OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies 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, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the Secretary-General of the OECD.

© OECD 2007

No reproduction, copy, transmission or translation of this document may be made without written permission.
Applications should be sent to **rights@oecd.org**.

Foreword

This Recommendation was developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP). The work was led by Jennifer Stoddart, Privacy Commissioner of Canada, with the support of a number of representatives from privacy enforcement authorities participating as part of their country delegations. It has also benefited from a constructive consultation with other key stakeholders in the privacy and data protection community. It was adopted as a Recommendation of the OECD Council on 12 June 2007.

Preface

OECD work on privacy law enforcement co-operation was undertaken in the context of increasing concerns about the privacy risks associated with the changing character and growing volume of cross-border data flows. Globalisation, the emergence of "follow the sun" business models, the growth of the Internet and falling communication costs dramatically increase the amount of personal information flowing across borders. This increase in transborder information flows benefits both organisations and individuals by lowering costs, increasing efficiency and improving customer convenience. At the same time, these personal information flows elevate concerns about privacy, and present new challenges with respect to protecting individuals' personal information.

When personal information moves across borders it may put at increased risk the ability of individuals to exercise privacy rights to protect themselves from the unlawful use or disclosure of that information. At the same time, the authorities charged with enforcing privacy laws may find that they are unable to pursue complaints or conduct investigations relating to the activities of organisations outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. In this context, a consensus has emerged on the need to promote closer co-operation among privacy law enforcement authorities to help them exchange information and carry out investigations with their foreign counterparts.

The importance of cooperation in the enforcement of laws protecting privacy is recognised not just within the OECD, but also in other forums, including the International Conference of Data Protection and Privacy Commissioners, Council of Europe, Asia Pacific Economic Cooperation, and the European Union and its Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Article 29 Working Party). Indeed, there are an increasing number of regional instruments and other less formal arrangements to facilitate cross-border co-operation. As none of the existing arrangements has global reach, however, OECD Member countries have committed to developing a new instrument to help fill the gap in a forward-looking way.

In fact, the need for improved law enforcement co-operation has been a recurring theme in OECD privacy work, dating back to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines"), reiterated in the 1998 Ottawa Ministerial Declaration, and more recently highlighted in the 2003 report "Privacy Online: Policy and Practical Guidance." Though the Privacy Guidelines serve as the starting place for the current initiative, the landscape has changed.

When the Privacy Guidelines were adopted, only about one-third of Member countries had privacy legislation. Today, nearly all OECD Member countries have laws protecting privacy and have established authorities with enforcement responsibilities. This can be seen as a clear recognition that protecting the privacy and security of personal information is essential in democratic societies and promotes consumer confidence in both domestic and global markets. While looking ahead to address the privacy challenges

© OECD 2007

inherent in a global economy dependant on the free flow of information, the current initiative is firmly rooted in the privacy principles established some twenty-five years ago.

The approach reflected in the Recommendation is one which focuses on the common problems that need to be addressed rather than on the differences in laws or powers of enforcement authorities. Effective enforcement co-operation can be accomplished despite variations in domestic approaches. Although making that co-operation a reality will not happen overnight, a long term commitment to implementing the principles articulated in the Recommendation will help ensure that privacy enforcement authorities can do their part in safeguarding the personal information of individuals no matter where it is located.

© OECD 2007

RECOMMENDATION OF THE COUNCIL ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY

THE COUNCIL,

Having regard to articles 1, 3, and 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960;

Having regard to the *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* [C(80)58/FINAL], which recognises that Member countries have a common interest in protecting individuals' privacy without unduly impeding transborder data flows, and states that Member countries should establish procedures to facilitate "mutual assistance in the procedural and investigative matters involved";

Having regard to the *Declaration on the Protection of Privacy on Global Networks* [C(98)177, Annex 1], which recognises that different effective approaches to privacy protection can work together to achieve effective privacy protection on global networks and states that Member countries will take steps to "ensure that effective enforcement mechanisms" are available both to address non-compliance with privacy principles and to ensure access to redress;

Having regard to the Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders [C(2003)116)] and the Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws against Spam [C(2006)57], which set forth principles for international law enforcement co-operation in combating cross-border fraud and deception and illegal spam, respectively, and which illustrate how cross-border co-operation among Member countries can be improved;

Recognising the benefits in terms of business efficiency and user convenience that the increase in transborder flows of data has brought to organisations and individuals;

Recognising that the increase in these flows, which include personal data, has also raised new challenges and concerns with respect to the protection of privacy;

Recognising that, while there are differences in their laws and enforcement mechanisms, Member countries share an interest in fostering closer international co-operation among their privacy law enforcement authorities as a means of better safeguarding personal data and minimising disruptions to transborder data flows;

Recognising that, although there are regional instruments and other arrangements under which such co-operation will continue to take place, a more global and comprehensive approach to this co-operation is desirable;

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

© OECD 2007

RECOMMENDS:

That Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:

a) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.

b) Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.

c) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.

d) Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

That Member countries implement this Recommendation, as set forth in greater detail in the Annex, of which it forms an integral part.

INVITES non-Member economies to take account of the Recommendation and collaborate with Member countries in its implementation.

INSTRUCTS the Committee for Information, Computer and Communications Policy to exchange information on progress and experiences with respect to the implementation of this Recommendation, review that information, and report to the Council within three years of its adoption and thereafter as appropriate.

© OECD 2007

ANNEX

I. Definitions

1. For the purposes of this Recommendation:

   a) "Laws Protecting Privacy" means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines.

   b) "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.

II. Objectives and scope

2. This Recommendation is intended to foster international co-operation among Privacy Enforcement Authorities to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located. It reflects a commitment by Member countries to improve their enforcement systems and laws where needed to increase their effectiveness in protecting privacy.

3. The main focus of this Recommendation is the authority and enforcement activity of Privacy Enforcement Authorities. However, it is recognised that other entities, such as criminal law enforcement authorities, privacy officers in public and private organisations and private sector oversight groups, also play an important role in the effective protection of privacy across borders, and appropriate co-operation with these entities is encouraged.

4. Given that cross-border co-operation can be complex and resource-intensive, this Recommendation is focused on co-operation with respect to those violations of Laws Protecting Privacy that are most serious in nature. Important factors to consider include the nature of the violation, the magnitude of the harms or risks as well as the number of individuals affected.

5. Although this Recommendation is primarily aimed at facilitating co-operation in the enforcement of Laws Protecting Privacy governing the private sector, Member countries may also wish to co-operate on matters involving the processing of personal data in the public sector.

6. This Recommendation is not intended to interfere with governmental activities relating to national sovereignty, national security, and public policy ("ordre public").

III. Domestic measures to enable co-operation

7. In order to improve cross-border co-operation in the enforcement of Laws Protecting Privacy, Member countries should work to develop and maintain effective domestic measures that enable Privacy Enforcement Authorities to co-operate effectively both with foreign and other domestic Privacy Enforcement Authorities.

© OECD 2007

8. Member countries should review as needed, and where appropriate adjust, their domestic frameworks to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Protecting Privacy.

9. Member countries should consider ways to improve remedies, including redress where appropriate, available to individuals who suffer harm from actions that violate Laws Protecting Privacy wherever they may be located.

10. Member countries should consider how, in cases of mutual concern, their own Privacy Enforcement Authorities might use evidence, judgments, and enforceable orders obtained by a Privacy Enforcement Authority in another country to improve their ability to address the same or related conduct in their own countries.

A. Providing effective powers and authority

11. Member countries should take steps to ensure that Privacy Enforcement Authorities have the necessary authority to prevent and act in a timely manner against violations of Laws Protecting Privacy that are committed from their territory or cause effects in their territory. In particular, such authority should include effective measures 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;

    c) Permit corrective action to be taken against data controllers engaged in violations of Laws Protecting Privacy.

B. Improving the ability to co-operate

12. Member countries should take steps to improve the ability of their Privacy Enforcement Authorities to co-operate, upon request and subject to appropriate safeguards, with foreign Privacy Enforcement Authorities, including by:

    a) Providing their Privacy Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to possible violations of Laws Protecting Privacy;

    b) Enabling their Privacy Enforcement Authorities to provide assistance to foreign authorities relating to possible violations of their Laws Protecting Privacy, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved or things.

IV. International co-operation

13. Member countries and their Privacy Enforcement Authorities should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy. Such co-operation may be facilitated by appropriate bilateral or multilateral enforcement arrangements.

© OECD 2007

A. Mutual assistance

14. Privacy Enforcement Authorities requesting assistance from Privacy Enforcement Authorities in other Member countries in procedural, investigative and other matters involved in the enforcement of Laws Protecting Privacy across borders should take the following into account:

a) Requests for assistance should include sufficient information for the requested Privacy Enforcement Authority to take action. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request.

b) Requests for assistance should specify the purpose for which the information requested will be used.

c) Prior to requesting assistance, a Privacy Enforcement Authority should perform a preliminary inquiry to ensure that the request is consistent with the scope of this Recommendation and does not impose an excessive burden on the requested Privacy Enforcement Authority.

15. The requested Privacy Enforcement Authority may exercise its discretion to decline the request for assistance, or limit or condition its co-operation, in particular where it is outside the scope of this Recommendation, or more generally where it would be inconsistent with domestic laws, or important interests or priorities. The reasons for declining or limiting assistance should be communicated to the requesting authority.

16. Privacy Enforcement Authorities requesting and receiving assistance on enforcement matters should communicate with each other about matters that may assist ongoing investigations.

17. Privacy Enforcement Authorities should, as appropriate, refer complaints or provide notice of possible violations of the Laws Protecting Privacy of other Member countries to the relevant Privacy Enforcement Authority.

18. In providing mutual assistance, Privacy Enforcement Authorities should:

a) Refrain from using non-public information obtained from another Privacy Enforcement Authority for purposes other than those specified in the request for assistance;

b) Take appropriate steps to maintain the confidentiality of non-public information exchanged and respect any safeguards requested by the Privacy Enforcement Authority that provided the information;

c) Co-ordinate their investigations and enforcement activity with that of Privacy Enforcement Authorities in other member countries to promote more effective enforcement and avoid interference with ongoing investigations;

d) Use their best efforts to resolve any disagreements related to co-operation that may arise.

© OECD 2007

B. Engaging in collective initiatives to support mutual assistance

19. Member countries should designate a national contact point for co-operation and mutual assistance under this Recommendation and provide this information to the OECD Secretary-General. The designation of the contact point is intended to complement rather than replace other channels for co-operation. Updated information regarding Laws Protecting Privacy should also be provided to the OECD Secretary-General, who will maintain a record of information about the laws and contact points for the benefit of all Member countries.

20. Privacy Enforcement Authorities should share information on enforcement outcomes to improve their collective understanding of how privacy law enforcement is conducted.

21. Member countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.

C. Co-operating with other authorities and stakeholders

22. Member countries should encourage Privacy Enforcement Authorities to consult with:

a) Criminal law enforcement authorities to identify how best to co-operate in relation to privacy matters of a criminal nature for the purpose of protecting privacy across borders most effectively;

b) Privacy officers in public and private organisations and private sector oversight groups on how they could help resolve privacy-related complaints at an early stage with maximum ease and effectiveness;

c) Civil society and business on their respective roles in facilitating cross-border enforcement of Laws Protecting Privacy, and in particular in helping raise awareness among individuals on how to submit complaints and obtain remedies, with special attention to the cross-border context.

© OECD 2007