

Moving Europe forward – a strong single market for citizens, businesses and banks

The German private banks' EU policy positions
for the 2019-2024 legislative term



Brussels, November 2018

4. Digitalisation – Europe as a centre for the “banking” of tomorrow

Banking is unquestionably about to undergo a sea change. If Europe is not to be left behind by developments in third countries, then here, too, we need a single European market, whose size can produce internationally competitive pan-European companies. New rules will have to be developed at European level from the outset, since digital applications know no borders.

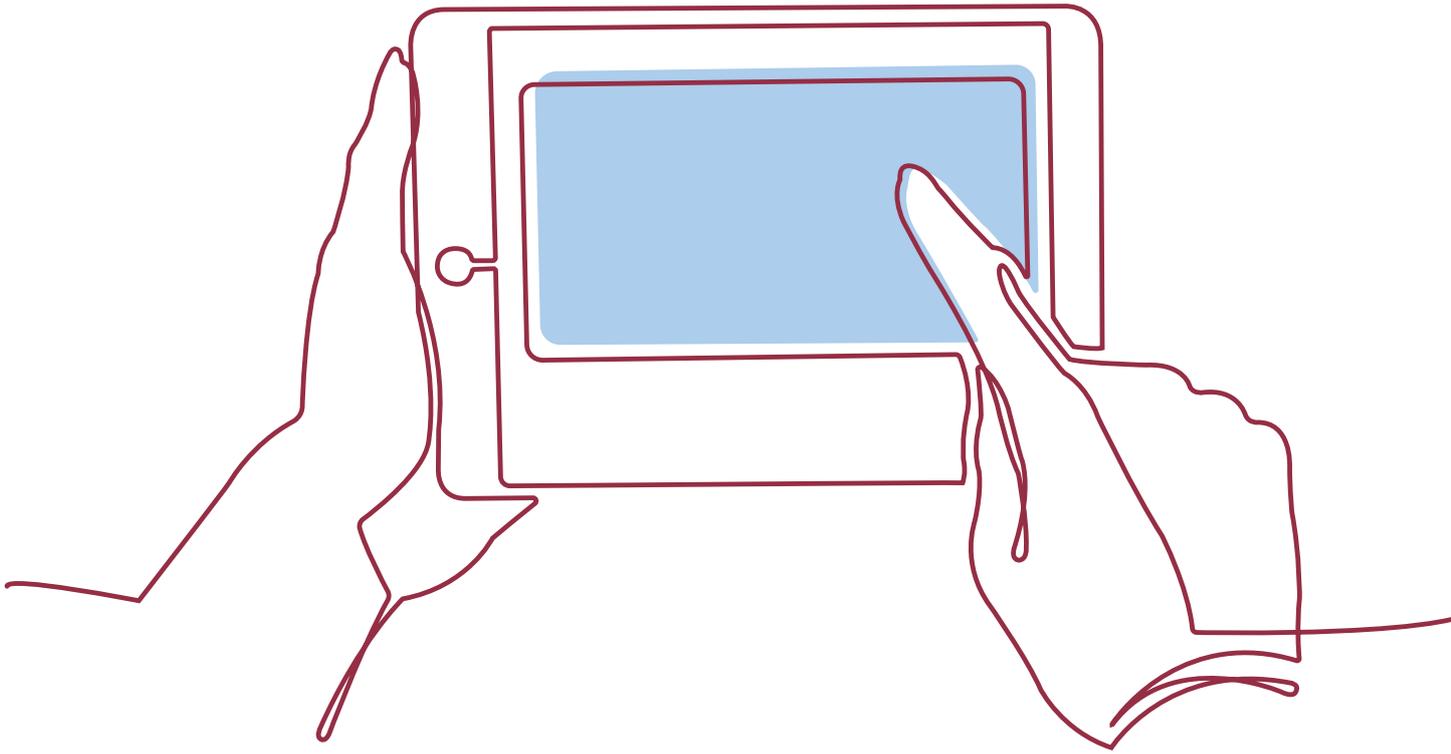
Rules for a single digital market: European and technology-neutral

To avoid being left behind by other economic regions or newly emerging markets, we need to create an innovation-friendly environment throughout Europe for the “banking” of tomorrow. Europe must hone its profile as a centre for digital excellence. There is also room for improvement in teaching the basics of information technology in schools. The number of workers needing this rudimentary knowledge to survive in the workplace will steadily rise. To tackle this problem, we should promote both basic IT skills and continuous on-the-job training at national and European level.

At present, there is often a lack of Europe-wide impetus and standardised rules for new technologies. What is true in

general, also applies to the single digital market: new rules and standards should not fragment the European market. At the same time, new rules must be not only uniform throughout Europe, but also technology-neutral so that they can be adapted to rapid changes in products and technologies. New market participants bring fresh impetus and boost competition. We warmly welcome this, as it increases the range and quality of services offered to customers. It must, however, be ensured that competition is fair and does not come at the expense of customers’ security. It is therefore essential that the same rules should apply to all providers of comparable products and services – be they banks, fintechs or bigtechs.

The primary focus should be on the big international internet platforms: they dominate digital communication and social media and infrastructure in Europe, hold large amounts of data and, through their customer interfaces, are gaining increasing influence over other industries. There is a threat of competitive distortion if market participants are not treated equally. It is unacceptable, for example, that the Payment Services Directive (PSD2) requires banks to make their customer data available to third parties via an interface, while big data companies can benefit from this but do not



have to grant access to their ever-increasing collections of data. Regulatory asymmetries to the detriment of banks run counter to the principle of fair competition and should not be tolerated.

It is surely in the interest of the EU to retain the right to decide how new technologies are used, especially where fundamental social values such as the right to personal data are concerned. This can only be achieved if the EU becomes a leading centre for digital technologies.

Data protection – strike a balance between protection and innovation

Uniform data protection rules across Europe are a prerequisite for an effective single financial market. It is therefore essential to ensure that the new European General Data Protection Regulation (GDPR) is now uniformly implemented and interpreted in member states. Guaranteeing data sovereignty and transparency is an important ancillary condition. Maintaining customer confidence in data security while at the same time offering up-to-date and user-friendly applications is, after all, a critical success factor for banks. A high level of data protection, both accorded by law and

applied in practice, should therefore be seen as a locational advantage. Nevertheless, data protection should not act as a brake on future business models, but should facilitate them, and should be continuously refined to accommodate new technical possibilities. High legal standards must not be allowed to put paid to technological innovation from the outset.

It is debatable, with this in mind, whether the principles of data economy and strict purpose limitation in European data protection law are really appropriate given the current pace of innovation and the huge potential of big data. Do they perhaps, instead, cause opportunities for customers and providers to be wasted in a way that does not happen in other parts of the world? In a global data economy, data protection must also be judged by its ability to avoid placing excessively high barriers in the way of new business models. On no account should it encourage providers to migrate offshore. A balance therefore needs to be struck between the ability to innovate, on the one hand, and sensible and effective data protection, on the other. It is crucial that customers have transparency and clarity about how their data will be used. We should not, however, overwhelm them with a flood of information which may ultimately be ignored.

The German private banks therefore recommend an approach that is tailored to the needs of the customer: customers should be informed transparently and concisely about what data will be used by whom and for what purpose, about whether the data will be passed on to third parties and about where the data will be stored.

Strengthen cybersecurity

Not only banks are increasingly exposed to cyber risks – cybersecurity has become a key issue for society as a whole. Banks, which store and process sensitive data, have long protected themselves against such risks and continue to refine their standards. In addition to the state-run points of contact to which cyberattacks can be reported, there is also a need to promote other platforms where companies from all sectors can exchange information. This would enable stakeholders to consolidate their efforts more effectively, would increase efficiency and would further boost protection against attacks. On top of that, cross-border cooperation should be enhanced in the field of cybersecurity, both within Europe and beyond.

Make digital onboarding possible

The uneven implementation of anti-money laundering rules makes it difficult for a firm to acquire and onboard new customers throughout Europe. Not only do the identity documents accepted for verification purposes vary from one member state to another, but the security features of identity documents differ too. Different member states require the collection of different know-your-customer data, some of which not all consumers in the EU even have at their disposal. To make matters worse, the data collected differ not only from one country to another, but also from product to product (current account vs. securities account,

for example). As a result, the “passporting” of verification methods, meaning their cross-border use across the internal market, is only possible to a very limited extent.

We are therefore in favour of user-friendly, innovative and standardised KYC processes for the EU internal market. This will require a common decision on what KYC data should be collected, the standardisation of identity documents which can be used for verification purposes (including their security features), and the specification of a standard EU identification feature (number or certificate). EU countries need to be open to new verification procedures that have been approved in another member state and can therefore be deemed sufficiently secure (principle of “most favourable treatment”): there should be uniform criteria for allowing KYC processes that have been carried out in accordance with EU law to be reused elsewhere. The Association of German Banks therefore welcomes the establishment by the European Commission of two high-level expert groups to investigate regulatory obstacles to innovation in the financial markets and analyse electronic identification and remote KYC processes. It is to be hoped that their findings will give rise to further projects in the new legislative period.

Make access to (cloud) outsourcing simple and legally certain

We are in favour of creating uniform EU-wide definitions of, and guidelines for, outsourcing. The guidelines should include concrete examples of what does and does not constitute outsourcing from a regulatory point of view. The European Banking Authority has launched a review of the 2006 CEBS (Committee of European Banking Supervisors) guidelines on outsourcing. Updated guidelines are scheduled to take effect in the course of 2019. They are intended for use by national supervisors and (for the first time) by banks subject

to the Capital Requirements Regulation (CRR). In principle, we welcome a revision of the CEBS guidelines, but would prefer more binding, EU-wide rules on outsourcing in the form of technical standards, for instance. The definition of outsourcing needs to be tailored specifically to banks. It would be helpful, in addition, to describe various concrete cases of outsourcing, thus making it possible to identify beyond doubt when a situation would need to be classified as such.

We also recommend a European licensing requirement for cloud service providers wishing to offer their services to financial institutions. To obtain a licence, the provider would have to demonstrate that it met European requirements for outsourcing. This would ensure that each individual bank did not have to invest time and money in checking the cloud service provider itself. Licensed services would comply with European standards and could be used throughout the EU. Central licensing would, moreover, make the use of cloud services less expensive for customers.

Facilitate the exchange of experience in a sandbox environment

We recommend creating a European sandbox, where financial services providers and supervisors could exchange experience and views on new technologies and business ideas. The sandbox should be located at European level to give it an overview of the entire EU market. It should be open to all innovators, i.e. banks and fintechs alike. Market participants would have the opportunity to develop innovations and discuss them with supervisors at an early stage. Supervisors would gain rapid insight into market developments. Both sides would thus be able to learn and benefit from each other. In a second step, limited test phases could be conducted in which supervisors had the option of applying certain requirements less strictly or not at all

without lowering the level of security for customers. All market participants should have access to the sandbox in accordance with the principle “same business, same rules”.

Promote forward-looking technologies: distributed ledger technology/initial coin offerings

For new technologies such as distributed ledger technology (DLT), it is especially important to develop robust, competitively neutral standards at European level. Otherwise, European banks risk being left behind by these developments.

The most common application of DLT in the financial markets at present is initial coin offerings (ICOs). In 2017, the amount invested in ICOs significantly exceeded traditional venture capital investment. It is becoming apparent that this form of crowdfunding initiative involving the issue of digitalised assets, rights of use or stakes in a company in the form of coins or tokens will grow further.

Views across Europe differ, however, on the legal classification of ICOs and their tokens. This will give rise to considerable civil and criminal law risks for all parties involved. It is therefore vitally important to create a robust legal and regulatory framework for both investors and token-issuing companies without delay, or at least to harmonise supervisory practices with the help of the European supervisory authorities. The Association of German Banks considers the current inertia the wrong approach, not least with investor protection in mind. This is not how to respond to the rapidly progressing digitalisation and tokenisation of services and assets, nor will it allow us to fully exploit the potential unlocked by the digitalisation of very different kinds of processes and services.

As for the use of DLT, which normally forms the basis for creating these tokens, we see a need for dialogue on, and for an adjustment of, the national civil law rules and regulations governing securities. Beyond these considerations about securities, there is also a need to analyse other possible applications of DLT and develop a taxonomy for new digital products that can be generated as tokens. It is important that this debate takes place in a highly regulated environment and with the involvement of financial supervisors. Discussions should begin right away on possible legal solutions and a suitable regulatory framework for the use of DLT and for trading in products which DLT applications may give rise to and which are unregulated as things stand.

Digital payments: more competition needed

The European Commission is pursuing an ambitious growth target of creating a single digital market for goods, people, services and capital as part of its Europe 2020 strategy. Major prerequisites for achieving this single market are the promotion of mobile payment solutions with a wide reach and more competition between payment methods in e-commerce.

Mobile payment methods enable consumers to pay quickly and easily. Particularly for direct transactions between private individuals (P2P) and at the point of sale (POS), mobile methods offer an efficient, convenient and widespread alternative to traditional means of payment. They have a high level of acceptance and coverage, and at the same time are extremely secure. Essential infrastructures and technologies for processes such as authentication (e.g. by fingerprint scanner) or data transmission (e.g. by near field communication [NFC]) should be open to all payment service providers.

In e-commerce, consumers are offered various payment methods, which meet very different standards with respect to cost, security, liability and the commercial use of data. In major e-commerce segments, moreover, consumers and merchants have only limited freedom of choice when it comes to payment methods. We need clear, Europe-wide standards for payments and fair competition between payment methods and between providers. —