Data sharing and sovereignty issues

Burkhard Balz

Member of the Executive Board, Deutsche Bundesbank

Effective data sharing requires data sovereignty

We have recently discovered a new world: the digital world. This entails both great potential and great risk at the same time. On the one hand, the combination of increasing amounts of data and advancing technical possibilities leads to added value in the use of personal data. This includes, for example, discounts on products and seemingly free usage of digital products. On the other hand, there are risks of becoming dependent on data companies, losing our data sovereignty, and facing monopolistic market structures. These dangers arise in particular due to the growing role of platforms.

The recently emerged platform economy, with its small number of large and often global network companies, warrants special attention in this regard. Personal data in combination with machine learning may be used to gain the upper hand. For instance, data could be used not only to assess a potential borrower's creditworthiness, but also to identify the highest rate that they would be willing to pay. It is even more concerning that this discrimination may not necessarily be intentional. A sophisticated algorithm may be biased by finding an underlying cause.

In order to protect the right to informational self-determination, regulators have introduced a variety of rules. The most prominent of these, the GDPR, sets out a legal framework for data protection. Its major achievements are the required express consent for the collection and usage of data as well as the right to demand the deletion of personal data. However, the practical implementation of these provisions presents a number of challenges. Therefore, in order to achieve full data sovereignty, further steps may be necessary. Developing a user-friendly technical tool that allows users to conveniently control the usage of their own personal data could be one potential solution. Based on a secure and neutral data infrastructure, the data owner would maintain the right to decide independently on the use of their data and would be able to fully or partially share their data with companies or authorities for a designated period of time. This would potentially ensure that data access and usage can be tracked and controlled effectively and that property rights, such as deletion of data, can be exercised with ease. Such a facility would not block data sharing; instead, it would facilitate it under fair conditions and therefore help to increase competition.

Beside this new digital world, existing market structures appear to be disrupted. Data is collected at near-zero marginal cost, which means that new services are easily scalable. Once sufficient scale has been achieved and a captive ecosystem established, potential competitors have little chance to catch up. This restricts innovation and competition. A legal framework is necessary to create a level playing field. PSD2 has successfully established such a framework for financial institutions. Banks have to share their data with certified companies if this has been authorised by the customer. In order to create a level playing field for data sharing in other markets as well as between different markets, a legal framework analogous to the PSD2 model should be established at the European level. ●

Carsten Hess

Head of Digital Policy, Banco Santander

Five principles for an innovative European data economy

For the EU's economy to remain competitive on the global stage, Europeans need to turn the necessary digital transformation of its traditional industries into a global advantage.In Santander we support the EU Commission's plan to create a 'data agile economy' where data and fair rules around its sharing and usage are key to create a more innovative digital economy.

However, we believe it is critical to accelerate on an open cross-sectorial data framework that, while empowering users and putting them in the centre to control the data they generate, would contribute to developing a level playing field in all sectors. We strongly support the vision of a single European data space where personal (and non-personal) data is secure and where businesses (including SMEs) also have easy access to industrial data. While empowering users and putting them in the center, opening cross-sectorial data would also multiply the opportunities for disruptive innovation and contribute to developing a level playing field in all sectors and with platforms that leverage in data from diverse markets and contexts. We therefore support the horizontal ambition of the EU's data strategy.

When it comes to banking, more data, and especially data that is uncorrelated ▶

▶ with the traditional one, can help improving services in the benefit of customers and trigger innovation, just as it happened some years ago with PSD2. Non-financial data has a huge potential to improve banks' predictions and thus enable customers access to finance. It will also trigger similar levels of innovation outside the financial space.

In order to create these conditions for success, we propose a set of five principles creating a data agile economy by contributing to opening-up data across sectors in a way that individuals and business users can benefit in fair manner. Those principles will also help providing choice within a secure framework to make their choice to share data from all sectors with their chosen providers.

1. Give control to the user by creating a framework that is consumer centric. People and businesses, as owners of their data must be in control and decide freely with whom and for what purpose they share it.
2. Create the right conditions for the secure transmission of data. APIs are the preferred method for this as they are safe, efficient and provide access to data on an immediate & ongoing basis. In addition, access can also be easily stopped whenever the user decides to.
3. Clarify the different nature of data to be shared. Users are the owners of their raw & observed data; but companies building "value" around the data need to be able to retain this value. Elaborated or inferred data should not be mandatory shared.
4. The data regulatory framework should enable greater access to data improving services to the benefits of users. The focus of any future data sharing framework should be put on the revision of the online intermediation services regulation, since this is where most amount of data lies.
5. A fair cross-sector approach is also needed to ensure maximum benefits to our society. No mandatory data sharing should be triggered in a sector (banking) where players from other sectors also compete but don't have similar requirements. ●

Tsvetelina Penkova

MEP, Committee on the Internal Market and Consumer Protection, European Parliament

The EU towards data sharing economy

Globally, there are deeper and deeper concerns regarding the market dominance of tech giants. There is a continuing and ever increasing corporate concentration, where governments have explored different measures, from breaking up tech giants to creating public alternatives to exercise strict controls and transparency. In Europe, a number of measures to tackle competition have been adopted, non-exhaustively in industries like telecoms or energy, however, when it comes to the 'Big Tech', experience has shown that ex-post measures like fines imposed by the European Commission have neither restored fair competition, nor avoided growing market dominance. This is a reason why, in the Group of the Progressive Alliance of the Socialists and Democrats in the European Parliament, we call for a review of the EU competition rules, which should take into account the future competition in the digital economy, including market-dominance driven predatory pricing strategies, and which should allow for preventive measures to tackle uncompetitive behavior and guarantee a level-playing field.

> *"Taxes should be paid where the profits are generated.*

Such companies are accumulating huge amount of data and often prevent others, including the data subjects, from accessing and using it. GDPR and the ePrivacy directive provide users with the right to access and use their data but there is often a lack of tools and standards to do so in a practical way. The European Commission is trying to address these issues, i.e. through data interoperability and governance, in their newly published European strategy for data. As much as this strategy brings revolutionary initiatives like common sectorial data spaces, also for the finance sector, it brings a number of questions and challenges. What would be the incentives for companies to share data, especially rare or important data? What data could be shared? Is there a price for this data? The Commission believes that there is a merit in thinking about extending the approach taken in PSD2 to other sectors, thus extending open banking to open

finance. This brings additional questions with regards to the scope and application. In any case, the experience with the PSD2 can serve to future debates on the need for a standardised approach for sharing data and a high level of trust among actors.

Finally, we are also of the view that the way added value is created through digitalization and tax regulations should be adapted accordingly. While huge profits are global, some companies optimise their profits in only a few tax advantageous countries. This is unfair to both the consumers and the competition. Taxes should be paid where the profits are generated. ●

Sébastien Raspiller

Head of Department, French Treasury, Ministry of Economy and Finance, France

A sustainable European data ecosystem at the service of the financial sector

The EU financial area could only stand out from the crowd with a well-protected, well-regulated, well-advised while highly open, sovereign data ecosystem.

When it comes to financial data, the GDPR is broad in scope and also has a large set of sector-specific requirements in terms of security. Some of them (e.g. from payment cards) are undeniably considered "highly" personal given their criticality and the GDPR provides for some ex-ante measures such as the conduct of a data protection impact assessment in the case of personal data processing likely to generate risks for consumers.

Whether sectoral or not, a safe and secure environment for data and high-value information is at the heart of the Single Market concerns. Initiatives ranging from e-IDAS regulation and EBA Regulatory Technical Standards (RTS) to the trades secret European directive allow for a common area of data where citizen's rights are preserved, consumers are highly-protected and the non-EU investors or suppliers are truly welcome as long as the EU requirements are fulfilled.

The core EU values could be undermined or weakened notably by an increasing reliance on systemic non-EU third-party providers of crucial services such as data (including cloud computing) or even cybersecurity and algorithms This raises the question of the supervision of non-financial players and the robust assessment of the systemic risks linked to their use as much as taking into account intertwined public policy objectives such as financial stability, fair competition and its implications for the free flow of data, portability, personal and non-personal data business models.

The cross-borders nature of data also hampers information and data sharing through the creation of determined circles of trust that are essential to build a sovereign European data ecosystem, but eminently remains a puzzle hard to solve. At the meantime, conflicts of sovereignty could occur regarding sensitive data location such as computer vulnerability data (e.g. bug bounties platforms) or highly personal ones and non-EU domination of certain activities (e.g. security standards, sovereign rating agencies) with a serious lack of European counter-models, that is damaging not only in terms of international outreach but also for the full control of our critical infrastructures.

However, it is clear that transboundary and cross-sectoral issues require both EU and international responses and enhanced synergies between public and private players in correspondence with EU rules and values. A well-designed common European financial data space and a high-reaching European Strategy for data (European Commission) would be a promising step ahead in that sense. ●

Kostas Botopoulos

Advisor to the Governor of the Bank of Greece & Former Chair, Hellenic Capital Markets Authority

Data restrictions in times of emergency

The extraordinary times we are living in because of the outburst of the coronavirus pandemic have an impact on nearly every aspect of private and public life. This is also true for the field of data protection: instead of debating on data sharing and the impact of technology on European financial markets, as we were supposed to be doing in Zagreb, we are suddenly confronted with two completely different, and much more problematic, sets of issues: on the one hand the very survival of the European financial markets, and on the other the legality and legitimacy of restrictions of data protection which are already taking place all over Europe in the effort to combat and contain the pandemic. Leaving aside the economic consequences, which would perhaps merit a special Eurofi conference once the nightmare is over, I would like to highlight some of the legal and operational aspects related to data restrictions.

The data-protection framework in the EU is comprised by three sets of principles: constitutional provisions in some member states (for example, Art 9A of the Greek Constitution), the "horizontal" GDPR provisions and relevant national legislation enacted on the basis of the GDPR. All three sets of provisions enshrine a robust protection of privacy and personal data but also cater for exceptions. The principles of legality and proportionality

apply in the constitutional framework, be it on the national level (Art 25 of the Greek Constitution) or through the EU Charter of Fundamental Rights. In the EU we have, since 2018, the GDPR, as ▶

complemented by relevant provisions of Directive 2002/58 on the protection of privacy in electronic communications. Art 6, 1, e (and also whereas no 46) of the GDPR provides for exemptions from consensual processing for the protection of vital public interests (among which health is first and foremost), whilst Art 9,2, i specifically mentions health issues as providing an exemption whereby even sensitive data (such as health data) may be processed without consent. This does not mean, however, that said processing may be done in contravention of the fundamental principles laid down in Art 5 of the GDPR: legality, limitation of goal, minimization, exactitude, limitation of storage, confidentiality.

Consequently, measures taken by public authorities, such as compulsory data gathering, processing and exchange of data between member states and authorities, would be admitted if based on a specific legal act setting out the conditions and the duration of the emergency (in the case of Greece it took the form of a so-called "act of legislative content", a presidential decree ratified by the Parliament on a later stage and used only in exceptional and urgent circumstances) and respect of above DGPR core principles.

Private sector entities, usually regulated by the relevant national legislation such as Law 4624/2019 in Greece, can, in principle, also impose restrictions on data protection, based on a specific national legal base and respecting the core GDPR principles. Statistical use, such as the one made by some member-states but also requested from the Commission, is also permitted under the proportionality and anonymization conditions. For every processing act the possibility of judicial action against measures considered as contravening the core protection principles should be guaranteed by member states. On all those issues, the European Data Protection Board rendered a public statement on the 19th of March 20120. Obviously, full protection, sovereignty, and even use of technology are secondary in times of such emergency. Even in such times, however, the European state of law remains in place. ●

Benjamin Angel

Director for Direct taxation, Tax coordination, Economic analysis and Evaluation, DG Taxation and Customs Union, European Commission

New challenges lay ahead, prompted by financial innovation

Recent scandals have put the financial sector under scrutiny by legislators. For the last decade, the fight against tax evasion and avoidance has been a priority for governments around the world. From the strengthening of anti-money laundering requirements to the automatic exchange of financial account information for tax purposes, financial institutions were called upon to strengthen their procedures and share customer information with the authorities.

In 2016, for the first time, EU financial intermediaries were required to collect and report customer information to the tax authorities. The alignment of the Directive on Administrative Cooperation to the OECD common reporting standard ensured the minimisation of the potential burden for EU financial institutions. This Directive was recently amended and will require that intermediaries, including financial intermediaries, report aggressive tax planning schemes.

However, new challenges lay ahead, prompted by financial innovation. Innovative financial technologies and products bring efficiency gains but also new demands for the industry and legislators. Due diligence and customer identification obligations set forth in legislation still rely mainly on traditional requirements, while technologies such as electronic signatures and seals or even biometric data sensors recognition are being considered by the industry. In this context, the regulatory framework will need to remain fit for purpose while both governments and financial institutions must ensure the protection of clients' data and its security.

New financial products such as virtual assets are now under the scrutiny of legislators. What started as a minor alternative means of payment has now been taken up by key market players, often outside the boundaries of the financial industry. Such "outsiders" are not subject to as stringent regulatory framework as the financial sector, which may lead to a biased playing field. The financial sector will need to reinvent itself while ensuring it keeps its competitiveness in an ever-changing environment. At the same time, as it evolves from simple low-value payments into a means of investment and storage of value, virtual assets are relevant for taxation purposes as well as other areas such as the fight against money laundering.

Lastly, a comprehensive review of the taxation of Multinational enterprises is ongoing within the OECD. It remains unclear how and to what extent it will affect the taxation of the financial sector. The latest draft notes that most financial services are supplied to commercial customers and therefore not within scope, but only goes so far as to say that there is a "compelling case" for consumer-facing services to be excluded, on the basis that they are already subject to heavy regulations.

Any legislative action must foster innovation in the EU, or at the very least not impede it. The way forward must keep up with innovation and new financial realities, while relying on the synergies between the different legal frameworks. A "whole-of-government" approach is the only way to avoid the duplication of procedures and avoid unnecessary costs for governments and economic operators. Action in the area of taxation, anti-money laundering and financial regulation needs to be consistent and mutually reinforcing. ●