COLUMN:
DATA LOCALISATION REQUIREMENTS ACROSS COUNTRIES

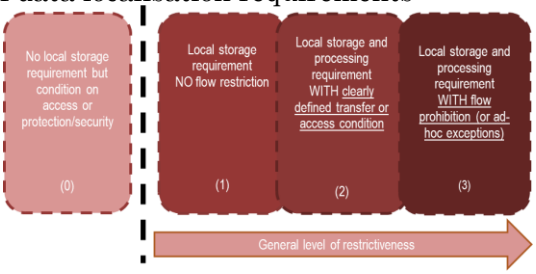
In recent years, rules and principles for the free flow of data across borders to promote global economic development are being established, through various EPAs/FTAs and international frameworks. On the other hand, there has been an increase in the number of countries introducing regulations requiring data to be stored within the borders (data localisation requirements) for reasons such as security and industrial policies. In order to provide an overview of such international trends, the OECD conducted a survey on data localisation requirements, as part of the "Osaka Track", a process launched at the G20 Osaka Summit in 2019 for the establishment of international rules on the flow of data and e-commerce, and published the results in a policy paper in 2022. In addition, the OECD conducted a survey to analyse the effects of such requirements on companies as well as economic impact therefrom, and published thein a policy paper in 2023. The 2023 G7 Trade Ministers' Statement welcomed the work being done by the OECD on data localisation requirements in light of the increase in the number of countries adopting such requirements worldwide, and stressed the importance of further discussions on this issue. This column reviews the findings of the OECD on these data localisation requirements.

1. CLASSIFICATION OF DATA LOCALISATION REQUIREMENTS

There is no consensus on what regulations should fall under category of data localisation requirements. EPAs/FTAs provide provisions banning data localisation requirements in a clause entitled "Location of Computing Facilities". Countries also adopt data localisation requirements for a range of purposes, specifically for: (1) protection of personal data and privacy; (2) regulatory purposes, such as audits, and facilitation of access to certain information; (3) national security, such as protection of or access to sensitive information on security; and (4) development of the digital industry. Understanding the purpose behind restriction on the flow of data across borders adopted by each countries is important for identifying unjustified restrictions to the free flow of data that are arbitrary and lack transparency.

The OECD has defined three categories to provide a full picture of the various data localisation requirements (see Figure 1.).

Figure 1. Categories of data localisation requirements



Source: OECD

Category 1 refers to measures that require local storage of data, without prohibiting storage or processing

in other countries. One example that belongs in this category is the Swedish Accounting Act 1999. The Act imposes an obligation to store and retain accounting information within Sweden for seven years. The U.K. Companies Act 2006 also requires that accounting information be kept at registered offices and made available for inspection by company officers at all times.

Category 2 refers to measures that require local storage and processing but allow international access or transfers on the basis of clearly defined conditions. Although there are few cases applicable to this category, for example, the Australian Personally Controlled Electronic Health Records Act 2012 requires health record information be stored in Australia but allows to such information to a foreign country in cases a subject of medical record information located in a foreign country or a specific healthcare provider needs to do so. In addition, the Personal Health Information and Access Act in New Brunswick, Canada, 2009 requires personal health information be stored within Canada, while enabling information to be transferred out of the country with the consent of the subject of the information or when it would be disclosed in accordance with the Act.

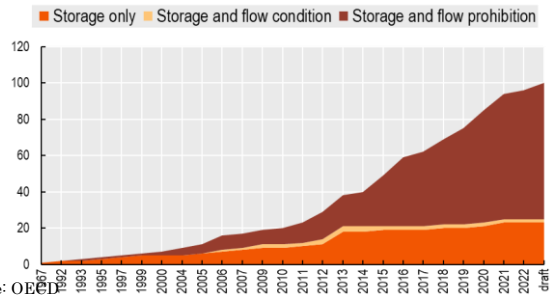
Category 3 refers to measures that mandate local storage and processing of data while also prohibiting transfers to other countries or only on the basis of ad-hoc authorizations. The regulations within the scope of this category can apply to data in a wide range of areas. In addition, the scope of application of these regulations is often less transparent and more ambiguous. For example, Indonesia's Regulation 71 concerning the Implementation of Electronic Systems and Transactions presumes that all data is managed, processed and stored in Indonesia. While exceptions to this rule arise in the event that storage technology is not available domestically, the criteria for the exceptions are determined by a government authority. China's Cybersecurity Law, which requires important data to be stored within the country, is unclear in its definition and ambiguous in its standards, potentially making it more restrictive than necessary for companies.

In addition to the above three categories, a new category of regulations that requires companies to guarantee access to data rather than storage is also emerging (Category 0). These regulations primarily target less sensitive data, such as non-personal data. For example, New Zealand's Goods and Services Tax Act 1985 requires tax-related information such as accounting information to be maintained for up to seven years, but does not specify the location therefor, while prescribing certain criteria regarding access.

2. TRENDS IN DATA LOCALISATION REQUIREMENTS

The number of countries adopting data localisation requirements is increasing, with 96 measures identified in 40 countries as of the first half of 2023. Moreover, not only is the number of cases increasing, but also more restrictive regulations are being adopted. By the first half of 2023, more than two thirds of the identified regulations adopt Category 3 regulations (see Figure 2. for details).

Figure 2. Countries adopting data localisation requirements are on the rise and restrictive regulations are increasing

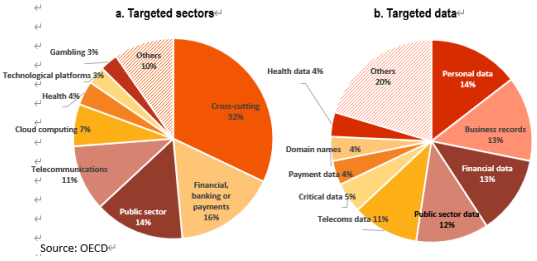


Source: OECD

An analysis of trends by industry shows that 32% of data localisation requirements are cross-cutting,

meaning that they have implications across all sectors of the economy.. The analysis by data types also revealed that personal data (14%), business records (13%), financial data (13%), public sector data (12%), and telecoms data (11%) were the top five data types affected by data localisation requirements (see Figure 3. for details).

Figure 3. Data localisation requirements affect various data types and a wide range of business sectors



Furthermore, the country-by-country analysis revealed clear differences between OECD and non-OECD member countries. For example, for data localisation requirements applied to cross-cutting and less sensitive data, OECD member countries require data to be stored domestically without restrictions on the cross-border flows of data, while non-OECD member countries mainly adopted Category 3 regulations.

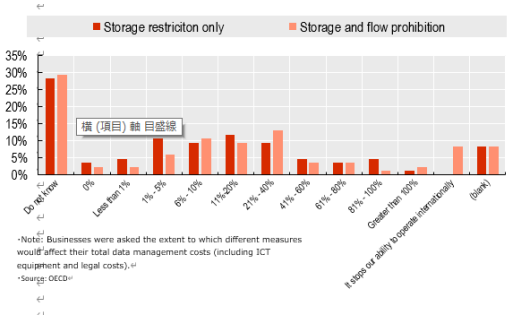
3. IMPACT ON BUSINESS ACTIVITIES

(1) RESULTS OF SURVEY

The OECD and the WTO conducted a business survey on the impact of Category 1 and Category 3 data localisation requirements on business activities between March and June 2022.

The results suggest that companies perceive that Category 1 regulations can lead to an average increase in data management costs of approximately 16%. In the case of Category 3, the impact is perceived to be even higher, increasing data management costs by approximately 55%. Importantly, 8% of respondents said that application of Category 3 regulations would stop their ability to operate internationally (see Figure 4. for details). In addition, when asked to what extent data localisation requirements contributed to achieving other legitimate public policy objectives, such as privacy protection and data security, 70% of respondents answered they did not think or were uncertain that there were any contributions.

Figure 4. Perceived impact of data localisation requirements on data management costs



(2) RESULTS OF TARGETED SURVEYS AND INTERVIEWS WITH BUSINESSES

In order to ascertain the impact on business activities of companies, the OECD conducted interviews with businesses in three sectors between February and April 2023. The results of the interviews are summarized

as follows.

◆Cross-border Electronic Payment Service Providers

This sector tends to be subject to Category 3 regulations in non-OECD member countries. This includes regulation in India requiring system operators to store all payment data domestically, as well as regulation in China requiring that copies of payment data to be stored in domestic servers for access by regulators. Companies expressed concern that the increased cost of operating their business due to data localisation requirements would reduce the efficiency of electronic payment systems and increase the risk of cyberattacks by reducing the security of services. It was also pointed out that these factors could impede the competitiveness of SMEs seeking to expand their business online. In addition, there were opinions that data localisation requirements could impede the detection and prevention of fraud through data analysis using cutting-edge AI technologies. Indeed, in 2023 the International Institute of Finance (IIF) found that the adoption of data localisation requirements combined with prohibitions to share this data could lead to a 50% loss in fraud modelling.

◆Cloud Computing Operators

Many data localisation requirements in this sector relate to public sector data and both OECD and non-OECD member countries tend to adopt Category 3 regulations. For example, India has introduced guidelines requiring cloud service providers to store and process public sector data domestically. Saudi Arabia also has a cybersecurity framework that obligates financial institutions to only use cloud services located in the country. The United States also has a strict data localisation policy for defence-related data requiring that cloud service providers that store government data must store them within the country. Türkiye has also introduced a circular requiring public sector data on the cloud to be stored within Türkiye. Cloud operators have expressed concern that this could reduce the ability of operators to take advantage of economies of scale in the location of servers, leading to growing operational costs, as well as hampering the mobility of "threat data" related to cyberattacks, which will increase cybersecurity risks.

◆Air Travel Companies

There are established practices for passenger data based on the Convention on International Civil Aviation (the Chicago Convention), and the benefits of these practices may be undermined if countries take their own measures. In addition, passenger data held by airlines are constantly updated in real time based on changed bookings and other passenger and airline activities, and it is essential that there is a single source of information and that the data can be shared across borders. In light of these factors, it is clear that any form of data localisation requirement that may impede the flow of passenger data can have a negative impact on the industry.

4. POLICY RECOMMENDATIONS FROM THE OECD

In light of the above findings, the OECD has proposed the following to ensure that measures are not trade restrictive and are based on legitimate public policy objectives.

- Continued monitoring of the evolving regulatory environment to stay on top of evolving trends and wider engagement in transparency exercises.
- Continued discussions around moving, in principle, towards less restrictive forms of data localisation where possible.
- Continued cooperation on these issues, in dialogue with regulators, trade policy makers and other relevant stakeholders, including from the private sector.
- Continued efforts to realise rules to address data localisation requirements through opportunities for discussion in the WTO Electronic Commerce negotiations and elsewhere.