OECD publishing

Please cite this paper as:

OECD (2011-10-31), "Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data", *OECD Digital Economy Papers*, No. 185, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5kg2b7l7pljk-en

OECD Digital Economy Papers No. 185

Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

OECD

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

31-Oct-2011

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2011)4/FINAL
Unclassified

Working Party on Information Security and Privacy

TERMS OF REFERENCE FOR THE REVIEW OF THE OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER DATA FLOWS OF PERSONAL DATA

JT03310307

English - Or. English

FOREWORD

The review of the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("privacy guidelines" or "guidelines") arises out of the *Seoul Declaration for the Future of the Internet Economy*, which was adopted by Ministers in June 2008. The Seoul Declaration calls for the OECD to assess the application of certain instruments, including the Privacy Guidelines, in light of "changing technologies, markets and user behaviour and the growing importance of digital identities"[1].

The review of the Guidelines is being conducted by the OECD Working Party on Information Security and Privacy (WPISP) and began with a questionnaire circulated to member governments and stakeholders from business, civil society and the Internet technical community. The responses received suggest that there is interest in continuing the work of the review by conducting a deeper examination of the OECD privacy framework, though the responses reflect a range of views as to areas of emphasis and approaches. Furthermore, the priority placed by OECD members on globally interoperable approaches to privacy at the June 2011 High Level Meeting on the Internet Economy, as expressed in the Communiqué on Principles for Internet Policy-making,[2] provides additional motivation and direction for work in the area.

The Terms of Reference are intended to memorialise the results of the review thus far, and provide orientation for further expert group discussions. They begin with some initial statements about the current context for privacy – largely derived from the report on "The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines," which has been declassified and is available on the OECD website.[3] The Terms of Reference articulate a shared view about current issues and approaches and provide the rationale for further work, concluding with a set of questions about the principles that would be used to guide the future work.

The title of the Terms of Reference highlights as the goal of this work to ensure the continued relevance of the OECD Privacy Framework. The Terms of Reference have been formulated in a way that avoids prejudging the ultimate outcomes of the review. The range of outcomes is wide, and could include, for example: a conclusion that the guidelines have stood the test of time and do not need modification; or that one or more aspects need revising; or updating the explanatory memorandum; or producing a new document or instrument – or some combination of these or other steps.

The document was prepared by the WPISP and declassified by the Committee for Information, Computer and Communications Policy through a written procedure concluded in October 2011.

This document is published under the responsibility of the Secretary-General of the OECD.

1 See, *//www.oecd.org/dataoecd/49/28/40839436.pdf.*

2 See, *://www.oecd.org/dataoecd/40/21/48289796.pdf*

3 See, *//dx.doi.org/10.1787/5kgf09z90c31-en*

TERMS OF REFERENCE FOR ENSURING THE CONTINUED RELEVANCE OF THE OECD FRAMEWORK FOR PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA: PRIVACY PROTECTION IN A DATA-DRIVEN WORLD

As an interim conclusion of the review of the 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD members have agreed on terms of reference to ensure the continued relevance of the OECD framework for privacy and transborder flows of personal data.[4] These terms of reference articulate a shared view about current issues and approaches and provide the rationale for further work as outlined in sections IV and V below.

I. The evolving privacy landscape

The OECD guidelines have proven remarkably influential in shaping privacy frameworks around the world. Yet, the three decades since the release of the OECD guidelines have brought significant changes to the environment in which the privacy principles must operate, both in terms of the benefits of responsible uses of personal data and the challenges of protecting privacy effectively. Changes in scale are illustrated by increases in:

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

[4] In addition to the 1980 Guidelines, the OECD Privacy Framework could be considered to include the Declaration on Transborder Data Flows (1985), Ottawa Declaration on Privacy Online (1998), Privacy Online: OECD Guidance on Policy and Practice (2002), and the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007).

II. Elaborating a vision for privacy for a data-driven economy

Privacy frameworks should be reviewed, developed and adapted to reflect the broader scale of today's uses of personal data with a view to more effectively protecting a fundamental value and to foster both individual trust and the economic and social benefits associated with responsible and innovative uses of personal data. Privacy frameworks 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.

Recognising that cross-border flows of personal information are now critical to national and global economic and social development, privacy protection regimes should support open, secure, reliable and efficient flows, taking into account an analysis of the privacy risks.

III. Creating an enabling environment for more effective approaches to privacy and trans-border data flows

In the current context, a number of elements can already be identified as key to improving the effectiveness of privacy protections. Efforts by all stakeholders, including individuals, governments, business, civil society, and the Internet technical community, are needed to foster approaches that:

- Recognise the need for globally interoperable privacy frameworks that ensure effective respect for globally recognised norms of privacy protection and support the free flow of personal information around the world
- Elevate the importance attached to the protection of privacy to the highest levels within governments, including through the development of national privacy strategies
- Redouble efforts to develop a globally active network of privacy enforcement authorities, empowered with resources, tools and mechanisms to work co-operatively across borders to protect personal data
- Increase the level of attention attached to the protection of privacy to the highest levels of organisations, particularly those making significant uses of personal data
- Create a culture of privacy among organisations and individuals that collect, store or use personal information, including through privacy literacy initiatives
- Cultivate a commitment by organisations to develop and implement privacy by design, through approaches that include privacy impact assessments, robust privacy management processes, and privacy-enhancing tools, particularly for high-risk uses of personal data
- Encourage organisations to design and implement easy-to-use privacy controls, informed by empirical research and supported as needed by openly developed global standards and practices
- Foster privacy regimes that support individual choice and control and encourage industry best practices
- Recognise the dynamic nature of innovative business models through privacy regimes characterised by technology-neutrality and context-sensitivity.

IV. Issues for further consideration

The current context also has implications for the effectiveness of privacy protection regimes which require further consideration. The OECD's Working Party on Information Security and Privacy (WPISP) will host multi-stakeholder expert discussions of the OECD framework in the current environment. As a starting point the discussion should build on the shared views stated above and consider questions including the following:

The roles and responsibilities of key actors

- Recognising the range of actors now capable of putting privacy at risk, should the scope of privacy regimes be accordingly expanded? Should different types of actors have different roles or responsibilities?

- What is the appropriate role of decision-making by individuals as a means to protect their privacy? Can the challenges for individuals in assessing information risks be addressed through greater transparency and clarity in notices from organisations? When is consent impractical? Is there a role for concepts like withdrawal of consent?

- In light of the economic and social benefits enabled by technological innovations, including in areas like data analytics, how should risks of unanticipated uses of personal data be addressed? Is there a role for concepts like the reasonable expectations of individuals, beneficial reuse, and data retention limitations?

Geographic restrictions on data flows

- What is the impact of geographic-based restrictions on flows of personal data? Is the analysis affected by developments related to web-based services, cloud computing, global standards, or the protection of personal data flows through binding and demonstrable organisational accountability? What types of approaches will contribute to the development of globally-scalable privacy rules and practices?

Proactive implementation and enforcement

- How can the challenges of securing personal data be better addressed? What incentives are needed to ensure a proactive approach to implementing policy, technical and organisational measures to address the security of personal data and other privacy-related risks? What is the role for concepts such as data minimisation, data stewardship, data portability, accountable information flow and data breach notification?

V. Modalities

The WPISP's multi-stakeholder discussions will include experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community. In addition, participation from representatives of several international organisations will be invited, reflecting the importance of improving global compatibility of privacy frameworks. The experts will work electronically and via teleconference, supplemented by occasional in-person meetings. To the extent possible the meetings would be held on the margins of already-planned events.

The purpose of these discussions is to explore and make recommendations to the OECD membership, based on the reflections outlined above, with a view to ensuring the continued relevance of the OECD framework for privacy and the transborder flows of personal data. The range of recommendations is wide, and could include, for example: a conclusion that the Guidelines have stood the test of time and do not need modification; or that one or more aspects need revising; or updating the Explanatory Memorandum; or producing a new document or instrument -- or some combination of these or other steps. The experts will be invited to provide preliminary recommendations to the WPISP within one year, with a possible extension for further work in particular areas if needed. The WPISP would then make a determination about how to act on the options presented by the group.