**Open Finance**

**Open finance should go hand in hand with efforts to strengthen the EU framework and supervision on data protection.** We have strong concerns whether the current EU framework on data protection has enough resources to properly address and respond to the risks associated with open finance. Certain fundamental rights such as: data control of the data subject become an illusion if proper supervision and European coordination is limited (due to resources or inadequacies in the legal framework). Furthermore, rules in order to protect the data subject do not always play out as they were intended. Despite the possibilities for private persons to retain or obtain their right based on the GDPR, this will not have the desired effect in a considerable amount of cases. There are several reasons for this: consumers often do not understand what happens to their data or do not have an overview, it is difficult for large groups of individuals to achieve their rights in a vertical dependence relationship with a large institution and consumers often do not like it or find it too cumbersome to dive into the matter so they can get their right. A way to overcome these issues is to strengthen the GDPR framework. Possible ways to do this is:

* Require organizations to develop **meaningful consent** procedures and processes, so that it provides overview and insight, and certain private settings should be easy to adjust.
* Focus more on whether an organization has a **legitimate interest** to ask and obtain
* Enhance supervision with regards to the **journey of the data**. With journey we mean: is it sold to third parties, is it removed and ‘cleaned’ in a proper way, how is it stored, etc. If do not strengthen these fundamental pillars for decent use of data, we might and up creating some sort of data jungle in which it hard to determine where things went wrong and whose responsibility it is.

**Additionally, there is a strong need for an adequate basis within the EU framework for cooperation and a basis to exchange confidential information between different types of sectoral regulators / supervisors**, such as competition authorities, data protection authorities and financial regulatory and supervisory authorities. Our current EU framework has a so-called closed system for sharing confidential information. This means that confidential financial information can only be shared with other financial authorities that have equivalent mandates and frameworks. In the digitalized environment we believe this system outdated.

* For example: the current EU legal framework makes it difficult to share IT incidents / information on possible IT vulnerabilities with other supervisors and agencies. This results in situations where a data protection supervisor is aware of a possible IT incident or inadequate operational and IT risk management at a financial institution, while the financial supervisor is not. Furthermore, under the NIS directive there are agencies/supervisors for critical digital infrastructure. If they have information on vulnerabilities they should be able to directly share that information with supervisors of institutions depending on those digital infrastructure service providers. This is a cross-border issue since data and IT infrastructure as well as capital flows are not bound by national borders.

**Let us draw lessons from PSD II!** By implementing PSD II we came across certain fundamental principles within the different respective frameworks that are at odds with one another, respective authorities should be held responsible to convene with each other in order to provide clear answers to market participants on these matters (on a European level).

* **Example:** **Lesson Learned PSD II**

The past years a lot has been said about PSD II and although it has just been put into force, let us take the liberty to draw an important lesson learned. While people have focused on implementing PSD II and trying to deal with what is and what isn’t allowed in processing personal data. Fundamental questions regarding the interplay between financial services and data protection regulations have hardly been answered. And this interplay is not just bound to PSD II, but is relevant to the whole retail domain of the financial sector. Yet besides companies dealing with GDPR, we see and hear very little about the overlap/interplay of both types of regulations. Why is this so relevant? Well because in some cases both regulations strengthen each other and in some cases they tend not to. Sometimes the interests regulations are to protect are odds with one another:

* think of the principle of consent and purpose limitation vs. the financial duty of care. The duty of care requires financial institutions/advisors to collect as much information on individual as possible in order to get a complete picture of its clients’ needs. From a data protection perspective: a client might not want to share certain types of data (consent) or the purpose limitation may restrict a financial institution from using types of data that might not have a direct relevance (at first glance).
* Now let’s take the same privacy principles vs. internal controls of the business (an important principle in our financial regulatory frameworks). Based on the ability to predict certain patterns as set out in the example, doing this on a large scale could make certain risks assessments more accurate (requirements under CRD, liquidity ratio’s etc.). But again it could be difficult to do this in accordance with the GDPR.

What do we learn from this? Apart from the teaching about the interplay between retail financial services regulation and the framework on data protection there is another important lesson. In our day-to-day work in applying rules of both frameworks we are forced to interpret fundamental values on which these frameworks are built. These type of interpretations play an essential role in constructing a framework of principles on ethics in AI that have effect in practice.

**Could *Open Finance* be the Trojan Horse for BigTechs?** Although Open Finance could make room for all kinds of new business opportunities we wonder how the possible future impact is assessed and whether there is a risk of dominant tech companies becoming more powerful to the detriment of smaller competitors and diversity of the market and ecosystems. In order for the EU to find new ways to look at dominant market positions we would recommend not to just look at a certain market in which a certain market player can be dominant, but also look at this principle from an ecosystem angle.