DATA PROTECTION, FAIRNESS AND SHARING

1. Making the necessary and appropriate changes in response to the changing data and privacy landscape

1.1. The GDPR has created new mechanisms enhancing the protection of individuals

It is one year since the General Data Protection Regulation (GDPR) came into force in the EU. Similar legislation has been developed in other jurisdictions. Financial entities have to face increasing data related competition, as well as adaptation challenges related to the recently adopted regulations.

A regulator emphasised that the GDPR created new mechanisms in order to enhance the protection of individuals throughout the European Union. Any person may file a complaint with any supervisory authority. Data controllers may have recourse to some innovative mechanisms of co-operation and consistency. There is a new mechanism through which data controllers may go to a single interlocutor in the European Union, which is the data protection authority where the data controller has its main establishment. GDPR allows both controllers and individuals to find a better position to ensure both the protection of their fundamental rights and the free movement of information throughout the EU.

An industry representative noted that though the conceptual thinking behind GDPR enhanced existing rules, the real game changer is the associated enforcement and empowerment, which has really helped to bring an unprecedented level of attention to the topic. GDPR has also made data protection a more holistic concept and implies a great deal of individual responsibility and self-regulation.

1.2. GDPR is not yet able to provide answers for a world, which is becoming further digitalised

An official suggested that the real game changer is the world, which is becoming fully digitalised, rather than GDPR itself. This will result in changes that GDPR is not yet able to provide answers for.

Consequently, there are significant ethical questions to be tackled, particularly for liberal democratic societies. The norm is that individuals have to be protected from the power of the many, including the state.

However, conversely there are also now scalable groups of individuals who can present a threat to the state with only a cell phone. That has to be balanced out with the legitimate concern about protecting the data of individuals. There are also security concerns. Balancing those and building anew the value proposition to citizens, while making sure that they are completely protected, is a very difficult task.

1.3. Data fairness specificities regarding the insurance sector

An industry representative raised the question of the extent to which there needs to be an overlay of additional, sector specific regulation notably regarding the insurance sector. This is related to the question of what 'fairness' means in the insurance sector. Indeed, data is the basis of what insurers do and is used to assess riskiness and set the premiums for those who want to enter a risk pool and be insured. Conversely, there are other business models in which collecting data is the purpose, which is very different from insurance companies' activities. Involved in fairness in insurance, there must always be a consideration of there being both an individual policyholder and a collective of all policyholders. The stake is notably to find the right balance between the protection of the individual and the collective.

1.4. The transitional journeys of organisations to achieve privacy and appropriate use of AI

In this context, regulation will change and there will be a move towards a financial consumer protection thinking, which is closer to the consumer on many points of the regulation and legislation than has been the case.

An industry representative stated that the financial services industry is on a journey and conforming fully is extremely challenging. In addition to the privacy question an important issue is whether machine learning and AI are to be used in deciding customer outcomes. Finally, financial entities must further refine their approach to the whole data challenge. Given that in addition, regulation and legal framework are the starting points, the industry is on a journey regarding how it uses data in order to demonstrate that the outcome for the end customer is defensible and also that it shares data with an ethical consideration.

A Central Bank official noted that in this context, Central Banks are in the midst of the dilemma between protection, privacy and the openness of data.

One additional important challenge for Central Banks and the financial industry is to address the volume of data. While the institutional and policy frameworks are being rethought and reorganised, there are huge organisational IT impacts. Should there be a breach of data from a Central Bank, the impact is much more important and systemic than from other semi-public or public organisations.

Another challenge is how to make both the participants in internal system and the public at large aware of the challenges and the new landscape. Awareness is improving but needs further improvement. Central Banks also have to play a role as go-betweens for the public and the private sectors on data protection.

An industry representative believed that GDPR is a journey for any organisation. However, it is less of a challenge for insurers as their business model is already based on data. Long before GDPR, data was at the core of their businesses. The insurer's relationship with the consumer runs on trust, so the fact that insurers had to handle their data meant they were in a slightly different position from other types of business.

The representative's journey on fair handling of data started long ago and before GDPR, just by it doing business. Indeed, by 2013 there were binding corporate rules, which regulated the flow of data between companies in the group. In 2015 a data privacy advisory panel, made up of external people, was created. Finally, data privacy commitments aligned with GDPR were issued in 2016 and have been applied since 2018.

2. The balance between individuals and organisations in an increasingly regulated environment

2.1. Data fairness: a permanently evolving cross sectoral ethics challenge, in the international context

An industry representative suggested that the impact of what is now in place in terms of regulation is a game changer because of the fines. It has resulted in a new degree of attention paid

to data protection across sectors. GDPR could be the new standard in other regions and has been an important step.

An official noted that there is often consideration about when the market for data developed, and now there are fines that may set quite a high price. The financial sector has been in the business of trust, and reputational risk is very important. The technological change taking place would drive financial entities to think about the ethical issues in any event and to contemplate how best to protect customers. GDPR changes the way entities have to think about things, and the fines make it extremely efficient.

A regulator believed it is important, before considering the fines for breaching GDPR, to be aware of the importance of respecting the GDPR legal provisions. The European Data Protection Board (EDPB) is a newly established European Union body composed of representatives of data protection authorities. In less than one year it has already issued a significant number of guidelines and opinions to help data controllers understand the GDPR legal provisions and to improve their implementation in daily practice.

There are guidelines on data portability, transparency and consent that also give concrete examples from the authorities' experiences, and which clarify the notions and legal provisions of GDPR.

However, the ethical limits are yet to be defined. In addition, it is a challenge to figure out what happens next, particularly with the suggestion of financial entities becoming platforms. Platforms so far, particularly social media platforms, have been evading responsibility. When that business model change happens, it is hoped that respectability and trust will remain.

A Central Bank official added that understanding the complexity of the whole issue is an issue, and there are various levels of complexity. GDPR creates new and eventually harder problems. GDPR is not very attuned to the needs of the financial sector, for instance on market abuse regulation and the need to gather data for the regulators to do their job.

The level of greatest complexity is the need to find a balance between the national and the supranational. In addition to the EDPB there is the European supervisor, who is part of the board, but who works on a different set of provisions. The EU has a different set of data protection provisions for the institutions of the EU. Within the national remit, there is both the regulation and national rules.

2.2. Improved transparency and accountability should enable the deepening of data privacy and fairness

An industry representative queried whether rules and regulations alone can frame the issue appropriately and capture it. Litigation funds over the last 12 months have raised money in order to go after the deep pockets in life sciences, technology and financial services, and class actions are emerging. The principle of respecting human agency includes the fact that it is the end citizen or customer's data and not those of institutions.

GDPR tries to emphazise the question of fairness. There is a great deal of pressure to combine the personal data with machine learning and AI in order to come to a decision about how to demonstrate fairness. That leads into the question of transparency. Many people talk about black boxes being applied to data, but it should instead be about glass boxes which can be opened up to regulators.

It is very important that people at board level should appreciate these issues and accountability within organisations is defined according to who can do what. The chief data officer (CDO) currently has no regulated role. Seemingly no organisation in financial services has a head of ethics or is looking at the ethical outcomes. There is a rush to hire data scientists without understating the behavioural impact of data or employing data scientists who look at the unforeseen consequences of taking somebody's data, processing it and sharing it in a particular way.

3. The international situation

3.1. Combining data fairness and innovation

The Chair noted that Mark Zuckerberg is calling for more regulation. Regulation can probably help to give clear guidelines for accountability and make financial and economic institutions more comfortable complying with the rules when they are well known. GDPR is based on a territoriality principle linked to the consumers and citizens within the EU, and that probably raised awareness in third countries. EU consistency is also one of the objectives the European Commission had in mind when it proposed the regulation instead of a directive.

Another important factor, in addition to fines, is the way the courts will be applying and interpreting the provisions of GDPR. It may be fruitful to start thinking about a transition of the EDPB towards being a semi-European institution like the European supervisory authorities. Technology may catch up and change the rules of the game before any revision of GDPR.

Having a good data protection policy in place is already a certification of being bona fide when a company is competing in European or global markets. Data protection itself has become a good economic asset. The old perspective of merchandising data has to change somewhat, because the most important thing is to bear in mind the interests of the individual who is the owner of personal data. GDPR puts an emphasis on transparency obligations for the data controller. For many aspects of the processing carried out by data controllers, transparency and consulting the data subjects are part of any privacy policy.

A speaker noted the desire to find the right balance between protecting consumers and not standing in the way of innovation.

The information asymmetries in the systems would be greatly reduced if there was open, widely shared data that somehow ethically respected the individuals' right to say no and to take their data with them when they want to. The question is how to tackle the development of that sort of market and transparency, particularly with learning algorithms, black boxes and cognification. It is not clear how to regulate when something that is completely opaque is allowed to make the decisions. It is an interesting question as to whether ethics can be taught to such black boxes.

A Central Bank official stated that it is very difficult to have a global agreement on how to tackle the issues. Within the existing sectors it is impossible to find real harmony between the competing objectives. GDPR has not even start to tackle the artificial intelligence and big data issues.

An industry representative stated that GDPR did not tackle AI and big data. GDPR was a catch up. Some governments and jurisdictions are going to think about it in the appropriate way, including the European Union. Some state actors and others will diverge from that. That is inevitable.

True AI is not yet deployed anywhere. There is plenty of machine learning, and it has inherent biases written into it. The programmers are predominantly male, and so there is a gender bias in machine learning.

The industry has to catch up and will continually be doing so. Laws and regulations take too long. The private sector getting together and looking to implement principles is going to use a far more expedient approach. Some organisations are

going to employ their ethical use of data as a differentiator and see it as part of their value proposition.

3.2. The challenges imposed by existing diverse data privacy ethics globally

There is a question of whether a balance is to be found at the EU level, given the awareness of EU citizens regarding data privacy. An industry representative suggested that that goes beyond data protection, and GDPR specifically, and into the ethical considerations that need to be taken into account. It is the technological and societal development that leads to those questions. It is not clear that the ethical questions are even understood.

The other challenge is that there is no universal concept of ethics for data privacy. It might differ in different regions, and it might also change over time as society and technology further develop. There is a challenge there even before considering whether regulation could help. There will eventually be a regulation of the boundaries and the red flags from an ethical standpoint, but the political and societal debate has not developed far enough to be able to set up the red flags.

Trust is a licence to operate. Whatever happens in an area where there will be red flags, it will have a significant impact on the reputation of the relevant company and others. There will be spill-over effects. There is also a set of questions about whether something specific is needed for financial services and insurers.

The Chair queried how the potential contradictions arising out of different notions of ethics and data privacy awareness around the globe can be dealt with, and whether any aspects or competing views should be taken into account. He questioned whether the Clarifying Lawful Overseas Use of Data (CLOUD) Act in the US raises worries amongst supervisors or regulators.

An official noted that different countries have independently chosen different paths in developing their views. The challenge is with those nations that maintain that they are allowed to spy on their citizens and nudge them in a direction the citizens may not have wanted. It is difficult for there to be global agreement on how to protect data when the US comes from such a different angle.

However, there will be a consumer push on all continents, and there will be some form of convergence. It comes back to the point about the ethics and the value systems put in place. It is a political question.

3.3. Challenges to level the competition field between financial entities and BigTechs

The Chair indicated that there had been a first sanction for non-compliance regarding GDPR. It was from a French data privacy body resulting in a €50 million fine for Google. One question is whether GDPR and the sanction process is something that can help financial entities to be competitors in the field, because they know how to respect the data privacy of their clients, or whether it is a challenging matter for the financial sector.

The Chair queried whether people are more willing to trust GAFAs than insurance companies on data handling. An industry representative replied that it depended on the generation of the people.

An industry representative emphasised the importance of the regulation being cross-sector. The representative's organisation is very attentive to the protection of personal and consumer data prior to GDPR. An industry representative emphasised that financial services organisations, as well as FAANGs and BigTech, do not own the data; they are the custodians of individuals' data. Fines for not applying the rules incentivise greater caution in new entrants.

The game changer is the change of the economy and the way the economy is functioning. There is an emergence of platforms and the fragmentation of the financial business, the disruption of the way business is done and the introduction of new players in the chain of value.

As the pressure has come onto financial services organisations for returns on equity and capital etc., and they have been the providers of product, they have looked over the approaches of technology companies, and have seen their valuations, and have responded by indicating that they need to consider becoming platform-based businesses rather than product-based businesses.

There is a moral hazard element to that, because in moving to a platform area some of the previously abided by regulation can break down. Very often people use a data scientist for particular situations and ingest vast quantities of data. Regulation is not considered when doing so. Outcomes can result in non-conformance with rules and regulations as they apply to financial services, but that can be acceptable for BigTech. Pressure is something the financial industry has to be very wary of in migrating to more platform-based businesses.