i. What is the aim of the Regulation on non-personal data?

The digitization of our economy is accelerating. Electronic data is at the center of all modern innovative economic systems and can generate great value when analysed or combined with services and products (Internet of Things, artificial intelligence and machine learning, etc.).

The effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, two types of obstacles to data mobility hamper the effective and efficient functioning of data processing and the development of the data economy in general: (i) data localization requirements imposed by Member States; and (ii) contractual vendor lock-in practices in the private sector, i.e. situations where customers are dependent on a single (cloud) provider technology and cannot easily switch to a different vendor without substantial costs, legal constraints or technical incompatibilities.

The aim of the new regulation is to lift these main obstacles and to boost the data economy through facilitating cross-border exchange of data by enabling companies to store non-personal information anywhere in the EU. However, this will not impede the competent authorities from accessing data on the basis that the data is processed in another Member State, i.e. the Regulation does not affect the powers of competent authorities to request or obtain access to data in accordance with Union or national law, and they cannot be refused access to data on the basis that the data is processed in another Member State.

ii. What is non-personal data?

Non-personal data in the framework of the Regulation is electronic information that cannot be traced back to an identified or identifiable natural person (or has been anonymized as such). Specific examples of non-personal data include aggregate and anonymized datasets used for big data analytics, data on precision farming that can help to monitor and optimize the use of pesticides and water or data on maintenance needs for industrial machines.

iii. Facilitating cross border data storage

One of the main issues tackled by the Regulation are 'data localisation requirements', i.e. the obligations imposed by Member States for companies to host data centers in the national territory of a Member State and/or the obligation to process data domestically. These data localisation requirements are stifling the development of the EU Digital Single Market since they (i) obstruct the emergence of data innovation ecosystems across European borders; (ii) require
European companies to copy their IT infrastructure in several Member States; (iii) increase the cost for data storage (providers) and (iv) decrease potential European wide competition.

Consequently, legislation harmonizing and abolishing these data localisation requirements across Europe was a coveted innovation, which the new Regulation now delivers by banning Member States to impose any requirements to either localize or process data domestically and allowing for the emergence of more efficient and centralized data storage systems (e.g. cloud services, which provide a centralized storage space for large datasets).

**iv. Self-regulation of companies against vendor lock-in**

A second deficiency that is tackled by the Regulation is the vendor lock-in, i.e. service providers making it more difficult for users to switch to other service providers and leading to a lack of competition between cloud service providers in the European Union and a lack of data mobility.

The Regulation now facilitates and encourages EU companies to develop self-regulatory codes of conduct in order to improve the competitive data economy based on the principles of transparency, interoperability and open standards.

It is important to note that the Regulation is not imposing an additional regulatory obligation as such, but rather chooses the path of self-regulation. Companies that provide data processing services (such as cloud storage providers), however, should be aware that some self-regulatory codes of conduct may have to be introduced to ensure the provision of clear and transparent information and thereby avoiding vendor lock-in.

In practice, the Regulation enables data storage users to transfer their data from one provider to another or back to their on-premise systems in a way that is easy, clear and transparent, by way of codes of conduct. These should be comprehensive and should cover at least the key aspects that are important during the process of transferring data, i.e. (i) the processes used for, and the location of, data back-ups, (ii) the available data formats and support, (iii) the time required prior to initiate the porting process and the time during which the data will remain available for porting, etc.

**v. How does the Regulation interact with the GDPR: ‘mixed datasets’?**

In the case of a data set composed of both personal and non-personal data, the Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, the GDPR will have preference and will have to be applied to the entire data set.

**vi. Any compliance issues?**

Where the Regulation does not pose any immediate compliance risk for companies, it demonstrates the importance of delineating personal from non-personal data (even when the personal data might seem insignificant).

A thorough analysis of the data flows remains necessary, especially for companies using data analytics in their business models (Internet of Things, artificial intelligence and machine learning, etc.).