Kluwer Competition Law Blog

EU Data Governance Regulation – A Wave of Regulatory and Antitrust Reform Begins

Jay Modrall (Norton Rose Fulbright, Belgium) · Monday, November 30th, 2020

On November 25, 2020, the European Commission (EC) published its proposed Data Governance Regulation (the DGR), which will create a new legal framework to encourage the development of a European single market for data. The DGR, proposed in the EC's February 2020 Digital Strategy, is the first of a wave of regulatory and antitrust reforms targeting the digital sector, which will include additional legislative proposals in 2020 and early 2021, as well as significant changes to the EC's enforcement of European Union (EU) competition rules.

The Data Governance Act has three main objectives:

- Creating a mechanism to promote the sharing and re-use of certain categories of protected public sector data that are subject to personal data protection, intellectual property or commercial confidentiality rights and therefore falls outside the scope of the 2019 Open Data Directive.
- Creating a new legal regime for so-called data sharing service providers, who will have to remain neutral as regards the data exchanged, will be prohibited from using data for other purposes, and will be subject to fiduciary duties towards individuals.
- Facilitating so-called data altruism, i.e., individuals or companies voluntarily consenting to the use of their data for the common good, and creating a new system to register organizations engaging in data altruism to increase trust in their operations.

The EC's digital regulatory and antitrust agenda is highly ambitious, including not only the Digital Strategy but also the EC's white paper on artificial intelligence and consultations on the Digital Services Act package, a "New Competition Tool" (NCCT) to allow the EC to investigate and require changes in market structure without showing an antitrust infringement and the EC notice on market definition. On December 9, 2020, the EC is due to publish two important legislative proposals, the Digital Services Act and the Digital Markets Act (DMA). The DMA will impose new transparency and other obligations on online platforms, create a new regulatory framework for so-called gatekeeper platforms and include investigative powers similar to the broader powers originally proposed as part of the NCT.

The EC is also engaged in the most far-reaching review in a decade of its approach to

assessing antitrust compliance of agreements among competitors (horizontal agreements) and between suppliers of goods and services and their distributors or agents (vertical agreements), including notably the sharing of competitively sensitive information.

The EC's Data Strategy sets out a vision of a common European data space, a Single Market for data. The Data Strategy proposed the establishment of nine European data spaces for data sharing and pooling, including health, mobility, manufacturing, financial services, energy, and agriculture. Notably, the DGR does not contain any provision specific to these data spaces but rather aims to create an institutional framework for them. Further measures will likely be set out in the so-called Data Act, originally expected in the second quarter of 2021 but delayed until at least the third quarter. Similarly, the DGR will not create any obligation to share or right to re-use data or alter the intellectual property rights of third parties or limit the exercise of these rights in any way except as set out in the DGR.

The Digital Governance Regulation

As mentioned, the DGR creates new legal frameworks to encourage sharing and re-use of data held by public sector bodies; creates a new category of data broker called data sharing services; and encourages "data altruism," among other things by creating a new framework for registered data altruism organizations.

Public-sector data sharing. The idea that data generated at the expense of public budgets should benefit society has been part of EU policy for a long time. The Open Data Directive requires the public sector to make more data easily available for use and re-use, but commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties (including trade secrets and personal data) are generally excluded. Due to the sensitivity of such data, certain technical and legal requirements must be met before they can be shared, leading to underutilization. Some Member States have taken measures to encourage this type of re-use, such as the French health data hub, but this is not the case across the EU.

Public sector bodies (but not State-owned businesses, or "public undertakings") will be required to establish principles for re-use of data they hold that are non-discriminatory, proportionate and objectively justified, while not restricting competition. When entering into agreements for re-use of such data, they must avoid as far as possible the conclusion of exclusive agreements, except when necessary for the provision of a service of general interest, for example where there is only one entity specialized in the processing of a specific dataset. In any case, such agreements must be awarded consistent with EU public procurement and State aid rules and for periods of no more than three years.

Any conditions attached to the re-use of data should be limited to what is necessary to preserve the rights and interests of third parties and the integrity of public sector

bodies' information technology and communication systems. Personal data should be fully anonymized and disclosed only where allowed under the EU General Data Protection Regulation (the GDPR), including with the data subject's consent. Similarly, data subject to intellectual property rights should only be transferred where allowed by EU or national law or with the rightholder's consent. Public sector bodies should facilitate obtaining individuals' or companies' consent to the re-use of their data, without providing contact information that allows re-users to contact data subjects or companies directly.

Public sector bodies must modify data containing commercially confidential information in such a way that no confidential information is disclosed. The DGR does not explain how this should be done but approaches typically considered sufficient for competition law purposes include aggregating data in such a way that it is not possible to reverse engineer competitively sensitive information and, in some cases, anonymizing data (for instance, by removing names and sales amounts from lists of key customers or suppliers). As mentioned, the EC is currently reviewing its guidance on the assessment of information sharing, which currently focuses on anti-competitive information sharing (e.g., in the cartel context). The EC has recognized that more guidance is needed on pro-competitive information sharing, but updated guidance likely won't be available until 2022.

Where the provision of anonymized or modified data would be insufficient, on-premise or remote re-use of the data within a secure processing environment could be permitted. Public sector bodies may make the use of such a secure processing environment conditional on the re-user's signature of a confidentiality agreement prohibiting the disclosure of any information that jeopardizes the rights and interests of third parties.

To protect non-personal data protected by intellectual property rights, special requirements would apply to transfers of data to non-EU countries. Data should be transferred to such countries only where appropriate safeguards are provided, for example where equivalent measures ensure that non-personal data benefits from a level of protection similar to that under EU or EU Member State laws on the protection of intellectual property rights. The DGR empowers the EC to designate such countries based on their legislation on public security, defence, national security and criminal law concerning the access to and protection of non-personal data, public authorities' access to the data transferred, the existence and effective functioning of independent supervisory authorities responsible for ensuring and enforcing compliance with the applicable legal regime or the countries' international commitments.

A public authority may transfer data to a country not subject to an EC designation only if the country declares that it provides a level of protection essentially equivalent to that provided by EU or Member State law and the re-user commits to comply with the DGR and accepts the jurisdiction of the relevant Member State in the event of disputes.

The DGR provides that public sector bodies may impose stricter conditions on transfers to non-EU countries of highly sensitive types of non-personal data, such as

public health data held by public hospitals. Such highly sensitive data will be defined in EU measures, for example in the context of the European Health Data Space or other sectoral legislation. Conditions attached to the transfer of such data should be proportionate, non-discriminatory and necessary to protect legitimate public policy objectives, such as the protection of public health, public order, safety, the environment, public morals, consumer protection, privacy and personal data protection.

The conditions should also correspond to the risks identified in relation to the sensitivity of such data, including in terms of the risk of the re-identification of individuals. These conditions could include terms applicable to the transfer or technical arrangements, such as using a secure processing environment, limitations as regards the re-use of data in third-countries or categories of persons which are entitled to transfer such data to third countries or who can access the data in the third country. In exceptional cases, they could also include restrictions on the transfer of the data to non-EU countries to protect public interests.

The DGR also includes "shielding" provisions to limit EU citizens' and companies' obligation to provide data under non-EU Member State legal procedures. Judgments of non-EU courts or tribunals or decisions of administrative authorities requiring such transfer or access would be enforceable only if based on an international agreement, such as a mutual legal assistance treaty, between the requesting third country and the EU or a Member State. Absent a relevant agreement, transfer or access would only be allowed where the non-EU-country requires the reasons and proportionality of the decision to be set out, the court order or the decision is specific and reasoned objections of the addressee are subject to judicial review.

Public sector bodies could charge for the re-use of data, but their fees must be reasonable, transparent and non-discriminatory. Lower (or no) fees could be charged for certain categories of re-uses (such as non-commercial re-use, or re-use by small and medium-sized enterprises), to stimulate research and innovation and support companies that typically find it more difficult to collect relevant data themselves.

Member States must establish a single information point to act as the primary interface for re-users that seek to re-use such data held by public sector bodies. Member States must also designate bodies to support the public sector bodies allowing re-use of protected data, including by providing secure data processing environments to allow data analysis in a manner that preserves the privacy of the information. Such bodies could also support the management of consents.

New regime for authorized data sharing service providers. The EC anticipates that providers of data sharing services, or data intermediaries, will play a key role in facilitating the aggregation and exchange of substantial amounts of relevant data. These data intermediaries must be independent of both data holders and data users to facilitate the emergence of new data-driven ecosystems independent from online platforms with significant market power.

Data sharing service providers authorized under the DGR would have as their main objective the creation of legal and potentially technical relations between data holders and potential users, assisting both parties in exchanging data. Their business must aim at intermediating between an indefinite number of data holders and data users, rather than a closed group. Other excluded categories include:

- providers of cloud services;
- service providers that obtain data from data holders, aggregate, enrich or transform the data and license the use of the resulting data to data users, such as an advertisement or data brokers;
- data consultancies;
- providers of data products resulting from value-added to the data by the service provider;
- services that focus on the intermediation of content, in particular on copyright-protected content;
- data exchange platforms used by one data holder in order to enable the use of data they hold;
- platforms developed in the context of objects and devices connected to the Internet-of-Things;
- regulated entities such as consolidated tape providers and account information service providers; and
- data altruism organizations (see below).

The DGR provides for a specific category of data intermediaries focusing exclusively on personal data and seeks to enhance individual agency and the individuals' control over the data pertaining to them. These service providers would assist individuals in exercising their GDPR rights, in particular managing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure or right "to be forgotten," and the rights to restrict processing and data portability.

The DGR would prevent misaligned incentives that could encourage individuals to make more data available for processing than what is in the individuals' own interest. This could include advising individuals on uses of their data they could allow and making due diligence checks on data users before allowing them to contact data subjects, in order to avoid fraudulent practices. In certain situations, it could be desirable to collate actual data within a "personal data space" so that processing can happen within that space.

The DGR also contains rules on data cooperatives, which would seek to strengthen the position of individuals consenting to data use, influencing the terms and conditions attached to data use or potentially solving disputes on how data can be used when such data pertain to several data subjects within that group.

To increase trust in data sharing services, the DGR creates an EU-level regulatory framework with highly harmonized requirements. Data sharing service providers would be required to be neutral as regards the data exchanged between data holders and data users, and could thus act only as intermediaries, without using the data exchanged for any other purpose. The DGR would require structural separation

between the data-sharing service and any other services provided to avoid conflicts of interest. Data sharing service providers should be separate legal entities that do not engage in other activities. Data sharing service providers intermediating exchanges of data between individuals as data holders and legal persons should also be subject to fiduciary duties to those individuals.

Providers of data sharing services would be required to have a place of establishment in the EU or to designate a representative in the EU. The representative would act on behalf of the data sharing services provider under a written mandate. Data service providers would have to be authorized and supervised by the competent authority in the Member State where they are established or their legal representative is located.

Encouraging data altruism. The DGR aims to tap the potential to increase the use of data made available voluntarily by individuals or companies for purposes of general interest, such as healthcare, combating climate change, improving mobility, compiling official statistics, improving public services and supporting scientific research. The legal framework established by the DGR would contribute to the formation of data pools with sufficient size to enable data analytics and machine learning.

Companies seeking to support purposes of general interest by making available relevant data based on data altruism at scale and meet certain requirements would be able to register as "Data Altruism Organisations recognised in the Union." Registration would be valid across the EU, facilitating cross-border data use within the EU and the emergence of data pools covering the several Member States. The voluntary compliance of such registered entities with a set of requirements should foster trust that data made available for altruistic purposes serves the general interest. Such trust should result in particular from a place of establishment within the EU, as well as from the requirement that registered entities have a not-for-profit character, from transparency requirements and from specific safeguards in place to protect rights and interests of data subjects and companies.

Further safeguards should include offering data processing within a secure processing environment operated by the registered entity, oversight mechanisms such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, and the technical means to withdraw or modify consent at any moment, based on the information obligations of data processors under the GDPR.

Recognized data altruism organizations would be able to collect relevant data directly from natural and legal persons or to process data collected by others. Typically, data altruism would rely on the consent of data subjects in accordance with the GDPR. Individuals and companies participating in these activities would consent to specific purposes of data processing, but could also consent to data processing in certain areas of research or parts of research projects.

For additional legal certainty, the EC will develop a European data altruism consent form to contribute additional confidence and transparency on how data subjects' data will be accessed and used. Use of the form could also streamline data altruism by

companies and provide a mechanism allowing companies to withdraw their permission to use the data. To take into account the specificities of individual sectors, including from a data protection perspective, there should be a possibility for sectoral adjustments of the European data altruism consent form.

Relation to competition law rules

The DGR specifies that it does not affect the application of EU competition rules, in particular rules on the exchange of competitively sensitive information between actual or potential competitors through data sharing services. The DGR specifies that public sector bodies must comply with competition rules in their principles for re-use of data they hold and avoid exclusive agreements. Data sharing service providers will have to establish competition law compliance programs.

Indeed, the activities of data sharing service providers may lead to the sharing of competitively sensitive information, such as information on prices, production costs, quantities, turnovers, sales or capacities. Information sharing may distort competition by enabling businesses to become aware of market strategies of their actual or potential competitors. The DGR provides that data sharing service providers must modify competitively sensitive information to ensure that it is not confidential, but does not say how. As mentioned, the EC's current guidance on information sharing among competitors may discourage even pro-competitive information sharing. The revised guidance, scheduled for 2022, is expected to provide more clarity on pro-competitive information sharing and allow companies to seek guidance from the EC.

More broadly, the DGR should be seen as part of a broader antitrust and regulatory reform agenda targeting the digital sector, in particular online platforms that collect large amounts of data. The data-sharing service providers and data altruism organizations contemplated by the DGR are designed to encourage (predominantly) European alternatives sources of data in competition with large "gatekeeper" platforms. On December 9, 2020, the EC will propose a new regulatory framework for gatekeeper platforms in the DMA. The DMA will include an extensive list of prohibited practices, such as self-preferencing, and give the EC new powers to investigate market distortions and order remedies, potentially including access to data held by large platforms.

The EC's future data-related initiatives, including the Data Act 2021 and potential measures to promote European data spaces, will also need to take account of EU competition rules and in particular the risk of exchanging competitively sensitive information. The full relationship between the EC's regulatory and antitrust reform agendas will only emerge in the coming years.

Key Takeaways

Promoting competition and European "sovereignty" in digital markets are twin goals of the Von der Leyen Commission. The Commission is melding antitrust and regulatory

tools to an unprecedented extent in an effort to achieve its goals. The DGR is the first legislative proposal to flow from the EU's Digital Strategy. It is intended to promote the formation of the nine European data spaces, but the DGR's new legal regimes are largely permissive, encouraging sharing of information already held by public sector bodies and facilitating the formation of new market actors. Perhaps surprisingly in light of its name, the DGR says remarkably little about the actual governance of those actors or the future European data spaces.

The EC's plans for the DGR have given rise to concerns about the potential to create a "fortress Europe" for data. Indeed, a draft of the DGR leaked in October 2020 provided that data shared by public sector bodies could only be processed in the EU. The final DGR regime allows the transfer of data held by public sector bodies outside the EU, but only subject to strict conditions. Experience under the GDPR and other EU regulatory regimes requiring the EC to identify "equivalent" legal regimes suggests that these conditions may be difficult to satisfy. When rightholders' consent to disclosing their data but prohibit the data's export outside the EU, and such data are commingled with other data, the export of the entire dataset may become impracticable.

The relatively modest scope of the DGR, and steps taken to preempt criticism that it is protectionist, may smooth the DGR's path through the EU legislative process. However, the practical effect of the DGR will likely depend on how it relates to other proposed EU legislation, including the DMA, the Data Act, and specific measures proposed to create European data spaces. The DGR's potential will also depend on EC antitrust reform efforts, including in relation to information sharing and data access requirements.

To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe here.

This entry was posted on Monday, November 30th, 2020 at 9:34 am and is filed under Data protection, Digital economy, European Union, Regulation
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.