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

1. BACKGROUND

The 'Organisation for Economic Co-operation and Development' (OECD)[1] is an important global actor in setting standards in the field of data protection and privacy. An example of OECD's work is the OECD Privacy Guidelines; a set of recommendations adopted to address privacy concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. These recommendations, originally adopted in 1980 and amended in 2013, however allow for exceptions for national security and law enforcement purposes.

Figure 1 - OECD logo

Subsequently, the absence of **common principles on access of national security and law enforcement agencies to personal data** was criticised for its negative effects on cross-border data flows and, consequently, global digital economy.[2] The review of the implementation of OECD Privacy Guidelines, completed in 2021, identified a critical need for common pronounciation of safeguards that countries adopt to protect human rights and freedoms when they access personal data held by private entities for national security and law enforcement purposes.

On 14 December 2022, 38 Ministers and high-level representatives of the OECD Members and the EU adopted the Declaration on Government Access to Data held by private sector entities (the Declaration).[3] The Declaration proclaims to be "the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes".

> "Today's landmark agreement formally recognises that OECD countries uphold common standards and safeguards. It will help to enable flows of data between rule-of-law democracies, with the safeguards needed for individuals' trust in the digital economy and mutual trust among governments regarding the personal data of their citizens."[4]
> **Mathias Cormann, OECD Secretary-General**

The Declaration is not legally binding for those that adhere to it. However, it offers some level of clarity around the values shared by governments when accessing individual's data, trying to increase trust among them and create greater confidence for private entities on the protections that apply to affected individuals.

2. SCOPE

The Declaration has **three sections**. The first two "Legitimate government access on the basis of common values" and "Promoting trust in cross-border data flows" set the context for the central part, "Principles for government access to personal data held by private sector entities" (the Principles).

The Declaration does not create any new legal instruments or tools for government access to personal data. It constitutes a set of shared principles that governments and other policy makers should respect and, if needed, consider introducing in their domestic legal frameworks.

A- LEGAL REGIME COVERED

[1] OECD counts 38 Member countries. European Commission participates in the work of the OECD, in accordance with the Supplementary Protocol to the Convention on the Organisation for Economic Co-operation and Development.

[2] Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy - OECD

[3] The Declaration is also open to non-Member countries.

[4] OECD Digital Economy Ministerial Meeting (14 December 2022). Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access - OECD

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

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

The principles apply to access to and processing of personal data held by private sector entities when **governments** are pursuing **law enforcement and national security purposes** in accordance with their national legal frameworks.

B- DATA COVERED

The Declaration refers to **personal data** in the **possession or control of private sector entities**. Like in the OECD Privacy Guidelines, personal data in the Declaration comprises any information relating to an identified or identifiable individual.[5]

The scope of application of Declaration is wide, covering **all data categories** (subscriber information, traffic data and content data).

It also covers **data not located within the respective country** if the government has the authority to order the production of such data to the private sector entities under the national legal framework.[6]

C- ENTITIES COVERED

The Declaration uses the term "**private sector entities**" which includes individuals and any non-governmental organisations.

As regards its territorial application, the Declaration covers private sector entities, which fall, in accordance with their respective national legal frameworks, under the territorial jurisdiction of the countries that signed the Declaration. It therefore includes situations where domestic law empowers countries to order private sector entities that are not located within their territory to provide data to the government (for example, domestic legal measures adopted on the basis of Article 18(1)(b) of the Convention on Cybercrime or Article 6 and 7 of the Second Additional Protocol to the Convention on Cybercrime).

3. DEFINING THE TOOLBOX

The Declaration identifies **seven common principles** in the existing legal frameworks (applicable laws and practices) of the adhering countries:

- Legal basis
- Legitimate aims
- Approvals
- Data handling
- Transparency
- Oversight
- Redress

A- LEGAL BASIS

The first principle requires the **existence of legal basis** for government access.[7] It also sets out the qualities that the legal framework establishing and regulating such access must have.

In particular, the legal framework must be adopted and implemented by democratically established institutions, which operate under the rule of law. It must set out the following elements of the government access:

- Purposes
- Conditions
- Limitations
- Safeguards.

B- LEGITIMATE AIMS

Government access must pursue **specified and legitimate aims** (set out in the legal framework, see principle Legal basis).[8]

The following **legal standards** apply when access to personal data is sought:

[5] See also, the definition of personal data in Article 3(1) of the Law Enforcement Directive Article (Directive (EU) 2016/680) and Article 4(1) of the General Data Protection Regulation (Regulation (EU) 2016/679).

[6] For example, Article 18(1)(b) of the Convention on Cybercrime; Article 6 and Article 7 of the Second Additional Protocol to the Convention on Cybercrime.

[7] Compare and contrast, Article 4(1)(a) and Article 8 of the Law Enforcement Directive regarding the requirement of lawfulness of processing by the law enforcement authorities.

[8] Compare and contrast, Article 4(1)(b) and (c) of the Law Enforcement Directive.

- Necessity
- Proportionality
- Reasonableness
- Other standards protecting against the risk of misuse and abuse

Governments must not seek access for discriminatory purposes or for suppressing or burdening criticism or dissent.

C- APPROVALS

The country's legal framework must set out the requirements for the prior **approval of access**, including the criteria for the approval, the procedure to be followed and the approval decision. The latter must be objective, based on facts and pursue a specified and legitimate aim. The approval does not have to be issued by judicial authorities, but it can also be given by "impartial non-judicial authorities".[9]

Any **emergency exceptions** to the requirement of approval of access must also be clearly determined in the legal framework (e.g. justification, conditions, duration).

The legal framework can provide for other protections against misuse and abuse, such as conditions and limitations on the access and effective oversight, so approval is not always required.

D- DATA HANDLING

The data obtained by the government can be **handled only by authorised personnel**. In order to protect privacy, security, confidentiality and integrity of data, physical, technical and administrative measures, as well as internal controls must be put in place.[10]

E- TRANSPARENCY

Everyone must be able to discern the potential impact of government access on their rights from the **clear and publically accessible legal framework**.

Governments can also put in place various **transparency mechanisms** (e.g. public reports of oversight bodies) and allow private entities to report on government access requests (see, for example, Apple Transparency Report).[11]

F- OVERSIGHT

Effective and impartial oversight must ensure the government's compliance with the applicable legal framework. The oversight mechanisms that countries put in place to this end come in various forms, e.g. internal compliance offices, courts, parliamentary or legislative committees and independent administrative authorities.[12]

G- REDRESS

The legal framework provides individuals with **effective judicial and non-judicial redress** to identify and remedy violations of the national legal framework.[13]

Given the sensitivity of the issues and the need to preserve confidentiality of national security and law enforcement activities, limitations on notification of the affected individuals about the requested access or disclosure may be put in place.[14]

4. WAY FORWARD

Although the Declaration is not binding (it is part of the so-called "**soft law**"), its text and implementation could be considered in

[9] See, judgments of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 120. "[i]t is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime". See, judgment of 2 March 2021, *H.K. v. Prokuratuur*, C-746/18, ECLI:EU:C:2021:152, paragraphs 48-51.

[10] Compare and contrast, Article 4(1)(f), Article 19 and Article 29 of the Law Enforcement Directive.

[11] For example, Recital 26 of the Law Enforcement Directive; Article 15 of the Digital Services Act (Regulation (EU) 2022/2065).

[12] For example, Chapter VI of the Law Enforcement Directive.

[13] For example, Chapter VIII of the Law Enforcement Directive.

[14] For example, Article 14(12)(i) of the Second Additional Protocol to the Convention on Cybercrime.

preparations of domestic or international legal instruments in the field of national security and law enforcement access to protected data.

The recitals in the Declaration set the basis for further work by the OECD to identify existing common safeguards in OECD Member countries in the context of **access to publicly available personal data** (see Article 32 of the Convention on Cybercrime), and **voluntary disclosures** of personal data for law enforcement and national security authorities.