EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 20/2023, 4 May 2023
Tags: Data Act, GDPR, International Data Transfer, Personal Data, Non-Personal Data
Topics: Data Protection and Digital Governance

The Data Act: a (slippery) third way beyond personal/non-personal data dualism?

By Barbara Da Rosa Lazarotto and Prof. Dr. Gianclaudio Malgieri

In the age of highly intensive data processing, personal and non-personal data are increasingly inextricable in datasets. Impressive computational capabilities are making it possible to identify data subjects even in datasets that – until recently – we would have considered "anonymous". However, the need to guarantee digital users' protection goes beyond the mere issue of identification, considering that many risks to fundamental rights online can occur even without any personal data processing. At the same time, intensive data processing is becoming essential in any critical or fundamental infrastructure of our society.

The EU institutions have acknowledged this reality and are trying to avoid the rigid dualism between the regulation of personal and non-personal data. Two clear examples are the Data Governance Act from 2022 and the proposed Data Act. Both embody a new generation of "data laws" that overcome the rigid dualism between personal and non-personal data, created by the GDPR (and related laws, such as the Law Enforcement Directive and the Digital Markets Act) and the regulation of non-personal data. However, as we explain below, this shift from dualism to a singular legal concept of "data" is often problematic, primarily due to two reasons: 1) some authoritative interpretations of the GDPR are still based on a black-and-white definition of personal data, according to which "non-personal data" implies zero risks of identification (see further Stalla-Bourdillon and Knight); and 2) the rules for personal data protection in the GDPR are so well-detailed that any hybrid personal/non-personal data regulation either risks to duplicate the GDPR or to create ambiguity and confusion about possible overlaps. The Data Act proposal is one example of this abandonment of dualism towards a singular legal concept of "data". Thus,

in this blog post, we aim to explore some problematic points of the proposal that derive from such an abandonment, namely its consistency with the GDPR, the new safeguards for international transfers of non-personal data, and enforcement issues faced by the national supervisory authority/authorities.

The Proposed Data Act

The Data Act was proposed in February 2022, with the main objective of removing the obstacles to the circulation of data collected by connected products and creating value from it through data sharing (for a more detailed analysis of the Data Act, see Lazarotto). The Proposal has gained attention due to its ambition to address complex concerns related to the data economy. In its legislative process, the proposed Act has passed through the Czech and Swedish Council Presidencies, and now has reached the EU Parliament for trilogues. Nevertheless, although the legislative process has been moving fast, we believe some points still must be discussed.

It is important to highlight that the Act has a broad scope which includes the design and access to data generated by connected products or generated during the provision of related services to the user of the connected product. Article 2(2) of the Proposal specifies what must be considered a connected product, meaning any item that obtains, generates, or collects accessible data concerning its use or environment and that is able to communicate data via an electronic communication service, a physical connection or on-device access. Thus, the Act aims to regulate a wide variety of products, ranging from virtual assistants to smart home devices, which, due to the nature of their tasks, have mixed datasets with both personal and non-personal data.

We observe that the measures proposed by the Data Act indicate that the EU institutions acknowledge the "inextricability" of personal and non-personal data, and are trying to create a non-explicit "third way" of protection by imposing new obligations to data processing services related to non-personal data. However, at the same time, by taking this route implicitly, the Proposal creates confusion and raises questions regarding the efficiency of the GDPR measures – listed in Chapter V of the GDPR, which aims to guarantee adequate data protection through different methods, such as adequacy decisions and international agreements – related to personal data transfers and the interplay between the proposed Data Act and other regulations, such as the GDPR.

The ambiguity with the GDPR: the example of data-transfer

As an illustrative example of questions arising from the interplay between the proposed Data Act and the GDPR, we could consider Article 27 of the Proposal, located in Chapter VII, focusing on international access and transfers of non-personal data. We know that the GDPR foresees specific rules for transferring personal data to extra EU countries. Articles 44-50 of the GDPR pose clear conditions for extra-EU data transfer, including the requirement of international agreements, or, as an alternative, in case the EU considers a third country as "adequate" for the protection of personal data or other appropriate safeguards (including binding corporate rules or standard data protection clauses) apply to that specific case. On the contrary, for non-personal data, no specific rules apply to extra-EU data transfer (except sectoral rules or rules relating to intellectual property).

This dualism seems revolutionised by the Data Act. Indeed, Article 27(1) seems to create a new layer of protection for international data access requests and transfers of non-personal data, imposing that providers of data processing services shall take technical, legal, and organisational measures to prevent non-personal data transfers in breach of EU law or Member State law. Article 27(2) goes further, detailing that any data transfer or access request done by a third country which falls under the scope of the Data Act must be based on an international agreement in force between the third country and the Union or the given Member State. In case of the absence of an agreement, Article 27(3) provides that the access or transfer shall only take place following a review by the relevant competent bodies or authorities, who must assess if the transfer or access request is proportionate. This decision must be subject to review by a competent court or tribunal conditions are met. In the case of mixed datasets, very common in connected objects such as smart home appliances, this becomes a greater issue, would the status of the data transfer be under the GDPR or under the Data Act?

Reading these provisions, we might wonder whether this would be a duplication of Articles 44-50 of the GDPR, with the same principles applying, or a separate set of rules. In more specific terms, what do these "legal and organisation measures" for non-personal data transfer imply? Can we consider the GDPR safeguards for personal data transfer here, or are data controllers free to set a lower standard for non-personal data? In the first case, the Data Act would bravely *de facto* extend the consequences of *Schrems 2* to non-personal data, with impressive implications in theoretical and practical terms since it extends a high standard data protection structure imposed by the GDPR to all other types of non-personal data. In the second case, more details and clarifications are necessary since imposing protection measures tailored to personal data also onto non-personal data would fundamentally change the landscape of data protection as we know it.

This discussion also takes us to explore the *enforcement* of the proposed Data Act. The broad scope of the Act – which includes different types of connected objects that perform a variety of tasks and that also collect a variety of data for different purposes – creates a rather complicated task of enforcement. Acknowledging this fact, Articles 31(1) and (2) indicate that the data protection authority (DPA) of each Member State shall be responsible for the enforcement of the Data Act insofar as the protection of personal data is concerned. At the same time, it mentions in Article 31 that different authorities might be competent to enforce the Act in different Member States, such as consumer protection authorities, and that an independent competent coordinating authority, designated by each Member State, will be responsible for the overall application and enforcement of the Data Act. Accordingly, many doubts remain on how different authorities will work together since mixed datasets of connected objects and the inextricability of personal data might push the competence of the DPAs or cause severe overlaps. This also complicates enforcement from the user's point of view since affected individuals might be confused and be left in a grey zone when it comes to lodging a complaint under different Regulations that overlap in several areas.

Conclusion

The Data Act Proposal brings a complementary and beneficial intention to the EU data regulation landscape due to its expansion of data access rights to connected objects (which collect a great amount of data which remains in the hands of private companies). Doubts still loom, however, on the nature of the rules applied to personal and non-personal data and their enforcement, which have the potential to hinder the full implementation of the Data Act if they are not properly addressed.