DJINGOV GOUGINSKI KYUTCHUKOV VELICHKOV

ATTORNEYS AND COUNSELLORS AT LAW

DJINGOV
GOUGINSKI
KYUTCHUKOV
VELICHKOV
ATTORNEYS AND COUNSELLORS AT LAW

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E:dgkv@dgkv.com
W: www.dgkv.com

Significance of December 2022 OECD Declaration on Government Access to Personal data held by Private Sector Entities

By:

Ralitsa Gougleva - Counsel and Head of Data Protection Practice

Anita Dangova - Associate

In the context of cross-border data flows and the ever-increasing need of organizations to transfer personal data in a digitalized world lawfully, we revisit the *Declaration on Government Access to Data held by private sector entities adopted on 14 December 2022 by Ministers and high-level representatives of OECD Members and the European Union* (the "**OECD Declaration**").

The OECD Declaration is **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. **The OECD Declaration seeks to promote trust in cross-border data flows seeing them as a major tool of doing business globally**. As set forth in the OECD Declaration, "a critical gap … [was] identified [regarding] … 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 goal of the OECD Member States is to narrow and, if possible, close this critical gap to enable long-term recovery and development of the global economy.

To this end, the OECD Declaration sets forth the following **7 principles for government access to personal data held by private sector entities**:

1. **Legal basis**: government access to personal data held by private sector entities is provided for and regulated by the country's legal framework adopted and implemented in accordance with the rule of law;
2. **Legitimate aim**: government access supports the pursuit of specified and legitimate aims and is carried out in accordance with legal standard of necessity, proportionality, and reasonableness;
3. **Approvals**: prior approval requirements for government access are established in the legal framework;
4. **Data handling**: personal data acquired through government access shall be processed and handled only by authorised personnel in compliance with the law and following effective technical and administrative measures to maintain privacy, security, confidentiality, and integrity; internal controls shall be put in place to detect, prevent, and remedy data breaches and to report such instances to oversight bodies;
5. **Transparency**: the general legal framework for government access is clear and easily accessible to the public so that individuals are able to consider the impact of relevant government access on their privacy and other human rights and freedoms; the private

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E:dgkv@dgkv.com
W: www.dgkv.com

section entities are allowed to issue aggregate statistical reports regarding government access requests in accordance with the legal framework;

6. **Oversight**: mechanisms exist for effective and impartial oversight to ensure that government access in lawful;
7. **Redress**: the legal framework provides individuals with effective judicial and non-judicial redress for violations of the national legal framework.

The OECD Declaration was adopted by 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, Turkey, the United Kingdom, the United States, and the European Union.

It is not a binding legal instrument. Nonetheless, it has **important practical implications for cross-border transfers of personal data**. It is indicative of trends and expected changes in personal data transfers. To name a few of these, the OECD Declaration evidences that:

- OECD Members States recognize the difficulties that European and European-related businesses face when they need to transfer personal data cross-border and they want to do it lawfully, as well as the limitations of the existing unsynchronized regulations on the matter worldwide;
- OECD Members States search for a new regulatory solution to the risks of misuse and abuse of individuals' personal data in the context of cross-border data transfers and they see it rather as one multilateral agreement among many states than as a collection of numerous bilateral agreements between states;
- In the meantime, businesses engaged in cross-border data transfers can reflect the OECD Declaration in their updated transfer impact assessments when assessing the laws of a third country to which they transfer personal data provided that such third country is a party to the OECD Declaration; and
- Building a trusted, sustainable, and inclusive digital future for organizations - business and non-for-profit – and for individuals becomes a priority question of global politics and policies.

All this gives good reason to organisations processing personal data to **keep an eye on the developments that would follow on the topic in this 2023** and the next 1-2 years.

QUESTIONS?

Ralitsa Gougleva

Counsel and Head of

Data Protection Practice

E:ralitsa.gougleva@dgkv.com

Anita Dangova

Associate

E:anita.dangova@dgkv.com

Sofia 10 Tsar Osvoboditel Blvd. I Sofia 1000 I Bulgaria

T: +359 2 932 1100 I F: +359 2 980 3586

Berlin Schlegelstrasse 29 I 10115 Berlin (Mitte) I Germany

T: +49 30 2758 1561 I F: +49 30 2758 1562

WEB | LINKEDIN | YOUTUBE