Comments

of the German Insurance Association (GDV)[1]

ID-number 6437280268-55

on the European Commission's Consultation Document

"FinTech: A more competitive and innovative European Financial Sector"

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, D-10117 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brussels
Phone: +32 2 28247-30
Fax: +32 2 28247-39
ID-number 6437280268-55

Contact:
Dr. Klaus Wiener
Member of the Executive Board
E-Mail: k.wiener@gdv.de

Dr. Anja Theis
Economics
E-Mail: a.theis@gdv.de

www.gdv.de

[1] The Berlin-based German Insurance Association (GDV) is the federation of private insurers in Germany. Its 453 member companies offer comprehensive coverage and retirement provision to private households, trade, industry and public institutions through 431 million insurance contracts. With a total investment portfolio of over 1.5 trillion euros German insurers are the most important institutional investors in Germany. The German insurance industry moreover provides employment for 524,000 persons either as employees with insurers and in the intermediation business or as self-employed insurance intermediaries and advisers.

The German Insurance Association (GDV) welcomes the opportunity to provide input to the European Commission's consultation paper "FinTech: A more competitive and innovative European Financial Sector". Digitalisation and the use of new digital technologies are of great importance for the insurance sector. Potential benefits of FinTech applications in the insurance market ("InsurTech") include enhanced products and services for customers and additional ways to access insurance. InsurTech could also substantially contribute to a further risk prevention and risk reduction, to the benefit of private households, businesses and society as a whole. Therefore, we very much welcome the Commission's initiative and its efforts towards a regulatory framework that is innovation-friendly while at the same time ensuring high standards of consumer protection and financial stability.

The Commission's approach to base its policies regarding FinTech on the three principles of technological neutrality, proportionality and market integrity is supported by the German insurance industry. We also share the Commission's understanding that "FinTech" is not confined to start-ups based on new technologies but comprises any use of new technologies in business processes in the financial industry, regardless of the type and size of provider. With respect to market integrity, we believe that transparency is only one aspect and that high levels of consumer protection in general and the avoidance of systemic risks are also indispensable.

That said, the German insurance industry would like to highlight the following points:

- The most important contribution of the EU to foster FinTech innovations is to **avoid overregulation** and ensure a **level playing field between incumbents and new market players** so that market forces can work to the benefit of consumers and the competitiveness of the European financial system. Should supervisors want to make available innovative regulatory tools, then it is crucial that they are accessible to all market participants, independent of company type or size.

- We believe that adequate supervision of all FinTech providers is essential in order to ensure high standards of consumer protection and financial stability. **For the insurance industry, a comprehensive regulatory framework is already in place**. We expect the established standards to also guide oversight activities regarding new technologies and new providers in the market.

- In order to avoid unnecessary bureaucracy and to make innovation possible, **the principle of proportionality** must be consistently applied to both incumbents and FinTech start-ups.

- In addition, **regulatory barriers that unnecessarily impede FinTech should be reduced** at all levels, for example regarding paper requirements (e.g. in the new Insurance Distribution Directive) or overly strict requirements in case of outsourcing.

- The European Commission and the ESAs have an important role to play regarding FinTech, e.g. by closely monitoring and analysing developments and by ensuring that national FinTech initiatives are in line with the European regulatory framework. However, currently **we do not see the need for a European regulatory sandbox**.

- Regarding FinTech activities in the insurance sector, on European level, **EIOPA should be the responsible authority**, irrespective of whether newcomers or established insurers are concerned. Given the distinctive features of the insurance business model, it is vital that the responsible European supervisor has independent expertise in the field of insurance. Direct supervision must be conducted on national level by the national supervisory authorities which know their markets best.

- In view of **data protection, the future General Data Protection Regulation,** which applies from May 2018 onwards and regardless of technology, will provide an **effective framework** to meet the challenges that come from the use of new technologies and the protection of natural persons with regard to the processing of personal data. It is of further great importance that consumers are strengthened in their **freedom of disposition regarding the data created by them or at their request**. Notably, the internet of things raises urgent questions, e.g. who may access connected vehicles, smart homes or other connected devices.

- In order to ensure fair competition and to enable growth in the **data value chain**, an **appropriate and proportionate framework for data access and (re-)use** is needed. **Inappropriate concentration of data based market power** needs to be avoided. In particular, there should be a continuous evaluation of potential market disruption in multi-sided markets (e.g. regarding telematics data of car manufacturers).

- **Cybersecurity** is rightly seen as a priority and prerequisite to the widespread use of FinTech. **For the German insurance industry,**

a comprehensive framework for IT security is already in place. In general, a consistent approach is needed in working out guidelines and standards necessary to comply with legal obligations. The competent authorities need to find a harmonised approach, including authorities for cybersecurity, data protection and financial supervision.

Our detailed comments on the European Commission's consultation paper on FinTech can be found in our response to the Commission's questionnaire. We would like to invite the Commission services to contact us should further explanations be helpful. We hope to engage in an active dialogue with the European institutions on this important and fast evolving topic.

Berlin/Brussels, 15 June 2017

Annex: Answers to the Questionnaire on FinTech

1. Fostering access to financial services for consumers and businesses

1.1	What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

In the German insurance industry, almost all the activities in the value chain of insurance – be it client relations, underwriting, or claims management – are impacted by the digitalisation of economy and society. The use of FinTech by insurers has been steadily increasing over the last years. For InsurTech – the use of FinTech for the provision of insurance services – all the available FinTech applications are relevant, e.g. big data, artificial intelligence, sensor analytics and making use of the internet of things. The motivations for InsurTech usage are manifold, in particular expanding access to insurance cover, enhancing quality of products and services (e.g. providing solutions that are better tailored to an individual's situation), improving risk management and increasing cost efficiency (e.g. process optimisation).

We expect the role of new technologies to grow substantially, and the insurance industry has a good track record supporting new technologies in a a responsible and secure way. Which specific applications of InsurTech will prove successful and how widespread their adaptation will become in the German insurance market, however, is difficult to say at the moment, as we are still only at the beginning of this process. This will depend on various factors, e.g. the attractiveness of innovative product offerings to consumers, consumers' willingness to provide additional data as well as the effectiveness and additional value of innovative InsurTech uses compared to traditional solutions (e.g. regarding better risk assessment or cost savings). Fully automated decisions may increasingly become possible in some areas in the future. At the same time, the associated challenges, such as transparency regarding very complex algorithm decisions or the risk of failure in data or algorithms, will have to be handled. The speed at which the latter can be achieved will also influence how soon business activities imagined possible for the future will be implemented.

We believe that FinTech applications have great potential regarding financial services and in particular insurance provision. However, FinTech might not always provide better solutions than traditional practices and it is certainly not without cost. Building up FinTech capabilities and expertise requires significant investments, and it involves substantial maintenance costs (e.g. regarding cybersecurity).

Artificial intelligence and big data analytics for automated financial advice and execution

1.2	Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.) and at what pace? Are these services better adapted to user needs? Please explain.

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

For the insurance sector, there are indications that automated advice can reach new customers and extend access to insurance, in particular to consumers who are sceptical about a face-to-face consultation, open-minded to new technologies and price-conscious. However, the development is still in its early stages. For example, in the German market, InsurTech start-ups that are registered as insurance brokers do not offer any purely automated advice. Rather, they are insurance brokers who have digitised their business processes extensively. However, even brokers that apply highly sophisticated robo-advice solutions provide their customers with the option of personal advice in the form of chats or by telephone. Frequently, an automated advice process is offered, which can be supplemented by telephone or chat. Significant acceptance of this model can currently be found in the field of motor insurance.

The extent to which purely automated advice can better respond to the needs and demands of consumers depends decisively on the data base determined by the advisory tool as well as on the algorithms it is based on. One limitation is that automated advisory tools are not empathic. Also, automated advice will often reach its limits in the case of more complex insurance products and consumer needs that make extensive and personalised explanations necessary.

Regarding the entire topic of automated advice, we also refer to our answer to the discussion paper on automation in financial advice by the Joint Committee of the European Supervisory Authorities (JC 2015 080, 4 December 2015).

1.3	Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place? What could be effective alternatives to such a system?

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

We believe that adequate oversight of the use of artificial intelligence is crucial in the context of financial services. For example, when insurers use artificial intelligence in deciding on what risk level to associate with a product or an activity, they depend on the quality of the data, reliable algorithms and valid calculations. Otherwise, conclusions and predictions could be based on false assumptions, which could in turn lead to inaccurate underwriting and risk classification.

However, in the insurance industry, drawing on extensive data and using highly sophisticated methods of data analytics has been common place for many years. Thus, comprehensive regulatory and self-regulatory safeguards are already in place.

Quality and accountability of the data as well as the validity of mathematical formulas are part of the legal obligations of insurance companies. The same is true for the quality of distribution services and the qualification of insurance intermediaries. These established standards should also guide oversight activities in cases where algorithms using artificial intelligence are applied. While there is the risk of faulty algorithms, there are many opportunities in new technologies which are able to process large amounts of data, improve by self-learning or find new and valid correlations, thus generating valuable insights, e.g. for probability calculations. Therefore any supervisory activity should not aim at preventing the use of such technologies but instead foster valid and scientifically sound data analytics, including the use for customer advice, internal risk management, risk assessment and claims handling. Reliability of algorithms and fault-free functioning of new technologies is in the best interest not only of customers and a fair market but also of the insurers themselves in order to base their business models on sustainable grounds.

The transparency of algorithms used in new technologies such as big data or artificial intelligence has been disputed, especially with regard to self-learning machines or programs and the undetermined outcome of data processing. In principle, oversight of the insurance industry extends its

control to mathematical functions. However, it might prove difficult in the future to comprehensively assess how data is processed in algorithms deployed in new technologies. We believe that data processing must not be a black box but has to be compliant with common supervisory standards regarding data quality and mathematical validity. There needs to be an open discussion on how to best safeguard the high standards in the insurance industry, especially with regard to the use of data with no history of proven insurance relevance or with regard to non-insurance companies using data generated by their users, platforms or devices without any scientifically proven correlation to insured risks for insurance-related purposes. At the same time it needs to be noted that limitations in transparency of big data and/or artificial intelligence should not hinder the implementation of new technologies which might prove beneficial to risk assessment, insurability and access to insurance.

Future risks may emerge with the growing prevalence of artificial intelligence as well as further technologies that can involve artificial intelligence, such as robots. At this early stage though, for the insurance industry the current regulation, for example with regard to liability, is sufficient. Regulators should focus on abuse and malpractice cases for the time being. Lessons drawn from and actual needs defined based on this should guide any future thoughts regarding regulatory reform.

The same is true with regard to data protection issues. The new framework on personal data protection, with the General Data Protection Regulation (Regulation (EU) 2016/679) as its key part, will bring rules to provide a sufficient level of transparency for consumers. Companies have to inform consumers about the existence of fully automated decision making and have to explain the consequences and the underlying logic of such a fully automated data processing.

1.4	What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

In our view, due to the wide range of potential uses of algorithms (e.g. different applications, products and services, different types of consumers) a general answer to this question is not possible.

1.5	What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

As any technological progress, the ongoing process of digitalisation and in particular the increasing application of artificial intelligence and algorithms is, of course, not free from challenges and potential risks. Artificial intelligence and big data analytics certainly mark a new dimension of data usage and bring with them new questions and challenges. Examples are the question of adequate transparency regarding very complex algorithm decisions or the risk of failure in data or algorithms that has to be handled.

For the insurance industry with its long experience of extensive data usage and advanced methods of data analytics, comprehensive regulatory and self-regulatory safeguards, e.g. regarding data protection or the quality of the data, are already in place (see also our answer to question 1.3). Regarding the German insurance market, so far we do not have any indication that there might be potential detriment to any group of customers or providers. However, in view of the crucial importance of adequate insurance cover for the financial security of consumers, the German Insurance Association is continually monitoring the situation in the market. We also believe that supervisory authorities should closely monitor developments.

Social media and automated matching platforms: funding from the crowd

1.6	Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding?

- – Yes
- – No
- ✓ Don’t know / no opinion / not relevant

1.7	How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?

no direct relevance for insurance provision

1.8	What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

no direct relevance for insurance provision

Sensor data analytics and its impact on the insurance sector

1.9	Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

The new technologies and enhanced possibilities for collecting and analysing data have great potential for insurance provision. Sensor data analytics makes it possible for the first time to directly take into account risk-relevant behaviour during the term of the policy and to design corresponding "usage-based" insurance products. The possibility to monitor and understand risks better opens up new opportunities for enhanced insurability, better risk management and risk reduction. Insurers can take advantage of these opportunities to support policyholders in taking precautionary measures. For example, in the field of building insurance, intelligent building technology ("smart home") could help detect tap water damages and close the water supply valves, preventing major moisture damage. In motor insurance, policyholders could get feedback on their driving, helping to reduce accidents and improve road safety. Life insurers could support policyholders – including those with preconditions – to optimise their health status (improve, stabilise or slow down deterioration), thereby opening up new insurance options.

Currently, the use of sensor data analytics is at an early stage in the German insurance market. The most important application so far is in motor insurance: A number of German insurers are offering product variants that include telematics data on driving behaviour in the calculation of premiums, in addition to the common risk characteristics, often enriching their offerings with additional services. Another example is making use of intelligent building technology for home insurance building and household insurance. One life insurance product uses information generated with data of wearables and fitness applications. However, the market share of all these usage-based products is still low. As most of them have only recently come onto the market detailed experiences are not available yet. So far, there is no evidence that usage-based products displace traditional products. A sophisticated segmentation of policyholders according to risk clas-

ses has already been common practice in many business lines of the German insurance market for some time, in particular in motor insurance. Hence, the potential of further risk classification might be smaller in Germany than in some other countries.

In addition, customer acceptance is crucial. Here, we observe a wide range of consumer preferences. In a survey commissioned by the GDV from November 2016, 25 % of respondents replied that they can imagine taking out an insurance contract based on telematics. 67 % of respondents agreed that careful drivers should pay less than speeding motorists. Additional information can be found on the GDV's homepage.

One important challenge regarding the new possibilities is ensuring data protection and cybersecurity. In view of data protection, the future General Data Protection Regulation, which applies from May 2018, will provide an effective framework to meet the challenges that come from the use of new technologies and the protection of natural persons with regard to the processing of personal data. Especially, companies will be obliged to perform a data protection impact assessment when they implement new technologies which are likely to result in a high risk to the rights and freedoms of their customers. At the same time, in an increasingly interconnected world, the threat of cybercrime will continue to increase. This affects all types of companies and company sizes, not only the insurance industry. This is why small and medium sized enterprises need to strengthen the protection of their IT and invest in IT security. The demand for cyber insurance is also becoming more and more important and the existing offers and demands for cyber insurance will continue to grow. In Germany, efforts have also been made to strengthen the security of internet of things / smart home products to make it possible to include them in building and household insurance. German insurers are in contact with the legislator concerning the cybersecurity of these products and have developed possible solutions that the legislator could adopt.

1.10	Are there already examples of price discrimination of users through the use of big data? Can you please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

- Yes
- ✓ No
- Don't know / no opinion / not relevant

Though the use of big data is at an early stage in the German insurance market, there are already some examples where this has resulted in an

extension of risk segmentation, e.g. telematics products in motor insurance (see also answer to question 1.9). However, more individualised insurance pricing is by no means inconsistent with the collective principle of insurance and does not represent price discrimination in the sense of unfair and unjustified differentiation between customers. Private insurance has always been risk-based. Today, most communities of insureds are already composed of different risk classes, while the risks are still pooled across all policyholders and risk classes. Risk-based premiums are of key importance to the effectiveness of private insurance markets: They enable tailor-made insurance solutions and provide incentives for risk reduction. They also prevent adverse selection effects with regard to the conclusion of insurance contracts. Without risk differentiation policyholders with high risks might seek out especially high insurance cover whereas potential customers with low risks might buy less insurance or even abstain from taking out insurance at all, impairing risk pooling. Therefore, risk-based pricing is also a prerequisite for insurers' financial stability and reliable insurance cover for customers.

Taking individual risk behaviour directly into account can also help setting fairer premiums. For example, young and responsible drivers, who do not yet have a history of accident-free driving, could benefit from lower premiums because careful driving will become traceable.

Moreover, more granular risk segmentation does not necessarily result in less access to insurance cover for customers who want to insure higher risks. It has always been more difficult and/or more expensive to obtain insurance for very high risks, because the likelihood that the insurance benefit must be paid out is so much greater. Big data may in fact make insurance easier for these cases, as the availability of more data (especially when little to none was available previously) often simplifies premium calculations and opens up new risk management strategies (e.g. additional precautionary measures).

Looking at past advances in risk assessment, more and better data as well as knowledge about the factors influencing risks have always increased the possibilities to provide insurance cover. Also, with improved risk assessment, the need for safety margins in insurance premiums could be reduced and insurance made more affordable. For example, the analyses of extensive data sets together with medical progress have made it possible to provide carriers of the HI-virus with life insurance products under certain conditions. Flood insurance in high risk areas is another example: In Germany, a highly sophisticated system of flood risk classification ("ZÜRS") is in place allowing for near universal insurability even in high risk areas. The inclusion of additional data in 2016 further increased insurability and affordability of flood insurance in Germany.

New technologies, such as big data tools, therefore hold manifold new possibilities, not only for risk assessment, new products and services but also regarding fraud detection and understanding the customer's needs.

As many providers are currently considering the (increased) use of big data tools, this could lead to a further increase in risk classification. The extent of these changes is hard to predict, but it may be limited in many products. Even today, with traditional actuarial methods, highly sophisticated risk classification systems (e.g. highly individualised premium calculation in motor insurance) as well as mitigating measures (e.g. by considering soft facts/underwriting assessments, self-retentions, and other risk management measures) are in place. Furthermore, risk-based pricing is already limited by German regulation in some circumstances (e.g. by the Equal Treatment Directive or the national genome testing regulation). Therefore, the added value achievable by big data usage remains to be seen. As risk assessment and risk segmentation is already quite advanced in the German insurance industry, we believe there will be more of an evolution of current practices than a revolutionary development.

In any case, the German insurance industry endeavours to provide adequate insurance solutions for all groups of the population, both with a view to the responsibility that its role in social risk management brings and to fully make use of the available business opportunities in the German market. When insurance markets are evolving towards increased risk differentiation, this is usually accompanied by insurance providers extending their product range, with the aim of offering tailor-made insurance cover for higher risks instead of simply offering premium products many potential customers cannot afford.

Other technologies that may improve access to financial services

1.11	Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

We believe that mobile computing and the increasing prevalence of smartphones will be a substantial factor in improving access to insurance. In this context, mobile payment solutions can also play a role.

Regarding insurance, there are manifold (potential) applications of the new technologies to improve access to insurance cover and enhance products and services, for example:

- helping customers to prevent losses, e.g. through severe weather-warning apps or by use of data generated from smart homes, smart devices, connected cars etc.,

- creating value-added products with additional services, e.g. assistance in case of car accidents,

- use of Open Data to provide applications such as ZÜRS Public to enable customers to check their risk/insurability with respect to flood insurance,

- improved access to insurance cover by use of location-based data generated from smartphones that enables customers to find a short-term insurance product exactly targeted to their situation (e.g. travel insurance).

Mobile payment solutions may offer new opportunities as they might be integrated in services that are digital throughout and thus fit in seamlessly in digital processes. Security and trust are core issues concerning mobile payment as well as an adequate and proportionate regulatory framework. Legislation should aim at diminishing obstacles to mobile payment services, those offered cross-sector as well as those used within a specific service only. Mobile payment services offered cross-sector should be interoperable. Besides, measures need to be taken to avoid lock-in-mechanisms and to ensure anti-trust compliance.

As mobile computing and the use of apps for smartphones gain more importance in the digital value chain generally, they can bring about more opportunities for the financial industry. However, in this context the aspect of mobile connectivity as well as tackling legal and technological barriers to the use of mobile digital services need to be addressed. Digital identities and secure authentication via mobile appliances and devices need to be taken into view. E.g., where technologies such as Near Field Communication (NFC) could offer the possibility to use electronic identification cards by smartphones, open interfaces need to be strengthened on every platform.

2. Bringing down operational costs and increasing efficiency for the industry

2.1	What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

In the insurance industry, FinTech has great potential to improve risk assessment and contribute to the reduction of risks, making insurance more affordable (see answer to question 1.9). It also offers manifold opportunities for process optimisation.

Improved detection of fraud by deploying new technologies is a further example of potential cost savings for the insured as more fraudulent claims are identified and not paid for (in Germany, current estimates of annual losses from insurance fraud amount to 4 to 5 billion euros in casualty, accident and liability insurance alone).

The annual IT survey of the German insurance industry illustrates the perspectives offered by new technologies such as big data or cloud computing for more efficient processes. Efficient and secure data exchange and other digital services are the foundations of (future) insurance business.

High investments in IT and digitalisation not only lead to more efficient business processes but also generate customer satisfaction (e.g. the option to purchase insurance online, easier and faster claims handling), trust and help prevent data loss or damage. Especially, business processes related to the customer relationship (distribution, underwriting, contract management), payment processes and a growing number of processes in claims handling can profit from digitalisation.

Of course, automation of processes provides the basis for more efficiency as well. Especially completely digital (paperless) processes, e.g. in underwriting or claims handling, promise better and more efficient service and cost savings. Process automation holds huge promise. The same applies for the use of new technologies such as big data or advanced analytics in internal processes, e.g. cash flow.

The need for secure and highly performant information technology and data processing capacity contributes to continuously high investments of the insurance industry. Also, insurers need to make high investments in digitalisation to meet customers' expectations, e.g. concerning secure communication via digital channels. In 2015 the German insurance industry spent 4.41 billion euros on IT. This amounts to an increase of 3.8 % compared to the year before. At the same time gross premium income

increased by only 0.6 %. 30 % of the IT costs are allotted to specialised personnel (1.3 billion euros); hard- and software costs amount to 27.2 % of total IT costs (1.2 billion euros). External consultants account for 13.5 % of IT spending (595 million euros), while provider costs and outsourcing accounted for 18.6 % (820 million euros). New technology, interconnectivity, IT and data security as well as new communication channels require not only investments in hard- and software but also in specialised experts which explains the high percentage of IT costs for personnel and consultants.

2.2	What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

The most important contribution of the EU is to provide a regulatory framework that is innovation-friendly. We believe that giving companies the freedom to implement new technologies and make use of the chances of digitalisation by avoiding overregulation is the best way to foster innovation. The role of the EU as well as of national regulators should be to provide a level playing field and ensure that established consumer protection standards are held up by all providers and risks to financial stability are avoided. Rather than measures which might interfere with market developments, the EU should aim at a common supervisory approach, not only in insurance supervision but also concerning IT security. As security of critical IT infrastructures is of utmost importance, the recently passed NIS Directive provides a proportionate and adequate framework for the member states to implement into national law. FinTechs especially rely on high IT security as they handle very sensitive data.

In many areas, non-legislative measures such as the European Cloud Initiative, where relevant stakeholders assess best practices and develop practical solutions such as standard contracts, will be the first choice on the European level.

2.3	What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

With respect to the implications and challenges of digitalisation for employment in the insurance industry, we would like to refer to the Joint declaration on the social effects of digitalisation by the European social partners in the insurance sector from October 2016.

Main impacts on employment include:

- new / improved skills and resources required in areas like data analytics and data-driven decision making,

- shift of jobs from tasks that are likely to be automated (operations, support functions) in the near/mid-term future to other areas (analytics, product development, digital marketing).

As with FinTech in general (see answer to question 3.2.2), the consequences of FinTech for employment should be closely monitored (e.g. number of employees, qualifications and skills, working conditions). We believe that the EU has an important role here. For example, at the moment, little is known about employees in FinTech start-ups and the relevant working regulations and conditions (including information about participation in employer or employee associations / unions and trade associations). It would be valuable if the Commission were to evaluate these questions and provide the information.

RegTech: bringing down compliance costs

2.4	What are the most promising use cases of technologies for compliance purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

Insurance undertakings have to report a vast number of data to their supervisory authority under Solvency II. Consequently, in a few years undertakings will have submitted huge amounts of data to supervisory authorities and other stakeholders. Therefore, ensuring consistency of these data over time, archiving it and keeping it accessible is a challenge for undertakings which could be accomplished by the use of adequate technologies. The size of the undertaking is not decisive in this regard.

However, one should look at potential use cases for supervisory authorities as well. One RegTech solution could be to provide a platform where undertakings can upload their data sets. The RegTech could automatically validate the submitted data and give feedback to the undertaking immediately. Supervisory authorities and central banks could then access the validated data and use it for supervisory and statistical purposes. This would alleviate the reporting burden significantly as undertakings would need to submit data only once and receive the validation record promptly. Hence, necessary corrections could be made immediately. In Germany, the reports are currently validated twice, by the supervisory authority and the national central bank, which causes delay and additional effort for the undertakings. Another advantage of a supervisory platform as proposed would be that all stakeholders would rely on the same data and inconsistencies would be avoided.

RegTechs could also contribute to downsizing the reporting requirements. Currently, some information requested for group reporting on financial stability are identical to quarterly group reporting under Solvency II – the mere difference being that the former reporting has to be done on a best effort basis and that data has to be submitted three weeks earlier than the latter. If the data were analysed automatically, and therefore much faster, it might not be necessary to request information on a best effort basis earlier. This would also contribute to high quality supervision as supervisory authorities would not need to rely on estimates.

Another aspect where RegTechs should be used by supervisory authorities is technical implementation of reporting requirements. Solvency II requires that reports are submitted using a particular standard, the XBRL. To enable small and medium sized undertakings to fulfil this requirement, EIOPA provided the Tool for Undertakings (“T4U”) free of charge. This is a software to create and validate XBRL instances. However, EIOPA will not support this T4U for future releases of the XBRL-taxonomy. This means that undertakings are forced to either produce their own solution or to buy specific software. It is not desirable that undertakings are forced to contract with software providers solely for the purpose of complying with the formal requirement of using XBRL. Therefore, new technologies should be used by supervisory authorities to maintain the already existing T4U.

The example of the T4U also illustrates what is a major challenge regarding RegTech: RegTech has the potential to become a barrier for small and medium sized undertakings. This could be the case if the regulatory requirements cannot be fulfilled without the use of RegTech or if it becomes a requirement in itself to use RegTech. The development of RegTech can be costly and many small and medium sized undertakings may not have enough resources to develop RegTech applications themselves or to buy

those solutions. Therefore it must be ensured at EU level that the use of RegTech remains voluntary and does not become an obligation or that RegTech solutions are provided by supervisory authorities free of charge. The latter would enable all insurance undertakings to benefit from the advantages of using RegTech.

Recording, storing and securing data: is cloud computing a cost effective and secure solution?

2.5.1	What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services?

Using cloud computing services does not mean that the insurance undertaking is no longer responsible for the data processing which takes place at the cloud service provider. On the contrary, the use of cloud computing services entails an even higher need for justification in regard of legal requirements on data protection. Outsourcing data processing and storage capacity means that the undertaking transmits personal data into the sphere of a third party. Spreading the data might make it more likely that unauthorised persons are able to gain access to the data. Furthermore it might be more difficult to assess whether the service provider offers the needed level of IT and data security.

When companies use cloud computing services they often are not sure in which country data are processed. That means they must take into account that data are processed in third countries which do not have an adequate data protection level. Because of this they must meet all the data protection requirements for data processing in third countries (Art. 25, 26 Data Protection Directive 46/95/EC and from May 2018 Art. 44 ff. General Data Protection Regulation).

Nonetheless these obstacles can be overcome by controller-processor agreements between financial services firms and cloud computing service providers.

It should also be noted, that, especially where reasonable standards regarding data and IT security as well as data protection apply, in particular small and medium sized undertakings could possibly profit from a scalable modern infrastructure and highly available service in cloud computing.

According to Section 203 of the German criminal code the unlawful disclosure of private secrets is a criminal offence. Private health, accident and life insurance companies in Germany are bound to professional secrecy, so it is difficult for them to use (external) cloud service providers unless

they are released from confidentiality by the data subject. It requires great effort from the insurance undertakings to get consent from the data subject prior to each engagement of an external service provider.

In addition to data protection rules, for the insurance industry, European and German supervision law provide detailed formal requirements and material standards for the use of external services like cloud computing systems. Especially Art. 274 Delegated Regulation (EU) 2015/35, Section 32 VAG (German Insurance Supervision Act) and additional administrative requirements by the German supervisory authority (BaFin) are very far-reaching and complicate the use of external providers.

Cloud providers need to ensure an adequately high level of IT and data security in order for insurance companies to meet their obligations. Any regulation should clarify reporting obligations between the cloud provider and its customers (e.g. insurer).

2.5.2 Does this warrant measures at EU level?

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

In every revision of data protection law facilitating cloud computing should be taken into account. The development of best practices, e.g. concerning cloud computing contracts, in EU initiatives is appreciated and should continue. The EU should call on the member states to establish cloud friendly regulation. Data and IT security in cloud services needs to be ensured as well in order for users of cloud services to comply with their own regulatory requirements with respect to IT security (e.g. NIS Directive). A common standard for IT security certification and audits could be helpful in this respect.

For undertakings such as insurers that process very sensitive data it is of utmost importance to be assured about the level of cloud security as well as to find adequate safeguards in place that data stored and processed in clouds remains untouched and unaltered. Therefore it is essential to clarify the responsibility between cloud provider and cloud user with respect to compliance with IT security obligations. The cloud provider should not be put in the position to be obliged to comply with all sector-specific requirements of its customers (e.g. insurers). If any such obligation were the case the cloud provider would need its customers to disclose the data and its nature and/or the specific processing of data. For example, an insurance company may want to use a cloud provider for storage of customer data.

At the same time the insurance company has the legal obligation to notify the supervisory authority (such as the German Federal Office for Information Security (BSI)) of any IT-security risk to the data stored. However, the legal obligation has to remain at the insurance company and must not be transferred to the cloud computing provider. The fulfilment of legal obligations to notify any authority has to be made sure by a corresponding service level agreement (SLA) between the cloud provider and the insurance company. Otherwise the cloud provider would not be able to even know its legal obligations. This could seriously hinder the use of cloud computing for both parties: for the cloud provider because it wants to avoid being obliged to fulfil further regulations and for the insurance company because it has to make sure the data of its customers will not be disclosed to third parties more than needed.

See also our answer to question 2.5.1.

2.6.1	Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with?

- Yes
- No
- Don't know / no opinion / not relevant

For the German insurance market, the German Insurance Association provides sector specific services for insurance-related use cases in the Trusted German Insurance Cloud (TGIC) in a highly secure environment. As the TGIC holds an IT security certificate of the BSI, participants in TGIC-based services can be sure that an adequate level of IT and data security is guaranteed.

2.6.2	Should commercially available cloud solutions include any specific contractual obligations to this end?

- ✓ Yes
- No
- Don't know / no opinion / not relevant

In the German insurance industry, contractual clauses are used already that ensure compliance with any given legal obligation an insurer has to meet which apply to data stored or processed in a cloud service. As mentioned above (see answer to question 2.2) best practices and standard contracts as developed by the European Cloud Initiative, which take into account e.g. the NIS Directive and the processor obligations according to

the General Data Protection Regulation, could facilitate the use of cloud solutions.

Disintermediating financial services: is Distributed Ledger Technology (DLT) the way forward?

2.7	Which DLT applications are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs?

no direct relevance to insurance provision

2.8	What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

Both artificial intelligence and blockchain technology promise various opportunities but are still in their early explorative phase. A final judgement on their relevance is thus not yet prudent. Blockchain may eventually be employed in fraud detection or (in a B2B context) for capital market transactions. Generally, the interoperability of technical solutions is important in order to facilitate the digital value chain. This, of course, is true for blockchain technology as well, especially if different market players participate, e.g. banks and insurers or insurers and their business partners such as lawyers, medical doctors or insurance adjusters. Interfaces, standardisation as well as the fulfilment of minimum requirements, e.g. concerning trust and security, are issues which need consideration. In order to bring about common use cases for DLT in insurance these issues need to be resolved, as in the interconnected world there is a need for solutions which will work in an entire ecosystem.

Current initiatives show that B2B processes at this time are the most important use-cases for DLT and smart contracts in the insurance industry. If insureds were to partake in any DLT process the indispensable high standards of consumer protection and reliability as well as stability over long periods of time in insurance provision need to be met. While we see great potential in B2B uses of DLT, in light of the necessary high standards of consumer protection and reliability in insurance provision, at least for the foreseeable future we do not believe in the emergence of any imminent use-cases for disintermediated peer to peer insurance provision – using DLT or other technologies – in Germany.

2.9	What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

Whether and which obstacles may arise when implementing solutions in the insurance industry on the basis of DLT depends on the specific use case. Generally, regulation should be technology-neutral as should supervision. Any solution using DLT needs – among others – to be compliant with data protection and IT security requirements.

Even though at this point concrete regulatory or supervisory obstacles cannot yet be named as the development of DLT solutions is not very advanced, any legal norm requiring paper records of transactions could become a hindrance to transferring the process in question to DLT. As DLT virtually documents concluded and verified transactions, producing additional paper records would contradict the simplification provided by DLT.

One important challenge regarding the introduction of DLT use cases might be increased complexity in a potential transition phase when DLT and classical approaches exist in parallel.

However, we would like to underline that the discussions on DLT in insurance are at a very early stage, also within our association. Therefore, we would very much welcome if we could continue the dialogue with the Commission on this specific issue in the months to come.

Outsourcing and other solutions with the potential to boost efficiency

2.10	Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities?

- ✓ Yes
- – No
- – Don’t know / no opinion / not relevant

We assume that the current regulatory and supervisory framework creates severe obstacles for the use of digital solutions and FinTech in the insurance industry. The regulatory framework is too bureaucratic und too far-reaching. That makes it difficult to use external service providers or even special group-internal companies for digital business and innovation. Problems are especially the severe requirements for outsourcing contracts

related to important contractual objects and additional administrative requirements by the German supervision authority (BaFin) for the person in charge at the insurance company.

It would, for example, be very desirable if there were less restrictive regulatory requirements in case of group-internal outsourcing activities compared to the use of external service providers.

2.11	Are the existing outsourcing requirements in financial services legislation sufficient? Who is responsible for the activity of external providers and how are they supervised? Please specify, in which areas further action is needed and what such action should be.

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

For the insurance industry, the existing outsourcing requirements are overly rigorous. Art. 274 Delegated Regulation 2015/35 and especially national administrative requirements in Germany (e.g. "person in charge" for outsourcing activities of an insurance company, see also answer to question 2.10) are very far-reaching. There should be more reasonable facilitations for internal outsourcing activities in insurance groups in comparison to external outsourcing contracts.

Other technologies that may increase efficiency for the industry

2.12	Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

One of the main factors for technologically driven cost efficiency is the possibility to process data digitally throughout the whole process. Any disruption of processes, e.g. by requiring the use of paper/written form, leads to less efficient processes. Therefore innovation – not limited to the financial sector – in consistently digital processes needs to be fostered. Secure and easy digital payments, consultations via video chat or self-serviced products are examples where customer experience could be enhanced while at the same time improving efficiency in business processes.

3. Making the single market more competitive by lowering barriers to entry

3.1	Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

In order to facilitate competition between providers of all sizes and different business models, the consistent application of the principle of proportionality is crucial. For the insurance industry, it should also be considered to increase the threshold for the applicability of the Solvency II Directive.

With regard to the distribution of insurance products, the Insurance Distribution Directive applies to all insurance distributors, including automated advisory tools. In order to be able to optimally adapt the advisory processes to the business model, a paper requirement for the compulsory issuance of information should be avoided. It should be possible to provide advice in new, digital forms by giving information without media breaks.

3.2.1	What is the most efficient path for FinTech innovation and uptake in the EU?

What is needed for the insurance industry is an effective regulatory framework that allows market forces to work and encourages market advances in the interest of consumers and the economy, while at the same time ensuring high consumer protection standards and financial stability. Technology-neutrality and avoidance of unnecessary regulatory burdens (e.g. by a consistent application of the principle of proportionality) should be the guidelines for regulators and supervisors. In order to foster fair competition, regulators and supervisors must also make sure that the existing regulatory and supervisory framework for insurance markets is consistently applied to all competitors in this market and regulatory gaps in the provision of insurance cover are avoided (level playing field; same services and risk, same rule).

The application of new technologies needs space to develop and grow. Technology develops rapidly as does the amount of available digital data. Developments which would not have been thought of ten years ago are commonly applied technology today. Any new regulation, if necessary at all, should keep this in mind and be strictly technology-neutral. If new regulatory measures are to be considered they must aim at ensuring a fair

market in the digital economy, especially with respect to participating in the digital value chain.

3.2.2	Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants? If so, at what level?

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

Besides ensuring a level playing field and fair competition, we believe that regulators and supervisors have an important role to play in monitoring and analysing developments and providing information, but also providing platforms and forums for professional exchange. For example, a regular stocktaking of FinTech developments in Europe (e.g. business models, providers, key figures) might be helpful.

Regarding new business models and practices, regulators should focus on abuse and malpractice cases for the time being. They should not function as active matchmakers between potential new business partners. New and established market actors already have manifold opportunities to find potential partners, e.g. at business networking events or via matching websites.

In addition, regulators and supervisors should have potential barriers to a functioning market and fair competition in view. For example, where the consumer owning and using an interconnected device has the right to determine the use of the data generated and makes use of it by agreeing to a certain processing of this data, the data interfaces in consumer products should be open and follow interoperational technical standards in order to allow access to the data the consumer wants to share. This is a considerable factor in the road vehicle service market, where the user must be able to decide who has access to the data of his or her car.

Should supervisors want to make available innovative regulatory tools, then it is crucial that they are made available to all market participants. In any case, no insured customer should be left without protection or compensation by an undertaking involved in such a tool. In particular, activities of FinTech start-ups should be under the same regulatory regime as traditional providers of financial services. A consistent level playing field is important for consumer protection and functioning of the financial services market. Supervision should be oriented towards the principle "same services and risk, same rules". Otherwise there would be unjust benefits for

some providers (e.g. FinTech start-ups) and incalculable risks for the stability of financial markets.

FinTech has reduced barriers to entry in financial services markets, but remaining barriers need to be addressed

3.3	What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide the details.

While there is a large amount of cross-border business in insurance (via subsidiaries, branches or by way of freedom of services), most insurance markets are to a large extent still national markets. However, this is not due to unnecessary regulatory barriers. Insurance products are designed in function of the environment of the country in which the products are to be sold, e.g. regarding the risk situation. For example, liability insurance is closely tied to national liability legislation (rules of causation, proof of loss and liability determination) as well as cost-related factors surrounding personal compensation (cost of medical procedures for injury or loss of income due to disability caused by an accident). Motor insurance reflects similar factors as liability insurance, as well as other, road-related factors such as local driving behaviour, weather conditions or road terrain that affect driving ability, and local traffic conditions that can increase the risk of accidents. Life insurance is often contingent on national developments in social security systems and corresponding tax law. In addition, cultural preferences differ between countries which may result in different product choices by customers. Furthermore, a barrier from the consumers' perspective, especially regarding old-age provision, might be trust in the provider. Long-term business relationships between customers, insurers and distributors require trust in the insurers' and distributors' continuing services. To establish such trust, language and geographical distance between the individual customer and his or her distributor or insurer can become important factors. (See also the GDV's response to the European Commission's Green paper on retail financial services.)

Therefore, it is essential for any provider of insurance solutions, be it established or a new FinTech start-up, to have a thorough knowledge of the regulatory, tax and social law environment and potential administrative procedures of any country they want to become active in. This is a driving factor for the decision of European providers to market insurance products mainly through national subsidiaries with local know-how instead of creating a single product for all markets served by the company. The new tech-

nologies do not change the fundamental importance of national factors for the provision of insurance.

We also expect market developments regarding FinTech to be different in individual EU countries, depending, for example, on national consumer preferences (e.g. the readiness to provide the insurer with sensor data) or established business practices (e.g. the effectiveness of the current classification system for insured risks).

3.4	Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? If yes, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

- Yes
- ✓ No
- Don't know / no opinion / not relevant

3.5	Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market? If so, please explain in which areas and how should the Commission intervene.

- ✓ Yes
- No
- Don't know / no opinion / not relevant

In order to foster innovation in the financial markets it is key to avoid overcomplex rules and unnecessary bureaucracy. At the same time, high standards of consumer protection must be upheld and risks to the stability of the financial system avoided. In the light of the objective to achieve a level playing field this must apply to all providers of financial services enabled by new technologies irrespective of whether they are start-up companies or established undertakings. The European Parliament's report on FinTech rightly emphasises that a "same services and risks: same rules" principle should be applied. The consistent use of proportionality is a prerequisite to make innovation possible for all market participants as it is the key principle to regulate the financial industry. In general, regulated com-

panies with a simple risk profile should be granted more leeway with regard to proportionality than companies with a complex risk profile. For the insurance industry, proportionality under Solvency II must be established as a rule and not as an exception. Furthermore, rules which have proven to be unnecessary or overly burdensome need to be identified and revoked.

Especially small insurers are overburdened by the implementation of Solvency II rules, which were developed for large insurance groups. This is due to two reasons: some of the new provisions are too complex and time-consuming for companies with a small business volume, and the principle of proportionality is not sufficiently taken into account in supervisory practice. Therefore, it is necessary to examine whether – within the scope of the Solvency II framework – small insurers with a simple risk profile and business model might also meet existing supervisory standards by applying other, less complex requirements. This particularly applies to the governance system, ORSA, outsourcing, the review of the Solvency II balance sheet and the qualitative and quantitative reporting requirements.

Both newcomers and established market participants provide innovative products. Therefore, it is similarly important to identify and remove obstacles that hinder the use of proportionality. It would not be justified to give a competitive advantage to either of them when activity and risk are the same. When it comes to proportionality in practice, the individual risk situation must always be taken into account.

3.6	Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market? To what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions?

- ✓ Yes
- – No
- – Don’t know / no opinion / not relevant

Free flow of data is in particular relevant to the reinsurance business. By nature, reinsurance is a global activity that requires detailed data to offer protection. Restrictions on data movement and data localisation will present a challenge for many types of reinsurance thus limiting the available reinsurance capacity in different markets. This reduction in available reinsurance capacity could result in inadequate reinsurance programs, increase the possibility of basis risk (different coverage between original policy and reinsurance treaty), and eliminate certain reinsurers from the

market. Restrictions on data movement and data localisation will reduce the oversight of the risk that a cross-border (re-)insurance group is exposed to by limiting its ability to centralise, monitor, manage and analyse cross-border data including personal data.

3.7	Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

We support the Commission's approach to base its FinTech policy on the principles of technological neutrality, proportionality and market integrity (comprising fair competition, high consumer protection standards and ensuring financial stability). These three principles should not only guide the regulatory approach to FinTech activities. We believe that all insurance companies should be treated under these three regulatory principles.

In general, the principle of "same services and risk: same rules" must be applied. Special proportional rules for newcomers would distort competition and would penalise established firms.

We agree that the proportionality principle is a key factor in enabling a broad range of companies to be innovative (see also answer to question 3.5). The application of this principle must have a broad scope including start-ups, SMEs and small companies within a large group.

Role of supervisors: enabling innovation

3.8.1	How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation?

The ESAs today already dispose of a wide range of powers in order to coordinate and supervise the actions of national authorities (for insurance supervision see Art. 8 and 9 EIOPA Regulation). This also applies to innovation initiatives and new technologies. For example, the ESAs are in the position to monitor the market and exchange experience with national

regulators and supervisors as well as with stakeholders. We very much support these monitoring activities and the provision of a platform of exchange by the ESAs (see also answer to question 3.2.2). In order to make use of broader expertise on FinTech in supervision, it would also be helpful to strengthen EIOPA's stakeholder groups as regards their impact on regulatory and supervisory decisions.

3.8.2 Would there be merits in pooling expertise in the ESAs?

- Yes
- ✓ No
- Don't know / no opinion / not relevant

EIOPA should be the European supervisor as regards activity in the insurance sector irrespective of whether newcomers or established insurers are concerned. It is vital that the responsible European supervisor has independent expertise in the field of insurance.

While it is true that exchanging views may make sense in cross-sectoral issues, e.g. in the Joint Committee of the ESAs or the ESRB, any regulatory proposal must ultimately match the business models, products and risks in question. Only an independent insurance supervisor can live up to this task.

The insurance business model is fundamentally different from other financial service providers. The differences to banks and securities service providers are also reflected in the regulatory system introduced under the Solvency II Directive. For this reason, appropriate insurance supervision requires supervisors to have a deep level of expertise in particularities of the insurance business model and the workings of the insurance market. The special features of the insurance market can only be appropriately taken into account by an insurance supervisory authority with the relevant insurance-related know-how.

3.9	Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? If yes, please specify how these programs should be organised?

- Yes
- No
- ✓ Don't know / no opinion / not relevant

3.10.1	Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS?

- Yes
- ✓ No
- Don't know / no opinion / not relevant

There are different ways to foster innovation in the insurance market. All providers of InsurTech would profit from reduced complexity of supervisory provisions. As regards further instruments to promote InsurTech, it is important to carefully consider the peculiarities of the respective markets. This is not possible if specific tools are pre-determined on European level.

The role of EIOPA with regard to the supervision of undertakings is defined clearly: In its area of responsibility, EIOPA is in charge of ensuring coherent application of the law and of coordinating a uniform supervisory practice in the member states. Permission of insurers to the market and day-to-day supervision of the undertakings remain with the national supervisory authorities.

For these reasons, the German insurance industry also does not support the idea of a European sandbox as it is not within EIOPA's responsibility to set up a regulatory sandbox (see answer to question 3.10.2). If EIOPA were to develop a European regulatory sandbox, responsibilities would overlap. However, clearly delineated powers are key to efficient supervisory action and, accordingly, to acceptance with the undertakings supervised. Therefore, the German insurers do not support proposals to confer direct supervisory rights to the European level.

However, it is EIOPA's task to ensure that national initiatives, such as regulatory sandboxes, are in line with Solvency II and operate within its framework. It would not be acceptable if national authorities were to sus-

pend binding provisions, even if only temporary. Moreover, EIOPA has a role to ensure a level playing field: if such tools are established on national level, they need to be generally available to all providers of InsurTech irrespective of whether they are start-ups or incumbent insurers.

3.10.2	Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If so, who should run the sandbox and what should be its main objective?

- – Yes
- ✓ No
- – Don't know / no opinion / not relevant

3.11	What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above? If yes, please specify which measures and why.

In addition to an appropriate regulatory framework it is important to ensure that requirements to prove a customer's identity (for example for anti-money laundering purposes) are appropriate and workable. In particular, identification should be possible in a convenient digital way (e.g. Video-Ident, digital ID and digital signature).

Role of industry: standards and interoperability

3.12.1	Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision?

- ✓ Yes
- – No
- – Don't know / no opinion / not relevant

Regarding the insurance industry, standards, e.g. data formats, for supervisory purposes should not pose an unnecessary burden for insurers (see also our answer to question 2.4) but take into account common industry standards. This includes interoperable standards which should be the basis for supervisory purposes as well (e.g. XML standards in reporting).

Standardisation and interoperability are highly important in general for a data driven economy where cross-sectoral participation in the data value chain needs to be possible. Initiatives on the EU level fostering interoperability in public services therefore should be continued. Standards which are developed by relevant stakeholders thereby need to be taken into account by public authorities in order not to impose new data formats or technologies for regulatory or supervisory obligations.

With respect to supervision of IT security, there needs to be a clear distinction of responsibilities between authorities (e.g. EIOPA and ENISA or on a national level in Germany BaFin and BSI, among others) concerning the setting of reporting standards.

In the case of online platforms, data interoperability facilitates not only switching, thereby fostering competition, but also the concurrent use of several platforms (so-called "multi-homing") as well as widespread cross-platform data exchange, which has the potential to enhance innovation in the digital economy. The importance placed on fostering interoperability by the European Commission, aiming at the creation of an environment for the interconnected data economy, should therefore be continued. Any standardisation or interoperability requirement should include stakeholders, whereby in general market driven activities are to be preferred over regulatory initiatives.

3.12.2 Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

- – Yes
- ✓ No
- – Don’t know / no opinion / not relevant

Interoperability and standardised data formats generally facilitate the use of cloud computing which provide one possibility of outsourcing solutions. As cloud providers usually offer B2B solutions for a broad range of customers it is in their own interest to provide solutions on the basis of commonly implemented standards. Therefore market forces should be sufficient to make the use of cloud solutions efficient, readily usable and interoperable.

3.13	In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition-friendly approach to develop these standards?

no comment

3.14	Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses? What other specific measures should be taken at EU level?

- Yes
- No
- ✓ Don't know / no opinion / not relevant

Challenges

3.15	How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

For insurers, the digitalisation of insurance markets is a fundamental development with great potential but also big challenges. Insurers have to adjust their strategies to the digital world. One important consequence is their increasing use of FinTech applications. In this adaptation process, insurers are faced with new customer expectations and new market players. Though we expect changes in market positions including market exits – which is a normal process in a market economy – we do not expect that start-up companies will replace incumbent insurers. The German insurance market has traditionally been characterised by a wide range of providers with very different business approaches. Some further fragmentation of the value chain in insurance provision and an even more varied provider landscape (including innovative collaboration models) seem likely in the future.

One important area where new technologies help to increase insurers' efficiency is process optimisation and automation. FinTech applications provide new impulses in addition to the traditional methods that insurers have already been using extensively in order to make their processes more efficient. InsurTech also benefits insurance companies by providing

new scope for growth and product innovation (for example cyber insurance, on-demand insurance, combining insurance with innovative services, e.g. in case of accident).

In any case, with Solvency II, a highly effective insurance supervisory regime is in place to ensure the safety and soundness of the insurers and in particularly to safeguard obligations towards policyholders.

4. Balancing greater data sharing and transparency with data security and protection needs

4.1	How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

Availability of adequate data is crucial for many FinTech applications. However, data use and the flow of data are highly complex issues where many aspects have to be taken into account.

In general, a liberal data economy fostering fair access to and free flow of data enhances innovation and thus could facilitate better services and products. It is necessary to safeguard fair competition in the market to avoid inappropriate concentration at a certain point of the value chain (e.g. through platforms providers) as this, for example, might unduly prevent consumers from engaging directly and freely with their insurance coverage providers. In order to ensure fair competition and to enable growth in the data value chain, an appropriate and proportionate framework for data access and (re-)use is needed. For avoidance of market disruptions especially multi-sided platform markets (e.g. regarding telematics data of car manufacturers) need continuous evaluation, inter alia with respect to interoperability, interface design and data formats.

Regarding non-personal data, a free flow of data does not pose a danger of interfering with fundamental rights and freedoms and can be advantageous, but it might also negatively impact legitimate interests of involved or third parties or the functioning of markets. For example, if the data are generated by special business models, the investment of the service provider is a protected interest that should in general be respected. At the same time, fair competition and the avoidance of inappropriate concentration regarding data is also important. If the European Commission were to decide on new rules for data use in commercial relations, it would be high-

ly important that these rules apply to all, not only to FinTech start-ups. A level playing field in the sector of financial services has to be preserved regarding data as well.

The integrity of personal data has to be observed according to data protection standards. For personal data, the free flow of data within the European Union is guaranteed by the current Data Protection Directive (Directive 95/46/EC). This principle will be continued by the General Data Protection Regulation which will apply from May 2018. Hence, from a data protection perspective there should be no obstacles to a free flow of data within a Digital Single Market, as long as the controller has a valid legal basis for the data processing as such.

The use of data for any purpose, e.g. data generated during the usage of connected cars for use in an insurance contract, must be the user's choice. For the use of the data in commercial relations, consent of the data owner is the most important (but not always the only) legal basis for using personal data to provide services to customers. The use of these data to enhance the service quality for the customer (e.g. advanced roadside assistance services) should also be allowed because this purpose is most likely covered by the contract between provider and customer, and be it only implicitly.

Insurance companies process data for the purposes which are prescribed by the insurance contract. For the purpose of fulfilling the insurance contract, the processing of the data subject's personal data is absolutely necessary. The same applies to statistics and reinsurance. Consequently, in this situation there is no room for additional compensation by the insurer to the data subject.

The use of personal data for purposes that go beyond the direct relationship between provider and customer could be problematic in the context of the GDPR. Normal contract relations should provide for all the use cases that the data are stored for. There must be a purpose compatible with the purpose for which the data are collected or the data subject's consent. We believe that it would be very difficult to find an adequate compensation for a data use that lies beyond the terms of the contract. The question would be which institution should decide on the amount of money to be paid. In addition, infringements without the customer's (later) consent would be difficult to deal with.

Data portability is a right of the data subject according to Art. 20 GDPR. In this case of transmitting data to another company on demand of the data subject, there is no space for compensation.

Storing and sharing financial information through a reliable tool

4.2	To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

DLT is a promising approach but commonly implemented solutions in insurance may only be available in the future. Issues to be taken into account are standardisation, interfaces and the fulfilment of minimum requirements, e.g. concerning trust and security (see also answer to question 2.8).

4.3	Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

- – Yes
- ✓ No
- – Don’t know / no opinion / not relevant

Generally, not only in combination with DLT, secure and reliable identification in digital services is of very high importance. However, as of now there is a lack of usability in solutions which at the same time guarantee legal certainty. The acceptance for identification technology within business processes by customers especially needs a better usability. While regulatory measures beyond the e-ID Regulation (910/2014) are not necessary, the insurance industry would welcome more action on enabling and trust-building measures such as certification/seals of quality and funding for campaigns. These non-regulatory actions – especially certification/seals of quality – might also help not only to promote consistency in e-IDs across member states but also to give insurers and other companies who incorporate e-ID-services in their business processes the possibility to easily verify the compliance of the e-ID-provider with certain safeguards, e.g. on a technical level, which some member state laws see as prerequisite for compliant use in insurance business processes.

As DLT in itself incorporates a high level of trust of the participants amongst each other, thereby bringing forth a system of trusted partners within a DLT-based service, it should be noted by regulators as well that the technology may be part of an accepted and legally binding framework of trust in digital services, even parallel to other identification technologies.

4.4	What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

In order to protect personal data, a high level of IT and data security is warranted. This is especially true for any interconnected solution in which different companies, business partners and customers participate. DLT solutions therefore must guarantee an adequate assurance for IT and data security throughout the whole process and including all participants. Due to the distributed storage and data processing within a blockchain this poses a special challenge when implementing DLT solutions. If DLT based services are limited to a closed network, e.g. using a secure and closed infrastructure, ensuring a high level of IT and data security poses less of a challenge than in an open environment. Encryption as well as strong identification measures will need to be part of any trustworthy DLT solution processing personal data.

The power of big data to lower information barriers for SMEs and other users

4.5	How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

no direct relevance for insurance provision

4.6	How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers ? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

no direct relevance for insurance provision

Security

4.7	What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

Not only the NIS Directive and the national laws based upon the directive but also the EU General Data Protection Regulation hold requirements for

IT- / cybersecurity. Therefore a comprehensive framework is in place already. A consistent approach is needed in working out guidelines and standards necessary to comply with legal obligations, e.g. guidelines for privacy/security by design, risk management processes or cyber incident management/reporting. The competent authorities need to find a harmonised approach, including authorities for cybersecurity, data protection and financial supervision.

4.8	What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

As cyber incidents may include serious risks of reputational damages as well as exposure to new threats, when critical security leaks are revealed, naturally there is a reluctance concerning open communication and information sharing. Still it is of high importance to make threat assessments and breach information available in a timely manner in order to prevent others from falling victim to the same exploit.

The German insurance industry founded a Crisis Response Center (LKRZV) in 2010, ensuring secure and anonymised information within the sector about cyber incidents. The LKRZV acts as single point of contact to the BSI as well, thus ensuring communication and information sharing both ways, e.g. relaying warnings issued by the BSI to the sector as well as informing the BSI about serious incidents.

The recently passed German IT-Security Law provides a framework for information sharing between companies and the competent authority. In this regard there is no need for further regulation.

However, in order to facilitate information sharing the right balance between warnings and the protection of commercial interests (reputation) and trade secrets must be maintained.

Information sharing between companies can only work on a voluntary basis, such as within the LKRZV, where companies find a trusted framework to share information where trade secrets are protected.

4.9	What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

Generally, companies – among them insurers – are legally required to ensure an adequate level of cybersecurity. Compliance with legal obligations is subject to supervision. Penetration testing may be part of a certification process or auditing to which companies could subject themselves, especially if standards in cybersecurity (see answer to question 4.7) are established. As these standards should be the basis for supervisory action in ascertaining compliance there is no need for further compulsory penetration testing.

Cyber incident drills could be helpful to ensure a high level of alertness as well as the chance to detect potential problems in an alarm chain early on. Testing scenarios as are successfully applied within critical infrastructure companies and the German BSI could contribute to establish best practices for cyber incident drills EU-wide.

Other potential applications of FinTech going forward

4.10.1	What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

no further comments

4.10.2	Are there any regulatory requirements impeding other applications of new technologies to financial services to improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

- Yes
- No
- ✓ Don’t know / no opinion / not relevant