

**Unclassified****English - Or. English**

22 December 2020

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION  
COMMITTEE ON DIGITAL ECONOMY POLICY****Statement of the Committee on Digital Economy Policy**

This document sets out the text of the statement of the Committee on Digital Economy Policy (CDEP) on trusted government access to personal data held by the private sector, as approved by the CDEP by written procedure on 22 December 2020.

The Statement is also available online at: [www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm](http://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm)

**JT03469974**

## Statement by the CDEP

Digitalisation continues to transform economies and societies in the OECD and beyond, highlighting the increasing importance of data collection, access, sharing and use, while ensuring the necessary protection of individual rights. Data governance concerns all sectors of the economy, encompassing social, cultural, technical, and legal issues. Establishing trust and minimising disruptions in data flows is a fundamental factor in reaping the benefits of digitalisation. The 2020 OECD [Ministerial Council Statement](#) recognises the transformative potential of the digital economy by ensuring data free flow with trust, a dynamic further underscored by the role of data to the recovery from the COVID-19 crisis.

Data governance and privacy have long been a focus of the work of the Committee on Digital Economy Policy, most recently reflected in the establishment of a dedicated Working Party on Data Governance and Privacy (WPDGP) building on the OECD's historical leadership in these areas. In the context of the recent review of the implementation of the OECD's 1980 Privacy Guidelines, as revised in 2013 [[OECD/LEGAL/0188](#)], the WPDGP identified unconstrained and disproportionate government access to personal data held by the private sector as a crucial issue for data governance and the protection of individual rights and as a potential barrier to enabling the free flow of data with trust.

Given the globally interconnected nature of the digital economy, the Committee raised concerns about government practices that fail to preserve trust, namely through unconstrained, unreasonable, or disproportionate requirements by governments that compel access to personal data held by the private sector. The Committee also raised concerns that the absence of common principles for trusted government access to personal data may lead to undue restrictions on data flows resulting in detrimental economic impacts.

The Committee concluded that working toward trusted government access to personal data held by the private sector is an urgent priority requiring further international collaboration. The Committee noted the OECD's strength as a forum to foster discussion and collaboration among like-minded countries.

With this in mind and in line with its mandate and expertise, the Committee decided to conduct further work to deepen the understanding of approaches in OECD countries and to examine the possibility of developing, as a matter of priority, an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector. Such work would bring together and elaborate a set of common and coherent good practices and legal guarantees from across OECD countries for best reconciling law enforcement and national security needs for data with protection of individual rights. These may include safeguards relating to: the legal bases upon which governments may compel access to personal data; requirements that access meet legitimate aims and be carried out in a necessary and proportionate manner; transparency; approvals for and constraints placed on government access; limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards; independent oversight; and effective redress. Such safeguards and their application would facilitate the promotion and protection of data free flow with trust.

To this end, the Committee agreed to convene a drafting group comprised of nominated government representatives and experts, including from law enforcement and national

security agencies. The drafting group will start its work early in 2021 and develop a proposal for the Committee's consideration, with a view to its further elaboration, in consultation with other relevant OECD Committees, and transmission to the Council as soon as possible thereafter.