts to consider developments in privacy and data protection, and provide practical guidance on the implementation of the Privacy Guidelines in an ever evolving digital environment.

An inclusive process for developing and reviewing the OECD Privacy Guidelines

The importance of information and communication technologies and transborder data flows, and their implications for privacy first attracted the attention of the OECD in 1969, and the 1980 OECD Privacy Guidelines were the product of several years of analytical and consultative work. In 1974, the OECD held a seminar that looked at issues such as the right of citizens to access their personal data, and the rules for transborder data flows. Following a large symposium in 1977, an expert group chaired by the Honorable Michael Kirby of Australia was convened to work on the guidelines. The resulting work represented a consensus by OECD countries on personal data handling and protection.

The revision in 2013 was likewise the product of several years of analytical work. A volunteer group of privacy experts was formed to assist in the review process, made up of experts from governments, privacy enforcement authorities (PEAs), academia, business, civil society and the Internet technical community. As a result of this work, it was determined that there was no need to fundamentally rethink the core principles of the 1980 Guidelines, however it was considered appropriate to update the OECD Privacy Guidelines. The 2013 revisions focused on practical implementation of privacy protection through an approach grounded in risk management, and on a need for greater efforts to address the global dimension of privacy. New concepts were introduced, such as national privacy strategies, privacy management programmes and data security breach notifications. Other revisions sought to modernise the OECD's approach to data flows, centering on strengthening accountability and privacy enforcement.

The original 1980 OECD Privacy Guidelines were accompanied by an Explanatory Memorandum, and, in 2013, a supplementary Explanatory Memorandum was produced to support implementation of the revised parts of the OECD Privacy Guidelines.

Scope of the OECD Privacy Guidelines

The OECD Privacy Guidelines apply to personal data (whether in the public or the private sector) which, because of the manner in which they are processed, their nature, or the context in which they are used, pose a risk to privacy and individual liberties. The Recommendation aims to promote and protect the fundamental values of privacy, individual liberties and the global free flow of personal data to foster the development of economic and social relations among OECD countries.

The OECD Privacy Guidelines set out eight Basic Principles of National Application (in Part Two), namely collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The validity and pertinence of these basic principles were reaffirmed through both the 2013 revision and the 2021 report on implementation. Part Three of the OECD Privacy Guidelines, which was added in the 2013 revision, provides guidance on the implementation of the accountability principle. The OECD Privacy Guidelines further include a section on international application and legitimate restrictions on the free flow of personal data (Part Four), a section on the means for national implementation of the basic principles (Part Five), and a section on international co-operation and interoperability (Part Six).

*For further information please consult: <https://www.oecd.org/sti/economy/privacy.htm>.
Contact information: dataandprivacy@oecd.org.*

Implementation

Since their adoption, the OECD Privacy Guidelines have been widely disseminated and implemented. OECD countries adhering to them repeatedly refer to the OECD Privacy Guidelines as forming the bedrock of their own national frameworks, and they are widely recognised as forming the basis of other data protection frameworks – demonstrating their global reach. The [2021 report](#) to the Council on the implementation of the Recommendation revealed a decisive picture of implementation and dissemination. All Adherents who responded to the questionnaire have privacy legislation in place; over 84% are parties to at least one multilateral agreement or legal framework that defines legitimate restrictions on transborder flows of personal data; and all Adherents responding to the questionnaire have established privacy enforcement authorities as required by the 2013 revision.

Nonetheless, while the 2021 report concluded that the Recommendation itself does not need revision, it did identify that further implementation actions were needed – such as developing further implementation guidance, undertaking cross-cutting work with other relevant OECD work streams, and undertaking specific further analytical work. In 2023, the DGP developed an Implementation Guidance focused on accountability. This Implementation Guidance, the 1980 Explanatory Memorandum, and the 2013 supplementary Explanatory Memorandum are designed to complement each other and should be read and understood in conjunction.

The next reporting to the Council on the implementation, dissemination and continued relevance of the Recommendation is scheduled to take place in 2026.

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.

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, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, 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, more than 500 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** are adopted by Council and are legally binding on all Members except those which abstain at the time of adoption. They set out specific rights and obligations and may contain monitoring mechanisms.
- **Recommendations** are adopted by Council and are not legally binding. They represent a political commitment to the principles they contain and entail an expectation that Adherents will do their best to implement them.
- **Substantive Outcome Documents** are adopted by the individual listed Adherents rather than by an OECD body, as the outcome of a ministerial, high-level or other meeting within the framework of the Organisation. They usually set general principles or long-term goals and have a solemn character.
- **International Agreements** are negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.
- **Arrangements, Understandings and Others:** several other types of 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.