Position paper

FinTech action plan

Views of the German Insurance Association

Digitalisation is a central concern of the German insurance industry. Many insurance companies are currently modernising their IT infrastructures, moving to cloud solutions or investing in new technologies such as artificial intelligence (AI) or blockchain in order to provide enhanced products and services to their customers. The German Insurance Association therefore welcomes the European Commission's FinTech action plan.

As noted in the plan, a balanced approach must be taken, which ensures high consumer protection standards and financial stability while at the same time fostering innovation. For the insurance industry, the following seven points are key in achieving this balance:

- → Foster the consistent application of the **proportionality principle**
- → Strive for a **level playing field**, i.e. "same activities, same risks, same rules"
- → Ensure that current and future legislation is **technology-neutral**
- → Support innovation through the removal of **regulatory barriers**
- → Promote market-driven solutions such as **certifications** for **cloud** providers
- → Encourage more **coordination** between authorities, e.g. in the area of **cybersecurity**
- → Build a framework for non-discriminatory **access to data** from cars and machines

GDV
DIE DEUTSCHEN VERSICHERER

Our core positions explained.

1) Proportionality

For innovations to take place, companies need a regulatory framework which is supportive of their endeavours. One way to achieve this is through the consistent application of the proportionality principle to regulatory measures such as Solvency II or the IDD. Not only would this enable undertakings with a simple risk profile to devote more resources to innovation, it would also apply equally to new market entrants as well as existing companies. This is a necessary precondition for maintaining a level playing field.

2) Level playing field

Even though measures that facilitate innovation are welcome, they should not come at the cost of fair competition. Regulators and supervisors have to make sure that the existing regulatory and supervisory framework for insurance markets is consistently applied to all undertakings in the market. In line with the principle of "same activities, same risks, same rules", no special licensing regimes for InsurTech business models are needed.

3) Technology neutrality

In our view, it is crucial that the regulatory framework is technology neutral. While progress has been made in many areas, some cases remain where regulation is putting technologies at a disadvantage. For example, the IDD still sets out a default paper requirement. The compatibility of some blockchain implementations with the GDPR remains to be seen as well.

4) Removing regulatory barriers

Barriers to innovation are not limited to cases where legislation is not technology neutral. A holistic approach needs to be taken which addresses regulatory barriers in general. Hence, one of the most important tasks for regulators and supervisors is the removal of existing and prevention of new regulatory barriers, both at European and national level. One such barrier are complex and disproportionate (reporting) requirements stemming from Solvency II.

5) Cloud computing

With its large interior market, sound data protection standards and the Digital Single Market strategy the EU is well placed to take a leadership role in cloud computing services. However, the regulatory landscape for cloud computing and outsourcing is complex and fragmented. Greater coherence across the EU is needed. Moreover, we would encourage authorities to be supportive of market-based solutions such as certifications for cloud service providers. Additionally, the audit requirements resting with users of cloud services should be proportionate.

6) Cybersecurity

In an increasingly interconnected world, the threat of cybercrime will continue to increase. The insurance industry stands ready to support the collective efforts on improving cybersecurity with its expertise in innovative cyber insurance products. In terms of regulatory measures, priority should be given to harmonising existing regulation before considering additional elements. Specifically, the competent authorities for financial supervision and cybersecurity need to find a coordinated approach.

7) Non-discriminatory access to data

Future activities of the European Commission could discuss how non-discriminatory access of the insurance industry to large data sets originating from vehicles, industrial machinery and other sources could be organised on the basis of common standards and interoperable solutions. Having an agreed protocol for accessing, using and re-using this data in consent with its respective owner would support the effectiveness of insurance markets in many ways:

- → by extending the ability of the industry to cover risks,
- → by promoting innovative and more need-based products and services for insurance customers,
- → by facilitating risk assessment – thus contributing to the stability of the industry.

Digitalisation in the German insurance sector

Digitalisation is an ongoing transformational process characterised by many industries adapting to the emergence of new technologies, changing customer needs and new business models.

The insurance industry is particularly affected by this development, one reason being the intangible nature of its products and services. Thus, all the currently discussed applications of technology are relevant for insurance undertakings, including but not limited to big data analytics, artificial intelligence, cloud computing, sensor analytics, blockchain solutions, and cybersecurity.

Deploying these technologies for the benefit of private customers, businesses and society as a whole is a key objective. Insurance companies are currently at various stages of evaluating and implementing these technologies. A number of use cases with substantial benefits have already manifested, as shown below.

In order to further support the large-scale dissemination of these benefits, a proportionate, technology-neutral and activity-based regulatory framework is needed.

Applications of InsurTech

Better risk assessment/management

Description	Access to larger volumes of data and/or higher quality data enables insurance companies to conduct more accurate risk assessments.
Drivers	Access to new data sources (from public or private sector), computing power (through cloud), customer expectations, interoperable solutions
Examples	Thanks to the availability of more detailed geographical data, the German insurance industry was able to further increase insurability and affordability of flood insurance in Germany, allowing for near universal insurability even in high risk areas.

Digitalised/machine-supported processes

Description	Business processes can be improved in terms of speed, quality or cost through the use of technology, leading to efficiency gains and better customer service.
Drivers	Competitive pressure and customer expectations, investment in IT infrastructure and applications, process standardisation, innovative technologies
Examples	→ Fully automated processes for settlement of basic claims, for instance in motor insurance → Use of image recognition software to flag potentially fraudulent claims → 24/7 available chatbots to assist the answering of frequently asked questions → Smart contracts to detect insurance events automatically, for instance in flight delay insurance

New insurance products and access channels

Description	Insurers are adapting their product portfolios and distribution channels to changing customer preferences, new types of distribution channels and emerging risks.
Drivers	Online distribution and mobile apps, proliferation of seamless electronic communication, new sources of risk that need insuring (e.g. cyber threats)
Examples	→ On-demand insurance exactly targeted to the customer's situation accessible via smartphone, for example travel insurance or skiing insurance → Cyber insurance for private or business customers

Insurers as a partner in risk management

Description	Insurers assist private or business customers in preventing risks and mitigating damages in new ways.
Drivers	Availability of data, interconnectivity (e.g. IoT), customer preferences, non-discriminatory access to and re-use of data from vehicles, machines, etc.
Examples	→ Additional complementary services, e.g. motor insurance enhanced with an automatic emergency call system in case of a car accident → Use of sensor data analytics in the context of motor or building insurance or provision of location-based weather warnings to support policyholders in taking appropriate precautionary measures → Perks and rebates, for example for regular exercise or good driving

Barriers to innovation in the current regulatory framework

Reference: *This section refers to chapter 2.1 "Reviewing the suitability of rules and ensure safeguards for new technologies in the financial sector" in the FinTech action plan.*

The German Insurance Association supports technology neutrality as one of the FinTech action plan's guiding principles. We very much welcome the Technology-neutrality Suitability Review conducted by the expert group on "Regulatory obstacles to financial innovation."

At the same time, barriers to innovation are not limited to cases where legislation is not technology neutral. A holistic approach needs to be taken which addresses regulatory barriers to innovation in general.

Hence, one of the most important tasks for regulators and supervisors in order to promote InsurTech solutions is the removal of existing and prevention of new regulatory barriers, both at European and national level. Some examples of regulatory obstacles to technology neutrality and the adaptation of innovative solutions in the German insurance market are:

→ **Insurance supervisory regime currently overly complex:** Rules which have proven to be unnecessary or overly burdensome need to be identified and revoked. One important area is excessive reporting requirements. Under Solvency II, insurers have to submit reports for numerous reference dates. Additionally, submitted reports can comprise a large number of data sets, e.g. up to 120,000 data fields for quarterly reporting and up to 330,000 data fields for annual reporting.

→ **Principle of proportionality insufficiently applied:** The proportionality principle is a key factor in enabling a broad range of companies to be innovative. Proportionality in supervision must be established as a rule and not as an exception.

→ **Paper requirements still exist:** In order to enable companies to optimally adapt processes to the relevant business model, all paper requirements should be removed. For example, Article 23 of the Insurance Distribution Directive (IDD) sets out a default paper requirement. This is particularly challenging where customers expect a seamless digital experience with electronic communication.

→ **Requirements in case of outsourcing overly strict:** The current regulatory and supervisory framework regarding outsourcing creates severe obstacles for the use of InsurTech. For example, Article 274 of Delegated Regulation (EU) 2015/35 and national administrative requirements in Germany (e.g. "person in charge" for outsourcing activities of an insurance company) are very far-reaching. In particular, a more cloud-friendly environment is needed, for instance by supporting certifications of cloud service providers.

→ **Data processing under ePrivacy Regulation:** Electronic communication is a key element of InsurTech. It should be made sure that the ePrivacy Regulation will not prevent InsurTech business models. For this reason the rules for data processing should not be stricter than the provisions of the European Data Protection Regulation (Regulation (EU) 2016/679 - GDPR). The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment (Article 8 of the proposal for an ePrivacy Regulation, 2017/0003 (COD)) should be legal under the Conditions of Article 6(1) GDPR, especially if the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1) (b) GDPR).

→ **Lack of a framework for non-discriminatory data access and (re-)use:** Excessive concentration of data-based market power must be avoided. Insurers do not generally produce or control the online platforms that generate data, nor do they produce or control the data collection devices that comprise the Internet of Things (e.g. connected cars). The ability of producers of such devices and owners of such

platforms to deny or restrict access to raw data can lead to a monopoly position of services and products based on big data. Therefore, in the interest of ensuring free competition among market players and strengthening the innovative power of the parties involved, an appropriate framework for non-discriminatory data access and (re-)use is crucial. In our view, action is needed to ensure that the data interfaces in consumer products are accessible on fair terms to all interested companies (incumbents as well as newcomers) and follow interoperational technical standards in order to empower consumers to share their data with service providers of their choice.

→ **Digital identities:** Verification of the identity of the contractual partner is of vital interest to insurance companies. The uptake of market solutions that are currently in development could be supported with certifications or other trust building measures. Regulatory measures beyond the eID Regulation are not deemed necessary at the current stage.

Proposals on authorising and licensing approaches for innovative InsurTech business models

Reference: *This section refers to chapter 1.1 "Enabling innovative business models to scale-up across the EU through clear and consistent licensing requirements" and chapter 1.3 "Facilitating the emergence of innovative business models across the EU through innovation facilitators" in the FinTech action plan.*

In our view, it is crucial that the regulatory framework is innovation-friendly. Therefore, we very much welcome the efforts to facilitate innovative business models across the EU. At the same time, technology neutrality and a level playing field for all market participants must be guaranteed and protection of policyholders and financial stability ensured. Policyholders must enjoy the prescribed protection standards, regardless of the business model of the insurance undertaking. Hence, solely decisive for the scope of regulatory measures should be the risk and financial condition of the undertaking, i.e. the principle of "same activities, same risks, same rules" should be applied.

Regulators and supervisors have an important role to play in facilitating innovation. Of particular importance is the removal of existing regulatory barriers to InsurTech. In addition, supervisory authorities should provide platforms and forums for professional exchange on regulatory aspects of InsurTech. Therefore, we support the establishment of innovation hubs to give undertakings general guidance during the authorisation and licensing process and to foster the undertaking's understanding of regulatory requirements and supervisory expectations. Innovation hubs can be helpful as a platform for sharing information and views on InsurTech issues, including clarifications and guidance regarding the interpretation of relevant provisions. As already touched upon by the Commission, these facilitators should be equally open to newcomers and established financial institutions. Innovation hubs which allow the exchange of knowledge between supervisory authorities and undertakings would also improve the understanding of InsurTech trends by supervisory authorities and thereby could contribute to more effective supervision of innovative business models.

Existing regulatory requirements are often highly complex and might be difficult to meet. However, this is not only applicable to innovative business models, but it is a general problem, in particular of smaller insurance undertakings irrespective of their specific business model. Different kinds of small insurers are equally 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 simple risk profile, and the principles of proportionality and flexibility are not sufficiently taken into account in supervisory practice.

Proportionality and flexibility are also decisive in allowing innovative business

models to scale up across the EU and seem to be more suitable than special licensing requirements for innovative insurance business models. The latter would lead to an inconsistent supervisory framework. As a consequence, competition between undertakings with traditional and innovative business models would be distorted. Further, softer licensing requirements for innovative business models could give potential customers and investors the impression that these business models are less stable. Hence, we do not believe that licensing requirements for innovative insurance business models diverging from licensing requirements for traditional insurance business models are a suitable solution to foster innovative business models. Following from this, we do not consider European guidelines on licensing requirements for innovative insurance business models necessary.

Similarly, we believe that regulatory sandboxes are not an ideal instrument since they have difficulties satisfying the objective of facilitating innovative business models and ensuring fair competition and technology neutrality at the same time.

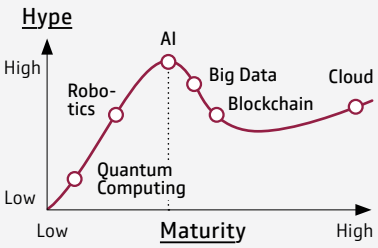
In order to ensure effective competition, the principles of proportionality and flexibility should be used in a consistent, technology-neutral manner. This would enable both established market participants and innovative business models to provide innovative products. Therefore, we believe that the application of these principles should be examined

New technologies challenge regulatory landscape – regulators and supervisors can support uptake by applying core principles consistently

1 Insurance technology

- **Artificial Intelligence**
- **Cloud Computing**
- **Blockchain**
- **Big Data Analytics**
- **Quantum Computing**

Hype-Maturity-Model



Source: GDV based on Gartner

A number of innovative technologies are currently on the way to maturity

2 Regulatory landscape

Major European legislation

IDD, NIS, SII, PSDII, GDPR

Challenges

- Complex SII reporting requirements
- Default paper requirements in IDD
- Complex rules on outsourcing/ cloud computing
- No framework for non-discriminatory access to data
- Diverging implementations of some directives (NIS)
- ePrivacy

New technologies and business models challenge the regulatory landscape

3 Priorities of the industry

Core principles

Proportionality; Technology neutrality; Level playing field

Many instruments are compatible with these principles ...

- Innovation hubs
- Workshops with regulators and industry
- Market-driven solutions (standards, certificates, codes of conduct)
- Expert groups, e.g. on technology neutrality

... though some are not:

- Regulatory sandboxes
- Separate licensing regimes

Dialogue is key!

Regulators and supervisors can support innovation by applying principles consistently

and the regulatory framework should be reviewed to allow for flexibility and proportionality. It should also be examined whether – within the scope of the regulatory framework – small insurers with a simple risk profile and business model, regardless of the technology used, might also meet existing supervisory standards by applying other, less complex requirements. In general, regulated companies with a simple risk profile should be granted more leeway with regard to proportionality than companies with a complex risk profile.

Cloud computing

Reference: *This section refers to chapter 2.2 "Removing obstacles to the use of cloud services" in the FinTech action plan.*

Cloud computing offers state-of-the-art, scalable IT infrastructures, platforms or applications on demand. Small and medium-sized enterprises benefit in particular, since they gain access to modern IT systems or software applications that might otherwise be uneconomical for them.

With its large interior market, sound data protection standards and the Digital Single Market strategy the EU is well placed to take a leadership role in cloud computing services. We therefore welcome the Commission's continued efforts to promote the use of cloud and outsourcing services across the European Union.

Cloud computing in particular needs a coordinated regulatory and supervisory approach. This requirement is currently only partially fulfilled. There are a number of regulations and guidelines for insurance companies on cloud computing and outsourcing in place, both at the national and European level.

For example, the German supervisory authority (BaFin) has recently issued a new regulation on IT requirements in the insurance sector ("VAIT"). Module eight of this regulation contains detailed requirements on outsourcing, e.g. detailed risk analyses for outsourced IT services such as cloud services. The BaFin is also considering a requirement for cloud users to physically access the premises of the cloud provider in order to fulfil inspection orders. Given the decentralised and remote nature of cloud computing, this appears impractical and prohibitive in terms of the time and costs attached.

The VAIT are certainly not the only instrument dealing with outsourcing, but further specify requirements stemming from the BaFin's minimum requirements for the business organisation of insurance companies (MaGO). VAG (German Insurance Supervision Act) and BSIG (Act on the Federal Office for Information Security) contain further regulation, resulting in an overall complex regulatory landscape on cloud computing.

Because of this we believe that additional regulations or guidelines on cloud computing are not required at the current stage, since they would further convolute an already complex regulatory landscape.

While we believe that no additional regulation is needed, we would like to highlight the necessity of harmonised regulatory practices across the EU. It should be avoided that future regulations or practices at national level result in diverging requirements across the EU.

Furthermore, we would favour greater support for market approaches where cloud providers hold a certificate verifying their quality standards and compliance with regulations. Cloud providers that are certified in such a way could also be listed in a public register serving as a central source to find and verify these providers.

As the Commission rightly points out, the essential nature of outsourced activities must be the deciding factor. For IT systems and processes that have no material impact on the business or the company's risk position, there should be no audit requirements or reporting requirements, i.e. the requirements should be proportionate.

On porting of data we are supportive of the free flow of non-personal data proposal (2017/0228 (COD)). Here, the call for self-commitment of providers to fair, pre-contractual and transparent information on the conditions under which data may be accessed and ported can be a step stone to the advancement of the European data economy.

Cybersecurity

Reference: *This section refers to chapter 3 "Enhancing security and integrity of the financial sector" in the FinTech action plan.*

Cybersecurity concerns everybody

In an increasingly interconnected world, the threat of cybercrime will continue to increase.

The German insurance industry is responding to this challenge in two ways. First, the industry stands ready to support other companies and industries with its expertise in innovative cyber insurance products. After all, cyber threats are not unique to the financial sector but concern all types of companies and company sizes. Second, the insurance industry is also ensuring the security of its own IT systems.

Model terms and conditions

The German insurance industry has developed non-binding model terms and conditions for cyber insurance policies. They mainly target companies with up to EUR 50 million in revenues and up to 250 employees. Cover is not restricted to data theft and business interruption, it extends to IT forensics and crisis communication.

Self-initiative for information sharing

Already in 2010 the German insurance industry instituted a crisis response centre named "LKRZV". The LKRZV acts as single point of contact to the German Federal Office for Information Security (BSI), thereby ensuring the secure and anonymised information sharing about cyber incidents and warnings between the BSI and the industry.

Another valuable tool is public-private partnerships which bring together supervisors, regulators and industry representatives. For example, on the German market, the "UP KRITIS" initiative has become an indispensable platform for information exchange and steering.

Many measures on cybersecurity already in place

Cybersecurity is rightly seen as a priority and prerequisite to the widespread use of InsurTech. For the German insurance industry, a comprehensive framework for IT security is already in place. The German IT Security Act aims to strengthen the German Federal Office for Information Security (BSI). The BSI as the national cybersecurity authority shapes information security in digitisation through prevention, detection and reaction for government, business and society and is therefore the appropriate institution in Germany.

Penetration and 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 they have to furnish proof of a reasonable security level. As these proofs should be the basis for supervisory action in ascertaining compliance there is no need for further compulsory penetration testing.

Existing efforts should be coordinated and studied for effectiveness before introducing new measures

There are already a number of regulatory measures on IT security in place. The priority should be to reduce overlaps, inconsistencies and divergences between these measures. Specifically, the competent authorities for financial supervision and cybersecurity need to find a harmonised approach (e.g. EIOPA and ENISA or at national level in Germany BaFin and BSI, amongst others).

Blockchain technology

Reference: *This section refers to chapter 2.3 "Enabling FinTech applications with the EU blockchain initiative" in the FinTech action plan.*

The German insurance industry has been at the forefront of analysing blockchain applications. For instance, under the umbrella of GDV, several workshops with industry members and blockchain experts were held to discuss the new technology.

There is no such thing as "the" blockchain

In practice, blockchain is often defined via the content of its data. As a result, it is often associated, if not equated with the world's most famous cryptocurrency: Bitcoin. However, Bitcoin uses a special public version of blockchain aiming at complete autonomy. In addition to that, there is a variety of options for distributed databases that, in turn, can be used in a multitude of different scenarios (cf. chart 2). The Business-to-Business (B2B) sector, for instance, often considers the use of consortium blockchains which include access controls and efficient consensus processes.

Alternative to traditional databases

A blockchain is a distributed database shared by several participants. It is different from other databases in that its participants are allowed to update data sets individually via clearly defined transactions. The technology uses algorithms to ensure that the data sets remain free of logical inconsistencies. This allows for the fully automated processing of transactions between participants. Transactions made in a public blockchain can be seen by all authorised users (in pseudonymised form); the result of the transaction cannot be modified or deleted. As opposed to the traditional, centralised approach, where an intermediary is responsible for the correct recording and processing of transactions, blockchain uses a purely technical solution based on algorithms.

Challenges posed by data protection

Due to the complexity of blockchain, compliance with applicable data protection legislation has to be assessed based on its implementation (public/private) and intended use (cryptocurrencies, smart contracts etc.). Therefore, only a few selected aspects can be discussed here.

Combining a public blockchain with personalised data is often viewed critically, given that sensitive data could potentially be accessed by all participants. Although pseudonymised data is used in such cases (which is to be welcomed considering the objective of data protection), said pseudonymisation has already been successfully circumvented, e.g. in the case of Bitcoin.

Moreover, the fact that data in blockchain cannot be modified directly contradicts the consumers' right to have their data rectified as well as the right to be forgotten/right to erasure.

As far as consortium blockchains are concerned, the challenge is to guarantee the confidentiality of data, so that the companies can only access transactions they have actually been involved in.

Depending on its individual implementation, the blockchain technology can also contribute to data protection, e.g.if only references to data in other sources are stored in the blockchain, which would be helpful considering the goal of data minimisation. In addition, blockchain solutions make it possible to release data blocks in a manner that is effective, safe and manageable for the person concerned.

Blockchain needs a functioning ecosystem

According to the analysis by GDV, blockchain or distributed ledger technology has the potential to make processes in the insurance industry faster, safer and more cost-efficient. Shared applications of the public and the private sector are particularly promising.

However, the large-scale application of the new technology is still uncharted territory; hence, several uncertainties remain to be addressed:

Technology neutrality

The underlying principles of blockchain technology pose challenges with regards to existing regulation, especially for implementations that use personal data. Here, data protection laws stipulate several rights of the persons affected, such as the "right to be forgotten" as well as the naming of an authority responsible. Blockchain, on the other hand, attempts to achieve immutability and decentralisation.

Blockchain infrastructure

For the development and implementation of blockchain use cases, highly specialised IT professionals are needed. Increased efforts are needed to ensure that such personnel are available EU-wide. Moreover, a modern high-speed communication infrastructure is required in order to ensure that data in blockchain applications can be synchronised without delay. Lastly, standardisation and interoperability are important for the uptake of the technology.

Lighthouse projects

Joint projects in the area of eGovernment could propel the technology by helping overcoming uncertainties often faced by early adopters. Here, blockchain offers a chance to connect public and private bodies in a safe and cost-efficient manner.

In light of these challenges, we welcome both the European Commission's and the European Parliament's initiatives in the area of blockchain technology. For instance, the EU Observatory and Forum are much needed tools for monitoring and supporting this still nascent technology.

Concerning interoperability and standardisation efforts, it is vital that all relevant stakeholders are engaged.

Standards and interoperable solutions

Reference: *This section refers to chapter 1.2 "Increasing competition and cooperation between market players through common standards and interoperable solutions" in the FinTech action plan.*

The German insurance industry is a long-time user and supporter of standards for business processes, interfaces or interoperable solutions. Examples for standards used by the German insurance industry are:

→ GDV and BiPRO standard data models for the structured exchange of data with business partners

→ GDV standard conditions of insurance, e.g. in the area of cybersecurity

For the insurance industry, standards are important since its ecosystem consists of a large number of partners that need to work together efficiently and effectively. Policyholders in particular benefit from standards in several ways:

→ Data standards can reduce frictions in processes between insurers, business partners and customers, thereby reducing costs throughout the value chain to the benefit of all parties involved. Furthermore, smoother process flows can offer the insurance industry a chance to refine service quality or extend their service and product portfolio.

→ Standards can support the uptake of new technologies by acting as a credible signal of commitment, thereby improving security of investment.

→ Standards can contribute to the quality of products and services by setting the bar.

→ To achieve these goals, a good standard should reflect the following criteria:

→ **Flexible:** The standard should strike a balance between general and specific provisions. It needs to be sufficiently specific to avoid uncertainty for those tasked with implementing it. At the same time, too many technicalities are prohibitive too, since they could conflict with industry-specific requirements, thus preventing an effective uptake of the standard.

→ **Value-additive:** The net benefits of implementing the standard should be larger than the implementation and operating costs.

→ **Supported:** The standard should have a strong mandate based on a broad consensus from its intended user base and relevant stakeholders.

→ **Up to date:** The standard should be regularly reviewed for required changes and updated where necessary.

The development of a standard is very much a collaborative effort. Therefore, initiatives aimed at standardisation or interoperability should include all relevant stakeholders. In general, market-driven activities are to be preferred over regulatory initiatives.

Standards do not only concern the private sector. For instance, efforts at EU level for increasing interoperability in public services therefore should be continued. Namely, public administrations should use structured, transparent and common approaches when evaluating and selecting norms. The guidelines issued by the EU and OECD on the subject matter should be considered in this context. Particular attention should be given to common standards for character sets for the communication of multinational companies with public authorities in the European Union.

Other proposals

Retail investment products

Reference: *This section refers to chapters 2.5 "Leveraging technology to support distribution of retail investment products across the Single Market" and 2.4 "Building capability and knowledge among regulators and supervisors in an EU FinTech Lab" in the FinTech action plan.*

GDV considers the diversity of financial products to be the natural consequence of well-functioning and competitive markets.

We agree with the European Commission that in recent years significant progress has been made in improving the comparability of retail investment products through disclosure requirements. For example, since 2018 insurers provide a three pages long key information document (KID) for insurance-based investment products. It aims at informing consumers in a standardised way about the key features of a product, such as risks, benefits and costs. For the PRIIPs review the EC is asked to conduct a market survey to determine whether online calculator tools are available (Article 33(4) of the PRIIPs Regulation).

First, it should be assessed thoroughly how insurance-based investment products can be compared in a way that the result is of added value for consumers. When compared to other investment products, with insurance products, the personal situation of a consumer, their demands and needs play a crucial role. The PRIIPs KID, however, contains non-personalised information which does not describe the situation of a concrete consumer. On the other hand, dynamic comparisons would lead to very sophisticated calculations: Features of insurance-based investment products depend strongly on age, sometimes occupation of the person and the recommended holding period. Furthermore, they cannot be linearly scaled.

Second, a thorough review of the PRIIPs provisions and their functioning needs to be carried out first. Then, consumers, insurers and supervisors need to gain sufficient experience with the KID to understand whether

and how products can be compared through such a tool.

All activities at the European level regarding to such a tool should be linked in a meaningful way. We believe that if online calculators or comparison tools were to be developed at the European level, they should fulfil a number of minimum requirements:

→ They should be run by a neutral, independent non-commercial entity

→ They should only compare products that are substitutes for consumers

→ They should not lead to additional information requirements for insurers

→ Finally, consumers should receive a balanced comparison which includes all key features, including risks, benefits and costs of the product. It should also be duly taken into account how non-quantitative features of products such as preferences, objectives and other characteristics of the customer and the target market can be compared.

EU FinTech Lab

GDV supports the European Commission's proposal to establish an EU FinTech Lab to build capability and knowledge among European and national regulators and supervisors regarding new technologies. We agree that it is crucial to ensure that regulators and supervisors are adequately informed about the nature of these technologies and how they are applied in the financial sector. Targeted sessions on specific innovations could be a valuable building block toward this goal. However, it is crucial that participation in these sessions is broadly based, representing the full range of solution providers and users of the technologies under discussion, e.g. both start-ups and incumbents. The German insurance industry stands ready to offer its expertise and experience with the deployment of new technologies in the insurance sector.

Imprint

Published by
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
German Insurance Association
Wilhelmstraße 43/43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: 030 2020–5000, Fax: 030 2020–6000
www.gdv.de, berlin@gdv.de

Responsible:
Patrik Maeyer,
Head of Business Process Management,
Digitalisation & IT

Editorial Deadline:
15.10.2018

Picture credits:
shutterstock / whiteMocca

Contact person:
Florian Baltruschat
Phone: 030 2020–5458
Email: f.baltruschat@gdv.de

Team of authors:
F. Baltruschat, A. Crasselt, C. Jansen, U. Kläsener, K. Krol, U. Müller, G. Sieck, A. Theis

All Issues ...
on GDV.DE