

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
DIGITAL POLICY COMMITTEE**

Working Party on Data Governance and Privacy

**Recommendation concerning Guidelines Governing the Protection of Privacy and
Transborder Flows of Personal Data: review of implementation, dissemination and
continued relevance**

Extended scoping note

14th Session of the Working Party on Data Governance and Privacy (WPDGP)
16-17 April 2026

This document presents the background and an extended outline for the 2026 report on the implementation, dissemination and continued relevance of the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/ 0188].

Action requested: Delegates are invited to discuss this document and provide input to inform the elaboration of the resulting report, in addition to providing responses to the questions presented in the Note by the Secretariat. Please submit feedback to the Secretariat in writing by 3 June 2026.

This report is a contribution to IOR 7.4 in the DPC's 2025-2026 Programme of Work and Budget.

Francesca Casalini: francesca.casalini@oecd.org
Giuseppe Bianco: giuseppe.bianco@oecd.org
Gaetan Goldberg: gaetan.goldberg@oecd.org
Clarisse Girot : clarisse.girot@oecd.org

JT03584941

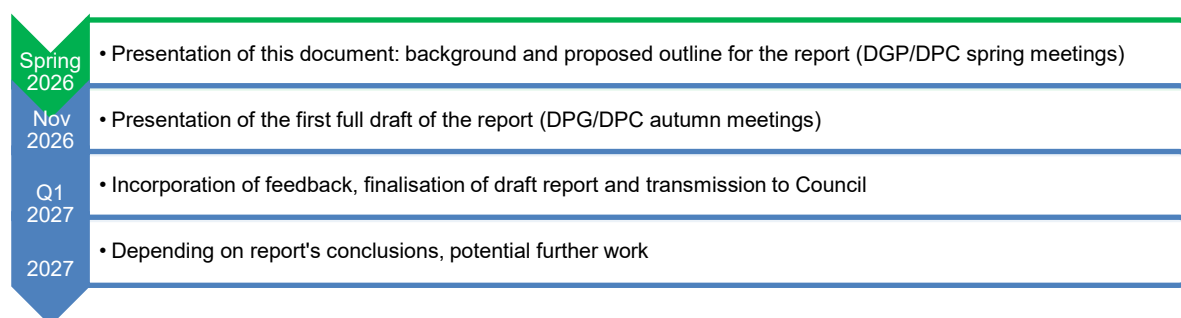
Table of contents

Note by the Secretariat	3
OECD Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data: report on implementation, dissemination, and continued relevance	4
1 Background	5
1.1. History of the Privacy Guidelines	5
1.2. Content of the Privacy Guidelines	6
1.3. Proposed scope and methodology for the report	8
2 Proposed outline of the report	9
2.1. Context	9
2.2. Developments in privacy policy since the last report to Council	9
2.3. Overview of national developments around the Privacy Guidelines' parts	10
2.4. OECD work advancing the implementation of the Privacy Guidelines	10
2.5. Potential outcomes	10

Note by the Secretariat

In recognition of the fundamental role of privacy and personal data protection in safeguarding individual rights and the importance of cross-border data flows, on 23 September 1980, the OECD Council adopted the Recommendation concerning the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereafter, “the Privacy Guidelines”) [\[OECD/LEGAL/0188\]](#). The 1980 Privacy Guidelines were revised into their current form in the context of their revision in 2013. A further review in 2021 did not recommend changes, however, implementation guidance was developed to support the Recommendation. In that context, the OECD Council invited a follow-up report on the implementation, dissemination, and continued relevance of the Privacy Guidelines to be produced within the following five years.

In line with the current Digital Policy Committee (DPC) PWB’s IOR 7.4, this document provides the background and proposes an outline of the report, including consideration of potential outcomes. The proposed outline will be expanded in the next version, considering delegates’ comments. The following timeline is envisaged.



Action requested

Delegates are invited to discuss this document and to provide responses to the three questions below, by 3 June 2026.

Questions for delegates

- Are there specific principles or themes within the Privacy Guidelines that should be prioritised in the report to reflect their current importance in your regulatory frameworks?
- To what extent have the Privacy Guidelines served as one of the foundational "anchors" for your national privacy framework? Do they support “leadership and commitment to the protection of privacy and free flow of information at the highest levels of government”? Please provide relevant examples.
- Do the Privacy Guidelines remain a relevant point of reference in international discussions on privacy and data protection? Please provide relevant examples.

OECD Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data: report on implementation, dissemination, and continued relevance

1 Background

1.1. History of the Privacy Guidelines

1. The OECD has a long history of working on the protection and promotion of privacy, personal data and cross-border data flows. Its work has spanned from foundational principles embodied in the 1980 OECD Recommendation concerning the Protection of Privacy and Transborder Flows of Data (hereafter, “the Privacy Guidelines”), which have influenced legislation and policy in OECD Member countries and beyond since then, to the contemporary global policy objective of “Data Free Flow with Trust” (DFFT) ([Data free flow with trust | OECD](#)).

2. The Privacy Guidelines were adopted by the OECD on 23 September 1980 [[OECD/LEGAL/0188](#)]. Drafted during the first wave of computer diffusion, the Privacy Guidelines were the first internationally agreed-upon set of principles regarding privacy and cross-border data flows. They had a dual objective to protect individual privacy while ensuring that differing national laws would not impede the free flow of information. They were directed primarily at its Adherents (governments), but several parts are intended to guide the actions of other actors, namely data controllers at public and private organisations, as well.

3. In 1985, the Declaration on Transborder Data Flows considered the Privacy Guidelines and the progress made in privacy policies at the national and international level to define policy issues of importance for the OECD Member countries [[OECD/LEGAL/0216](#)]. The Declaration on Transborder Data Flows aims to promote access to transborder data and services, and avoid unjustified barriers to data exchange. It also aims to seek transparency in related regulations and policies, common approaches, and to consider impact of actions on other countries.

4. As traditional territorial laws continued struggling to keep pace with borderless digital communication (as recognised in the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks (Ottawa) [[OECD/LEGAL/0301](#)]), a shift took place from purely substantive rules to procedural co-operation. This culminated in the 2007 Recommendation on cross-border co-operation in the enforcement of laws protecting privacy [[OECD/LEGAL/0352](#)], which addresses the capacity of national Privacy Enforcement Authorities (PEAs) to share information or co-operate on investigations involving multiple jurisdictions simultaneously.

5. By the time of the 2008 Seoul Ministerial Declaration for the Future of the Internet Economy, the focus had matured into “trust” among all stakeholders as a prerequisite for economic growth and cross-border data sharing, setting the stage for a modernisation of the original 1980 Privacy Guidelines [[OECD/LEGAL/0366](#)].

6. The 2013 review and resulting revision, which led to the Privacy Guidelines in their current form, retained the original principles but strengthened their implementation. It marked a shift towards a more operational accountability framework. Since then, data controllers have been expected not only to comply with the principles, but to demonstrate compliance through internal governance measures

and structured privacy management programmes. The 2013 revision also introduced a clearer risk-based approach, encouraging data controllers to assess and manage privacy risks based on the likelihood and severity of harm. It addressed emerging challenges by encouraging data breach notification where serious risks arise and by reinforcing cross-border enforcement co-operation among PEAs. In addition, it encouraged governments to adopt national privacy strategies to address privacy as a broader policy issue. It also identified a need to improve the evidence base in the area of privacy [[Explanatory memoranda of the OECD Privacy Guidelines \(EN\)](#)].

7. Between 2018 and 2021, the Committee on Digital Economy Policy (CDEP) (since renamed the Digital Policy Committee (DPC)), through its Working Party on Data Governance and Privacy (DGP), conducted a comprehensive review of the Privacy Guidelines. In the report to the Council which resulted from that review process, it was concluded that the Privacy Guidelines themselves remained important and relevant and did not need revision. However, the development of further implementation guidance was identified as a means to improve implementation, and cross-cutting work with other relevant OECD work streams and specific further analytical work has been carried out since then (OECD, 2021^[1]). In this regard, for example, the DGP developed an Implementation Guidance focused on accountability in 2023 (OECD, 2023^[2]).

8. The 2022 Declaration on a Trusted, Sustainable and Inclusive Digital Future [[OECD/LEGAL/0488](#)] emphasised the commitment to advance strong protections for personal data, laws and regulation fit for the digital age, to protect privacy and other human rights and freedoms in the face of new privacy risks and rapid technological developments, and to strengthen efforts to further a common understanding, and to work towards identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, including across borders, in order to foster future interoperability.

9. In line with the Council's 2021 invitation to "report to the Council in five years on the implementation, dissemination and continued relevance of the Recommendation" [[C/M\(2021\)8](#)], this document is intended to initiate discussions on the report, its outline and consideration of its potential outcomes.

1.2. Content of the Privacy Guidelines

10. It is worthwhile to recall that the Privacy Guidelines are composed of six parts (summarised in Box 1.1) and are complemented by the 1980 Explanatory Memorandum, the 2013 supplementary Explanatory Memorandum and the 2023 Implementation Guidance on accountability, all of which are designed to complement each other and should be read and understood in conjunction.

11. The Privacy Guidelines are designed to embody the consensus on a common international framework for protecting personal data while enabling the free flow of information across borders. They are drafted in concise, technology-neutral language, and their scope is broad, applying to personal data in both public and private sectors.

12. Rather than creating binding legal obligations, the Privacy Guidelines set out general principles intended to guide national legislation, and they are expressly defined as "minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties" (para. 6). By establishing this flexible baseline, the Privacy Guidelines create a shared conceptual framework that persists regardless of the growing sophistication of national regulations. Accordingly, it is proposed that the report focuses on examining the Privacy Guidelines' enduring capacity to orient national regulation and to facilitate international policy dialogue and co-operation on core privacy and data protection themes.

13. Some metrics are helpful to gauge the relevance of the Privacy Guidelines today. Views for the webpage of the Privacy Guidelines on the Compendium of OECD Legal Instruments were 13 584 in 2025, up from 12 933 from 2024, meaning a 5% increase year on year.¹ They were the second most consulted legal instrument in the Compendium in 2024 and 2025.

Box 1.1. Overview of the OECD Privacy Guidelines

Part one. General

This part provides definitions and the scope of the Guidelines.

Part two. Basic principles of national application

The Guidelines are organised around a set of eight core privacy principles. The validity and pertinence of these basic principles were reaffirmed through both the 2013 revision and the 2021 report on implementation.

- | | |
|-------------------------|----------------------------|
| • Collection limitation | • Security safeguards |
| • Data quality | • Openness |
| • Purpose specification | • Individual participation |
| • Use limitation | • Accountability |

Part three. Implementing accountability

Part three provides guidance on the implementation of the accountability principle.

Part four. Basic principles of international application: free flow and legitimate restrictions

This section represents the Guidelines' mechanism for balancing the economic necessity of data mobility with the imperative of protecting citizens' privacy and individual liberty. It represents a "risk-based" approach to international transfers.

Part five. National implementation

Part five calls on adherents to adopt laws, policies, and enforcement mechanisms that give effect to the core privacy principles within their domestic systems.

Part six. International co-operation and interoperability

Part six encourages countries to work together to facilitate transborder data flows, avoid unnecessary restrictions, and support mutual assistance between PEAs. It also identifies the need for Adherents to develop internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

¹ Downloads of booklets are not counted, this is only the views of the webpage. Google Analytics has changed in 2023 and, for the sake of consistency, data before 2024 are no longer compared.

1.3. Proposed scope and methodology for the report

14. As explained further in the following section, it is proposed to review national implementation, dissemination and continued relevance through a mix of desk-based research and information gathered from Adherents related to:

- Developments in the last five years in national legislation on the topics of the Privacy Guidelines to review their continued relevance in national priorities;
- Overview of the work conducted by the DPC and DGP expanding on the Privacy Guidelines' main themes, highlighting whether and how this work has supported Adherents in implementation and dissemination.

2 Proposed outline of the report

2.1. Context

15. The first section of the report will provide a summary of the origin and evolution of the Privacy Guidelines (expanding the background section above), to set the scene within which the report takes place. It will focus extensively on the 2021 review: what it reviewed, its main findings, and its outcome.

2.2. Developments in privacy policy since the last report to Council

16. The technological and regulatory landscape surrounding privacy, personal data and cross-border data flows has undergone a few important developments since the last review of the Privacy Guidelines in 2021. This section will provide a summary of key changes in the global landscape for privacy policy since the last report to Council:

- In terms of technology, the proliferation of generative AI and large-scale automated processing, including in new contexts such as the rapid expansion of neurotechnologies into clinical, research, workplace and consumer domains, has introduced new considerations for principles such as purpose specification and data minimisation. Because these systems increasingly depend on access to and processing of vast, unstructured datasets, advancements have been made in how traditional principles such as collection limitation, purpose limitation, and others, can be practically applied. Furthermore, the maturation of privacy enhancing technologies (PETs) suggests a potential transition from purely procedural safeguards toward their mix with more technical, "by-design" security standards. These advancements do not invalidate existing principles but warrant a reflection on their integration.
- On the policy and geopolitical level, the general increase in regulations and rules addressing specific risks arising from cross-border data flows has further shaped the context. With data policy being increasingly treated by governments as part of digital sovereignty policies and industrial strategies, the notions of trust and cross-border data flows are now looked at with a greater focus on how to harness data for economic growth and technological resilience. Government access to personal data held by private sector entities has also continued to represent a critical pivot point for international data flows. Furthermore, since 2021, the emergence of new policy frameworks addressing data use from different regulatory perspectives, such as on AI, digital markets or online safety, have layered additional obligations on top of existing privacy laws. This trend has expanded the role of privacy law from a standalone regime into a central but interdependent component of broader digital governance, at the same time raising challenges for legal clarity, consistency, and coordination across countries and regions.

2.3. Overview of national developments around the Privacy Guidelines' parts

17. This section will provide an examination of key developments in national policies against the parts of the Privacy Guidelines. This may include reforms, amendments, and case law or guidelines from across OECD Member countries. This examination will inform an assessment of dissemination and implementation efforts around core principles of the Privacy Guidelines at the international, national and sub-national level.

2.4. OECD work advancing the implementation of the Privacy Guidelines

18. Since the 2021 review of the Privacy Guidelines, the DPC and the DGP have increased the emphasis on the practical implementation and the “operationalisation” of trust among Member countries and beyond. The work has focused on ensuring that the Privacy Guidelines' core principles, such as accountability and individual participation, remain robust in the face of new developments, e.g. the complexities of AI and pervasive cross-border data flows.

19. This section will demonstrate how DPC and DGP work has expanded the Privacy Guidelines' concepts in the context of current policy challenges since the last review. For each workstream, it subsequently highlights how the DGP and DPC research and activities have informed the actions of Adherents and fed into work carried out by other key stakeholders.

20. The Privacy Guidelines have enabled the DPC and DGP to conduct such work by providing an anchoring framework. Relevant workstreams, and deliverables, informed by multistakeholder engagement, to be considered include:

- Operationalising consent in the digital ecosystem;
- Declaration on Government Access to Personal Data Held by Private Sector Entities [[OECD/LEGAL/0487](#)];
- Cross-border co-operation in privacy enforcement;
- Report on “Moving forward with DFFT”;
- Privacy enhancing technologies (PETs);
- Trusted data intermediaries;
- Privacy & AI;
- Privacy and cross-regulatory digital co-operation (including competition, health, life sciences, finance and payments);

2.5. Potential outcomes

21. In line with OECD practice, in addition to the submission of the report to the OECD Council and that report's publication, this report could also lead to proposing various potential follow-up actions, such as:

- further work to reinforce implementation and dissemination, with an indication of the specific actions envisaged (e.g. development of further implementation guidance or similar support tools) and who would be responsible for them (e.g. committee(s), Adherents, Secretariat);
- proposed revision of the Privacy Guidelines, with an indication of the areas concerned and a summary of the rationale for the possible changes.

22. The Secretariat's preliminary view is that the Privacy Guidelines remain relevant, with an open mind regarding the possibility of developing further work to support implementation and dissemination should target areas for such work be highlighted in the course of the report process.