

Brussels, 13.9.2017
SWD(2017) 305 final

COMMISSION STAFF WORKING DOCUMENT
EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF
THE COUNCIL**

on a framework for the free flow of non-personal data in the European Union

{COM(2017) 495 final}
{SWD(2017) 304 final}

Executive Summary Sheet
Impact assessment on the <i>Legislative proposal on a framework for the free flow of data in the EU.</i>
A. Need for action
Why? What is the problem being addressed?
In the European Union the possibility to build a data economy and to benefit from new technologies which rely on data is undermined by a series of barriers to data mobility, impacting businesses and their operations in the Single Market. In this context, obstacles to data mobility in the EU single market have been identified as the core problem. The underlying problem drivers are legislative and administrative localisation restrictions; data localisation driven by legal uncertainty and a lack of trust in the market; and vendor lock-in practices, which inhibit data mobility across data storage and/or further processing services providers and IT-systems.
What is this initiative expected to achieve?
The objective of the initiative is to achieve a more competitive and integrated EU market for data storage and/or processing services and activities. More specifically this means to reduce the number and range of data localisation restrictions, enhance legal certainty; facilitate cross-border availability of data for regulatory control purposes; improve the conditions under which users can switch data storage and/or processing service providers or port their data back to their own IT systems; enhance trust in and the security of cross-border data storage and/or processing.
What is the value added of action at the EU level?
Building a competitive European Data Economy means benefitting from economies of scale and data storage and processing on a cross-border basis in the EU. Action at Member State level could not achieve the legal certainty required for conducting this business across the EU, or remedy the lack of trust required for a thriving data storage and/or processing sector. EU intervention would also contribute to the development of secure data storage for the whole of the EU.
B. Solutions
What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?
<u>Option 0 – Baseline scenario.</u> This option would entail no EU policy change. <u>Option 1 – Non-legislative initiatives</u> This option would provide guidelines on a better enforcement of the existing EU instruments vis-à-vis unjustified data localisation restrictions imposed by Member States. Availability for regulatory control purposes should be facilitated in accordance with the Member States' existing rules. EU-level guidelines on best practices should enable easier switching of cloud service providers and porting data to another service provider or back to users' own IT systems. <u>Option 2 – Principles-based legislative initiative and cooperation framework.</u> This option would establish the principle of free flow of data within the EU prohibiting unjustified data localisation measures unless justified on national security grounds and requiring the notification of any new measure on data localisation. Companies which store and/or process their data in another Member State would need to provide data to a regulatory authority if requested in accordance with the law. The switching of cloud service provider and the porting of data to a new provider or back to users' own IT systems should be enabled and reliable common standards and/or certification schemes for the security of storage and/or processing of data should be promoted by dedicated provisions. Single points of contact designated by the Member States and a pan-European policy group comprised of such contact points should enable exchange and cooperation for the development of common approaches and best

practices and an effective implementation of the principles introduced.

A variant: - Sub-option 2a - instead of a legislative provision and co-regulation on data porting, this sub-option would foresee a self-regulatory approach to improve the conditions for data porting upon switching providers or porting data back to users' own IT systems, including the processes, timeframes and charging that may apply. On the intervention area of security of data storage and processing, the Sub-option would entail the clarification that any already applicable security requirements continue to apply to business users when they store or process their data in other Member States of the EU, also when this is subject to outsourcing to e.g. a cloud service provider.

Option 3 – Detailed legislative initiative. This option would establish fully harmonised rules on unjustified data location requirements (white or black lists). A mandatory cooperation framework would allow to enforce cross-border access to relevant data for regulatory authorities. Cloud service providers would be obliged to facilitate the porting of data and disclose with sufficient detail relevant processes, technical requirements and costs. Common standards and a separate European certification scheme for the security of data storage and/or processing for cloud services provided would be developed.

Who supports which option?

61.9% of respondents to the public consultation indicated that data localisation restrictions should be removed and 55.3% argued for a legislative approach in doing so. 16 Member States have explicitly called for a legislative approach in a letter addressed to President Tusk. Stakeholders seem therefore to prefer a legislative approach (Option 2 or 3) in addressing data localisation restrictions and availability for regulatory control to provide more clarity and certainty. However, evidence suggests that legislative action for security and switching and porting data should not be too detailed, as this could have counterproductive effects. Based on evidence-gathering EU businesses users of data storage and processing services prefer option 2 or 3, whereas Cloud service providers prefer option 2a. Member States' public authorities prefer option 2.

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise main ones)?

It would ensure the effective removal of existing unjustified localisation restrictions and the avoidance of future ones by establishing a clear legal principle in combination with a review procedure. As a result of awareness-raising on the legal principles established by the Regulation, it will also enhance legal certainty in the market. Moreover, by encouraging the development of codes of conduct for switching providers and porting data, it would lead to a more competitive internal market for cloud service providers.

What are the costs of the preferred option (if any, otherwise main ones)?

Data storage and processing service providers are most impacted by the initiative in terms of financial costs, albeit still at a moderate level. Compliance costs could arise from legal analysis, the development of new model clauses for contracts for switching of (cloud) data storage and processing service providers, the development of codes of conduct, standard setting, etc. Additional costs would be those for migrating data of ex-customers to a new location and a loss of market share to other/new cloud service providers.

How will businesses, SMEs and micro-enterprises be affected?

Start-ups and SMEs are strongly in favour of legislative action on free flow of data to improve legal certainty and switching, as this will directly cut costs for them and therefore lead to a more competitive market position. Specific costs that could be avoided are costs for duplication of IT-infrastructure, e.g. when an SME is active in multiple Member States and in one or more of those countries data localisation restrictions apply.

Will there be significant impacts on national budgets and administrations?
A moderate administrative burden for Member States' public authorities will emerge, caused by the allocation of human resources for structured cooperation between Member States in the 'single points of contact, and for complying with the notification and review process of the transparency mechanism, as provided for the Single Market Transparency Directive. In total, this could lead to an average annual cost of EUR 34.539 per Member State.
Will there be other significant impacts?
Yes, there will be broad positive impacts on economic development, through the enhancement of the European Data Economy and the creation of a more competitive market for data storage and processing services. This could, for example, lead to cost reductions for business users. The initiative would lead to the reduction of existing costs for business users. These cost reductions can be cost reductions for businesses making use of data storage and processing services and for businesses operating across borders, or intending to do this in the future, and lower costs for launching new products or services.
D. Follow up
When will the policy be reviewed?
A comprehensive evaluation could take place 5 years after the start of application of the rules. This evaluation will be executed in close cooperation with and relying on the information provided by the single points of contact of the Member States.