volciuc · ionescu

Briefing

6 March 2019

Impact of the upcoming application of the EU Regulation on the free flow of non-personal data

EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union (the "**Non-personal Data Regulation**") will become directly applicable in the EU Member States as of May 2019. The main purpose of the Non-personal Data Regulation is to allow mobility of non-personal data across borders and ensure the freedom to provide data processing services within the EU, which are sometimes prevented by certain national legal requirements to locate data in a specific territory.

This will encourage competition and quality of services for companies looking, for example, to outsource their data storage and processing activities to a service provider located in another Member State.

Scope of the Non-personal Data Regulation

The Non-personal Data Regulation applies to processing of non-personal data, which is any data that does not qualify as personal data under the General Data Protection Regulation 2016/679. By "processing" the Non-personal Data Regulation means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Free movement of data within the EU

The Non-personal Data Regulation establishes the free movement of data within the EU and provides that data localisation requirements (representing any obligation, prohibition, condition or other requirement provided for by a Member State which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State ("**Data Localisation Requirements**")) are prohibited. For example, in Romania, if the titleholder of a petroleum concession is a foreign company, the petroleum data must be kept in the archive of its subsidiary or branch located in Romania - the titleholder has the right to transfer copies of petroleum data in view of performing contractual obligations, to its headquarters, its operator or subcontractors located abroad, with the approval of the National Agency for Mineral Resources.

By exception, Data Localisation Requirements are allowed to be imposed by a Member State if they are justified on grounds of public security in compliance with the principle of proportionality ("**Public Security Exception**").

By 30 May 2021, Member States must review the existing laws or general administrative provisions laying down Data Localization Requirements and either eliminate them or keep them based on Public Security Exception and communicate them to the European Commission together with justification for maintaining it in force. The Commission will examine the compliance with the Public Security Exception and, if necessary, make recommendations to the Member State to amend or repeal that Data Localization Requirement.

Unclear meaning of the Public Security Exception

The Non-Personal Data Regulation does not provide a definition or criteria for the concept of "public security" - it only mentions in its recitals that the concept of "public security" within the meaning of Art 52 TFEU and as interpreted by the European Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety in order to facilitate the investigation, detection and prosecution of criminal offences. Exceptions based on "public security" require the existence of a sufficiently serious threat affecting one of the fundamental interests of society, such as public services, survival of the population, the risk of serious disturbance to foreign relations, or a risk to military interests. For example, "public security" would cover state records classified information, such as military and defence, state of emergency plans.

Data Localisation Requirements based on the Public Security Exception must comply also with the principle of proportionality, which, by today's standards as set out by the European Court of Justice, means that the measure: (i) is suitable to promote the objective of public security; (ii) is adequate in a sense that there is no other measure less restrictive from the point of view of free movement that is capable of achieving the same objective; and (iii) the positive effect of this measure on public security has to be balanced with the negative effect on the international market.

Data availability for competent authorities

Free flow of Non-personal Data Regulation will not affect the powers of competent authorities to request or obtain data or information performing their official duties in accordance with the national or the EU law. As such, the Non-personal Data Regulation provides that access to data by competent authorities may not be refused by data owners or processors on the basis that the data are processed in another Member State, and allows Member States to impose effective, proportionate and dissuasive penalties for failure to comply with this obligation to provide data.

Next steps

The Commission will publish informative guidance on the interaction of the Non-personal Data Regulation with the General Data Protection Regulation 2016/679, especially as regards data sets composed of both personal and non-personal data.

At national level, it is expected that each Member State will carry out a revision process of all its Data Localisation Requirements and will adopt necessary legal provisions to implement and comply with the Non-personal Data Regulation - so far, no such measures have been taken or announced in Romania.