Data utilization and data security– an unequal challenge for Europe

At the end of 2017 a BBC reporter registered in the Chinese surveillance system – 7 minutes took his walk until he was identified by omnipresent cameras and surrounded by the police. The US government demands cloud providers to deliver collected data from foreigners (me/you) from abroad (e.g. Europe) (Supreme Court decision is outstanding). Europe, in particular the EU and we believe that the control over one's own data is a fundamental democratic right.

How does this fit together and what are the consequences for our companies?

To generate tracing-performances like in China biometrical data of own and foreign citizens must be stored, area-wide surveillance must be assembled and most modern face recognition technology must be employed. China`s almost self-evident claim on all data of Chinese companies fits into this consideration. Also, the goal expressed at the 19th convention of China's communist party in October 2017 to introduce a social credit system for the well-behaviour of its citizens matches the Chinese picture of data usage and data protection.

Anyhow, the idea, to centrally delete my own data, like the idea to decide independently who can access it does not fit in this consideration. Thus, we must also worry that Chinese companies, by taking over European ones (like German medium-sized enterprises, Scandinavian car producers or EU Banks and Credit card providers), deliver data collected directly to the Chinese government. Chinese companies making business in Europe (like Alibaba or Bike rentals) are capable of using this data already without sparing a thought on European data protection standards (see EU-Data protection act). Europe must control this and demand reciprocity from China. Probably this is an illusion.

Fact is that clouds are booming: central software-maintenance, renting instead of buying and practically unlimited storage space, but also centrally guaranteed data protection provided by the best specialists in software industry are arguments explaining clouds` triumph. Especially US giants like Amazon, Google, Microsoft and Apple fight for market dominance. These companies recognized the platform idea, the sharing economy, the business potential of data availability and big data early and adopted it.
They are all tracing our data. Who else owns more biometrical data than these Internet giants with all their users verifying themselves via finger prints and voice recognition? This data is crucial for our private sphere. As long as the USA accept the European basic right on its citizens` data privacy, the data dominance of US enterprises is merely a competitive challenge for Europe and its companies. If, on the other hand, the USA do not accept

European data protection and allow no reciprocal legislation, we Europeans and our companies face an unequal challenge.

The creation of a general framework on data usage, data which is today the raw material for of companies' business models, is a political challenge:

Data from European citizens and companies can only be utilized according to European data protection legislation (EU Data protection legislation starting May 2018). All over the world. The political challenge is not only to implement data protection regulation with high sanctioning for European enterprises.
At the same time it must guarantee that these regulations are kept by other countries and their companies. Otherwise competitive disadvantages threaten: Our production and market data surpass EU-borders, are linked worldwide, processed into algorithms and are available to anybody but European companies. European artificial intelligence applications lose out on competitiveness (lacking data) and we must repurchase the data processed in algorithms for robot control, marketing campaigns etc. costly.
A second political challenge consists in cyber-security. Tangible property enjoys strong legal protection; there is visible presence of the police to protect property. However, data is stolen by hackers, not by thieves. Stealing data appears to be a trivial offence. A trivial offence that, believing mutual accusations, is being protected or at least tolerated by governments!

As long as data ownership is materially and judicially not equal to tangible property, we must not talk about data protection at all. 72% of Austrian enterprises reported in 2017 that they were target of cyber criminality. It is the modern form of industrial espionage that is today also targeting processes and client data. But where is the police? Where are the tracing achievements? It seems as if companies must protect themselves just like in medieval times.

Data usage and data protection are a question of competition.

Which technologies can guarantee data protection and data utilization? Why do other nations exhibit such technological advantages that make us feel as if we are facing such an unequal challenge in protecting our data and utilizing it for business?

We wonder how far web competition is a global or regional affair. In western societies we discuss net neutrality, namely the question whether any fee can be charged for superior data connection.
Meanwhile, the more decisive question is whether free internet access is preserved only in some countries and nationally restricted in others. For Europeans a selective ban of network services is inconceivable. In Russia, China and other countries this is common practice. Google, Twitter, Facebook etc. are either banned or filtered by the government. Thus, the internet is neither global nor neutral. Some countries allow net information available for all while others take and give information selectively. They have a firm grip on the internet and its information, as can be seen from current protests in Iran.

This can be motivated politically, but in many cases has a commercial background, to protect the own enterprises or data. Hence, the greatest competition for American internet giants is coming from China. What would have happened if Google, Facebook & Co had open access to the Chinese market like in Europe? The one-sided opening and access to the internet is harming those who are committed to free access and limited data usage: our European enterprises.

In consequence, the question arises: How can we protect our data according to our European regulation? In this respect, payment systems will play a central role: the more financial data on clients and businesses is retrieved by foreign providers, the less Europe knows about itself. Not only Swift, PayPal and the Credit card industry (e.g. the Europeans sold their Visa shares in 2015) have their seat outside Europe, new competitors are once more mentioned internet giants (all of them bought European banking licences and, partly, are already active, for example Apple Pay).

To keep our European financial data and information according to our data protection principles, a collective and superior European payment system is elementary. Again it seems, that Europe is offering the entire world self-servicing in the European data household (see PSD2 guideline) while failing to demand reciprocity concerning data protection. However, a superior inner-European payment system which is building up on SEPA and – new – instant payment, is attempting to foster European transactions. The engine driving this project is the ECB.

Equal conditions on data utilization and security are fundamental for Europe`s future

If Europe fails to establish competitive parity concerning data utilization and protection our companies will fall behind: in financing (who owns data for credit assessment?), in marketing and sales (who knows clients and clients behaviour in the future?), in the, for Europe important, automatization and robotization (Who owns big data to constantly enhance Artificial Intelligence?) and in the access to foreign markets (who is getting a China visa after a critical China comment in the future?).
The digitalization is challenging our politicians, especially those of the EU. It is demanding for all of us – with exciting challenges for everybody delighted to accept them!!

We wish you a successful 2018!

Dr. Hannes Enthofer Patrick Haas
Partner Finance Trainer

Luxembourg, 8.1.2018