Declaration on Government Access to Personal Data Held by Private Sector Entities

OECD Legal Instruments

OECD

BETTER POLICIES FOR BETTER LIVES

Please cite this document as:
OECD, *Declaration on Government Access to Personal Data Held by Private Sector Entities*, OECD/LEGAL/0487

Series: OECD Legal Instruments

Photo credit: © SOMKID THONGDEE/Shutterstock

Background Information

The Declaration on Government Access to Personal Data Held by Private Sector Entities was adopted by Ministers and high-level representatives of OECD Members and the European Union on 14 December 2022, on the occasion of the Ministerial meeting of the Committee on Digital Economy Policy (CDEP) held in the island of Gran Canaria, Spain.

As the first intergovernmental agreement on common approaches to safeguard privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes, it seeks to promote trust in cross-border data flows, a critical enabler of the global economy.

OECD work on cross-border data flows

The review of the implementation of the 1980 Recommendation concerning OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188], completed in 2021, identified policy gaps affecting the cross-border flow of personal data, which are essential for business transactions and operations as well as for social interactions online. A critical gap identified was the lack of a common articulation at the international level of the safeguards that countries put in place to protect privacy and other human rights and freedoms when they access personal data held by private entities in the course of fulfilling their sovereign responsibilities related to national security and law enforcement.

The importance of such an articulation is two-fold: i) increase trust among rule-of-law democratic systems that, while not identical, share significant commonalities in order to support cross-border flows of personal data between them; ii) and provide a standard for how democratic, rule-of-law based systems limit and constrain government power in contrast with approaches that are unconstrained, unreasonable, arbitrary or disproportionate, in violation of human rights and in breach of international obligations.

Process for developing the Declaration

The CDEP began work on this topic in February 2021 following discussions at its November 2020 meeting and building on prior work and discussions of the Working Party on Data Governance and Privacy (WPDGP) in the context of the Report on implementation, dissemination and continued relevance of the Privacy Guidelines [C(2021)42].

To this end, an informal drafting group of experts, ultimately consisting of experts from 33 OECD Members and the European Union, was convened. The drafting group met 18 times in 2021-2022. Drawing on these sessions, expert and stakeholder input and two fact-finding surveys, the OECD identified seven common principles that reflect OECD Members' existing laws and practices, and are at the heart of this Declaration.

Scope of the Declaration

The Declaration consists of three main sections:

1. "Legitimate government access on the basis of common values," recognising the important role data transfers play in the global economy and recalling the rationale for government access to personal data, the importance of safeguards to protect privacy and other human rights and freedoms, and the existence of commonalities between OECD Members in this regard;

2."Promoting trust in cross-border data flows," reaffirming countries' commitment to data free flow with trust, considering the principles in section three of the Declaration as an expression of their democratic values, and recognising their effective implementation by a destination country as a positive contribution towards facilitating cross-border data flows;

3.“Principles for government access to personal data held by private sector entities,” listing seven principles which reflect commonalities across OECD Members based on their existing laws and practices, and complement each other in protecting privacy and other human rights and freedoms: legal basis; legitimate aims; approvals; data handling; transparency; oversight; redress. This section further includes definition and scope for the application of these principles.

For further information please consult the CDEP Ministerial meeting website: https://www.oecd-events.org/digital-ministerial/ or contact: digitaleconomypolicy@oecd.org.

WE THE MINISTERS AND REPRESENTATIVES OF 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, the United States, and the European Union, met in the Island of Gran Canaria in Spain, on 14-15 December 2022, under the leadership of Spain as Ministerial Chair and with Denmark, Japan, Türkiye, the United Kingdom and the United States as Vice-Chairs, for the meeting of the Committee on Digital Economy Policy (CDEP) at Ministerial level under the theme "driving long-term recovery and economic growth by building a trusted, sustainable, and inclusive digital future".

Legitimate government access on the basis of common values

WE RECALL our shared commitment to upholding democracy and the rule of law, protecting privacy and other human rights and freedoms, promoting data free flow with trust in the digital economy, and maintaining a global, open, accessible, interconnected, interoperable, reliable and secure Internet.

WE RECOGNISE that ongoing digital transformation is creating more data, including personal data, as digital technologies are used across all sectors of the global economy.

WE FURTHER RECOGNISE the central role of data in the functioning of our societies and economies, and that cross-border data flows underpin international trade and global commerce and economic co-operation and development; greatly contribute to innovation and research and development across sectors; and are necessary to conduct business and to advance economic and societal goals.

WE RECALL the 1980 Recommendation concerning OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, last revised in 2013 [OECD/LEGAL/0188] (hereafter, "OECD Privacy Guidelines"), which provides a basic common reference point for the protection of personal data, whether in the public or private sector, and promotes and facilitates the transborder flows of personal data while upholding democratic values, the rule of law and the protection of privacy and other human rights and freedoms.

WE RECOGNISE the sovereign duty and responsibility of every country to protect the safety of its population by preventing, detecting and confronting criminal activity and threats to public order and national security, in adherence to democratic values, the rule of law, and the protection of privacy and other human rights and freedoms.

WE ACKNOWLEDGE that government access to personal data held by private sector entities is recognised in our national legal frameworks as essential to meeting these sovereign duties and responsibilities, and that law enforcement and national security authorities are therefore vested with powers to lawfully access such data.

WE REJECT any approach to government access to personal data held by private sector entities that, regardless of the context, is inconsistent with democratic values and the rule of law, and is unconstrained, unreasonable, arbitrary or disproportionate. Such approaches violate privacy and other human rights and freedoms, breach international obligations, undermine trust and create a serious impediment to data flows to the detriment of the global economy. By contrast, our countries' approach to government access is in accordance with democratic values; safeguards for privacy and other human rights and freedoms; and the rule of law including an independent judiciary. These protections also contribute to promoting trust by private sector entities in meeting their responsibilities in this context.

WE EMPHASISE, taking into account the justified exceptions to the OECD Privacy Guidelines on grounds of law enforcement and national security, the importance of enhancing trust based on a common understanding of the protections that our countries apply when accessing personal data held by private sector entities in these circumstances.

WE RECOGNISE that our existing practices and safeguards, in this regard, while not identical to one another, are founded upon similar principles that reflect a shared commitment to protecting privacy and other human rights and freedoms.

WE NOTE stakeholders' calls for additional work and engagement to identify existing common safeguards in OECD Member countries to protect privacy and freedom of expression, and therefore promote trust, in the context of purchasing commercially available personal data, accessing publicly available personal data, and receiving voluntary disclosures of personal data by law enforcement and national security authorities.

WE REITERATE our ambition to build a shared understanding among like-minded democracies of protections for privacy and other human rights and freedoms in place for law enforcement and national security access to personal data held by private sector entities in order to better inform efforts to promote data free flow with trust.

Promoting trust in cross-border data flows

WE REAFFIRM our commitment to data free flow with trust as a means of providing confidence to individuals and businesses when transferring personal data internationally.

WE REGARD the below principles as an important expression of our shared democratic values and commitment to the rule of law, which distinguishes our countries from other countries whose law enforcement or national security access to personal data are inconsistent with democratic values and the rule of law, are unconstrained, unreasonable, arbitrary or disproportionate, or amount to violations of human rights.

WE RECOGNISE that where our legal frameworks require that transborder data flows are subject to safeguards, our countries take into account a destination country's effective implementation of the principles as a positive contribution towards facilitating transborder data flows in the application of those rules.

Principles for government access to personal data held by private sector entities

WE DECLARE the following shared principles as reflecting commonalities drawn from OECD Members' existing laws and practices. These principles:

- complement each other in protecting privacy and other human rights and freedoms;
- apply to government access to and processing of personal data in the possession or control of private sector entities when governments are pursuing law enforcement and national security purposes within their respective territories in accordance with their national legal framework, including situations where countries have the authority under their national legal framework to mandate that private sector entities provide data to the government when the private sector entity or data are not located within their territory (hereafter referred to as "government access");
- are interpreted subject to national legal frameworks and may be applied by countries in different manners, depending on the specific context and circumstances, such as the type of access sought;
- should be read in light of the following definitions:
    a) "Personal data" refers to any information relating to an identified or identifiable individual.
    b) "Legal framework" for government access to personal data refers to national laws, executive or judicial orders, administrative regulations, case law, and other legally binding instruments or requirements, including legal obligations arising from international and supranational law as applicable in the country.
    c) "Private sector entities" refers to individuals and any non-governmental for-profit and not-for-profit organisations.

These principles are:

I. Legal basis

Government access to personal data held by private sector entities is provided for and regulated by the country's legal framework, which is binding on government authorities and is adopted and implemented by democratically established institutions operating under the rule of law. The legal framework sets out purposes, conditions, limitations and safeguards concerning government access, so that individuals have sufficient guarantees against the risk of misuse and abuse.

II. Legitimate aims

Government access supports the pursuit of specified and legitimate aims. Governments seek access only for such aims, in conformity with the rule of law. Government access is carried out in a manner that is not excessive in relation to the legitimate aims and in accordance with legal standards of necessity, proportionality, reasonableness and other standards that protect against the risk of misuse and abuse, as set out in and interpreted within the country's legal framework.

Governments do not seek access to personal data for the purpose of suppressing or burdening criticism or dissent; or disadvantaging persons or groups solely on the basis of characteristics including, but not limited to: age, mental or physical disability, ethnicity, indigenous status, gender identity or expression, sexual orientation, or political or religious affiliation.

III. Approvals

Prior approval ("approval") requirements for government access are established in the legal framework to ensure that access is conducted in accordance with applicable standards, rules and processes. They are commensurate with the degree of interference with privacy and other human rights and freedoms that will occur as a result of government access. Such requirements specify the criteria for seeking and granting approval, the procedure to be followed, and the entity providing the approval.

Stricter approval requirements are in place for cases of more serious interference, and may include seeking approval from judicial or impartial non-judicial authorities. Emergency exceptions to approval requirements are provided for in the legal framework, and are clearly defined, including justifications, conditions, and duration.

Decisions on approvals are appropriately documented. They are made objectively, on a factual basis in pursuit of a specified and legitimate aim and upon satisfaction that the approval requirements are met.

In situations where approval is not required, other safeguards established in the legal framework apply to protect against misuse and abuse, including clear rules that impose conditions or limitations on the access, as well as effective oversight.

IV. Data handling

Personal data acquired through government access can be processed and handled only by authorised personnel. Such processing and handling is subject to requirements provided for in the legal framework that include putting in place physical, technical and administrative measures to maintain privacy, security, confidentiality, and integrity. They also include mechanisms to ensure that personal data are processed lawfully, are retained only for as long as authorised in the legal framework in view of the purpose and taking into account the sensitivity of the data, and are kept accurate and up to date to the extent appropriate having regard to the context.

Internal controls are put in place to detect, prevent and remedy data loss or unauthorised or accidental data access, destruction, use, modification, or disclosure, and to report such instances to oversight bodies.

V. Transparency

The general legal framework for government access is clear and easily accessible to the public so that individuals are able to consider the potential impact of government access on their privacy and other human rights and freedoms.

Mechanisms exist for providing transparency about government access to personal data that balance the interest of individuals and the public to be informed with the need to prevent the disclosure of information that would harm national security or law enforcement activities.

These mechanisms include public reporting by oversight bodies on government compliance with legal requirements as well as procedures for requesting access to government records. Other measures include, for instance, regular reporting by governments and, where applicable, individual notification.

Private sector entities are allowed to issue aggregate statistical reports regarding government access requests in conformity with the legal framework.

VI. Oversight

Mechanisms exist for effective and impartial oversight to ensure that government access complies with the legal framework.

Oversight is provided through bodies including internal compliance offices, courts, parliamentary or legislative committees and independent administrative authorities.

Countries' oversight systems are comprised of such bodies acting according to their individual mandates and that have powers that include the ability to obtain and review relevant information, conduct investigations or inquiries, execute audits, engage with government entities on compliance and mitigation, and address non-compliance. In addition, such bodies receive and respond to reports of non-compliance to ensure that government entities are accountable, and may also exercise redress functions in response to individuals' complaints.

In the exercise of their functions, oversight bodies are protected from interference and have the financial, human and technical resources to effectively carry out their mandate. They document their findings, produce reports, and make recommendations, which are made publicly available to the greatest extent possible.

VII. Redress

The legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework.

Such redress mechanisms take into account the need to preserve confidentiality of national security and law enforcement activities. This may include limitations on the ability to inform individuals whether their data were accessed or whether a violation occurred.

Available remedies include, subject to applicable conditions, terminating access, deleting improperly accessed or retained data, restoring the integrity of data and the cessation of unlawful processing. They may also include, depending on the circumstances, compensation for damages suffered by an individual.

WE WELCOME the work of the OECD on data free flow with trust and **WE CALL** on the Organisation to support countries in their promotion of this Declaration.

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, around 460 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** 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.

- **Arrangement, Understanding 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.