

BaFin Perspectives

Issue 1 | 2019



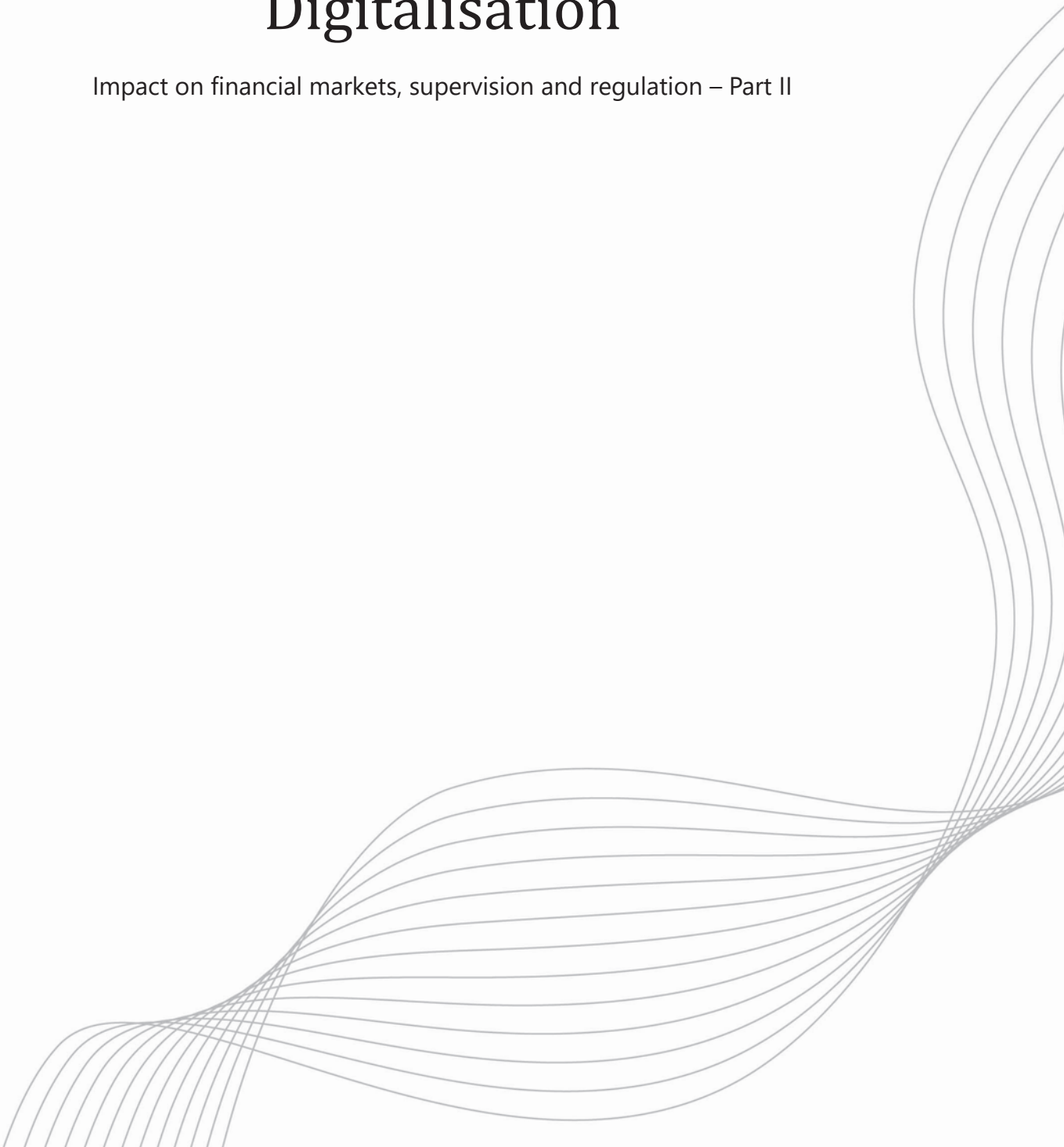
BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht



Digitalisation

Impact on financial markets, supervision and regulation – Part II



Contents

Foreword	8
-----------------	----------

I. We have to seize the opportunities AI presents, but also face up to the risks it poses	10
--	-----------

Government, society, business, administration and academia have to seize the opportunities AI presents, but also face up to the risks it poses. It is important that its application is in the public interest and is rooted in fundamental democratic principles.

Interview with Dr Jörg Kukies	11
--------------------------------------	-----------

II. Big data meets artificial intelligence – results of the consultation on BaFin’s report and interview with Felix Hufeld	14
---	-----------

BaFin received numerous responses regarding its report “Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services”. Industry associations, individual institutions, national and international authorities and representatives from academia contributed to the consultation. This article provides an overview of the responses and includes an interview with BaFin President Felix Hufeld, offering an initial analysis of the results. Jörn Bartels and Dr Thomas Deckers

1 Introduction	15
2 Financial stability and market supervision	17
3 Supervision of institutions	23
4 Collective consumer protection	31
5 Interview with Felix Hufeld	38

III. When banks outsource IT services	42
--	-----------

Outsourcing activities and processes allows banks to focus on their core competencies and to improve their services. However, outsourcing can only work if institutions can ensure that risks are kept under control. In the age of digitalisation, banks and supervisors are facing new challenges. Raimund Röseler and Ira Steinbrecher

1	Introduction	43
2	Standardisation of IT services	44
3	Outsourcing to the cloud	44
4	Risks of outsourcing	45
5	Requirements for outsourcing to cloud service providers	46
6	Guidance on outsourcing to cloud service providers	47
7	Discussions on the power to give instructions	47
8	To what extent can audit rights apply?	48
9	Limits to outsourcing	49
10	Outlook	50

IV. The community of policyholders in an era of Big Data and

Artificial Intelligence

52

Rate setting and pricing in the insurance business are based on extensive historical data resources and forecast values. The increasing availability of Big Data (BD) and the rapid, innovative development of Artificial Intelligence (AI) are also changing the opportunities for developing individual rates. This article examines their impact on the balancing of risks in the community of policyholders. Prof. Dr Fred Wagner and Kristina Zentner, M.Sc.

1	Introduction	53
2	Definition of insurance	54
3	How insurance works: the actuarial principle of equivalence	57
4	The digital revolution	59
5	How Big Data and Artificial Intelligence affect calculations and rate setting	63
6	Impact on the community of policyholders	64
7	Assessment	66
8	Summary	67

V. The status of digitalisation at savings banks

68

This article outlines the positioning of the Savings Bank Finance Group regarding key aspects of digital transformation. It explains the various dimensions in which digitalisation impacts the savings banks and reveals how the institutions specifically shape the associated challenges and opportunities. Dr Joachim Schmalzl and Frank Weigand

1	The importance of digitalisation	69
2	Savings banks and digitalisation	71
3	The Savings Bank Finance Group's digital agenda – An organisational roadmap	73
4	Trust in the digital world – cybersecurity as a competitive factor	82
5	New business models for the Savings Bank Finance Group	84
6	Outlook	87



VI. En route to the world of digital insurance – A report from the engine

room of change

88

Insurers' business is set to experience fundamental change. Dr Jörg von Fürstenwerth, Chair of the Executive Committee of the German Insurance Association (GDV), analyses the seven possible megatrends and their potential as agents of change. Dr Jörg Freiherr Frank von Fürstenwerth

1	Introduction	89
2	The battle for customer contact	91
3	New technologies: Artificial Intelligence, cloud and blockchain	93
4	Creative destruction: new business models and products	95
5	The process revolution	100
6	New competitors, greater diversity of providers	103
7	Competition for talent	106
8	Agile supervisors	108
9	Summary	109

Imprint

110

Foreword



BaFin is devoting another issue of BaFin Perspectives to the topic of digitalisation – and with good reason. The advancement of digitalisation is bringing about change across the board, and the financial market is no different. This, however, is a market that has always been heavily regulated because it relies, more so than other markets, on people being able to have confidence in its functioning, stability and integrity. Creating a solid basis for this confidence is BaFin's role, which is why, in August 2018, it formulated its digitalisation strategy, setting out three basic questions:

- How should the market changes that digitalisation brings be handled in supervisory practice and regulation?
- How can BaFin ensure that innovative technologies and IT systems and the data that supervised undertakings use are secure?
- How does BaFin itself need to adapt and evolve to meet the demands of ongoing digitalisation – both internally and at its points of interaction with the market?

BaFin needs to continually reassess its digitalisation strategy in order to keep pace with the changing situation. To this end, it keeps in active contact with the financial industry, academia, politics and other authorities – a good example of this being the consultation for its report "Big data meets artificial intelligence".

In this issue, Jörn Bartels and Dr Thomas Deckers, both from BaFin, provide an overview of the responses to this consultation, and I give my initial analysis. In an interview, Dr Jörg Kukies, State Secretary at the Federal Ministry of Finance, explains the German federal government's planned framework for artificial intelligence. My colleague on the Executive Board, Raimund Röseler, and Ira Steinbrecher, also from BaFin,




address the topic of banks outsourcing IT services. Professor Fred Wagner, who is a member of our administrative council, and Kristina Zentner, both of Leipzig University, have written about the community of policyholders in this era of Big Data and Artificial Intelligence. Dr Jörg Baron Frank von Fürstenwerth of the German Insurance Association (*Gesamtverband der Deutschen Versicherungswirtschaft e.V.*), and Dr Joachim Schmalzl and Frank Weigand of the German Savings Banks Association (*Sparkassen- und Giroverband*) report on how the insurance industry and savings banks are dealing with the challenges posed by digitalisation.

We hope you enjoy reading it.

A handwritten signature in blue ink, which appears to read "F. Hufeld". The signature is written in a cursive, somewhat stylized script.

Felix Hufeld
President of BaFin



I

Government, society, business, administration and academia have to seize the opportunities AI presents, but also face up to the risks it poses. It is important that its application is in the public interest and is rooted in fundamental democratic principles.

We have to seize the opportunities AI presents, but also face up to the risks it poses

Interview with

Dr Jörg Kukies

State Secretary at the Federal Ministry of Finance (BMF)



State Secretary, the Federal Government adopted the national AI strategy at the Digital Cabinet meeting on 15 November 2018. What is it about?

This strategy marks the first time that the Federal Government has established an end-to-end political framework for developing and applying Artificial Intelligence (AI) in Germany. It will pursue three main objectives. First, it is designed to make Germany and Europe a leading location for developing and applying AI technologies – including to secure Germany’s future competitive position. Second, it is designed to ensure the responsible development and deployment of AI in the public interest, and third, it is designed to embed AI ethically, legally, culturally and institutionally in society through a broad social dialogue and by actively shaping the political framework. The government is earmarking a great deal of money to achieve these objectives, with planned investments totalling three billion euros.

The strategy also includes essential aspects for the financial industry and thus incorporates recommendations by the Fintech Council at the Federal Ministry of Finance. AI and Big Data enable innovations that are transforming the financial market. All this requires technical and professional expertise, and supervisors, too, must respond accordingly. BaFin’s study on Big Data and AI¹ is an important first step in this direction.

¹ BaFin, Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services, www.bafin.de/dok/10985478. BaFin prepared the report in cooperation with PD – Berater der öffentlichen Hand GmbH, Boston Consulting Group GmbH and the Fraunhofer-Institute for Intelligent Analysis and Information Systems.

Where do you see the greatest opportunities and potential risks in using Big Data and AI in the financial market?

The challenge to government, society, business, administration and academia is to seize the opportunities AI presents, but also to face up to the risks it poses. With its AI strategy, the Federal Government has established a basis for creating the conditions for leveraging the potential AI has to offer. BDAI must be developed and deployed to ensure human-centric application, in the public interest, for the economy and society, rooted in fundamental democratic principles.

The interplay between AI and Big Data is leading to autonomous systems that are currently fuelling the rapid pace of digitalisation in all sectors of the economy. In the near future, these developments could also lead to changes in our financial system. We can already observe how BDAI is being used in the capital markets. And BDAI is also increasingly being recognised as an opportunity by banks and insurers.

BDAI applications could, for example, be used in institutions' risk assessment models or to facilitate claims processing in insurance undertakings.

It is important when deploying BDAI technologies to ensure that financial stability and integrity are not compromised. Another factor is that consumers must not be left behind, meaning that they must not lose sovereignty over their personal data in a world of BDAI.

Do you think it is possible that the increased use of Big Data and AI will lead to new types of systemic risk?

No systemic risks can be identified at the present time because the use of Big Data and AI in the financial industry is still too low. But this can change quickly. That is why it is important for supervisors to keep an eye on possible risks to financial stability so that they can address them quickly if necessary.

The application of Big Data and AI also frequently raises data protection issues. How do you think financial supervision should approach this?

When companies analyse huge volumes of data in a self-learning process, they must ensure that their customers

stay in control of their data. The GDPR², which came into force last year, established important standards for this across Europe, i.e. customers must consent to their data being processed for pricing purposes. At the same time, customers must be sensitised to an even greater extent to the fact that they generally pay for faster and better service with their data. But the companies, too, have to ensure that customer data is handled responsibly.

The Federal Government has therefore set itself the goal in its AI strategy of convening a round table with data protection supervisors and industry associations that will devise joint guidelines for developing and applying AI systems that comply with data protection rules, and to prepare examples of best practice applications.

Compliance with data protection rules is a matter for the responsible authorities of the *Länder* and the Federal Commissioner for Data Protection. If the relevant requirements are met, BaFin may also intervene as part of its supervision of violations of consumer protection law. In particularly extreme cases, the suitability of management board members would also have to be called into question.

In the first edition of BaFin Perspectives, BaFin President Felix Hufeld described the problem of unintentional discrimination by Big Data and AI. How can this problem be solved?

Algorithms are not underpinned by a certain world view; they draw their conclusions from the data records. However, depending on how these records are selected or what the analysis will be used for, this can result in discrimination. The Fintech Council drew attention to this problem in its recommendations for action at the end of 2017. Part of a responsible approach to AI that bears the public interest in mind is also for companies using AI to ensure that discrimination is prevented – if necessary by using human control mechanisms. For the financial industry, this means that using AI technology does not absolve the management board from its overall responsibility for ensuring a proper business organisation.

² General Data Protection Regulation.

Big Data and AI make it possible to link heterogeneous data. This may also allow companies to explore customers' maximum willingness to pay – and, given corresponding market power, to exploit it. What is your view on this?

Pricing is linked to numerous issues that go far beyond supervisory law. As in other areas, the bounds of what is acceptable are reached when the company exploits its market power at the expense of consumers. If pricing is based on personal data, the protection afforded by the GDPR also applies here.

The Federal Government has set itself ambitious goals with its AI strategy. What do you expect from BaFin?

The Federal Government wants to take the lead in the further deployment of AI in public administration and

hence contribute to improving the efficiency, quality and reliability of administrative services. BaFin can also play an important role here. It laid the foundations for this with its BDAI study, and it is now time to build on them. BDAI applications can add value especially in supervisory areas where BaFin has structured data in sufficient quality and quantity. One area that springs to mind, for example, is the reporting system for securities supervision. BaFin should be ambitious and examine whether the analysis of large structured data volumes can be managed more often by AI in the future. BaFin should also aim to enhance its digitalisation strategy in this context so as to further strengthen financial supervision in the long term.

Dr Kukies, thank you for the interview.



III

BaFin received numerous responses regarding its report “Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services”. Industry associations, individual institutions, national and international authorities and representatives from academia contributed to the consultation. This article provides an overview of the responses and includes an interview with BaFin President Felix Hufeld, offering an initial analysis of the results.

Big data meets artificial intelligence

Results of the consultation on BaFin's report and interview with Felix Hufeld

Authors

Jörn Bartels

Division for Strategy Development
Federal Financial Supervisory Authority (BaFin)

Dr Thomas Deckers

Division for Innovations in Financial Technology
Federal Financial Supervisory Authority (BaFin)

1 Introduction

On 16 July 2018, BaFin launched a public consultation¹ on its report "Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services"² (BDAI report for short³). The consultation focused particularly on the strategic key questions in the chapter "Supervisory and regulatory implications"⁴ regarding the future development of supervision and regulation in times where the use of big data and artificial intelligence is increasing.

BaFin received 31 responses in total. Both industry associations and individual institutions took part in the consultation. Comments were also submitted by national and international authorities as well

as members of academia. All of the respondents welcomed the open and broad discussions that BaFin initiated with the report. It was also pointed out that it would be important to coordinate any BDAI-related adjustments to supervision and regulation at international level. Moreover, it was stressed that, even in the age of BDAI, German financial service providers should not be compared with bigtech companies – for instance, in terms of how customer data is handled.

This article provides a summary of the responses to the BDAI report and is – like the report itself – divided into three main topics: financial stability and market supervision, the supervision of institutions, and collective consumer protection. Each of these topics and subtopics is introduced with a text box summarising the views stated in the BDAI report.⁵ These are followed by an anonymised summary of the responses received in the course of the consultation.⁶

1 BaFin, "Consultation on BDAI report", www.bafin.de/dok/11251536.

2 BaFin, "Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services", www.bafin.de/dok/11250046, retrieved on 23 January 2019. BaFin worked on the report in collaboration with PD – Berater der öffentlichen Hand GmbH, Boston Consulting Group GmbH and the Fraunhofer Institute for Intelligent Analysis and Information Systems.

3 "BDAI" stands for big data and artificial intelligence.

4 BaFin, loc. cit. (footnote 2), page 164 et seq.

5 The views in the BDAI report that are referred to in this article can mostly be found in the chapter "Supervisory and regulatory implications".

6 Each topic also takes into account relevant information from responses that concern other sets of topics.

Due to the diversity of the respondents (institutions, associations, authorities and academics), representative majorities could not be given for the responses as they would need to be weighted (e.g. an individual institution compared to an association). In this article, all of the responses were given the same weighting for simplification purposes.

As this article is intended to provide an overview, it does not cover all the details contained in the responses. It should also be noted that BaFin has not yet evaluated

the statements presented in this article. Neither does the article answer the question of what feedback is to be reflected in supervisory practice and regulation. This will take some time to determine.

In an interview about the consultation, BaFin President Felix Hufeld offers an initial analysis of the results.⁷

⁷ See page 38.



© iStock/From2015

2 Financial stability and market supervision

2.1 Consultation results on the emergence of new companies and business models

In a nutshell

Key points from the BDAI report

New providers are emerging in the financial sector as a result of BDAI-driven innovations. This could intensify the disaggregation of the value chain, particularly if existing businesses cooperate with new specialised providers. BDAI is a phenomenon that could also give rise to new types of business models and market participants that are not yet adequately covered by the current regulatory framework. It is vital that such cases are identified and that the range of providers and companies to be supervised is expanded accordingly.⁸

2.1.1 General market observations

Many of the respondents stated that the emergence of new value chains can be observed across all sectors. In particular, the companies that are able to bring data processing to a new level using BDAI are entering the market, according to these respondents. Some of the consultation participants assume that only those that establish themselves at the digital customer interface will be able to secure their position on the market in the long run. The overall trend that can be observed is that, by making intelligent use of data, providers of

search engines, social networks or online (comparison) platforms are advancing into areas that used to be the sole preserve of specialised and often regulated providers. According to these respondents, this also includes data that can be obtained on the basis of the Second Payment Services Directive (PSD 2).

2.1.2 Level playing field: financial market regulation

The majority of the respondents consider the existing technology-neutral and principle-based financial market regulatory framework to be adequate in principle – also in relation to financial stability issues. They also see the risk that premature regulatory reactions to new technologies could be detrimental to technology neutrality and that a more rules-based approach would be adopted. There were calls for the removal of regulatory obstacles. Existing paper copy requirements are cited as an example.

However, the respondents also highlighted that restricting the application of existing regulations to institutions and insurance companies could lead to distortions of competition. In particular, there is a perceived discrepancy between the supervisory and regulatory assessment of traditional business models and new business models which rest on the analysis of financial and alternative data for own purposes or for third parties.⁹ It is assumed that new market participants will deliberately attempt to avoid regulation in order to drive innovation. In this context, it was also proposed to examine the extent to which new sales channels, such as targeted marketing measures of platform providers, are to be subject to adviser liability. Some also criticised the fact that new players, such as fintech companies, do not contribute to the funding of supervisory authorities, which leads to distortions of competition.

Although the anticipated additional competition with fintech and bigtech companies could reduce the profits of established providers on the financial market in the short term, the tools currently available to assess

⁸ These and other views in the BDAI report that are referred to in this article can mostly be found in the chapter “Supervisory and regulatory implications”.

⁹ See also section 2.2.

the solvency situation of supervised financial services providers are deemed adequate. However, some of the respondents pointed out that there could be increased pressure on margins particularly if bigtech companies gain entry into the financial market with free and/or cross-subsidised financial services.

2.1.3 Level playing field: competition policy and supervision

A number of respondents indicated that, overall, digitalisation exacerbates the risk of “winner-takes-all” market structures, which could emerge due to monopolistic structures in the area of data access. It was also noted that, for insurers, access to vehicle data, for instance, is important for offering telematics rates. According to these respondents, effective competition policy and supervision are more than ever a prerequisite for a viable financial market – especially in the age of BDAI.

Open markets could also mitigate systemic risk – particularly as far as data access is concerned – as they would result in a wider variety of market participants. It was also pointed out that sufficient competition is important for effective pricing as well.¹⁰ A few of the respondents referred to PSD 2 as a positive example for enabling free access to data. Offering interfaces to the data of bigtech companies in a manner similar to that under PSD 2 is another idea that was put forward.

All in all, the respondents were in favour of closer cooperation between competition authorities and financial supervisory authorities.

2.1.4 Maintaining a level playing field – categorisation of data as a legally protected right

One of the respondents asked how, beyond data protection law, data is to be categorised as an individual legally protected right/legally protected good. It was also noted that a convincing answer needs to be found

¹⁰ See also section 4.1.

for this legal-political and highly complex issue in order to be able to adequately address, in particular, the issues surrounding business models that are primarily data-based. An expedient approach that was suggested would be to draw parallels with intellectual property law.

2.2 Systemic importance and interconnectedness in the age of BDAI

In a nutshell

Key points from the BDAI report

The systemic importance of providers with data-driven business models could rapidly grow due to their scalability and reach. However, systemic importance may also arise if central data or platform providers make identical or very similar structures for processes or algorithms available to a wide range of market participants. Systemic importance could also emerge as a structure from the interaction between various market players. This raises the question of whether and how the banking- and insurance-based concept of systemic importance needs to be redefined in order to keep pace with new business models and market structures.

2.2.1 Redefining and addressing systemic importance: divided opinions

The respondents hold divided opinions on the potential broadening of the notion of systemic importance. On the one hand, it was pointed out that, at the present time, with many technologies still in the developmental stages, it would be premature or would even impede

innovation to lay down new definitions and criteria. In particular, these respondents argue that it is not clear whether BDAI actually increases systemic risk or whether the growing number of market players will not even reduce dependence on banks and insurance companies. In any case, it must be clearly demonstrable on empirical grounds that certain risks may arise in a way that would actually jeopardise the existence of institutions.

On the other hand, many respondents consider that it is important to redefine systemic importance in relation to BDAI. Some even consider that this could be an argument for developing a Basel V framework. It was also noted that categories such as interconnectedness

and complexity are already covered by the current definition of systemic importance. But as the level of interconnectedness and complexity is increasing as a result of digitalisation, more emphasis should be placed on this, making the case for an international discussion on the definition and measurement of interconnectedness within the context of the Basel Committee on Banking Supervision. There were also calls not to restrict the measurement of system risk to traditional financial services providers but to include fintech and bigtech companies that have not been supervised to date. In particular, business models that are based on the monetisation of data should also be taken into account.



2.2.2 Addressing providers that have not been regulated to date based on their interconnectedness with the financial market

Some of the responses indicated that, in many cases, institutions that have not been regulated to date could become essential for the functioning of the entire industry. Cloud service providers, telecommunications providers, automobile manufacturers (see above: "telematics rates", page 18), algorithm and code providers, and providers of data or evaluations such as scorings and ratings were given as examples. With their expertise, these companies could erect monopoly-like structures vis-à-vis consumers and other market players. Another issue perceived as problematic is that procyclical effects may arise if many financial services providers rely on the data and analyses of a single provider, for instance.¹¹

According to these respondents, expanding the notion of critical infrastructures could be one way to address the fact that institutions that have so far not been supervised may become systemically important. In doing so, the same minimum technical requirements could be enforced for both regulated banks and data, platform and algorithm providers that have not been supervised to date. There were also calls for the definition of systemic importance to be broadened in order to include functional and process-related factors. This would allow key companies to identify themselves

more easily, and financial services providers would be able to take this into account.

2.2.3 Ideas to adapt outsourcing systems in the case of fragmented value chains

It was argued that, as value chains are becoming increasingly fragmented, current outsourcing systems, where financial institutions are the only point of contact, may no longer be adequate. It was also pointed out that infrastructure and data providers are, in many cases, direct competitors on the financial market as well. One proposed option would be to use a type of digital signature, especially for products that are created in a fragmented value creation process. Every company involved in the value creation process would have to be named when using such a signature. Overall, these respondents deem that it is necessary to consider whether supervisors should shift their focus from individual institutions to sustaining entire value chains. Smart contracts with a back-up party that would take on any element within the value chain if a company cannot provide it were suggested as a measure to sustain value chains.

Capital buffers, on the other hand, were considered less suitable as a mitigating measure to absorb shocks from outside the financial sector, such as the failure of an IT service provider. Measures aimed at minimising the likelihood of such occurrences are deemed more appropriate. In this context, these include minimum technical standards, targeted scenario analyses and – the subject of the next section – using technology to limit undesirable developments. Volume limits could be another appropriate measure.

¹¹ It should be noted, as a caveat, that another respondent argued that at least credit risk models are closed systems within the individual institutions that could not cause inter-institutional cascade effects.

2.3 Using technology to limit undesirable developments

In a nutshell

Key points from the BDAI report

Closely interconnected systems are susceptible to the rapid and uncontrolled spread of disruptions – not only on trading venues but also elsewhere. This raises the question of whether the technological safeguards which are already widespread on trading venues would also be necessary and could be usefully applied outside of trading venues in the age of BDAI. For example, decoupling mechanisms for data streams could be considered, as the significance of data supplies is increasing considerably as a result of BDAI.

2.3.1 Technological safeguards may be necessary but only if there is a risk of significant losses

Technological safeguards aimed at limiting cascade effects are considered to be potentially necessary. Addressing cascade effects is thought to be difficult, though, if parts of the market within the relevant cascade are not subject to supervision or regulation. The risk of herd and cascade effects is perceived to be greater in the banking sector and on the capital market than in the insurance sector, where key processes – such as risk and benefits assessments – are only initiated by the customers themselves. The respondents suggest examining where new developments, such as real-time payments, are actually needed in the real economy and justify the risk of undesirable developments. The respondents pointed out that, generally speaking, a deceleration with specified minimum time frames and reversibility can limit undesirable developments.

Technological safeguards are, for instance, thought to be worth considering if the level of algorithmic differentiation is too low when using BDAI. Cyber network interfaces could also be sought to reduce the risk of significant losses. Setting up redundant emergency systems could be considered in this context. The diversification of data providers is suggested as another (non-technological) measure. Interfering with data streams is only thought to be justified in situations of extreme risk. Under no circumstances should tools such as circuit breakers be triggered by self-learning algorithms, even with more precise calibration, as market participants would no longer be able to predict when the halt will occur.

2.4 Technology from a supervisory perspective: maintaining transparency and monitoring new structural relationships

In a nutshell

Key points from the BDAI report

Greater interconnectedness could result in greater complexity in the market, for instance, if a market participant's formerly internal processes are distributed among several market participants, including those that have not been supervised to date. The changing structures of dynamic markets and the resulting risks must therefore be monitored, evaluated and addressed from a regulatory and supervisory point of view.

2.4.1 Humans and not computers must bear responsibility – also in the area of financial supervision

The respondents clearly expressed the expectation that humans must continue to bear ultimate responsibility – also in the area of financial supervision – and that this responsibility cannot be passed on to computers. However, the majority of the respondents consider the increased use of technology in supervisory activities to be absolutely necessary. To detect systemic importance, supervisors could also use more external data and take this into account using methods such as network analyses. Interesting external data could be, for instance, consumer expenditure, household saving behaviour or open source data, which in turn could also be of interest for detecting fraud.

2.4.2 Real-time access to data – using API in supervision

According to the responses, analyses that are based on data that is gathered once or on a monthly/quarterly basis will increasingly lose relevance as the market becomes ever more dynamic. Supervisors should therefore seek to maintain real-time access to specific corporate data using application programming interfaces (APIs) and use this to conduct ongoing analyses, such as cash flow analyses, in order to identify new risks and business models at an early stage. Setting up APIs is also considered to be useful for a smooth exchange of data between different (supervisory) authorities. Making use of the interplay between APIs and BDAI would also allow supervisors to monitor outsourcing more effectively. This would mean that the relationships between the institutions involved could be taken into account in supervisory analyses automatically.



3 Supervision of institutions

3.1 BDAI governance

In a nutshell

Key points from the BDAI report

BDAI will create additional opportunities for automating standard market processes. When designing (partially) automated processes, it is important to ensure that they are embedded in an effective, appropriate and proper business organisation. Responsibility remains with the senior management of the supervised institution, even in the case of automated processes. Appropriate documentation is required to ensure this. It may also be necessary to extend established governance concepts, such as the “four eyes” principle, and to apply these to automated processes.

3.1.1 Existing concepts are adequate to a large extent – but interpretation guidelines would be welcome

Most of the respondents consider that the existing supervisory framework is generally adequate, even if the use of BDAI is increasing. BDAI applications do not necessarily involve a higher level of risk and could be regarded as analogous to existing process changes. As a result, they could also be embedded in existing business organisations and the relevant regulations.¹² It was also

¹² For example, under no. 164 of the Minimum Requirements under Supervisory Law on the System of Governance of Insurance Undertakings (*Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen – MaGo*), an analysis of the operational risks must be carried out before products, processes and systems are implemented or are subject to a significant change. The results of this analysis must be included in the decision-making process. In the banking sector, the Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement – MaRisk*) in relation to organisation and documentation (AT 5 and AT 6) are to be observed.

pointed out that current requirements allow supervisors to perform spot checks on processes in a risk-oriented manner. There are also strict requirements concerning senior management that are already incorporated into law. It was also stressed that the use of BDAI is regularly covered by outsourcing requirements, but that responsibility and liability for artificial intelligence cannot be outsourced. If outsourcing to regtech companies were to increase, this could weaken risk culture and expertise within supervised institutions.

The respondents pointed out that some aspects still need to be clarified in relation to how existing provisions are to be applied to BDAI and that supervisors should consider specifying requirements in interpretation guidelines. Irrespective of the complexity of the underlying processes, supervisory requirements must not be weakened under any circumstances.

3.1.2 Ideas to extend existing governance concepts

In contrast to the opinion above, a number of respondents explicitly stated that there is a need to revise existing regulations and supervisory practice in the medium term. In the case of algorithms, for instance, the requirement to implement and cross-check different sub-systems could be examined. In the case of self-learning systems, this would generally mean the use of different learning processes and possibly different training data as well. Outlier mining could also help to detect potentially erroneous decisions. There is also the question of whether current regulations (adequately) cover the validation of BDAI algorithms.

Changes to existing business organisations can be observed in places due to the increased use of BDAI, respondents said. They stated that it is important that institutions change the culture of how mistakes are dealt with to take into account lifelong learning and the associated ongoing changes in algorithms and models. In addition, data quality management (DQM), which has so far been a purely administrative task, is becoming an analytical and conceptual task that will play a key role in companies. The appointment of algorithm officers – comparable to data protection officers in



© iStock/From2015

certain respects– and the establishment of a data ethics commission in companies were also suggested. However, it is essential to ensure that an unclear allocation of responsibility is avoided.

3.2 Traceability and explainability of algorithms and decisions

In a nutshell

Key points from the BDAI report

It is the responsibility of supervised institutions to ensure the explainability and traceability of BDAI-based decisions. At least some insight can be gained into how models work and the reasons behind decisions, even in the case of highly complex models, and there is no need to categorise models as black boxes. For this reason, supervisory authorities will not accept any models presented as an unexplainable black box. Due to the complexity of the applications, it should be considered whether process results, in addition to documentation requirements, should also be examined in the future.

3.2.1 Two levels of explainability: the model and the individual decision

The respondents first indicated that there are two levels of explainability and traceability to be considered: the general model that is used for decision-making on the one hand and the (individual) decision that is reached on the other. They added that the explainability of a model based on machine-learning necessarily depends on the complexity of the processes and data used. However, the reasons for supervisory intervention or regulatory adjustments should not be based exclusively on the complexity of a model or the use of BDAI. Rather, they should always take into account the individual application and the anticipated risk situation.

Traceability is considered particularly important when dealing with customers and is thus important in individual cases since customers often ask for the reasons behind a decision. Only the reasons behind decision-making allow those concerned to correct inaccurate data and decisions based thereon. As in an audit trail, the individual steps in the decision-making process must be traceable at all times. At the very least, the traceability of decisions should always be ensured so that they can be used for forensic purposes.

3.2.2 How to create explainability and traceability

Ensuring the explainability and traceability of algorithms, models and processes is in the institutions' own

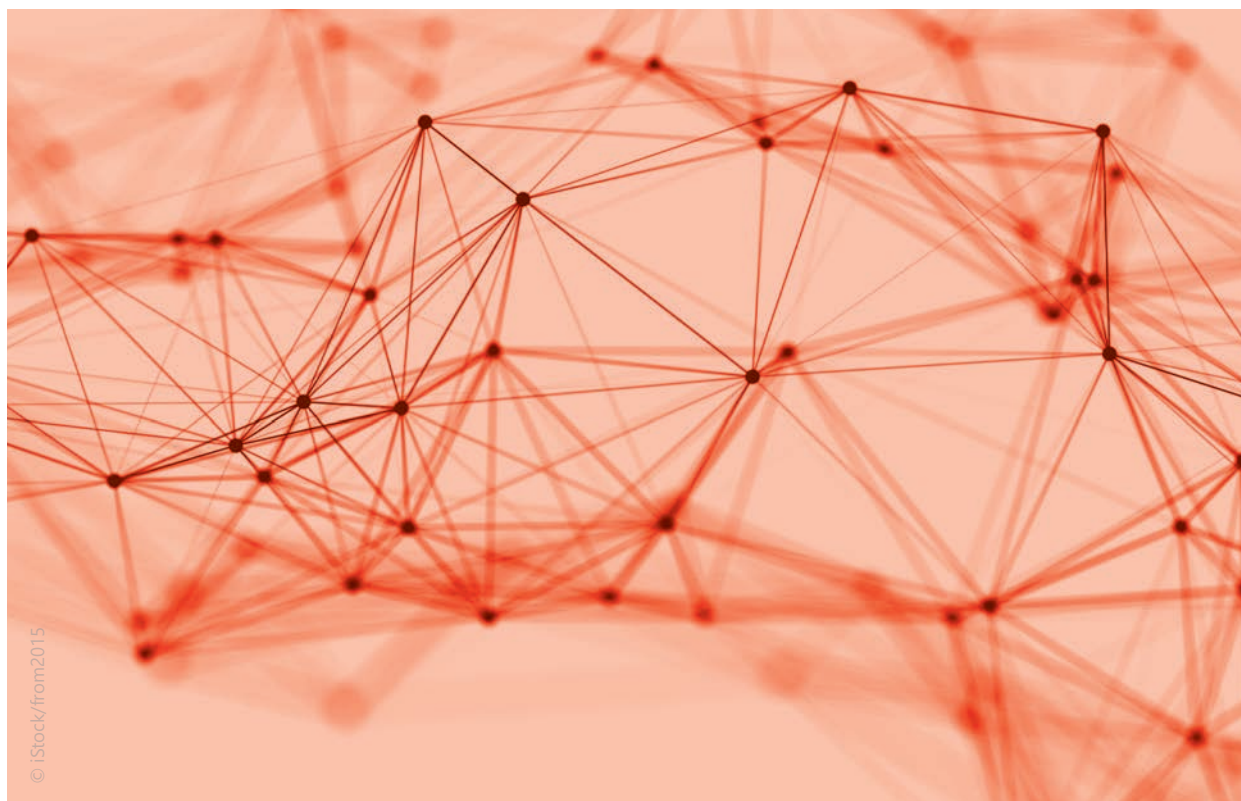
interest, according to a number of respondents. The many (self-)governance measures that exist, such as product oversight and governance requirements (POG) or the internal control system (ICS), are to be noted here. In practice, the model-finding and calibration process often includes backtesting and, in the following application, warning and alarm signals that ultimately result in manual and/or human intervention. Many of the respondents stressed that there must be ways to perform (manual) corrections and general revisions. There must also be processes to shut down BDAI applications that are erroneous or to be discontinued.

One way to ensure traceability is to run existing models and those based on BDAI in parallel. In doing so, it is possible to understand which influencing factors exist. Complex models can also be approximated using simple models. This allows approximations to be made and individual decisions can be explained locally using a simple model. In this context, defining minimum validity for the approximation is key.

3.2.3 Diverging opinion: explainability and traceability as unreasonable restrictions

A number of respondents argued the opposite, stating that it is difficult or impossible to trace the decision-making process of an algorithm in detail due to the nature of BDAI processes. In particular, highly complex processes, such as deep learning, can only be explained with great difficulty. They feel that imposing algorithm explainability as a requirement would create unreasonable restrictions. Due to the complexity of models, supervisors should focus on the validation of results. However, these respondents doubt the usefulness of test scenarios for testing the algorithms of institutions since the inclusion of predefined scenarios entails the risk of overfitting in such scenarios.

In particular, the respondents find it unrealistic to require that every customer profile – i.e. individual decision – is checked. Contrary to the opinion expressed



© iStock/From2015

in the BDAI report, these respondents stated that there is already a limit to explainability due to the complexity of data alone. What is important and technically possible, in their opinion, is to provide evidence on the forecast quality and stability of the models used. The respondents are opposed to the idea of a supervisory approval process for BDAI applications in this context, as this would stifle innovation at institutions. In their view, financial enterprises would be unreasonably disadvantaged compared to other (unregulated) institutions, such as bigtech companies.

3.2.4 Ideas for the supervision of BDAI models

The respondents also raised the question of how BDAI models can be examined by supervisors. If BDAI is used to a significant extent in critical business processes, extended requirements may be needed, e.g. for code

review processes, simulation and penetration tests and reviewing sample profiles. The respondents indicated that requirements for the documentation, explainability and traceability of BDAI applications should be specified, using best practice guidelines, for instance. Effective supervision must also go beyond the examination of documentation and individual cases.

According to these respondents, supervisors must be able to understand complex processes, such as deep learning, and must themselves test the applications of institutions with a risk-sensitive approach. Requirements should be extended but only depending on how critical the relevant process is – also in relation to consumers. For financial supervisors, the use of algorithm-based decision-making systems offers the opportunity but also the obligation to check that algorithm-based decision-making processes and thus large parts of business activities comply with supervisory requirements and civil law.



© iStock/From2015

3.3 Internal models subject to supervisory approval

In a nutshell

Key points from the BDAI report

Any use of BDAI in models that are subject to supervisory approval would also have to be approved by supervisory authorities on a case-by-case basis. Beyond the individual case, it is to be examined whether existing legal (minimum) requirements for the data used and model transparency are sufficient in relation to BDAI or whether additional requirements would be necessary. In the case of dynamic BDAI models, it is necessary to examine which general modifications constitute a model change in the supervisory sense, which banks or insurers, e.g. in line with the model change guidelines for insurance companies, would have to report to supervisors and may have to secure approval for.

3.3.1 BDAI not yet used in models that are subject to supervisory approval

Firstly, the responses indicated that BDAI has so far not been used for internal models that are subject to supervisory approval. Since the stability of internal models is crucial, BDAI models are rather expected to be used for support applications. There are doubts as to whether BDAI models could be approved when notifiable model changes are automated due to a change in data.

3.3.2 Diverging opinions on existing regulation

There are differing views on the applicability of BDAI in models subject to approval, particularly in relation to the model change process.

On the one hand, it was argued that BDAI applications are generally suitable for use in models subject to supervisory approval. These respondents said that using BDAI applications offers a significant opportunity to improve risk modelling. They do not expect that the definition of a model change has to be altered and do not consider that additional regulations need to be created either. They focus on the argument that the requirement to report model changes depends primarily on the impact on risk-weighted assets rather than on the (BDAI) technology used. These respondents do not consider it necessary to extend existing (minimum) requirements for the explainability of models and data either. They acknowledge, however, that this may need to be reviewed if BDAI methods turn out to have a significant impact on the parameters that are relevant in this context. Under certain circumstances, they say it may be necessary to extend regulatory technical standards.

However, other respondents argued that the approval process should be changed. For instance, institutions should be given the possibility to change the models they use more flexibly without having to go through lengthy approval processes for model changes beforehand. Supervisors should allow for quicker “validation feedback loops”. These respondents consider that it would also be desirable not to consider model changes based on the reassessment of parameters as model changes if a model-inherent process determines the need for the reassessment. Some respondents also argued that, already today, a change in parameters does not constitute a model change, at least in the insurance sector. In addition, it was proposed that regular, automated and highly standardised monitoring on a BDAI basis be established for the supervision of BDAI models in the hope that reports on such activities would simplify communication with supervisors. Increasing the use of validation tools, such as stability analyses, sensitivity analyses and backtesting, could be useful, too.

Finally, it was also noted that it would be necessary to examine whether the extensive use of BDAI leads to (undesired) capital relief or a circumvention of supervisory requirements due to a significant decrease in risk-weighted assets.

3.4 Fighting financial crime and conduct violations

3.4.1 Standards already set out in regulations – but it may be appropriate to extend requirements

In a nutshell

Key points from the BDAI report

BDAI can improve the detection rate of anomalies and patterns, and thus increase the efficiency and effectiveness of compliance processes, such as money laundering detection or fraud prevention. If BDAI technology were to make the detection of money laundering far more effective, criminals could potentially turn to companies that are less advanced in this area. It is therefore necessary to monitor whether this will materialise. The results of algorithms must be sufficiently clear to ensure that they can be checked by supervisory authorities and used by the competent authorities (e.g. law enforcement agencies). Minimum requirements may need to be developed for this purpose from a regulatory and supervisory point of view.

The vast majority of the respondents consider it disproportionate and inadequate to impose the use of BDAI in order to fight fraud and prevent money laundering. However, many of the respondents were in favour of introducing general minimum standards, also beyond BDAI applications. Such standards could increase the effectiveness of processes to identify financial crime and breaches of conduct and improve the detection and prevention of money laundering. Since BDAI is developing quickly and individually, these standards should be principle-based. Documentation, particularly in the case of sanction and intervention measures, should be sufficiently clear to ensure that humans can examine it, for instance. It was also suggested that supervisors assess the effectiveness of anti-money laundering systems using, for instance, standardised audit records to be reviewed at least on a yearly basis – as in the case of penetration testing.

Other respondents, however, indicated that there are enough standards set out in the existing principle-based regulations, particularly with the implementation of the 5th EU Anti-Money Laundering Directive. In addition,

special BDAI standards are not considered absolutely necessary as they can be derived directly from academic standards set by the machine learning community.

3.4.2 Feedback loops are indispensable for model calibration

How effectively BDAI models can be used to prevent money laundering depends to a large extent on whether they were calibrated with reliable data. The respondents stated that feedback on model predictions is therefore crucial for the calibration and improvement of models. They added that recent feedback from the German Financial Intelligence Unit (*Zentralstelle für Finanztransaktionsuntersuchungen* – FIU) or law enforcement agencies would be desirable. In this context, the compatibility of data systems is to be considered with regard to data standards and, where applicable, technical implementation using an API. This, it was stated, is the only way to exchange data between companies and investigating authorities without conversion.

3.4.3 Advantages of pooling solutions, particularly for companies that are less familiar with BDAI

Cross-institutional data pooling was also suggested, e.g. to support smaller institutions with a smaller database. Pooling expertise and using joint metrics could also be considered in this context. Being part of a network offering access to an information pool in which information that is relevant to money laundering could be stored and downloaded is viewed as offering the advantage that members would have a holistic view of customer risk – even without BDAI. Some respondents also expressed the wish that supervisors and legislators support such know-your-customer platforms (KYC platforms).

Another suggestion was that supervisors should support institutions whose money laundering detection systems are less advanced in terms of BDAI. However, institutions must also be willing to invest more in new technologies, and supervisors should make their expectations clear to institutions.

3.4.4 Multi-dimensional approach to combating money laundering

Some of the respondents argued in favour of a multi-dimensional approach for combating money laundering, such as a combination of BDAI analyses with peer group comparisons, public data and KYC scores. In addition, some expressed the wish to use the findings made in the detection of money laundering for other purposes – such as credit risk ratings – as well. However, the respondents pointed out that the prohibition of arbitrariness must be observed when using BDAI. Characteristics must not be linked via BDAI arbitrarily – otherwise individuals would be wrongfully prosecuted. Direct or indirect discrimination, as described under Article 3 (3) of the Basic Law (*Grundgesetz* – GG) should not occur either.

3.5 Handling information security risks

In a nutshell

Key points from the BDAI report

The growing complexity caused by BDAI presents new challenges in managing information security risks. The disaggregation of value chains supported by BDAI and ever-larger data volumes are also creating a larger attack surface while simultaneously reducing each individual provider's ability to control the data that is used and distributed. Data manipulation attacks on certain BDAI algorithms may also occur, e.g. in the form of adversarial or poisoning attacks. However, BDAI can also be used to mitigate information security risks, e.g. to analyse and detect danger. Certain encryption systems that allow BDAI methods to be used directly on encrypted data could also be used to strengthen resilience against such risks.

3.5.1 Principle-based regulation for information security risks can also be applied to BDAI

It was also pointed out that information security risks could increase with the use of BDAI technologies – especially due to the growing level of interconnectedness and the resulting increase in the number of weak points. It should be noted, though, that this involves security aspects similar to those to be observed in other software solutions. For this reason, the respondents do not see a need for any (extensive) regulatory adjustments. It was noted that numerous requirements, such as the Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT – BAIT*), the Supervisory Requirements for IT in Insurance Undertakings (*Versicherungsaufsichtliche Anforderungen an die IT – VAIT*), the MaRisk or certain ISO standards, are already taken into account for the use of BDAI. But there are still calls for certain requirements, such as the BAIT, to be further specified in relation to BDAI. If further amendments turn out to be necessary in the future, they should be principle-based as far as possible and

be supplemented with rules-based provisions only where required. Overall, the respondents believe that it is risky to set standards as information technology is developing very quickly.

The respondents all confirmed that it is possible to use BDAI to tackle or detect cyber attacks.

3.5.2 Encryption is no panacea

In order to minimise the fallout from security incidents, data should, in principle, be extensively anonymised or pseudonymised as much as possible. However, it was emphasised that the idea of eliminating BDAI-related risks to data protection with cryptographic processes is unrealistic. Encryption systems may give a false sense of security. It was noted that, from a technical point of view, it is not to be expected that machine learning can be successfully applied to encrypted data outside special applications. One respondent suggested a general ban on data trading for the purpose of data monetisation in order to minimise information security risks and ensure data protection.



4 Collective consumer protection

4.1 Taking advantage of individual customers' willingness and ability to pay

In a nutshell

Key points from the BDAI report

BDAI could make it easier for providers to customise products, services and the corresponding prices at a low cost (and on a large scale). This would allow companies to set higher prices on a case-by-case basis without incurring higher costs. Individualisation could make it more difficult to compare prices overall. BDAI could also allow providers to take advantage of customers' (situational) willingness and ability to pay if they have this information. In particular, BDAI could help to link financial data and behavioural data to other (sources of) data and make it easier to estimate how much customers are willing to pay. In theory, this data could promote the extraction of consumer surplus, also outside the regulated financial sector. A BDAI-driven trend towards only a few key customer interfaces ("winner-takes-all" market structures) could further promote such developments thanks to enhanced data access and evaluation synergies. For this reason, consumers need to be made more aware of how their (financial) data may be used and the significance it has.

4.1.1 Distinction between risk-adequate price differentiation and taking advantage of individuals' willingness to pay

In the financial sector, a distinction is to be made between pricing based on an individual's willingness to pay and price differentiation, which is generally necessary due to the individual risk costs incurred. According to the respondents, such price differentiation should also be possible in the future to ensure risk-adequate pricing. It was also noted that situational insurance, for instance, is regularly calculated on the basis of (a multi-annual or) an annual premium and is more expensive than long-term insurance as it is often based on a period involving higher risks.

4.1.2 Competition and long-standing business relationships are arguments against the extraction of consumer surplus on the financial market

Most of the respondents stated that using BDAI would not make it easier to extract consumer surplus. In particular, fierce (price) competition for customers was given as a counter-argument. Effective competition policies and competition supervision were attributed a key role in preventing unilateral pricing. A market failure, such as the formation of monopolies and oligopolies or pricing agreements and agreements that restrain competition, is seen as a prerequisite for taking full advantage of the consumer surplus.

It was also indicated that regulations such as the German Regulation on Price Indications (*Preisangabenverordnung* – PAngV) are applicable in the banking sector. For these respondents, pricing that is alleged to be arbitrary or based solely on the individual is therefore hardly imaginable on a large scale in the customer business. For financial services providers, fairness towards customers and keeping their trust are of vital importance for customer relationships. Fair pricing is thus in their own interest and is often already incorporated in company codes of conduct. Other respondents argued that consumers are themselves

¹³ Consumer surplus is the difference between the maximum price that a consumer is willing to pay for a product or service and the price that they actually have to pay on the market.

responsible if, by giving their data, their willingness or ability to pay is taken advantage of. The proposition that financial and behavioural data is widely used outside the core business was countered by the argument that no such usage can be observed at present.

4.1.3 BDAI could increase transparency for product alternatives

Another argument cited against the extraction of consumer surplus is the fact that BDAI makes it easier for customers to gain an overview of prices and the product alternatives that are available. Strong market dynamics fuelled by BDAI could even lead to a drop in prices, it was argued. In particular, customers with a low willingness to pay may also have new consumption options thanks to BDAI applications.

4.1.4 Greater market concentration could give rise to new risks in the future

Some of the respondents disagreed, noting that it may already be possible to partially extract consumer surplus as there are only a few online platforms. If data-based price differentiation methods were to be more widely used, this could exacerbate asymmetries of information between consumers and institutions – to the consumer's disadvantage. If this were to result in new risks, the initiation of supervisory or regulatory measures would need to be considered. In addition, common requirements should be laid down on the obligation to provide information on the data that would be used for pricing. Respondents also noted that suitable regulations should be in place for the use of data stemming from the Internet of Things.



4.1.5 Consumers need to be given more information

Some of the respondents explicitly stressed that it is important and necessary to inform and educate consumers. Consumers must be able to reach informed decisions in relation to their personal data and financial products. Consumer protection organisations, which are responsible for informing customers of any changes in market supply and potential pitfalls in the selection of products available, have a key role to play in this context, it was asserted. According to the respondents, it would also be beneficial to enhance the data sovereignty of customers.

4.2 Differentiation and potential discrimination

In a nutshell

Key points from the BDAI report

Using BDAI can increase the risk of discrimination: algorithms could be based on features for which differentiation is prohibited by law. Approximations are still possible, even if unauthorised features are not used, as there is a lot of other data available allowing conclusions to be drawn. There is also the risk that differentiations are made on the basis of false assumptions or false conclusions drawn by algorithms, and that consumers may in fact be discriminated against – even if this is unintentional. When programming algorithms and evaluating results, providers must take special care to ensure that individual consumers are not discriminated against. This raises the question as to what monitoring and transparency mechanisms could be useful in this context.

4.2.1 Risk of indirect discrimination is increasing – evidence of freedom from discrimination is essential

The risk of indirect discrimination (as described above) could increase with the use of BDAI, according to some of the respondents. Providers should therefore provide proof that their systems run in a non-discriminatory way and that the variables used are relevant. There were calls for algorithms to be checked regularly – by third parties and within institutions. One respondent even called for a state monitoring system for all BDAI algorithms, including those outside the financial sector. In addition, potential discrimination must already be looked into during the development of models, using methods such as bias correction, for instance. It was noted that overall, imposing a ban on discrimination in the context of BDAI would be a difficult task, from a technical point of view, for which a completely satisfactory solution has yet to be found. Retrospective spot checks of individual decisions are, according to the respondents, the only feasible approach at present.

4.2.2 Many anti-discrimination rules are established in the insurance sector

In the insurance sector, there are already a number of sector-specific provisions that must be observed in addition to general requirements such as the German General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz* – AGG) and the German Genetic Diagnosis Act (*Gendiagnostikgesetz* – GenDG). Reference is made in particular to the German Equal Treatment Act for Life Insurance (*Gleichbehandlungsgrundsatz für Lebensversicherungen*) (section 138 (2) of the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz* – VAG) and the German Insurance Contract Act (*Versicherungsvertragsgesetz* – VvAG) (section 177 (1) of the VAG). Furthermore, it was claimed that supervisors have an extensive set of tools that are considered adequate for dealing with violations of consumer protection law. Any additional microregulation or micromanagement of product features and pricing models would stifle innovation.



Illegal discrimination is easier to prevent in the insurance sector than in other industries, respondents stated, since every characteristic, with the exception of gender, can only be a differentiating factor if it is risk-relevant.

4.2.3 Definition of discrimination and freedom from discrimination

In cases where a characteristic has only two variants (e.g. smoker/non-smoker), freedom from discrimination is deemed to exist if both groups are just as likely to enter into a contract (on the same terms). In other words, two consumers with the same risk-relevant features should pay the same price. Respondents stressed that, in the case of characteristics that have not been gathered, it is not possible to guarantee that such characteristics have no influence over the result of a model decision. According to the respondents, if a characteristic is known, the model decision could in almost all cases be revised to prevent discrimination. Hence, some of the consultation participants deem that a data set containing precisely the characteristic to be ruled out is necessary in order to rule out any form of illegal discrimination.

4.2.4 Broader social debate appears to be necessary

The respondents see a need for a social debate in order to distinguish between desirable differentiation and unacceptable discrimination. This could promote the acceptance of new technologies. However, it should be noted that the greater differentiation made possible by BDAI could counteract phenomena such as moral hazard and adverse selection. If these opportunities are not used, the result could be unfair distribution or conditions in relation to risk-relevant information.

As regards differentiation, it was noted that highly segmented rates were not successful in the past. Some considered that refined segmentation jeopardises the basic principle of insurance coverage.

4.3 Access to financial products

In a nutshell

Key points from the BDAI report

Linking different types of data (sources) could be a particularly promising way to improve risk assessments in the financial sector. In future, customers could therefore be confronted with situations where they have to give access to more (new) data (sources) – such as social media accounts. It is therefore possible that future data requirements will go far beyond current requirements and that the price of a financial service will depend on whether this data is made available. In addition, BDAI selection mechanisms could inordinately hamper access for individual consumers to certain financial services. The situation can be particularly precarious if consumers are disadvantaged by having access to a narrower range of products but are unaware that this is due to their personal data. This raises the question of how access to (affordable) financial services can be maintained if customers cannot or do not want to grant access to (new) sources of data to a significant extent.

In this set of topics, the respondents focused on insurance products. However, many of the arguments that were given are generally applicable to financial services.

4.3.1 Data is essential for risk assessments

Most of the respondents pointed out that the provision of data is essential for risk assessments in the financial sector (e.g. creditworthiness assessments). For instance, the basic principle of private insurance, they stated, is that premiums are oriented towards insured risk since private insurance – as opposed to social insurance – is based on the idea that only the risk of random fluctuation is distributed between the community of policyholders. Whether and on what terms a customer can obtain (private) insurance – and, generally speaking, a financial service – therefore depends on the individual risk.¹⁴ It was also stressed that customers who disclose less risk-relevant data or information have a different risk profile. This means that premium rate conditions differ depending on how much relevant data is available.

4.3.2 Determining risk-relevant data is key

It is proposed that legislators, supervisors or industry (through self-commitment) create binding definitions to determine what data is actually necessary for appropriate differentiation. Government authorities could then ensure that consumers who only consent to their data being processed to the extent required are not refused access to financial services. Respondents noted, though, that it is unclear what risk category such consumers would fall into, i.e. whether freedom from discrimination can be deemed to exist if these customers are not denied access to a service altogether, but still obtain, where applicable, services on less favourable terms. Respondents also warned that the possibility of

the price for a financial product dropping if more data is provided could undermine the right to informational self-determination.

4.3.3 Competition governs access to financial products – also for customers who provide data only to the extent required

It was also noted that competition governs access to financial products – also for customers who provide data only to the extent required. The respondents observe a growing trend among providers highlighting contracts that can be entered into conveniently using data only to the extent required as a selling point. The amount of data and the form in which data has to be provided in order to enter into a contract is already a competition factor, according to the respondents. It was also noted that the requirements for data minimisation (*Datensparsamkeit*) are generally at odds with the fact that BDAI systems require a sufficiently large database. Requiring companies to offer products that no longer meet market standards and are based on obsolete technologies is no solution, respondents stressed. Such products would be of no interest to customers, and legal interventions would be obsolete as well.

4.3.4 Diverging opinion: proposal to expand basic products

To prevent the exclusion of customers who are reticent about sharing their data or who are non-digital, other respondents call for legal requirements obliging providers to offer non-digital contracts as well. Clearly defining when a contract is non-digital or conventional seems to be a highly complex task, according to the respondents. As with the introduction of the right to open a basic payment account, legislators could guarantee basic coverage, e.g. for health and long-term care insurance, personal liability insurance, occupational disability insurance and motor vehicle liability insurance, especially since growing differentiation could mean that certain groups of customers may no longer be insured at all or only at a very high cost. This would be particularly problematic for customers who are not able to influence risk themselves. It was also noted that supervisors could

¹⁴ Customers with the same risks receive the same terms, while customers with different risks receive different terms, respondents wrote, citing the VAG, where the principle of equal treatment is stipulated in section 138 (2), section 146 (2), section 147 and 161.

create a certificate for financial services requiring limited amounts of data, which, if accepted as a seal of quality, could minimise the risk that consumers who are reticent about sharing their data are not given access to services. However, the respondents also warned that special legal requirements for conventional financial products and products requiring limited amounts of data may suggest that the principle of data minimalisation does not apply to other (financial) products.

4.4 Consumer sovereignty

In a nutshell

Key points from the BDAI report

The potential of BDAI can only be exploited for financial services if it is possible to gain and maintain the trust of consumers by ensuring that their data is used as desired and in accordance with the law. Providers should particularly ensure that consumers are able to make sovereign decisions by ensuring that consumers are adequately informed about the potential reach and consequences of the use of their data and that they are given reliable options to control how their data is used and have genuine freedom of choice. It is not enough to provide consumers with highly complicated terms and conditions, which are usually accepted without being read. In particular, technical (data protection) measures (e.g. privacy-preserving data mining) or a “privacy by design” concept could also bolster consumer trust in BDAI innovations.

4.4.1 Data sovereignty regarded as a key issue

Most of the respondents clearly stated that the data sovereignty of consumers is a highly relevant issue – not only in the financial market but also in other sectors.

They noted that it must be ensured that consumers are given clear information on what their data is going to be used for, that they are aware of the implications and that they are able to make a well-informed decision when sharing their data. Genuine freedom of choice is deemed to be an essential requirement. Social and financial pressure, lock-in and network effects, on the other hand, are considered problematic and counterproductive. Any regulatory measures must take into account these factors in addition to the limited ability of consumers in general to gather and process information. In this context, a minimum level of data protection is proposed, which would also apply after consent has been given. But if all requirements are met, the scope of action of financial services providers should not be further restricted, according to the respondents.

4.4.2 Financial supervisors are not primarily responsible – but a dialogue with other authorities is necessary

The respondents stressed that they do not consider that financial supervisors are responsible for reinforcing the data sovereignty of consumers. In this context, supervisory activities should focus on and be limited to the supervision of violations of consumer protection law. Other authorities and society as a whole need to be involved. Digital training, consumer education and learning opportunities for children and adults were proposed among other measures to raise awareness of the pros and cons of “paying with personal data”. A closer dialogue between financial and data protection authorities is deemed necessary.¹⁵

4.4.3 Ideas to strengthen and ensure data sovereignty

According to the respondents, data sovereignty can be guaranteed, in principle, by complying with legal provisions such as those set out in the General Data

¹⁵ There were also calls for financial supervisors to work more closely with competition authorities and competition supervisors – see section 2.1.3.



Protection Regulation and a transparent information policy geared towards consumers. To ensure that consumers have a better overview of the data they agree to share, the development of a data protection cockpit, for instance, was suggested. It must be generally ensured that personal data is to be used only in clearly defined and documented processes. Consumers must be given a point of contact that they can turn to, regardless of where in the chain of events damage or problems occurred. According to the respondents, consumers need a complete overview of who assumes liability, even in fragmented value chains.

It was also noted that industry standards in the financial sector could become de facto minimal requirements for the use of personal data if they are accepted or embraced by customers. This would allow customers to themselves choose reliable partners for the provision of financial services. For instance, it was noted that insurers, in cooperation with data protection authorities, have recently undertaken to ensure that data is used only to the extent required in a code of conduct that was published. Finally, it is assumed that there will be service providers specialising in the enforcement of informational self-determination. Such providers could

use BDAI methods to find out where a user's personal data is stored. Service providers could then be asked to delete such data at the user's request.

4.4.4 Ways to ensure data protection using technology

The general view was that trust can be fostered by using processes such as privacy-preserving data mining and, as far as possible, pseudonymisation and anonymisation. Calling for the establishment of privacy-preserving data mining as a basic requirement to be strictly observed is considered problematic, as this often involves considerable restrictions for the development of algorithms.¹⁶ It was noted that privacy-preserving data mining relies on a trusted third party in practice. Financial institutions could play an important role here. However, the respondents noted that government authorities may also be required to take on the role of a trusted third party due to the potentially high liability risk.

¹⁶ There is also the opposing view that the potential of BDAI could often be fully taken advantage of even if these processes are used.

We will no longer only look at individual companies

Interview with

Felix Hufeld

President of BaFin



Mr Hufeld, the respondents to BaFin’s consultation point out that, by making intelligent use of data, providers of search engines, social networks and online (comparison) platforms are advancing into areas that used to be the sole preserve of specialised and often regulated providers. What is your opinion on this?

If these and other tech or platform-based companies were to offer regulated financial services, they would, of course, have to meet the same supervisory and regulatory requirements as all the other institutions. But even if they do not provide any regulated financial services themselves, the respondents rightly pointed out that these companies could become essential for the functioning of the entire industry – e.g. as providers of cloud services, algorithms, data, and evaluations such as scores and ratings. These have been around for a while, but once BDAI and automated interfaces come into play, the impact of these services on the financial market could be even more immediate.

The respondents put forward a number of interesting ideas on how to address the growing importance of these providers for the financial market from a supervisory and regulatory point of view. One suggestion was that outsourcing companies should be

subject to minimum technical standards similar to those for regulated banks. Another idea was a digital signature that lists all the companies involved in the development or provision of a product. This, it is argued, would help customers to understand more clearly who is behind a product or service. Above all, accountability would not lie solely with the financial services provider involved but would be extended to other companies along the entire value chain. In addition, a back-up party could also be agreed upon for every element within a product’s value chain, which would be obliged to step in if one of the companies involved cannot provide the expected service. Tech solutions, such as blockchain-based smart contracts, could play a part here.

All these considerations confirm the proposition we put forward in our BDAI report, which is that, as regulators and supervisors, we will no longer only look at individual companies but will increasingly consider value chains that are spread across multiple companies. Supervisors would then also focus on the activities of companies that are not part of the regulated financial sector but can still have an impact on customer trust and the integrity of the financial market as such. I am not saying that BaFin should supervise bigtech companies that do not provide financial services as a whole. What is important

to me are some of the activities and conduct of such companies in order to establish a direct supervisory mandate in this respect.

Let's continue with value chains. Value can be created by linking data from various sources – for instance at key customer interfaces on platforms. How could the growing importance of (financial) data be taken into account?

We agree with most of the respondents on this matter. The growing importance of data in the age of digitalisation is also based on the fact that data from different sources is combined and compared, allowing new information to be obtained. By connecting data on financial transactions and data on the behaviour of consumers, it is possible to have a fairly clear idea of the amount of money that customers are willing and able to pay for products and services. In addition, the emergence of platform-based business models is breaking down information silos, and information from one area can have an impact on other areas. It is only logical that the authorities supervising different areas of economic life collaborate more closely and share information with each other – provided that this is permitted by law, of course. As the use of BDAI is increasing, data protection authorities and competition watchdogs are particularly important for us as financial supervisors. Our supervisory counterparts abroad are not to be forgotten either.

Of course, market participants see great economic potential in digging up treasure troves of data. But with data mining – as with any conventional process of prospecting, mining and utilising resources – we must keep a watchful eye on the associated risks. For us supervisors, it is crucial that consumers and providers are confident that the financial market is stable and that things are being done as they should be. We also need to consider what negative spillover effects there can be when financial data is used in value creation processes outside the financial market – even if formal consent has been given in accordance with the law. Social achievements, such as the protection of privacy

and informational self-determination, should not be undermined under the guise of innovation – e.g. by obtaining people's consent to share their data by giving them the impression that there is no alternative. Not everything that is technically possible, innovative and economically sensible in the short term is all the above if looked at from a holistic and long-term perspective.

Let's take another look at the financial market. Do you consider that the use of data is a key issue that could become more relevant for the financial market as a result of BDAI?

The argument that data is necessary for assessing risk could be used to justify the need to gather virtually all data in the context of providing financial services – although such practices have not been observed on the German financial market to date. The responses to our consultation have made one thing clear to us: we have to increasingly ask ourselves which data is really needed for an appropriate assessment of risks – in other words, for a suitable differentiation as required by supervisors. Insurers that took part in our consultation have, in cooperation with data protection authorities, already pledged to minimise the use of data in a code of conduct that has been published. But what I find interesting in this context is the fundamental question of where the limits of data collection and analysis should be in the case of BDAI. At what point does a marginal improvement in risk assessment justify the collection of more data? Which data can we categorise as offering real long-term and material advantages while ensuring a balance between the information that needs to be obtained and other objectives such as data minimisation (*Datensparsamkeit*)? I think we need to have a broad dialogue with all those concerned – but we also need to ask ourselves, as a society, where we want red lines to be drawn in the brave new world of data.

Let's now turn to responsibility in the context of self-learning decision support systems. In the BDAI report, BaFin pointed out that humans must always bear ultimate responsibility and that this responsibility cannot be passed on to computers.



This also applies to financial supervision, according to the respondents. What is your view?

The Fraunhofer Institute for Intelligent Analysis and Information Systems was one of the institutions that assisted us with our BDAI report. Fraunhofer stressed that the successes of machine learning have so far only been observed in highly specific applications and that approaches for the general simulation of human intelligence are still not foreseeable. We can therefore expect to rely on the interplay between artificial and human intelligence in the foreseeable future. Responsibility will and must therefore continue to rest with humans in the area of financial supervision, too. Financial supervision is and will remain a flexible process that focuses on the assessment of complex issues. But artificial intelligence can support us as supervisors and help us prepare decisions and establish better and quicker processes. In highly data-driven areas – such as market abuse analyses or, perhaps in the future, money laundering prevention – supervisors will not be able to do without BDAI.

In the responses to the consultation, there were calls for manual or human intervention in decision support systems based on artificial intelligence. However, imposing algorithm explainability as a requirement is seen as unreasonable restrictions. What is your opinion?

In my opinion, blind trust in technology is dangerous. Humans must be able to intervene and it must be possible to switch off automated processes. As mentioned earlier, humans, not machines, bear ultimate responsibility. We need to bear this in mind when evaluating new processes.

As far as the explainability of AI systems is concerned, we stressed in our report that a distinction should be made between explainability and transparency. Transparency means that the behaviour of the system as a whole can be understood in its entirety. Fraunhofer pointed out that this is often impossible to achieve as many models are inevitably highly complex. On the other hand, explainability is a criterion that is

far easier to fulfil from a technical point of view, according to Fraunhofer, as it focuses on identifying key influencing factors behind a specific decision reached by a system.

Respondents to our consultation also hold the view that we as supervisors are confronted with the question of whether and how BDAI models can be examined. Extended requirements for business-critical process areas were suggested, including the use of code review processes, simulation and penetration tests and the assessment of sample profiles. Respondents also called on BaFin to lay down specific requirements for documentation and the explainability of BDAI applications. But do not expect us supervisors to shoot from the hip. We should first deepen the dialogue with academia and industry and make sure that industry best practices are developed. Once we know if and how they

work, we can, as a next step, consider to what extent we will derive standards from them.

What are the next steps for BaFin now that the consultation has closed?

We have started evaluating the responses, which we have summarised in this article. A number of subject areas are becoming apparent and we intend to prioritise and deal with these based on how urgent and significant they are. To address all the aspects of this complex topic, we need to work even more closely with industry, academia and other authorities in some areas. This is something we intend to do in the near future. But we have already achieved something with our BDAI report and the consultation: we have looked into the burning questions surrounding this topic – and placed them in the public eye.

Mr Hufeld, thank you for the interview!

III

Outsourcing activities and processes allows banks to focus on their core competencies and to improve their services. However, outsourcing can only work if institutions can ensure that risks are kept under control. In the age of digitalisation, banks and supervisors are facing new challenges.

When banks outsource IT services

Authors

Raimund Röseler

Chief Executive Director
of Banking Supervision,
Federal Financial Supervisory Authority (BaFin)

Ira Steinbrecher

Division for Policy Issues relating
to IT Supervision and Inspections,
Federal Financial Supervisory Authority (BaFin)

1 Introduction

For companies, outsourcing activities and processes has always been an efficient way to benefit from the division of labour. As early as 1776, Adam Smith stated that the greatest improvement in the productive powers of labour seems to have been the division of labour.¹ Banks are also taking advantage of outsourcing for many different reasons: in a comparative study conducted by BaFin in 2013, all of the institutions examined stated similar motives: cost savings, process optimisation and – especially in the case of IT – quality improvement, access to specialist knowledge, using synergies and saving resources. Saving costs was the primary motive for all of the banks.²

Over the last few decades, institutions have been increasingly relying on IT systems to support their processes and activities. Digitalisation is therefore nothing new for these institutions – but it has so far mainly taken place internally.³ As IT infrastructures are becoming increasingly interconnected, the opportunities for a division of labour between market players have multiplied in the area of information processing. This has allowed banks to outsource IT services, meaning that parts of the value creation process are no longer covered exclusively by the institutions but sourced from third parties as IT services. Value chains are therefore becoming increasingly split and decentralised.⁴

1 Smith, *The Wealth of Nations: Books I-III*, Penguin Classics: 1982, page 109.

2 See BaFinJournal expert article “Outsourcing: BaFin compares outsourcing by institutions” dated 15 August 2013.

3 Gampe, Digitalisation and information security in the financial and insurance sectors as a focus of regulatory requirements, in: BaFinPerspectives, Issue 1/2018, page 70.

4 See also Felix Hufeld’s speech on 28 May 2018, Digitalisierung – Chancen und Risiken in der Kredit- und Versicherungswirtschaft (Digitalisation – risks and opportunities in the banking and insurance sectors), www.bafin.de/dok/10976554, retrieved on 4 January 2019.

2 Standardisation of IT services

Standardised IT services allow companies to achieve economies of scale and thus save costs as described above. IT service providers, such as data centre operators offering standardised services to many different clients and customers (multi-client service providers), have been meeting the demand for such standardised services for a few years already. Banks predominantly outsource activities and processes in the area of IT, which is a trend BaFin analysed as early as 2013 and that can still be seen today.⁵ As digitalisation progresses and the importance of information technology and financial technology (fintech) grows, institutions are adjusting their business

models, processes and systems to make use of these technologies. IT has now become one of the most outsourced activities for this reason.⁶ This goes hand in hand with the fact that outsourcing – in addition to seeking cost savings exclusively – is increasingly gaining a strategic dimension as credit institutions are seeking to focus on their core competencies and thus improve their services by outsourcing activities and processes.⁷

5 loc. cit. (footnote 2).

6 EBA/GL/2019/02, page 6.

7 See also PricewaterhouseCoopers (PwC), *Fit für die Zukunft – Wie sich bankfachliche Dienstleister erfolgreich für den Business Process Outsourcing Markt 2020 aufstellen* (Fit for the future – how banking service providers are successfully preparing for the 2020 business process outsourcing market), *Business Process Outsourcing Study*, Frankfurt am Main, page 27.

3 Outsourcing to the cloud

A current example of outsourcing where both costs and strategy play an important role is the noticeable increase in the use of cloud services.⁸ Cloud service providers offer a wide range of services, from providing storage space or computing power (Infrastructure as a Service – IaaS) and making developer platforms available (Platform as a Service – PaaS) to set up websites, for instance, to providing software applications and web applications (Software as a Service – SaaS)⁹ that run on the cloud service provider's systems. The use of such cloud services allows institutions to find new ways to

make parts of their business processes more efficient in terms of IT and, as described above, to focus on their core competencies and pursue new data-driven big data business strategies.

8 See EBA/GL/2019/02, page 6.

9 BaFin Merkblatt, *Orientierungshilfe zu Auslagerungen an Cloud-Anbieter* (BaFin's guidance notice on outsourcing to cloud service providers), page 4, www.bafin.de/dok/11681598, retrieved on 4 January 2019.

4 Risks of outsourcing

However, outsourcing does not only offer advantages; it entails risks for the outsourcing institutions, too. If risks are no longer within the organisational structure of institutions, there is a risk that they can no longer be fully identified or managed.¹⁰ This has prompted

German legislators and supervisors to develop specific requirements for risk management in the context of outsourcing. These requirements are generally technology-neutral and can therefore be applied to cloud service providers as well.

¹⁰ Hufeld, "Supervision and regulation in the age of big data and artificial intelligence", in: BaFinPerspectives, Issue 1/2018, page 16.



© iStock/from2015

5 Requirements for outsourcing to cloud service providers

Firstly, all forms of outsourcing are subject to the requirements under sections 25a and 25b of the German Banking Act (*Kreditwesengesetz* – KWG) in conjunction with AT 9 of the Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement* – MaRisk).¹¹ In addition, material outsourced activities and processes that are identified by the institution itself as part of a risk analysis are subject to special requirements concerning, for instance, the drafting of contracts and the termination of the outsourcing arrangement. Furthermore, material outsourced activities and processes must be managed and monitored and clear responsibilities must be defined. These provisions – sections 25a and 25b of the

KWG in conjunction with AT 9 of the MaRisk – were, however, specifically developed for certain outsourcing arrangements where contracts may be drawn up individually to include the corresponding powers to give instructions and conduct audits.

Given the considerable importance of IT, BaFin published its Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT* – BAIT)¹² in November 2017, which includes specific requirements for outsourcing and the procurement of other external IT services in Module 8. One of the primary objectives of the BAIT is to raise awareness of IT risks in institutions, especially at management levels.

¹¹ Circular 09/2017 (BA) – Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement* – MaRisk).

¹² See also Gampe, Digitalisation and information security in the financial and insurance sectors as a focus of regulatory requirements, in: BaFinPerspectives 1/2018, page 68 et seq.



6 Guidance on outsourcing to cloud service providers

Outsourcing to cloud service providers comes with new challenges for both institutions and supervisors. For this reason, BaFin published a guidance notice on outsourcing to cloud service providers (*Merkblatt "Orientierungshilfe zu Auslagerungen an Cloud-Anbieter"* – only available in German) in November 2018.¹³

¹³ The guidance notice is aimed at companies in the financial sector that are supervised by BaFin (credit institutions, financial services institutions, insurance undertakings, *Pensionsfonds*, investment services enterprises, asset management companies, payment institutions and e-money institutions). This article focuses on institutions such as those listed under section 1 (1b) of the KWG (credit institutions and financial services institutions).

With this guidance notice, BaFin and the Deutsche Bundesbank sought to clarify how they assess this form of division of labour and various contract clauses in particular. Another objective was to make supervised institutions aware of the issues relating to cloud services and the associated supervisory requirements. To achieve this, the guidance notice refers to key aspects that supervised companies should observe when outsourcing to cloud service providers, e.g. when analysing risks and drawing up contracts. However, BaFin has not set out any new requirements in the guidance notice and has only provided information on current supervisory practice.

7 Discussions on the power to give instructions

In its guidance notice, BaFin addressed current discussions regarding the extent to which the requirements under AT 9 of the MaRisk are to be complied with when drawing up outsourcing arrangements for standardised IT services, for instance in relation to agreements on the power to give instructions. When outsourcing activities and processes, institutions must be able to give service providers individual instructions on outsourced activities and processes and the underlying controls accordingly. However, it may be difficult to issue instructions when using standardised services as these can also have an impact on the services that cloud service providers perform for other customers. This is why institutions may refer to the note on AT 9 number 7 of the MaRisk in cases like these, which allows them to waive explicit agreements granting institutions the power to give instructions if the service to be performed

by the service provider is specified sufficiently clearly in the outsourcing contract. These waivers may also be applied when outsourcing to cloud service providers.



8 To what extent can audit rights apply?

Another key question is currently under discussion: to what extent can the stipulated unrestricted audit rights apply to cloud service providers? Firstly, the guidance notice makes it clear that it is necessary to ensure that institutions receive the information they need to appropriately manage and monitor the risks associated with outsourcing.¹⁴ In order to be able to manage and monitor these risks appropriately, institutions must be able to inspect not only the outsourced activities and processes but also the underlying control processes. Cloud service providers must therefore grant them unrestricted audit rights.

Cloud service providers consider that the exercise of audit rights by institutions entails risks for operations (e.g. for data centres) if multiple audits are conducted at the same time. The guidance notice therefore sets out various simplifications that institutions can use. For instance, in cases where material activities and processes are outsourced, the internal audit function of a bank may, under certain circumstances, waive conducting its own audit activities in accordance with BT 2.1. number 3 of the MaRisk. Audit activities can then be performed by the cloud service provider's internal

audit function, the internal audit function of one or more outsourcing companies supervised by BaFin on behalf of the outsourcing bank (pooled audits), a third party appointed by the cloud service provider or a third party appointed by the outsourcing institutions.¹⁵

Another simplification: institutions may, as a rule, rely on evidence or certifications based on current standards,¹⁶ the audit reports of recognised third parties or the internal audit reports of the cloud service provider; however, they should take into account the scope, level of detail, up-to-dateness and suitability of the certification body or auditor of the evidence, certifications and audit reports. If the internal audit function uses such evidence, certifications or audit reports for its activities, they should be able to verify any evidence underlying the above.¹⁷

14 BaFin Merkblatt, *Orientierungshilfe zu Auslagerungen an Cloud-Anbieter* (BaFin's guidance notice on outsourcing to cloud service providers), page 8, www.bafin.de/dok/11681598, retrieved on 4 January 2019.

15 BaFin Merkblatt, *Orientierungshilfe zu Auslagerungen an Cloud-Anbieter* (BaFin's guidance notice on outsourcing to cloud service providers), page 9, www.bafin.de/dok/11681598, retrieved on 4 January 2019.

16 Such as the International Organization for Standardization's International Information Security Standard ISO/IEC 2700X and the Cloud Computing Compliance Controls Catalogue (*C5 Anforderungskatalog Cloud Computing*) of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik – BSI*).

17 BaFin Merkblatt, *Orientierungshilfe zu Auslagerungen an Cloud-Anbieter* (BaFin's guidance notice on outsourcing to cloud service providers), page 9 et seq., www.bafin.de/dok/11681598, retrieved on 4 January 2019.

9 Limits to outsourcing

Institutions can make use of the simplifications described above in order to outsource to cloud service providers as efficiently as possible and maximise economies of scale in this way. However, outsourcing to cloud service providers has its limits, too. BaFin President Felix Hufeld has repeatedly pointed out that the management bodies of outsourcing companies remain ultimately responsible.¹⁸ The European Banking Authority (EBA) has also made it clear that the responsibilities

of an outsourcing institution's management body can never be outsourced. Outsourcing must not lead to a situation where an institution becomes an "empty shell" that lacks the substance to remain authorised. To this end, the management body should ensure that sufficient resources are available to appropriately support and ensure the performance of its responsibilities, including overseeing the risks and managing the outsourcing arrangements.¹⁹

¹⁸ See also Felix Hufeld's speech on 28 May 2018, loc. cit. (footnote 3); Mußler, FAZ, 8 December 2018, page 26.

¹⁹ EBA/GL/2019/02, page 7.



10 Outlook

Irrespective of the guidance notice, which shows the current status of supervisory requirements and administrative practice, there is the question of whether other or more detailed provisions will be needed to manage risks when outsourcing IT services. International standard-setters, such as the G7, the Basel Committee on Banking Supervision (BCBS) and the EBA, are currently looking at third-party and outsourcing risks. BaFin will examine on an ongoing basis whether supervisory provisions and administrative practice are appropriate and will adjust them if necessary. Guidelines such as the G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector, published in October 2018, and the EBA's guidelines on outsourcing arrangements, published on 25th February 2019, will play an important role in this context.

There is also the question of whether and to what extent it is useful and expedient to set specific requirements for multi-client service providers in general and cloud service providers in particular in order to take into account their potentially systemic importance for the financial sector. An initial step for future regulatory considerations could be conduct of business obligations or a code of practice, which is already planned in the area of data protection for cloud service providers, for instance.²⁰

In order to find out how supervisory requirements will evolve in the future, it is important to observe the application of existing provisions in practice in particular. For instance, pooled audits which are authorised for certain participating institutions are likely to require greater coordination efforts, which ultimately has an impact on the number of institutions that can conduct audits together. A number of institutions have already conducted their first pooled audits in recent months.

BaFin is therefore observing the implementation of pooled audits, also in terms of feasibility and the potential consequences for administrative practice and regulation. The same applies to the question of to what extent using audit reports and certifications based on current standards is enough to manage risks effectively.

The risks that may be associated with outsourcing to multi-client service providers are of particular interest from a supervisory and regulatory point of view. This type of outsourcing leads to greater interconnectedness between the financial sector and IT service providers and greater complexity in the market. This can result in new risks, for instance at the interfaces between market participants. As these risks do not arise within the organisational structure of supervised banks, institutions might not be able to fully identify and manage these risks. This is why it is important, from a regulatory and supervisory point of view, to assess and, if necessary, prudentially mitigate the structure of this dynamic market and the resulting risks.²¹

Risks can also arise when a large number of institutions outsource to a limited number of service providers. The EBA has noted that concentration of outsourcing arrangements at a few service providers may in extreme cases lead to disruptions where multiple institutions fail or are not any longer able to provide their services smoothly. If service providers, e.g. in the area of information technology or financial technology, are no longer able to provide their services, this may cause systemic risks.²² In other words: the entire financial market may suffer the consequences. The need to monitor and manage concentration risk is particularly relevant to certain forms of IT outsourcing which are dominated by a small number of service providers.²³

20 Data Protection Code of Conduct for Cloud Service Providers Revised v1.0 of 22 June 2016; the Code was prepared by the Cloud Select Industry (C-SIG), which was convened by the European Commission (DG Connect and DG JUST). The Code consists of a set of requirements for cloud service providers.

21 BaFin, Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services, page 14 et seq., www.bafin.de/dok/11250046, retrieved on 4 January 2019.

22 EBA/GL/2019/02, page 14.

23 loc. cit. (footnote 21).

BaFin is currently examining how the risks described above can be monitored appropriately in the context of outsourcing to multi-client service providers. BaFin does not, as a rule, supervise service providers – including multi-client service providers and IT service providers. In order to gain a better understanding of such multi-client service providers, BaFin would have to be authorised to request information from them directly and order inspections to be conducted. BaFin's current practice is to exercise these rights at supervised institutions only; it is to be examined whether this approach is sustainable in the long run.

But what can be done if multi-client service providers are not only specialised in the companies that BaFin supervises? Cases like these do not only entail risks for the German financial services sector; they can lead to risks for the economy as a whole – beyond Germany's borders. Monitoring such service providers should therefore not be limited to national financial supervision. More than ever, regulation and supervision must take place on a multilateral level – in order to create a genuine level playing field.²⁴

24 loc. cit. (footnote 3).



© iStock/From2015

IWV

Rate setting and pricing in the insurance business are based on extensive historical data resources and forecast values. The increasing availability of Big Data (BD) and the rapid, innovative development of Artificial Intelligence (AI) are also changing the opportunities for developing individual rates. This article examines their impact on the balancing of risks in the community of policyholders.

The community of policyholders in an era of Big Data and Artificial Intelligence

Authors

Professor Dr Fred Wagner

Institute for Insurance Studies,
University of Leipzig

Kristina Zentner, M. Sc.

Institute for Insurance Studies,
University of Leipzig

1 Introduction

Big Data and Artificial Intelligence (BDAI) have become widely discussed buzzwords that are associated in the public mind with a strong force for disruption and a high potential for changing existing business models. In particular, they are increasing the opportunities for individualising products and prices, for contacting customers and for automating every possible business process.

These trends are also affecting the insurance industry. Among other things, they are resulting in potential applications in risk selection, (individualised) premium calculation and rate setting, raising questions above and beyond the areas of data security and data protection. At the same time, aspects relating to the reliability and admissibility of Big Data applications and possible discrimination against policyholders with higher risks due to their personal life circumstances are being discussed. Last but not least, many people are wondering whether and to what extent the balancing of risks in the community of policyholders, and hence the principle underlying insurance, still works when premiums are calculated and rates set individually.

To come straight to the point: individualised insurance premiums that can be calculated with far greater precision based on Big Data and Artificial Intelligence do not generally harm the community of policyholders and the balancing of risks – in fact the opposite is the case. The precise impact of these digital and technological trends on the balancing of risks in the community of policyholders is analysed in the following.



2 Definition of insurance

“Insurance provides cover for funds that are needed and whose specific amount is uncertain but are estimated in the aggregate on the basis of the balancing of risks in the community of policyholders and over time.”

Dieter Farny¹

This definition encompasses both the key characteristics and the actual business model of an insurance under-taking. An adequate understanding of the concept of private-sector insurance cover requires a more detailed explanation of the individual components of this definition.

“Cover for funds that (...) are estimated in the aggregate.”

Stochasticity is a key feature of the insurance business. In simple terms, stochastics deals with probability distributions of events and their outcomes.² Based on past experience and the law of large numbers³, probability distributions with expected values and scattered outcomes of random events are projected into the future. The more individual values that are used for the calculation, the more reliable the probability distributions will be. One example is the outcome when dice are thrown. Although the individual outcome is determined by chance, the expected value for the number of pips is always 3.5 and the distribution of the outcomes ranges from 1 to 6. The probability of reaching 3.5 pips with only a single throw is zero. However, the more often the random experiment is repeated with an average then being calculated, the

more reliable the estimate will be of obtaining an outcome close to the expected value of 3.5.

Most insurance business covers the economic consequences of the occurrence of undesirable real-world events, i.e. perils. Comprehensive contents insurance⁴, for example, covers the perils of burglary, water damage, storm and fire. The economic consequences are termed “risks”⁵ and are losses measured in cash or funds needed to finance the events that have occurred.⁶ The individual policyholder thus receives a compensation payment specified in the insurance contract if one of the insured risks and hence an economic risk materialises. However, because this depends on chance, the benefit to be paid is not known in advance. Based on statistical historical values and taking risk factors (e.g. residential address, design) into account, expected values are calculated for the frequency and amount of claims in a portfolio of insured risks, and the total funds required to be covered by the insurer are estimated. As in the example of the dice, the more random experiments a community of policyholders consists of, i.e. the more risks (= individual insurance relationships) that are included in the portfolio, the more accurate the estimate will be.

A reliable estimate, however, requires a substantial degree of homogeneity of the insured events or risks. That is because an estimate of average losses from heterogeneous risks at Insurer A would lead to an inflated calculation of the funds required for the risks with a below-average exposure to losses and thus also to inflated insurance premiums. Conversely, risks exposed to above-average losses would be calculated too low and underpriced. Under competitive conditions

1 Farny: Versicherungsbetriebslehre (Insurance Business Management), 5th edition 2011, page 8.

2 Schmidt: Versicherungsmathematik (Actuarial Science), 3rd edition 2009, page 292 et seq. or Kamps, in: Roberts/Mosena/Winter (ed.), Gabler Wirtschaftslexikon (Business Lexicon), 17th edition 2010, page 2886.

3 Albrecht, in: Wagner (ed.), Gabler Versicherungslexikon (Insurance Lexicon), 2nd edition, page 364.

4 For more information see Andersch, in: Wagner (ed.), Gabler Versicherungslexikon (Insurance Lexicon), 2nd edition 2017, page 962 et seq.

5 See Albrecht, in: Wagner (ed.), Gabler Versicherungslexikon (Insurance Lexicon), 2nd edition 2017, page 754.

6 Not all insurance business insures risks in the sense of negative real-world events. There are also cases of insurance against highly desirable events, such as longevity, although these also entail a need for funds – in this example, for instance, to finance the further cost of living. The economic loss in this case is the financing gap that would arise if the funds needed were not covered by insurance benefits. In the interests of simplification, however, reference is made in the following to (insured) losses and claims.

with a competitor B who calculates correctly, and with corresponding market transparency, the consequence would be an anti-selection of excessive risks at average premiums at Insurer A.

“whose specific amount is uncertain”

A functioning insurance business requires the occurrence of each individual insured event to be uncertain; if not, a fundamental condition for the insurability⁷ of risks will not be met. It does not make sense to insure an event that is certain because the risk premium would have to match the amount of the (certain) loss; administrative expenses would additionally be incurred. And an event that will definitely not happen does not require any commitment to provide cover. There must therefore be a random factor affecting the occurrence of a loss. This means that both the policyholder and the insurance undertaking do not know in advance whether, in what amount and/or when the individual loss will occur. To avoid information asymmetry and hence both sides trying to outsmart each other when insurance decisions are made, the degree of uncertainty on both sides should be roughly the same. In reality, though, the insurance business is strongly characterised by information asymmetries.⁸ As a rule, the policyholder knows their personal risk much better than the insurer and can even influence it. Insurance undertakings can reduce such information asymmetries with the help of application questions, inspections and (in the personal insurance business) medical examinations and obligations.⁹ On the other hand, their extensive statistics also give insurers an information advantage about the probability distributions of losses, which they could play off against policyholders in the form of inflated risk premiums. However, since price transparency increases in a time when comparison portals and online brokers

have multiplied, this sort of behaviour would tend to be punished by the mechanisms of the competitive market.

Balancing risks in the community of policyholders

The primary focus of an insurance contract is the transfer of a probability distribution¹⁰ of losses from the policyholder to the insurance undertaking. Since an insurance undertaking covers a range of loss events affecting a large number of policyholders, it also has a large number of risks in its insurance portfolio that balance each other out.

In this case too, the example of the dice can be used to explain how risks are balanced in the community of policyholders. With a fair dice, the probability of all possible dice outcomes, i.e. throwing the different numbers of pips 1, 2, ... 6, is the same. Since a range of random events (in this case individual dice throws) result in outcomes that are independent of each other, higher and lower dice outcomes will tend to balance each other out in relation to the expected value, and the average outcome will settle at 3.5 in accordance with the original estimate – and the more frequently the dice is thrown, the more reliable this will be (law of large numbers, see above). The same applies in real life to insured risks. However, another condition is that the risks must be independent of each other. If there is no independence, for example in the case of storm damage within a defined region, risks impacted by claims and claim-free risks can no longer compensate each other and risk balancing fails.

Whereas the homogeneity of the individual risks is therefore of great importance for the estimation community (see above), this does not apply to the balancing of risks in the community of policyholders. This is where there is often a misunderstanding about the principle underlying insurance. Heterogeneous risks, measured in terms of expected claims, can also balance each other out provided they are backed in each case by the right insurance premium. For example, insureds of different ages and hence different mortality

7 Wagner/Elert/Luo, in: Wagner (ed.), Gabler Versicherungslexikon (Insurance Lexicon), 2nd edition 2017, page 985.

8 For further reading on the phenomena of information asymmetries, see Akerlof, The Market for “Lemons”: Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics, 3/1970, pages 488 et seq.

9 See Beckmann/Schirmer, in Wagner (ed.), Versicherungslexikon (Insurance Lexicon), 2nd edition, 2017, page 621.

10 See Schmidt, in: Wagner (ed.), Gabler Versicherungslexikon (Insurance Lexicon), 2nd edition 2017, page 1036.



probabilities can also be included in a community of term life insurance policies if, under otherwise identical circumstances, older insureds pay a higher premium – commensurate with the risk – than younger insureds. The balancing of risks will not then be disturbed. Before this can happen, however, estimating the risk and thus calculating the premium has to be differentiated in line with the age of the insureds.

Balancing risks over time

Balancing risks in the community of policyholders only ever has a limited observation period and typically never functions perfectly. Within a period, there will regularly be above- or below-average claims, although these will also tend to offset each other over time. In other words, periods with below-average claims balance out periods with above-average claims. This explains how risks are balanced over time; at the same time, it requires and shapes the long-term nature of the insurance business. The ideal conditions for balancing risks over time are constant characteristics of all individual risks in the insurance portfolio as well as no change in the portfolio composition. This means that, as far as possible, the expected claims and the loss distribution are not subject to any deviation risk, or that the deviation risks will tend to balance each other out within the overall community of policyholders. In practice, however, the overall community of policyholders is rarely constant over time, as the insurance portfolio is characterised by inflows and outflows as well as a changing risk environment. Because of the limitations on risk balancing in the community of policyholders and over time, there is always a residual underwriting risk for the insurance undertaking.

Underwriting risk

Underwriting risk describes the possibility that the effective claims in the community of policyholders will exceed the expected claims in the community, thus exposing the insurer to the risk of loss or even ruin, as the risk premiums collected may not be sufficient to pay the losses incurred.¹¹ In terms of cause, underwriting risk can be broken down into the risk of random fluctuation, change and error.¹²

The risk of random fluctuation occurs when effective claims differ from expected claims because an above-average number of losses and/or a high level of losses have randomly occurred.¹³

The risk of change is based on the possible case that the risk conditions will undergo an adverse change over time compared with the assumptions originally used to calculate the premiums, and that the effective claims will therefore ultimately exceed the expected claims.¹⁴

What risk of error means is already apparent from its name. Risk of error materialises in the case of incorrect estimates or assumptions.¹⁵

11 See Farny, *Versicherungsbetriebslehre (Insurance Business Management)*, 5th edition 2011, page 82 et seq.

12 See *ibid.*

13 See Albrecht, *loc. cit.* (footnote 3), page 1094.

14 See Albrecht, *loc. cit.* (footnote 3), page 37 et seq.

15 See *ibid.*, page 469 et seq.

3 How insurance works: the actuarial principle of equivalence

The conceptual basis for calculating risk premiums¹⁶ is the actuarial principle of equivalence. Under the actuarial principle of equivalence, the risk premium corresponds to the expected claims relating to the covered risk.

A further distinction can be made between community and individual actuarial principles of equivalence. In the case of premiums calculated according to the individual actuarial principle of equivalence, the amount of the risk premium payable by the policyholder is equal to the amount of their individual expected claims. Under the community actuarial principle of equivalence, the aggregate risk premiums from an insurance portfolio correspond to the aggregate expected claims for the community. The individual actuarial principle of equivalence includes the community actuarial principle of equivalence, as it were, because if each policyholder pays the risk premium for the share of their expected claims in the overall community, the sum of the individual risk premiums will also correspond to the aggregate expected claims of a community of policyholders.¹⁷ Conversely, the risk premium for the community divided by the number of policyholders does not have to equal the individual expected claims. In the case of heterogeneous risks, there is then an average premium for different risks, i.e. some risks with an above-average loss exposure and some risks with a below-average loss exposure for which insurance premiums offering insufficient coverage or excess coverage would be required – with the consequences of anti-selection, as described in the following:

Let us assume that several insurance undertakings operate in a transparent insurance market under competitive conditions. In this market, Insurer 1 charges risk premiums that are aligned with the individual expected claims, and a second insurer, Insurer 2, charges average risk premiums for its insurance portfolio. In this case, utility-maximising rational policyholders with below-average risks (i.e. policyholders with lower expected claims than the average) take out insurance with

Insurer 1 and pay correspondingly lower risk premiums. Policyholders with above-average risks (i.e. policyholders with higher expected claims than the average) will opt for Insurer 2 and its average risk premium, as this is lower than their actual expected claims. If Insurer 2 does not align its risk premium quickly enough with the new composition of its community of policyholders, it runs the risk of ruin.

As things stand today, a risk premium can at best be calculated approximately based on the individual actuarial principle of equivalence. A greater degree of approximation is not possible at present because there is no reliable data pool, and nor are there adequate IT processes. The data pool basically comprises information about risk characteristics that must essentially meet three requirements:

1. There must be a statistically significant correlation between the values of the risk characteristics on the one hand and the shape of the loss distribution¹⁸ (with the expected claims and the loss distribution) on the other.
2. The relationship must be plausible so as to rule out spurious correlations.
3. The insurance undertaking must be in a position to operationally capture the values of the risk characteristics.

Capturing them is made easier today because of the preponderance of “objective risk characteristics”¹⁹ whose values tend to be easily and reliably obtained from external sources. Examples in motor vehicle insurance are the type class of the automobile, the residence of the owner (regional class), how long the driver has held a licence, etc. With over 100 risk characteristics used throughout the market, motor insurers are already in a position today to break down the actuarial principle of equivalence into the smallest rate cells containing only a few – in some cases only individual – risks. The number of rate cells that can be

16 The discussion in the following ignores operating costs, capital costs and savings elements.

17 See also Albrecht, loc. cit. (footnote 3), page 1021 et seq.

18 See Albrecht, in: Wagner (ed.), Gabler Versicherungswörterbuch (Insurance Lexicon), 2nd edition 2017, page 822.

19 See Farny, loc. cit. (footnote 1), page 31 et seq.

formed with the given risk characteristics according to the rules of combinatorics is probably significantly higher than the market-wide number of insured risks. The sum of the individual premiums calculated in this way, when extrapolated for the community of policyholders, is likely to result in a total premium that is highly correlated with the actuarial principle of equivalence. However, the individual actuarial principle of equivalence still remains imperfectly satisfied. What is missing above all is the collection and processing of subjective risk characteristics that represent in particular the attitudes, abilities and behaviour of drivers and that are particularly relevant for the likelihood of losses occurring – but that could not yet be captured, or only marginally. In light of this, the objective risk characteristics in many cases serve as imperfect substitute characteristics for the subjective

risk characteristics.²⁰ To be more specific: the type class of the vehicle, the residence of the owner and how long the driver has held a licence are not responsible for whether the driver causes an accident while driving. However, they are statistically significant, plausible and easily recordable indicators of the attitudes, abilities and behaviour of the policyholder on the road. On average, these correlations may be correct; but in individual cases, there are frequently likely to be deviations from these plausible assumptions and statistical values.²¹

20 See *ibid.*

21 This does not alter the fact that the objective risk characteristics are, in part, also highly relevant. For example, the type class of the vehicle directly impacts the probability of accidents for which the driver is responsible via the vehicle's equipment features (e.g. assistance systems).



© iStock/from2015

4 The digital revolution

4.1 Fundamentals of digitalisation

The speed and momentum with which technology, and above all IT, is advancing is both impressive and challenging. The development of new sources of data, technologies and potential processes is often faster than the willingness and ability of companies and entire industries to apply them in a legally still partly uncertain environment. The enthusiasm, interest and sometimes mere normality with which the new technologies are being used by the general public and by consumers encourage further developments all the more. The sense of entitlement to and expectations of digital applications can even be observed in public administrations and schools.²²

In the first instance, the term “digitalisation” itself refers only to the transformation of numbers, letters, texts, images, videos and other types of data into a digital format, as well as their storage and processing using different computer technologies.²³ The German insurance industry also needs to rapidly and successfully develop corresponding digital skills if it wishes to remain competitive compared with other industries and internationally. The factors of Big Data and Artificial Intelligence are presented in the following as important drivers for insurance undertakings, and their potential impact on the community of policyholders is examined in detail.

4.2 Big Data

Big Data refers to the availability of large volumes of digital data and the technical means for exploiting them. The trend towards Big Data is being driven and accelerated by the expanding storage capacities and growing processing speed of new computer technologies.²⁴

Four dimensions of criteria can be used to characterise big data: volume, velocity, variety and value.²⁵

“Volume” describes Big Data using the available volume of data and the byte size as the unit of measure. The volume of digital data generated annually will grow sharply in the next few years. Whereas 16.1 zetabytes²⁶ of digital data were generated worldwide in 2016, this figure is expected to increase tenfold by 2025.²⁷ The “velocity” criterion stands for the speed of data generation and processing. Data diversity is the subject of the “variety” criterion. This does not merely mean different file formats (e.g. images, emails, Word and PDF files, videos), but also the degree to which they are structured. Data is unstructured if it does not correspond to a formalised system. This is normally the case with images and emails. Semi-structured data either does not have any fixed type of structure, but only a hidden structure, or it is structured differently overall. In addition to the file formats, which must be compatible with the company database, structure also refers to the structures of the field types (for example Title_Source_Date) that describe a file in a database in greater detail.²⁸

Investments in information technologies for storing and processing Big Data should pay off, of course, and increase enterprise value. If not, collecting, storing and evaluating Big Data will not be a worthwhile business exercise. This objective is included in the “value” criterion.²⁹

When externally sourced data is used, its quality and informative value must be validated. Another factor that has to be considered is that where personal data is

22 Federal Agency for Civic Education, <https://www.bpb.de/gesellschaft/bildung/zukunft-bildung/213441/digitalisierung-und-schule>, retrieved on 3 12 2018.

23 See Hofer, loc. cit. (footnote 3), page 228 et seq.

24 See Hofer, loc. cit. (footnote 3), page 157.

25 See <https://www.ibmbigdatahub.com/infographic/four-vs-big-data>, retrieved on 3 12 2018.

26 1 zetabyte corresponds to approximately 10²¹ bytes.

27 See a study by Statista GmbH, <https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/>, retrieved on 3 12 2018.

28 Deutsches Institut für Vertrauen und Sicherheit im Internet (German Institute for Trust and Security on the Internet), Big Data, 2016, page 26.

29 Fasel/Meier, Big Data – Grundlagen, Systeme und Nutzungspotenziale (Big Data – Fundamentals, Systems and Potential Applications), 2016, page 6.

involved, the data subject has a right of access to any information about the source of the data pursuant to Article 15(1)(g) of the European General Data Protection Regulation (GDPR)³⁰.

³⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The transition from conventional databases and the way the data they contain is evaluated to Big Data is fluid. Traditionally, insurance undertakings have large data inventories with long histories, resulting for example from data collected from applications for coverage and claims experience. In many cases, however, this data is stored in distributed database systems and it has not been/will not be merged. Data quality – in the sense of continuous updating and harmonisation – also mostly needs improving. Data about subjective risk characteristics can now also be made available using smart gadgets. And



© iStock/From2015

there are growing opportunities for obtaining data from external sources. These include special data providers, websites and the social web.³¹ However, there is a large gap in particular to the US big techs (Google, Amazon, Facebook, Apple: collectively Gafa, etc.) and other industries because very little open data and real-time data is captured. "Open data" is "unfiltered, machine-readable electronic data that is available to everyone publicly, for no particular purpose and without obligation".³² It usually comes from the federal administration, with examples including information about traffic, tourism or the weather.³³ In the same way as all other companies in all industries, insurance undertakings are also free to additionally integrate open data to optimise their products, services and business processes, for example as a basis for rate setting.

In addition, real-time data can help to decipher the activities and behaviour of policyholders and insureds in order to draw conclusions about risk situations, among other things. Real-time data is already being collected today about users in large quantities, for example from smartphones and wearables, and evaluated by the manufacturers. Automobile manufacturers are able to measure the driving behaviour of drivers in real time. The question will be: who will be legitimised in the future by the sovereign owners of this data (they should always be the citizens who are themselves being measured) to use it for what purposes? Using personalised real-time data, insurers in turn would also be able, for example, to come much closer to the subjective risk characteristics.

However, the insurance industry is also making progress in the Big Data playing field. In motor vehicle insurance, for instance, pay-as-you-drive and pay-how-you-drive

premium rates are increasingly being developed and offered. With pay-as-you-drive rates, the insurance premium is calculated precisely per kilometre actually driven, whereas with pay-how-you-drive rates, the driver's personal driving behaviour is analysed and forms the basis of the individual premium calculation.³⁴

Pay-as-you-live rates represent further lines of development in other classes of insurance. In this case, data on personal everyday behaviour is read using wearables such as smart watches or transmitted to the insurance undertaking through smartphones or smart home technologies³⁵. However, insurers are still quite cautious about these concepts as a whole.³⁶

Managing Big Data is tied to technical, human resources and intellectual requirements. The trick is to generate Smart Data that meets other quality criteria, such as data protection requirements and social acceptance.

To be able to use Big Data efficiently and rationally in risk analysis and insurance rate setting, developments in the field of Artificial Intelligence offer new approaches.

4.3 Artificial Intelligence

It is very difficult to find a generally accepted definition of "intelligence". Characteristics of human intelligence, for example, are understood to include practical problem-solving skills, verbal skills and social skills.³⁷

31 Seufert, in: Fasel/Meier, loc. cit. (footnote 28), page 52.

32 Termer, F. (2018): Open Data bringt Mehrwert für Unternehmen (Open data brings added value for businesses), <https://www.bitkom.org/Presse/Presseinformation/Open-Data-bringt-Mehrwert-fuer-Unternehmen.html>, retrieved on 3 12 2018.

33 See Federal Ministry of Economics and Energy, Open Data: Mit öffentlichen Daten digitale Wirtschaft fördern (Open data: Using public data to promote the digital economy), <https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/open-data.html>, retrieved on 3 12 2018.

34 See GDV, Positionen. Den Fahrer im Blick (Positions. Focus on the Driver), <http://positionen.gdv.de/den-fahrer-im-blick/>, retrieved on 3 12 2018.

35 See OECD Digital Economy Papers, Consumer Policy and the smart home, 2018, No 268, <https://www.oecd-ilibrary.org/docserver/e124c34a-en.pdf?expires=1543255258&id=id&accname=guest&checksum=FFC7F6B9DB075CE596466A4198B8CDD4>, retrieved on 3 12 2018.

36 The GdV position paper on the requirements for smart home installations and devices in the Internet of Things dated 29 May 2017 provides additional information: <https://www.gdv.de/resource/blob/8254/346747549f0b20cd6a28b6a806a04152/anforderungen-smart-home-iot--900514353-data.pdf>, retrieved on 3 12 2018.

37 Sternberg, Advances in the psychology of Human influence, 5th edition, 1989, pages 91 et seq.



“Artificial Intelligence” refers to the problem-solving ability of computer technologies that otherwise only humans possess because of their intellectual processing abilities.³⁸ A distinction can be made by intelligence levels between weak Artificial Intelligence and strong Artificial Intelligence although the boundaries cannot be said to be well-defined.³⁹

Using weak Artificial Intelligence, computer-driven machines are able to develop solutions that are limited to certain tasks they have been taught to carry out. Examples include navigation systems and the correction functions in electronic writing media. Strong Artificial Intelligence is the term used when machines emulate human intelligence and achieve broader cognitive performance.⁴⁰ This is the case when machines can draw

logical conclusions, continually learn new things or make clever decisions when faced by uncertainty.

To develop Artificial Intelligence, neural networks, i.e. networks of nerve cells, in the human brain have been and continue to be researched, modelled using state-of-the-art technologies and thus imitated piece by piece. In the case of strong Artificial Intelligence, computer-operated machines are taught how to learn (machine learning⁴¹) and hence to make judgements and solve problems.⁴² Deep learning is an aspect of machine learning in which machines develop prediction abilities and the skills to make their own decisions.⁴³

38 <https://www.britannica.com/technology/artificial-intelligence>, retrieved on 3 12 2018.

39 Buxmann/Schmidt (ed.), *Künstliche Intelligenz – Mit Algorithmen zum wirtschaftlichen Erfolg* (Artificial Intelligence – With Algorithms to Economic Success), page 40.

40 National Science and Technology Council, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, retrieved on 3 12 2018.

41 Machine learning means that machines are trained to solve certain tasks on the basis of experience. See Buxmann/Schmidt (ed.), *Künstliche Intelligenz – Mit Algorithmen zum wirtschaftlichen Erfolg* (Artificial Intelligence – With Algorithms to Economic Success).

42 Ertel, *Grundkurs Künstliche Intelligenz* (Fundamentals of Artificial Intelligence), 4th edition, 2016.

43 <https://www.bigdata-insider.de/was-ist-deep-learning-a-603129/>, retrieved on 3 12 2018.

5 How Big Data and Artificial Intelligence affect calculations and rate setting

For the first time, Artificial Intelligence allows Big Data to be used rationally and efficiently. Innovative processes that draw on the power of Artificial Intelligence, such as developments in the field of smart data analytics, can harness large, unstructured masses of data by filtering, selecting and sorting them, and transforming them into a single format. Using Artificial Intelligence instead of human intelligence saves expensive human resources capacities and allows them to be deployed elsewhere. In addition, there are no symptoms of fatigue when Artificial Intelligence is used to process large volumes of data, making processing faster and more error-free.

Using pattern analyses, among other things the relationships between real-time data on the one hand and behavioural characteristics and loss potential on the other can be explored reliably and efficiently. This also significantly advances the analysis and evaluation of subjective risk characteristics.

These insights and “black box” processing of Big Data enable real-time rate setting, among other things.

Incoming behaviour-based data from the sensors of a motor vehicle, from a smart watch or other fitness trackers, as well as from a smart home, can be rapidly analysed at the insurer using intelligent, automated processes and processed in a personalised insurance rate with an individual premium. Bonus-malus rules could also be automated and implemented rapidly in the case of certain behaviour patterns defined in advance. Ultimately, the substantial gain in processing capacity, speed and flexibility can lead to almost entirely individualised insurance premiums. Moreover, through the meticulous analysis of Big Data, artificially intelligent processes can reduce existing information asymmetries that disadvantage the insurer.

As things stand today, however, some of the pre-requisites needed for using Artificial Intelligence in insurance undertakings still have to be established. This starts with explaining to policyholders the benefits of transferring data. Data that is already distributed across many older systems in the insurance undertaking must be centralised in compliance with data protection



regulations and made available for analysis. It should also be noted that, under Article 13(2)(f) of the GDPR, the insurance undertaking must inform policyholders about the logic involved in automated decision-making. This will in itself be problematic because in most cases, strong Artificial Intelligence is no longer based on an easily understandable algorithm that could be disclosed and communicated.

What this means is that Artificial Intelligence will not be able to completely replace human intelligence in rate setting under the current rules. It is certainly the case that the requirements of statistical significance and (together with the digital possibilities for data mining) the problems associated with recording behaviour patterns and subjective risk characteristics can be overcome using Artificial Intelligence, as described above. However, Artificial Intelligence makes the problem of verifying plausibility all the more critical. In BaFin's view, to the extent expressed, insurers must at all times also be in a position to explain the logic

of the algorithms in accordance with Article 13(2)(f) of the GDPR and, where appropriate, to verify adherence to certain ethical and legal principles (for example, compliance with the prohibition on premium rates based on gender and nationality).⁴⁴ A sceptical approach still appears justified as to whether these requirements are in any way compatible with the use of Artificial Intelligence. In light of this, if the use of Artificial Intelligence is restricted by (supervisory) law, the question arises of whether German insurance undertakings (and the German economy in general) will suffer critical disadvantages and be left behind in the international and cross-sectoral competitive environment. It is already the case today that the development centres for Artificial Intelligence are situated in the USA, China and India, rather than Germany.

⁴⁴ See also Dr Frank Grund's speech on 13 November 2018 (only available in German), "Neue Herausforderungen für Aufsicht und Branche", retrieved on 3 December 2018.

6 Impact on the community of policyholders

The objective of using Big Data and Artificial Intelligence in rate setting by insurance undertakings is therefore to calculate an insurance premium that is closer to the individual expected claims associated with the individual policyholder or risk. A premium that approaches the individual actuarial principle of equivalence can also be perceived as fairer or more performance-based.

An individually actuarially equivalent premium will, of course, prove to be advantageous for policyholders with below-average risks and disadvantageous for policyholders with above-average risks – for the latter in particular if their adverse risk characteristics cannot be positively influenced by some other behaviour (e.g. genetic risk factors in personal insurance). In the case of individual and behaviour-based insurance premiums, a question that will be increasingly asked is which factors, characteristics and behaviour patterns may or may not be included in rate setting.

In addition, whether the relationships between concrete behaviour patterns and their impact on individually expected losses have already been sufficiently researched still remains to be seen. For example, there is a need for a more detailed examination of how exactly speed, acceleration and braking behaviour in a motor vehicle actually affect the potential risks. In the case of pay-as-you-live premium rates, for example, it is necessary to investigate which foods are really health-enhancing or harmful for which groups of people, or which intensity and duration of which sports activities promote or damage physical and mental well-being in the long term – and all this with regard to both statistical significance and plausibility. Misleading conclusions, or at least conclusions that are not accurate to the greatest extent possible, can lead to unwarranted discrimination against certain groups of policyholders.



However, to the extent that rate setting on the basis of Big Data and Artificial Intelligence leads to individual premiums, the balancing of risks in the community of policyholders will not generally be impaired. In light of the fact that the community actuarial principle of equivalence is also necessarily satisfied when a premium is calculated in accordance with the individual actuarial principle of equivalence, the collective insurance premium of the community will be sufficient to cover the overall expected losses even if rates are set individually. This unequivocally counters the widespread misunderstanding that the community concept and hence the principle of insurance are no longer satisfied by an individualised premium. The opposite – see above – holds true: “Insurance provides cover for funds that are needed and whose specific amount is uncertain but are estimated in the aggregate on the basis of the balancing of risks in the community of policyholders and over time”. Even – and especially – in the case of an individual insurance premium that has been actuarially calculated correctly, risks in the community of policyholders are balanced and anti-selection is avoided. From a risk theory perspective, this also results in a fair premium. Whether this premium will also be viewed as fair by the general public is another question that will not be discussed here.⁴⁵

⁴⁵ See Wagner, *Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft (Business or conscience? The departure of insurance from the shared risk community)*, 2017, for more details.

Reduced operating and administrative expenses can be a significant advantage of using Artificial Intelligence and the associated black box processing in rate setting for insurance contracts. As with all innovations, however, a certain payback period must first be taken into account here. In turn, the entire community of the policyholders benefits from falling costs, as the cost advantages should be reflected in lower premiums.

With regard to compliance with data protection requirements, the use of Big Data and Artificial Intelligence currently still faces significant challenges. In particular the GDPR, with its requirements for data minimisation⁴⁶ under Article 5(1)(c) of the GDPR, storage limitation⁴⁷ under Article 5(1)(e) of the GDPR and purpose limitation⁴⁸ under Article 5(1)(b) of the GDPR, constrain the effective opportunities for deploying Big Data and Artificial Intelligence. In the absence of clearly defined rules so far, the real challenge in practice today is to explore the legally permissible scope for using and analysing available data.

⁴⁶ The collected data must be limited to what is necessary in relation to the purposes for which it is processed.

⁴⁷ Identification of the data subject is only permitted for no longer than is necessary for the purpose of data collection.

⁴⁸ Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

7 Assessment

In principle, using Big Data and deploying Artificial Intelligence can improve risk balancing in the community of policyholders through even sounder individual risk premium calculations. In addition, there are many opportunities for cost optimisation that will benefit the community of policyholders. It is important for the degree of individualisation in rate setting to go hand in hand with the pace at which social acceptance of these technologies and the related business models increases.

The extent to which the growing degree of individualisation will jeopardise the concept of solidarity and thus disturb the sense of justice among those responsible for consumer protection, policymakers and the general public is explicitly not an essential question in the private insurance industry business model. Private insurance does not follow the solidarity principle based on the criteria of “healthy for the sick, rich for the poor, strong for the weak” that lies at the heart of the pillars of the social insurance system, but rather the principle of risk balancing in the community of policyholders.⁴⁹ Nevertheless, private insurance companies also have to meet expectations, and they will face criticism if

they do not take solidarity sufficiently into account in their premium rate calculations. A prominent example is the debate about insurance premiums in liability insurance for midwives, which are actuarially correct but unaffordably high.

However, while there is the problem of high premium charges for certain above-average risks in the community of policyholders, there is also the possibility that positive behavioural effects may emerge. This is because, to the extent that undesirable behaviour patterns in policyholders or insureds are the reason for the excessive risk, the associated insurance premium might prompt them to correct or stop that behaviour. For example, if Big Data, Artificial Intelligence and real-time processing are used to show a significant premium supplement to a car driver on their dashboard display when there are indications that the driver is speeding, this could lead to an immediate adjustment to the driving behaviour and, in the long term, to desirable behavioural adaptations as well. Such consequences probably also do not disrupt the concept of solidarity; on the contrary, they strengthen responsibility for personal behaviour in the community of policyholders and hence also actuarial solidarity. However, the issue of demarcation here is difficult and lies in the grey area between the behavioural and fate-driven characteristics of policyholders and their underwriting risks.

⁴⁹ See Wagner, *Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft* (Business or conscience? The departure of insurance from the shared risk community), 2017.

8 Summary

Overall, integrating Big Data and Artificial Intelligence can bring benefits – for both insurers and policyholders. In the race for potential applications and deployments, however, insurance undertakings are facing competition from technology giants such as Amazon, Apple, Facebook and Google, among others, which are not only far more skilled at collecting and processing data, but also enjoy a higher level of social acceptance when they do this. Moreover, insurance undertakings' databases (still mostly distributed), their data quality (in need of improvement) and their IT systems (frequently outdated) are proving to be drawbacks to implementing promising, high-potential technologies. Insurance undertakings will be forced, and should do their utmost, to welcome innovation with open arms and exploit it to their advantage. It will not be easy to keep pace with the legal environment, especially in the field of data protection, as well as the economic opportunities (investment costs!) and, last but not least, social acceptance.

Another challenge will be to create a more profound level of trust at their customers and to prove their sovereignty in handling the data. There will continue to be a growing focus on generating genuine added value that is tangible for customers so as to persuade them that it is worthwhile revealing data on subjective characteristics.

In line with its title, this article has focused on and largely confined itself to the impact of Big Data and Artificial Intelligence on the community of policyholders. It has ignored other promising applications in the insurance industry, such as detecting fraud, claims management in general, end-to-end process optimisation as well as generating customer-centric value-added services above and beyond pure insurance cover. These aspects open up additional and probably even considerably greater and decisive potential future opportunities – and what's more: they are likely to be essential for the survival of individual insurance companies.



© iStock/from2015

W

This article outlines the positioning of the Savings Bank Finance Group regarding key aspects of digital transformation. It explains the various dimensions in which digitalisation impacts the savings banks and reveals how the institutions specifically shape the associated challenges and opportunities.

The status of digitalisation at savings banks

Authors

Dr Joachim Schmalzl

Member of the Executive Board,
German Savings Banks Association, Berlin

Frank Weigand

Head of Digital Innovation,
German Savings Banks Association, Berlin

1 The importance of digitalisation

Digitalisation is frequently termed the “digital revolution”. In the literature, revolution is commonly defined as a “drastic upheaval leading to severe, profound social and political structural changes”.¹ This very accurately describes the reach of digitalisation. The reason is that what was originally defined quite unspectacularly as the conversion of analogue values such as text or music into digital formats, i.e. data², is in reality a drastic disruption that affects society as a whole.³

Digitalisation is transforming private life, politics and the economy. It is only in the past few years that this has achieved widespread awareness, although digitalisation is hardly a new phenomenon. The beginning of the digital age can be charted back quite precisely to the origins of the world wide web at the beginning of the

1990s. It is not just the classic internet that has met with rapid global acceptance in the past 15 years. With the advent of smartphones and hence mobile internet use, the web has massively changed many people’s everyday life. It is even beginning to transform the values and norms of societies and communities of nations.⁴

At a political level, digitalisation in the European environment was strategically analysed for the first time in the “Digital Agenda for Europe” in 2010. At a national level, the “Internet and Digital Society” commission of inquiry drew up recommendations for the German Bundestag between 2010 and 2013. This was followed by the “Digital Agenda 2014 – 2017”, which formulated digital policy principles. In the meantime, the issue of digitalisation has now reached the cabinet.⁵ The coalition

1 Hillmann: Wörterbuch der Soziologie (Dictionary of Sociology), 4th edition 1994, page 737.

2 Gartner, IT Glossary, <https://www.gartner.com/it-glossary/digitization/>, retrieved on 12 December 2018.

3 McAfee, Andrew and Brynjolfsson, Erik, The Second Machine Age, 2014, page 9 et seq.

4 Lemke, Einführung in das digitale Zeitalter (Introduction to the Digital Era), 2014, page 19.

5 Die Bundesregierung, Digitalisierung wird Chefsache (Federal government, Digitalisation now a Cabinet Matter), <https://www.bundesregierung.de/breg-de/aktuelles/digitalisierung-wird-chefsache-1140420>, retrieved on 12 December 2018.

agreement covering the current federal government has defined a clear focus in this area.

Digitalisation is leading in the economy to a large number of new, data-driven business models. It represents a structural change because tech companies are supplanting traditional companies in the provision of services. Whereas Microsoft was the only tech group featuring as one of the most valuable companies in 2006⁶, companies from traditional industries only accounted for three out of the top ten in 2017. JP Morgan is the only bank still on the list.⁷

Many sectors of the economy – such as the music industry – have already experienced a complete transformation or – for example the financial sector – are in the midst of profound change. The debates in the past about whether digitalisation will have a lasting impact on the financial sector have given way to the question of how institutions can actively meet the challenges of digitalisation and reinvent themselves so that they stay relevant in the future.

But where is the industry today? Opinions about this differ sharply. The index of the level of digitalisation of German companies calculated in the Wirtschaft DIGITAL 2018 (DIGITAL Business 2018) monitoring report published by the Federal Ministry for Economic Affairs reports an above-average value of 61 points for financial and insurance services providers compared with the overall index (54 points). This makes the industry digitally advanced. The banking industry itself is expecting a further rapid rise in digitalisation by 2023.⁸ The index is based on a survey of senior business decision-makers.

On the other hand, a large number of current studies and publications regard progress in digitalisation at credit institutions as still insufficient to successfully master the known and future challenges. In particular, their traditional role as intermediaries is viewed as vulnerable.⁹ Digital applications have the potential to disrupt or otherwise massively transform existing business models.¹⁰

Experts also see a risk that the banking industry will understand digitalisation primarily as a means of achieving productivity and efficiency gains and will act too slowly, as in the past. They also often allege that banks do not take digitalisation seriously and sneer at the challenge posed by online competitors.¹¹ They claim that the industry still underestimates the fundamental transformation triggered and required by the new technologies and runs the risk of losing growing and significant market share in the future to digital platforms, non-traditional competitors and fintechs.¹²

The challenge for the banking industry will therefore be to integrate in its strategy the changing user behaviour of its customers, new technologies and, last but not least, new competitors from the technology arena.

6 The Economist, <https://www.economist.com/special-report/2016/09/17/the-rise-of-the-superstars>, retrieved on 7 January 2019.

7 FAZ, Technologie schlägt Industrie (Technology beats manufacturing industry), <http://www.faz.net/aktuell/wirtschaft/diginomics/das-sind-die-wertvollsten-unternehmen-der-welt-15364862.html>, retrieved on 12 December 2018.

8 BMWi, Monitoring-Report Wirtschaft DIGITAL 2018 (DIGITAL Business 2018 monitoring report), executive summary, pages 5, 8, 9.

9 See McKinsey, Banks in the changing world of financial intermediation, <https://www.mckinsey.com/industries/financial-services/our-insights/banks-in-the-changing-world-of-financial-intermediation>, retrieved on 12 December 2018.

10 See FAZ, Banken spüren wachsende Konkurrenz aus dem Internet (Banks are sensing growing competition from the internet), <http://edition.faz.net/faz-edition/finanzen/2018-11-10/fb7fb16b905ef973ea03ef35e18be74d/?GEPC=s1>, retrieved on 12 December 2018.

11 Wohlfahrt, Welt, <https://www.welt.de/wirtschaft/bilanz/article169443724/Die-sechs-groessten-Irrtuemer-von-Banken.html>, retrieved on 12 December 2018.

12 Finextra, <https://www.finextra.com/newsarticle/32860/most-banks-will-be-made-irrelevant-by-2030---gartner>, retrieved on 12 December 2018.

2 Savings banks and digitalisation

2.1 History

Digitalisation has played an important role in the savings banks' business model for many decades because the "production" process in banking consists "largely of processing information."¹³ Information technology plays a key role in each of the four relevant sub-processes: "acquisition", "agreeing transactions", "settling transactions" and "providing information".

For many years, for example, the gradual digitalisation of payment transactions remained largely invisible for customers. This changed in 1983 with the official introduction by *Deutsche Bundespost*, the former state-owned postal service, of BTX (videotex), the first online service in Germany. As early as 1984, customers at many savings banks were able to execute banking transactions on computers at home, view account balances or make bank transfers.¹⁴ However, it was only the development of the world wide web, which started the internet boom, that stoked rapid growth in the importance of online banking for savings banks and their customers.

Starting in the mid-1990s, the savings banks had an internet presence with their first own websites and browser-based online banking services.¹⁵ In the early days, these were still virtual business cards with pure information content, but they were steadily supplemented by interactive elements such as initial self-service advice offerings and expanded by a multitude of additional service and transaction elements.

Being close to their customers has always been crucial for the savings banks' business model. With the introduction of money transmission and clearing and the resulting need for payment sites, the nationwide branch network had become even denser in the 1950s and 1960s, and people were now used to finding a comprehensive advisory offering close to their home. The advent of the internet brought with it a requirement to provide the same quality of services online, from which the savings banks' multi-channel strategy emerged. This lays down that customer wishes should also be fulfilled across a variety of channels outside the already established self-service areas. The internet and telecommunications supplement the channel mix.

2.2 The current status of digitalisation in the Savings Bank Finance Group

Today, almost 19 million customers with over 40 million accounts use the option to conduct their banking transactions with the savings banks online. Access via mobile devices such as smartphones and tablets, whose share of the total volume of all transactions was already over 30 per cent in 2017, is becoming increasingly important. The savings banks' websites are recording 2.5 billion visitors each year, making them some of the most heavily used internet offerings in Germany.¹⁶

Digital offerings have long stopped being limited to offering just information and services online: they also increasingly serve as a distribution channel for selling banking products. Online presences are additionally playing an increasingly important role as central contact points for customer communication via email, audio and video chats, or messenger services.

¹³ Rebstock/Weber/Daniel, *Informationstechnologie in Banken* (Information Technology in Banks), 2012 and Moormann/Fischer, *Handbuch Informationstechnologie in Banken* (Manual of Information Technology in Banks), 1st edition 1999, pages 6, 7.

¹⁴ Sparkassenhistorisches Dokumentationszentrum des Deutschen Sparkassen- und Giroverbandes, *Geschichte der Sparkassen-Finanzgruppe* (Historical Savings Bank Documentation Centre of the German Savings Banks Association, History of the Savings Bank Finance Group), page 5.

¹⁵ Kreissparkasse Köln, *Technischer Fortschritt* (Technical Progress), <https://www.ksk-koeln.de/unternehmen/unternehmensprofil/ueberblick-zahlen/innovation-technik-fortschritt.aspx>, retrieved on 12 December 2018.

¹⁶ DSGVO, *Rundschreiben Jahreszahlen zu digitalen Kanälen* (Circular: Annual Figures on Digital Channels), 2018/151, 2018.



For many years, the online sales channel supplemented the branch business and was implemented largely in isolation. Qualified personal advice was the domain of the advisers in the local branches. Initial attempts by some savings banks to use digital advisory teams remained the exception at first. The focus of further developments is now increasingly on providing advice using digital channels. It is an integral element of the savings banks' sales strategy, which lays down that customers should receive all important services across all channels and be able to switch seamlessly between the access routes.

We assume that advisory expertise will remain a key competitive success factor in the future. There is also an evident need in the digital world for high-quality advice by people, for people, especially when it comes to complex financial matters. That's why for the savings banks, the provision of this advice will not be limited to branches.

The growing and rapidly increasing digital needs of their customers are the driver for the current and future strategy of the savings banks. In the past, the focus was strongly on the technology-driven expansion of digital solutions and on the cost-driven optimisation and centralisation of processes and the IT infrastructure. The spotlight is now on people.

What we are seeing is a clear interrelation, with curiosity and different expectations arising from new technical opportunities. In turn, behavioural changes make a growing number of new digital offerings possible and necessary. This applies to consuming music or videos using offerings such as Spotify and Netflix instead of CDs or TV, to shopping on the internet or to communicating via WhatsApp or FaceTime. In exactly the same way, this is also changing how banking transactions are conducted, namely increasingly online. Although the institutions will continue to be physically present through their branches, there will be a shift in the weightings between the different channels.

We are closely monitoring the new competitors, such as fintechs and other tech companies; we are analysing their strengths and performance promises and are using the results to derive inspiration for our own measures.

The staff and managers of the savings banks are both addressees of and participants in our digitalisation strategy. Technological transformation will directly impact the future working environment of all savings bank staff, and the working environment of customer advisers in particular. Imparting digital expertise is of particular importance so that high-quality advisory services can continue to be provided and employees will accept the digital transformation.

3 The Savings Bank Finance Group's digital agenda – An organisational roadmap

The various aspects of digitalisation were summarised in the savings banks' "Digital Agenda" at the end of 2016. This gave the institutions a roadmap and a tool for overcoming the practical challenges. The Digital Agenda was developed by the "Digitalisation Task Force", in which various institutions and other companies of the Savings Bank Finance Group participated.¹⁷ Based on the current situation, the aim was "to define the enhancements needed to selectively change or expand the organisational structure and so equip it for the challenges and opportunities offered by digitalisation."¹⁸

The items on the digital agenda are based on the savings banks' understanding of their mission to be the central point of contact for their customers for all financial services. Personal and regional closeness continues to be a key point of difference over the competition. Staff are seen as a unique selling point. Customer satisfaction and customer experience are improved by a performance-driven portfolio.

The Digital Agenda more clearly documents the aspiration to align digital solutions more systematically with customer needs. Customers should be able to – and can – choose the most suitable contact point for them depending on the circumstances. The multi-channel strategy is the core element of this. A critical success factor is not only being represented in all relevant sales channels, but also integrating them tightly. While the savings banks' multi-channel offering is already quite mature in the retail banking segment, the offering for the corporate banking business must be implemented comprehensively and further expanded both conceptually and functionally.

Based on the savings banks' business strategy, the Digital Agenda also incorporates the staff perspective and questions of operational efficiency. That is because constant, rapid transformation must be operationally achievable and accompanied by growth in skills and expertise. Both will be enabled or expanded by means of focused measures. In the future, the Savings Bank Finance Group's market-relevant digital solutions will be defined and developed and then deployed by savings banks more quickly so that retail customers, corporate customers and local authorities across Germany can also use these solutions.

The Digital Agenda sets ambitious standards in the following dimensions:

Innovation

Measured in terms of market-leading drivers of digitalisation in the financial services market, the Savings Bank Finance Group endeavours to be at least a follower, and also to be a pioneer for selected issues. Compared with traditional competitors, it generally aims to be a pioneer.

Economic efficiency

The opportunities offered by digitalisation to cut costs and boost earnings, as well as for rationalisation and process automation, will be systematically leveraged.

Relevance

The savings banks are the central point of contact for their customers for all financial services. They use digitalisation to safeguard jobs in the region as attractive employers. Digital expertise is also deployed for the benefit of the municipal trustees and the public.

¹⁷ Representatives of the following institutions were involved in drawing up the Digital Agenda: Förde Sparkasse, Stadtparkasse München, NordLB, BayernLB, Rheinischer Sparkassen- und Giroverband (RSGV), Ostdeutscher Sparkassenverband (OSV), Sparkassenversicherung Baden-Württemberg, Deutscher Sparkassenverlag (DSV Group), Finanz Informatik (FI) and German Savings Banks Association (DSGV).

¹⁸ DSGV, Digital Agenda, 2017, Objectives, page 1.

Moreover, the Digital Agenda defines the following core beliefs as guiding principles:

- The savings banks continue to consider themselves to be multi-channel banks; we do not wish to become an (online) direct bank.
- Staff should also remain relevant in the digital world, where they will be beacons of digital expertise.
- There is a need for new, relevant added value that will be rewarded by the customers.
- We offer all of our customers simple solutions to meet their needs.
- Savings banks are organisations that use data. We place the protection of our customers' personal privacy above our own economic interests.
- The information security of our systems has the highest priority.

The Digital Agenda has created a range of tools for the savings banks to achieve the defined ambitious standards and to allow the guiding principles to be measured. They help determine the current status and identify concrete measures to systematically leverage the digitalisation concepts and solutions already available today.

However, the Digital Agenda also indicates

- how contact with customers will be organised in the future,
- which innovations are necessary to do this
- and how the Group – including together with its customers – can develop and provide competitive offerings faster and continuously enhance them.

The individual tools are explained in greater detail in the following.



© iStock/from2015

3.1 The customer perspective in the Digital Agenda

3.1.1 Innovation management and customer centricity

“Customer is King” wasn’t invented by digitalisation, and was always the aspiration of successful business undertakings. Customer centricity has a long tradition at the savings banks. The heart of the savings banks’ entire business model is customer-centric, as this reflects the mission and roots of the savings banks. In fact, a large part of the creative power of digitalisation in society is because it makes people’s everyday lives easier and more comfortable and allows individuals to directly notice the benefits of this revolution.

In the branch-based world, the advisers were the sole intermediaries and translators between the customers and the supporting IT systems. In the digital world, customers interact directly with IT. Systems must therefore be as self-explanatory as possible and usable without effort and expert knowledge. It is true that the financial sector, and the savings banks in particular, have caught up in this respect. However, it cannot be denied that improvements are still needed.

This also means that classic product-centric practices must be challenged when new offerings are being developed using the waterfall model. That is because successful digital companies put new releases, updates or features into operation in rapid succession. In turn, this enables them to respond swiftly to customer feedback. It is no longer enough to bring new products to market in planning and implementation processes that may last for years – hoping that the original assumptions still hold true: all the more so because new technologies and user trends continue to evolve at high speed. What this means is that the longer the production times are, the greater the economic uncertainty will be.

The Savings Bank Finance Group is meeting these challenges at a variety of levels. What is important in the first instance is to have better knowledge about current technology trends in- and outside the financial sector, as well as about the success factors driving successful providers. That is why innovation hubs were established at various points in the Finance Group. One example is the Hamburg-based “S-Hub”, launched and sponsored by Finanz Informatik. Other institutions such as Deutscher Sparkassenverlag, the German Savings Banks Association (DSGV) and a range of enthusiastic savings banks also support the S-Hub with financial and human resources.

Besides identifying trends and evaluating existing fintech solutions (market screening), the primary mission of the S-Hub is to develop new product ideas together with customers and to develop prototypes: “by customers for customers”, as it were.

In doing so, the S-Hub systematically deploys agile methodologies such as design thinking. More than 20 prototypes were developed in product discovery processes over the past 18 months, and some of them are currently being transformed into real products. The aim here is to obtain customer feedback as early as possible in the design and development process so as to minimise the risk of developing products that fail to meet customer requirements. In early 2019, the S-Hub launched a central tester community for the savings banks that will significantly expand early prototype testing.

However, agile methodologies are not only being used in the idea generation and prototyping phase. A growing number of projects are also being implemented using agile elements, for example from SCRUM, to upgrade core systems, for example for the savings banks’ online presence called Internet-Filiale¹⁹, to the extent that this complies with the conditions defined by the regulator. The development and testing of decentralised innovative ideas by individual savings banks is also purposely desired and is being encouraged.²⁰

¹⁹ The Internet-Filiale is the savings banks’ online presence, and includes online banking access.

²⁰ DSGV, Digital Agenda, 2017, page 15.

The standing conditions for implementing creative innovations are that they do not visibly breach the law or ethical principles, or harm the brand, the philosophy, the reputation, the regional principle or the business strategy of the savings banks. Common guidelines were developed in the Group for this purpose.

3.1.2 The financial platform: the digital ecosystem of the savings banks

The Internet-Filiale and the savings banks app give the savings banks online points of contact that are regularly used by 17 million customers to conduct their banking transactions and contact the savings banks. The savings banks also seek to retain or expand the direct customer interface in the platform economy, and not to revert to the status of a pure infrastructure service provider, for example for fintech offerings.

The current account is therefore being embedded in a digital platform and developed into an ecosystem that is the digital home for all users (retail and corporate customers) and their financial needs, and aims to make life easier. The term “user” is used here consciously because this platform is not only open to customers of the Savings Bank Finance Group, but also, prospectively, to customers of other institutions. The financial platform is also intended to provide a regional and nationwide services offering outside of the core business.

The Internet-Filiale 6 currently used by the savings banks is being developed into a financial platform iteratively and also increasingly with the direct and continuous involvement of customers. A multi-banking capability was additionally made available to customers there in August 2018, thus laying the foundation for the further expansion of the platform:²¹ customers can now manage accounts with other (non-savings) banks in the online banking solution offered by their savings bank. In December 2018, the multi-banking capability was expanded to include interactive transactions such

21 Multi-banking capability has been a permanent function of the savings bank app since version 1.

as credit transfers and standing orders, as well as the first functionalities of a personal financial management feature. Additionally, the first components from partnerships with fintechs will be integrated by savings banks nationwide in their online presences in the first half of 2019.

As well as their own ecosystem, the savings banks also want to offer a customer experience in the ecosystems of other providers. Some examples of this have already been implemented, such as the integration of savings bank branch and ATM addresses in Google Maps and other navigation systems, or the placement of real estate offerings in the large internet portals.

3.1.3 The API²² strategy of the Savings Banks Finance Group

The German banking industry has had powerful interfaces since 1996 in the shape of the Home Banking Computer Interface (HBCI) and its successor, Financial Transaction Services (FinTS). They are primarily used by retail customers to access their banking data using third-party products. In particular, these interfaces can also be used to create a multi-banking capability.²³

The scope of FinTS functions was progressively expanded over the years. The technical specifications now cover more than 130 transactions from all areas.²⁴ There is also a range of interface standards for the corporate banking business, of which the Electronic Banking Internet Communication Standard (EBICS) is the best known. This replaced the former File Transfer, Access and Management (FTAM) protocol in 2008.²⁵

22 Application Program Interfaces (APIs) allow software to interact with existing systems by using enabled functions, content or other data. See e.g. EBA Working Group on Electronic Alternative Payments, Understanding the business relevance of open APIs and Open Banking for Banks, Version 1, May 2016, page 7.

23 FinTS, <https://www.hbci-zka.de>, retrieved on 12 December 2018.

24 FinTS, <https://die-dk.de/zahlungsverkehr/electronic-banking/fints/>, retrieved on 12 December 2018.

25 EBICS (Electronic Banking Internet Communication Standard) protocol, <https://die-dk.de/zahlungsverkehr/electronic-banking/dfu-verfahren-ebics/>, retrieved on 12 December 2018.



Whereas mainly classic banking software products used these interfaces in the past, FinTS is predominantly used in the savings bank sector today by smartphone apps for iOS²⁶ or Android²⁷ devices to enable mobile banking for customers. Especially mobile banking is becoming increasingly important. For example, more than 30 per cent of the savings banks' online banking customers already regularly use their smartphone to access their account. However, the FinTS interface was and is increasingly being also used by internet companies or third-party service providers as a basis for providing their services.

The Second Payment Services Directive (Payment Service Directive II – PSD2) is bringing in new challenges and requirements for the savings banks, affecting their relationships with both customers (and in particular access to online banking) and with competitors such as fintechs, and above all with international tech giants. From the viewpoint of the savings banks, however, PSD2 also makes an important contribution to legal certainty because it defines how third parties can access online banking data. The same applies to the “Regulatory Technical Standards on strong customer authentication and common secure communication” (RTS) published by the European Commission in early 2018. The RTS expand on the requirements of PSD2. Both rulebooks

26 Apple's operating system for its mobile devices (iPhone and iPad).
27 Google's operating system for mobile devices.

make clear that screen-scraping²⁸ is prohibited. Because of this, and because of the requirement for strong customer authentication (SCA), they make an important contribution to the security of online transactions. At the same time, the exemptions from SCA defined in PSD 2 meet the need of many customers for enhanced user friendliness.

The savings banks therefore also view PSD 2 as an opportunity for a customer-centric upgrade to their digital services through their online offering. The introduction of multi-banking in the institutions' financial platform is a first step in this direction. The statutory requirement to make interfaces available to other sectors (e.g. to tech groups) would be an important step towards a level playing field.

The Savings Bank Finance Group actively participated in the creation of the PSD interfaces right from the start through its significant involvement in the development of the NextGenPSD2 API by the Berlin Group, a European standardisation initiative.²⁹ The specifications

28 Press release by European Commission, Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments, http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm, retrieved on 12 December 2018.

29 Berlin Group press release, PSD2 Access to Bank Accounts, <https://www.berlin-group.org/psd2-access-to-bank-accounts>, retrieved on 12 December 2018.

implement a cross-border standard for an interface that meets the requirements of PSD2 and enables data interchange with account information service providers, payment initiation service providers and third-party card issuers in compliance with the legal requirements. As stipulated by law³⁰, the first tests will be made possible starting on 14 March 2019. The system is expected to go live on 14 September 2019.

Besides the legally stipulated interfaces in PSD2 and the established FinTS infrastructure, the Savings Bank Finance Group is working on a comprehensive API infrastructure for all application areas.

One-System-Plus (OSPlus), the savings banks' core banking system, already enables a range of options for integrating such offerings, for example through single sign-on mechanisms and access to technical banking

processes and data. In addition to public interfaces that can be used freely, the future API infrastructure will again offer private APIs that could be made available to certified contractual partners based on a defined framework.

The overall contractual, content-related and technical conditions for future access to the API infrastructure are currently being defined with the participation of various stakeholders. This could contribute to the more rapid integration of market solutions. However, it would also make it easier to develop market-ready prototypes in quick succession outside the traditional development cycles at the central data centre. In this way, product innovations in the form of MVPs³¹ that still comply with the legal and regulatory requirements could be tested for customer acceptance as quickly as possible, trialled at individual savings banks and, if successful, introduced nationwide in the Group.

30 EBA, Payment services and electronic money, <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money>, retrieved on 12 December 2018.

31 MVP = minimum viable product. The first iteration of a product with a minimum range of functions that has to be developed to meet customer, market or functional needs with a minimum of effort to ensure usable feedback.



3.1.4 Fintechs – partners or competitors?

In recent years, a large number of new providers offering financial services on the internet have emerged in the market for financial services. The importance of these companies, which are often referred to by the media as “fintechs” and are frequently start-ups, has grown significantly.³²

A particular feature that is typical of fintechs is their high level of technology expertise. They systematically remove individual processes from the value chain of traditional credit institutions and optimise them for the digital world. Right from the start, they opt for a different approach than existing financial service providers have used in the past.

Fintechs endeavour to maximise the focus on customer needs when they develop digital solutions and to involve customers in every phase of development. They automatically employ rapid development cycles so that they can quickly identify and respond to undesirable or new developments. Their approach therefore differs significantly from the classic development methodologies typically used by the savings banks. As a result, fintechs are often quicker to bring digital solutions to market. In individual cases, however, a higher propensity for taking legal risks and, connected to this, economic risks, can also be observed (e.g. in money laundering checks).

Although the savings banks claim that they have always had a customer-centric business model, this is not necessarily the case with every technical solution. They identified the new competition from fintechs at an early stage. However, the first phase of mutual antagonism, which was talked up especially in specialist

circles, is long gone. In fact, we see many opportunities how both sides can benefit from each other: fintechs score with their undoubted digital expertise, which manifests itself in a short time to market and the often high quality of the customer front ends. In addition to their large customer base and long-standing customer relationships, credit institutions contribute personal closeness to customers and the high quality of their advisory process, well-functioning and scalable support structures, and profound regulatory expertise.

The innovation hub described in the section entitled “Innovation management and customer centricity” (see page 67) plays an important role in the alliance between savings banks and fintechs. The hub employs the same methodologies as digital companies to develop product ideas jointly with customers. They also invite selected fintechs to contribute their expertise and solutions as part of their trend scouting activities. This has already resulted in the first partnerships. For example, more than 230 savings banks use video legitimation to simplify the account opening process, relying on proven solutions from fintechs. The institutions have also integrated external solutions for switching accounts.

The savings banks wish to further expand their partnerships with fintechs, for example, through their participation in the federal government’s Fintech Council or as a sponsor of the German Startups Association.

To safeguard collaborative partnerships in the future, the savings banks see a need for European standardisation based on legal requirements for which there is currently no common understanding. In particular, the development and use of interfaces to account and banking data can only be sufficiently driven forward if the legal environment allows the necessary infrastructures to be refinanced by their co-users.

³² The term “fintech” is not used consistently in this context. The European Parliament, the European Commission and the European Banking Authority understand it to mean new distribution channels and products in the financial sector, which is why they include start-ups and established institutions in their observations. (European Parliament’s report on FinTech, April 2017; European Commission’s Fintech Action Plan, March 2018; EBA Fintech Road Map FAQ, March 2018).

3.2 The savings banks' perspective in the Digital Agenda

In addition to the customer perspective, the Digital Agenda concentrates on the savings banks' digital fitness. To do this, it provides a range of tools that are designed in the first instance to help the savings banks capture their status quo – and then to support them in making further improvements.

These tools are presented in the following.

- Minimum digital standards – Where does the savings bank stand compared with the average for the Group?
- Digitalisation compass – A digital reference resource for savings banks that provides concrete, institution-specific recommendations for action.
- Documentation platform – A central information offering for exchanging digital ideas and innovations.

3.2.1 Minimum digital standards

The minimum digital standards set out how the institutions expect digital solutions to actually be used in the dimensions of customers, savings banks and staff. The measurement criteria defined to this end are worded in such a way that they can be achieved with centrally provided solutions and support measures. The minimum standard is defined as the average level of digitalisation across all savings banks. This means that the standard is not a fixed level, but continues to grow.

The minimum standards are calculated once a year. Today's average will be tomorrow's minimum requirement. This ensures the continuous, consensus-based dynamic development of the level.

3.2.2 Digitalisation compass

Based on the values it has achieved for the minimum standards, each savings bank can decide whether and, if so, in which aspects, it intends to make further progress

in digitalisation. The digitalisation compass tool reveals potential solutions for the concrete need for action. The digitalisation compass is designed as a digital reference resource that also supports the savings banks in the process of transformation and cultural change in the direction of digitalisation.

3.2.3 Documentation platform

The documentation platform is a web-based information offering that gives the savings banks a central overview of the innovation ideas that already exist, are available or are under development, as well as the available digital solutions of the Savings Bank Finance Group and its service providers. This explicitly includes solutions that individual institutions have identified on their own initiative or want to develop with others.

The documentation platform is designed to bring together idea providers, potential investors and implementers, and hence to support the development of further investments. At the same time, it serves to document what is already there. This aims to help avoid parallel developments in the Group as far as possible.

Users of the documentation platform can also have their project proposals reviewed – for example with regard to legal and trademark questions and the regulatory environment.

3.2.4 Staff digital expertise

Advancing digitalisation will substantially change the world of work and hence the working environment of savings bank staff. The savings banks see a need for highly qualified personal advice in the future digital world as well, while pure-play service activities could be increasingly superseded by automated processes. The same principle applies here: customers decide which services and which performance features they want to use on which channel.

To successfully master this change, the staff and managers of the savings banks must also develop digital expertise. As well as a natural understanding of the savings banks' own digital offerings, this also extends



© iStock/From2015

to a greater willingness to embrace constant change. That is why staff professional development and an open approach to the necessary changes are critical for success.

The Savings Bank Finance Group is addressing the necessary cultural change through a range of measures at centralised and decentralised levels. The digital expertise status quo is made transparent by the staff perspective in the minimum digital standards (see 3.2.1, page 81).

Staff qualification is enhanced through a series of training measures. The digital skills of applicants are becoming ever more important when it comes to recruitment and the selection of young talent. The Group's own professional development concepts and training offerings are being increasingly digitised and made accessible to staff through electronic media such as tablets. The reform of the German bank clerk (*Bankkaufmann/-frau*) occupational profile is also particularly important for the savings banks.³³

³³ DSGV, Financial Report 2017, page 199.

3.2.5 Automation

Another important aspect of digitalisation is the automation of process and decision-making steps and, related to this, the reduction of the need for manual activities by staff and customers.

The advantages of automation are self-evident. Processes are more customer-centric, faster, less error-prone and more cost-effective. Banks and savings banks still lag behind other sectors in these areas. In recent years, the savings banks and their central service provider Finanz Informatik have selectively extended process automation for both internal processes and transactions initiated directly by customers on the internet platforms. The aim is to implement as many completely end-to-end and hence seamless transactions as possible or to streamline processes to the best extent possible through automation. With this in mind, further efforts are being made and new technologies such as Robotic Process Automation (RPA) are being used. The aim of the DSGV's current "Operating Strategy of the Future" project is to significantly reduce the savings banks' administrative effort, among other things by more intensively using suitable automation measures and selectively developing new ones.

4 Trust in the digital world – cybersecurity as a competitive factor

The rise of digitalisation is making resilience to cyber risks (cyber resilience) an increasingly important factor. Cyber risks have now emerged as one of the top business risks.

The savings banks' Internet-Filiale, online banking and the savings bank apps are among the most attractive targets in Germany for hackers and cybercrime because of their high customer acceptance and the intensity with which they are used. A total of 12,000 cyberattacks reports were recorded in the first six months of 2018, at times 1,000 per week.

The security of the IT systems used for digitalisation is therefore one of the highest priorities for the savings banks and a deciding competitive factor. Customers trust that the savings banks will not only handle their data, and ultimately their money, with care, but will also protect them from unauthorised access by third parties. Cybersecurity contributes significantly to this trust.

The Savings Bank Finance Group is facing up to the challenge of adequately safeguarding the operational, technical, financial and reputational aspects of cyber risks in its risk management processes. Over the past few years, comprehensive organisational measures have been implemented and substantial amounts have been invested, for example to continuously enhance Finanz Informatik's multi-level security architecture and the savings banks' information security systems and processes.

Cybersecurity is a crucial interdisciplinary field and an integral element of the Savings Bank Finance Group's strategies. The internal measures adopted by the savings banks to ensure a high level of data and process confidentiality, integrity and security are aligned with the arrangements in place to safeguard a high level of system availability and reliability and the information security systems of the central service providers, not least through the "Secure IT operation" (*Sicherer IT-Betrieb*) application.





© iStock/From2015

However, cybersecurity also means working together with partners, market players and networks that advocate greater security on the internet. For this reason, the central cyber defence team at the Savings Bank Finance Group works very closely with the Federal Office for Information Security (BSI) and other government institutions to pre-emptively counter cyber threats. In 2017, the central cyber defence team sent 170,000 reports of dangerous malware, Trojans and phishing sites to anti-virus manufacturers, thus improving the protection offered by the anti-virus systems used by many savings banks and their customers.

Reflecting the growing cyber threat situation, lawmakers and regulators have continuously adapted and expanded on the requirements applicable to information security guidelines and information security processes at banks and savings banks. PSD2, which was primarily transposed by the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz – ZAG*), and the Minimum Requirements for Risk Management (MaRisk) issued by BaFin – supplemented by Circular 10/2017 (BA) “Supervisory Requirements for IT in Financial Institutions (BAIT)” – are the key requirements here.

The Savings Bank Finance Group follows the ISO27xxx series of information security standards. In addition,

all of these statutory and regulatory requirements for information security and a standards-based information security management system for the institutions of the Savings Banks Finance Group are mandatorily modelled by the “Secure IT operation” (*Sicherer IT-Betrieb*) application.

A large number of measures are necessary to implement these statutory and regulatory requirements. The Savings Bank Finance Group’s central cyber defence team supports the savings banks and Landesbanks in implementing them. The cyber defence team consists of a reporting office that receives warnings of cyber attacks, a situation centre that visualises the overarching impact of the attacks and a special defence unit that counters the attacks. As a complementary measure, a central anti-fraud team for the institutions of the Savings Bank Finance Group was established at Finanz Informatik.

The Savings Bank Finance Group is expecting a comparably high number of cyber attacks in 2019. It also expects that PSD2 will lead to more access to accounts by third party providers (account information services and payment initiation services), which will see a rise in the number of attacks and scamming attempts using targeted phishing and social engineering attacks.

5 New business models for the Savings Bank Finance Group

Big Data, Artificial Intelligence and blockchain attract intense debate and analysis today when new business activities for the financial industry are being considered.

5.1 Big Data/Artificial Intelligence (BDAI)

BDAI – Big Data and Artificial Intelligence (AI) – are critical digitalisation technologies because they help meet two key expectations for the benefits of digital transformation: they increase the speed with which requests and orders can be dealt with. And they can be used to optimise internal processes, checks and assessments. There is a general presumption that BDAI can make a significant contribution to massively transforming value chains and leveraging significant efficiency gains.³⁴

The customer-centric use of data shapes and transforms financial services. The savings banks have a strong starting basis in this respect. Data from more than 50 million customers gives them a wealth of data. Data analytics (“Savings Banks Data Analytics” – SDA) and data-based applications allow them to better understand customer needs and behavioural patterns. Building on this, services and value added for the customers can be improved or actually made possible for the first time, for example by means of individual advisory approaches. Another development stage is the “next best action”, which is used to offer customers exactly the right solution at the right time that meets their needs in every situation and in every channel.

In its data analytics, the Savings Bank Finance Group strictly ensures that only data whose use the customer has explicitly consented to in the form of a specifically detailed declaration of consent can be accessed within the limits laid down by law. The institutions’ strategy is guided by both principles: compliance with the statutory and the supervisory requirements, and in particular

the General Data Protection Regulation (GDPR), and safeguarding the interests of customers when using their data. The already high consent rate of 30 per cent demonstrates customer trust in the savings banks.

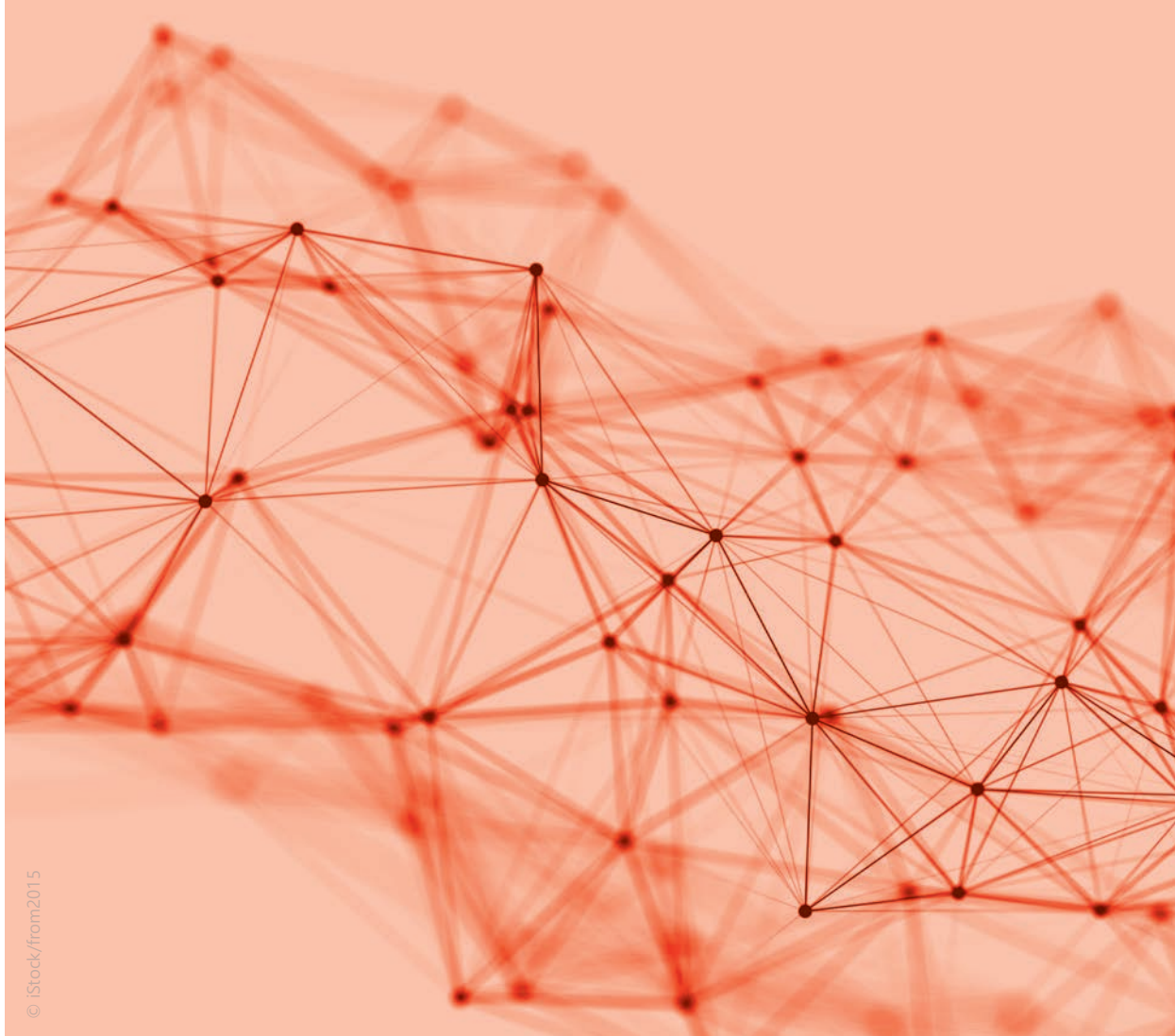
In the past, data was analysed using classical statistical methods (for instance multivariate analyses), for example to determine probabilities of default or product affinities using score cards. The computing power of IT systems has risen sharply in the past few years. Systems and processes based on Artificial Intelligence are thus also becoming more important.

New algorithms and machine learning will not only offer automatic, continuous optimisation of existing processes, but will also open up completely new applications and areas where they can be deployed. The conditions for this are training using existing data and the creation of closed loops in which the results of analyses and the events that have actually occurred are fed back into the system in order to make it more accurate by means of this reconciliation.

The Savings Bank Finance Group addresses the issue of Artificial Intelligence in a variety of fields. Neural networks are already being used today in particular in areas such as cybersecurity in order to ward off or minimise losses. We can also see applications in the automation of business processes that can be trialled in projects, for example to identify and classify incoming correspondence across different channels. The Group has also gathered initial experience of using bots and voice services in the area of direct customer contact. For example, the first savings banks are now using chatbot systems that not only answer customer questions about standard problems, but also optimise themselves autonomously based on their dialogue history.³⁵

34 BaFin, Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services, page 65 et seq.

35 IT-Finanzmagazin, Berliner Sparkasse setzt Beta-Version des KI-Chatbot „fred knows“ ein; nun sei er allgemein verfügbar (Berliner Sparkasse is using beta version of the AI chatbot “fred knows”, which is now generally available), <https://www.it-finanzmagazin.de/berliner-sparkasse-ki-chatbot-64861/>, retrieved on 12 December 2018.



The DSGV is currently developing a comprehensive Artificial Intelligence strategy for the Savings Bank Finance Group. Besides the legal and economic perspective, it will also address ethical principles and thus provide guidance to the Group on a broad range of issues.

Additionally, the DSGV has examined in detail the BaFin study "Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services" and participated actively in the dialogue launched by BaFin as part of the consultation exercise.³⁶

In light of the diverse application areas and the new business models that can now be observed, for example in areas related to credit ratings, sentiment analysis and automated customer contact, the Savings Bank Finance Group also sees – in addition to the tremendous opportunities – the need to monitor any risks at a conceptual level, to analyse them and to incorporate them swiftly into the regulatory system. In this context,

³⁶ BaFin, Consultation on the BDAI report, www.bafin.de/dok/11137698, retrieved on 12 December 2018.

we believe that it makes sense for business models and companies emerging from BDAI to be treated in line with the principle of "same risks, same rules", resulting in unrestricted equality of treatment to ensure a level playing field and safeguard consumer protection.

5.2 Blockchain

Blockchain, and in particular distributed ledger technology, has the potential to create an even more digitally networked global ecosystem. Digitalisation is already breaking up formerly fixed system and process boundaries and decentralising value chains. Blockchain and distributed ledgers can significantly accelerate this trend and thus encourage the development of dynamic new digital value networks (ecosystems).

Developments in the area of blockchain technologies and applications accelerated considerably in 2017. New blockchain-based business models, applications and consortia are currently emerging at a fast pace. A growing number of banks and insurance undertakings are recognising the concrete potential of this technology and are investing in corresponding projects or

participating in consortia. There is a particular focus here on combinations of private or consortium-based blockchains with the “smart contracts” concept.

The Savings Bank Finance Group has launched a range of initiatives since 2015 to evaluate the significance of blockchain and to test the suitability of prototype blockchain-based business models and applications. One example is the development of a blockchain-based platform for promissory note issuances by Landesbank Baden-Württemberg (LBBW) in 2017 (Daimler) and 2018 (Telefonica Deutschland).

Blockchain-based promissory note issuances enable direct, secure and transparent financial transactions in real time because data sets are only updated by a consensus. The decentralised storage of data blocks and cryptographic signatures make transaction processes more transparent, more secure and more efficient. However, these examples also highlight the current legal restrictions on establishing blockchain promissory note transactions as a genuine option for corporate finance activities. To achieve this, there would have to be sound legal confirmation of the option to securitise debt securities by means of digital certificates. In the case of the current blockchain-based promissory note transactions, the conventional issuance route was used in parallel to ensure the legally compliant documentation of the terms and conditions of the bonds in accordance with the German *Skripturprinzip*, which requires the terms and conditions of the bond to be incorporated in the bond certificate.

Once these promissory note transactions had been settled using blockchain technology, LBBW and the Stuttgart Stock Exchange created a marketplace for the end-to-end digitalisation of the promissory note process under the “Debtvision” brand. A large number of institutional investors such as savings banks, banks, insurance undertakings and occupational pension

schemes (*Pensionskassen*) have already joined this platform. Over the next few months, blockchain will be integrated into the platform, which will see the entire value chain being transferred to this innovative technology.

In 2017, NordLB developed a blockchain prototype together with the Fraunhofer Gesellschaft to optimise processes for documentary credits. It joined JP Morgan’s Interbank Information Network (IIN) in September 2018. IIN is based on JP Morgan’s blockchain “Quorum®” database and is specifically tailored to international payment transactions.

A multi-institutional initiative was also launched in 2018 by BayernLB, Helaba, LBBW and S-Servicepartner Berlin to establish a blockchain-based platform for the institutions of the Savings Bank Finance Group, based on which trading/financing processes as well as alternative financial products in the area of trade finance can be innovatively digitised and supported more efficiently.

The Savings Bank Finance Group is in close contact in the case of all these developments with the European savings banks, in particular with Erste Bank Group, CaixaBank and Swedbank, which are also operating blockchain initiatives.

Nevertheless, blockchain technology is still in its early stages technically and economically. The majority of the applications identified in the financial sector to date are currently at the conceptual or test phase, so they are still a long way from commercial use in the mass/volume business. Nevertheless, in particular the potential for improving process transparency and efficiency is driving forward development. For example, we can see opportunities to use blockchain as an efficient way of reporting to the supervisory authorities, for example to demonstrate the accuracy and completeness of transactions of various types.

6 Outlook

Digitalisation poses a multitude of challenges for the savings banks in different dimensions that they are addressing with a variety of measures at centralised and decentralised levels. The savings banks' Digital Agenda has defined ambitious standards and created tools to help the institutions to stay relevant in the future.

It is evident that digitalisation is not a static goal. Rather, digitalisation is a process that requires the ability not only to react promptly to changes, but also to shape them actively. The legal and regulatory framework is also particularly important. It plays a crucial role in deciding

whether the institutions will be able to compete in the future with the technology groups – some of which are still not yet regulated in Germany – that increasingly offer finance-related services, or whether they will have to hold their own in a legally unlevel playing field.

The savings banks are fully aware that digitalisation is an opportunity to change and enhance their business model, while maintaining the essence of their business – being close to their customers. The customer experience in particular will be the decisive factor for acceptance in the digital world.



WVI

Insurers' business is set to experience fundamental change. Dr Jörg von Fürstenwerth, Chair of the Executive Committee of the German Insurance Association (GDV), analyses the seven possible megatrends and their potential as agents of change.

En route to the world of digital insurance

A report from the engine room of change

Author

Dr Jörg Baron Frank von Fürstenwerth

Member of the Presidential Board, Chair of the Executive Committee German Insurance Association

1 Introduction

Prevailing opinion nowadays cannot manage without the proposition that, in a time of profound change, companies will only be able to adopt a sustainable business model if they are agile in every respect. Agility has become one of the keywords of the digital debate. The claim is that only agile companies are in a position to find an appropriate response to the disruption of their business models. There is a general belief that insurance undertakings face particularly high hurdles, especially as they do not exactly have a reputation for taking the lead when it comes to change. That is not entirely fair. And it is why I would like now to take a closer look at the engine room of change.

Although this will start with a look at the bigger picture: if there was any symbol for the dynamic change in business models and markets in the recent past, then it is the name “Cebit”. The concept behind the Cebit trade fair was unable to withstand the dynamic growth of digitalisation. Cebit is now history – and a cautionary

example of what happens if you underestimate the pace of change.¹

The signs of the times must be recognised and analysed quickly, action items must be defined and the necessary – and sometimes unpleasant – measures must be implemented with agility and above all with courage. One example of this is the race for domination in the field of Artificial Intelligence (AI). Many people today consider AI to be the most important technology since the steam engine.² Even though research into AI and the necessary algorithms has been ongoing for 70 years now, it is only today that the computing

-
- 1 Schnurer, NDR.de – Für Hannover ist das Ende der Cebit ein Desaster (The end of Cebit is a disaster for Hanover), https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Fuer-Hannover-ist-Ende-der-Cebit-ein-Desaster,cebit4234.html, retrieved on 5 December 2018.
 - 2 See Reuters, Altmaier – Künstliche Intelligenz nach Airbus-Vorbild vorantreiben (Encouraging AI based on the Airbus model), <https://de.reuters.com/article/deutschland-k-nstliche-intelligenz-idDEKBN1O30H1>, retrieved on 5 December 2018.

power of modern computer systems allows the full potential of the technology to be leveraged – looking to the future, quantum computing should be mentioned here. The Member States of the European Union (EU) have mobilised billions of euros to avoid being left behind in the global market of the future. The European Commission’s plan sets out actions in four key areas: “increasing investment, making more data available, fostering talent and ensuring trust.”³

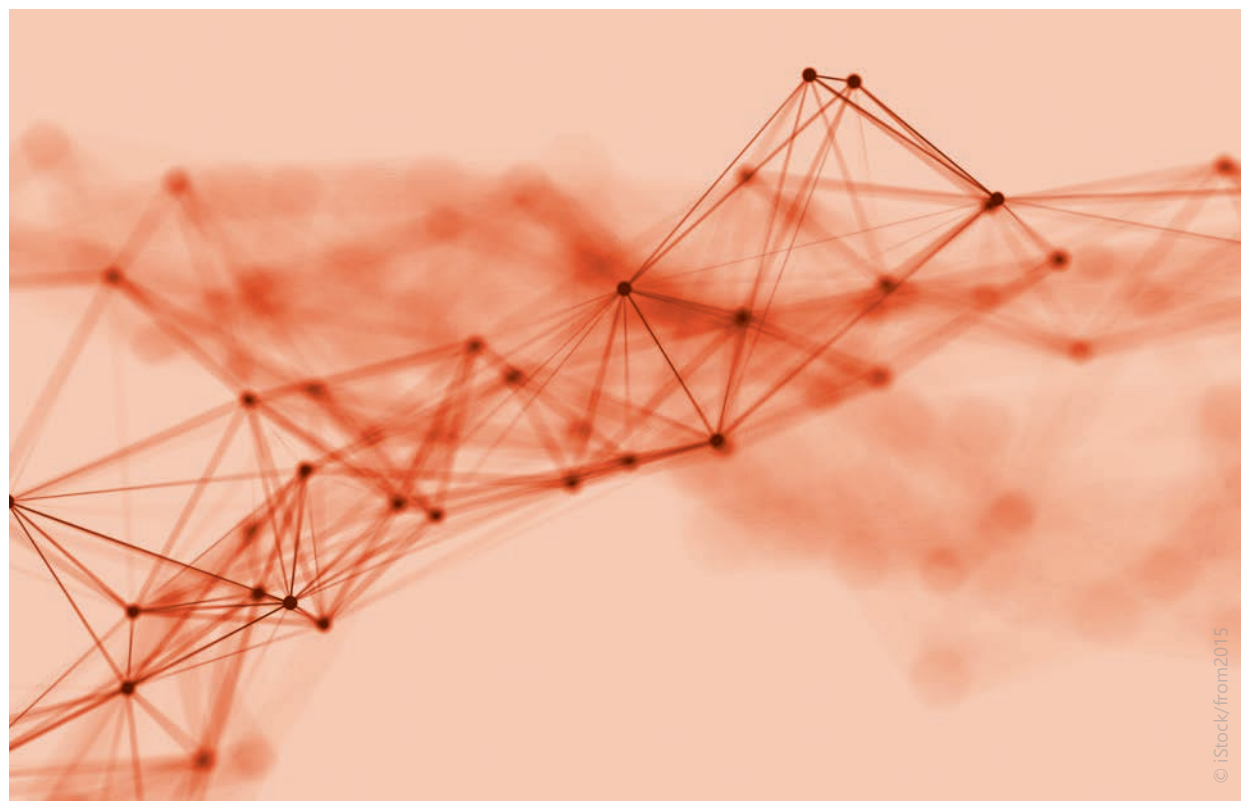
The federal government had already published its own AI strategy in November 2018. This will create 100 new chairs of AI and make available around three billion euros by 2025. However, research is not the be all and end all, because the results must also be translated – in a

3 See European Commission press release Member States and Commission to work together to boost artificial intelligence “made in Europe”, http://europa.eu/rapid/press-release_IP-18-6689_en.htm, retrieved on 5 December 2018.

competitive international environment – into viable and possibly fundamentally new, and hence disruptive, business models and new solutions for business and society. And AI is just one of many digital trends that could increasingly turn the economy inside out, turn old markets upside down and create entirely new ones – and of course the insurance industry is no exception here.

Seven megatrends – entailing both opportunities and risks – are identifiable at present that could potentially transform the business of insurers in the long term:

- The battle for customer contact
- New technologies: Artificial Intelligence, cloud and blockchain
- Creative destruction, new business models and products
- The process revolution
- New competitors, greater diversity of providers
- Competition for talent
- Agile supervision



2 The battle for customer contact

Consumers are heterogeneous

The financial and sovereign debt crisis that emerged in 2008 was a key lever for a fundamental overhaul of the image of the consumer⁴; consumer protection has never had such a high profile as it does today. Insurers have accepted this challenge and understand digitalisation to be an excellent opportunity: they are adapting the updated, differentiated consumer model and are endeavouring to better meet the diverse needs of their customers. Digitalisation is bringing new opportunities for our industry to communicate differently, individually and more intensively with customers than ever before.

The web is increasing competition – but not necessarily transparency

The web is inundating customers with data, and at the same time vacuums data up from them. Media reports are dominated by news about digital tools such as language assistants, chatbots, robo-advisers and apps. Some customers even trust these tools more than they do people. The fact is that a growing number of consumers are seeking out information and comparison platforms. And the insurers also go where the customers are. This explains why the number of cross-sectoral partnerships to distribute insurance cover is set to grow. Predictive analytics, i.e. the generation of predictions based on data, will also eventually play a role in the distribution of financial services. Compared with traditional intermediaries, it can often identify customer need for insurance cover faster or create it more selectively, as well as service it more conveniently. This will increase competitive pressure – but not necessarily transparency in the market, because altruism is also the exception in the world wide web. Comparison portals, for example, mainly give the impression that they are neutral, but they are not exactly disinterested. They pursue a clear business interest and do not normally cover the whole market. Everybody who uses these portals needs to be aware of this, so that is why it should also be clear for all to see.

4 See GDV, Verbraucherleitbild (Consumer model), <https://www.gdv.de/resource/blob/23930/5ee58e2831202f286c8c6bbec9d4609c/verbraucherleitbild-des-gdv-1016934987-data.pdf>, retrieved on 5 December 2018.

Linking digital communication and personal advice

Many customers buy insurance cover on the internet. By contrast, others make personal contact with an intermediary they trust after obtaining information online. Still others obtain information offline and then buy online. The customer journey is individual, situational and above all flexible.⁵ The preference for digital is no longer a question of a customer's age. The efficient integration of digital communication and personal advice is a must for everyone in distribution and a great opportunity to stand out from the rest in the battle for customers, because personal advice is still indispensable for many people and in many areas. This is a situation in which personal relationships with customers count, as well as qualifications and a professional approach. Empathy, accessibility, convenience, process speed and networking belong together. An efficient data flow is vital. From the customer's perspective, this blurs the traditional boundaries between distribution, operations, claims and benefits.

Paper will last and last... and it's here to stay

To leverage the pace of change as effectively as possible, it must be possible to model all processes in the company electronically – from applications for cover through to claims settlement. However, it is difficult to get away from paper. The EU Insurance Distribution Directive (IDD) stipulates that documents must be sent on paper as the standard case, and that departures from this principle are possible only under certain circumstances. But insurers often meet with a total lack of understanding if they send letters to their customers – not least because of the delay involved (although to be fair, it should also be mentioned that many customers still think it is important to hold a piece of paper in their hands).

5 Institute of Insurance Economics, University of St. Gallen & Synpulse Schweiz AG, Denken Sie noch in Kanälen oder erreichen Sie Ihre Kunden schon? Die Customer Journey in einer multioptionalen Welt (Do you still think in terms of channels or are you already reaching your customers? The customer journey in a multioptional world), <https://www.iww.unisg.ch/~media/internet/content/dateien/instituteundcenters/iww/studien/pm-customer%20journey%20mfz-studie2016.pdf>, retrieved on 5 December 2018.



© iStock/from2015

A level playing field

There must be a level playing field in the race to attract customers. This applies to both established providers in our industry and new ones. A new rulebook for insurance distribution (the IDD mentioned above) has been in place since February 2018. This EU directive has been transposed into German law, and all market participants must now comply with these rules. That is because not everything that is digital in origin actually benefits customers. At any rate, the European Commission is proposing to issue a regulation on promoting fairness and transparency for business users of online intermediation services. This also means introducing greater transparency regarding the parameters used to rank the results of online searches. It is designed to prevent arbitrariness in lists of providers. The Federal Cartel Office has also addressed comparison platforms in a sectoral investigation.⁶

⁶ See Federal Cartel Office, Sektoruntersuchung Vergleichsportale – Konsultation (Sectoral investigation of comparison portals – Consultation), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Vergleichsportale_Konsultation.html, retrieved on 6 December 2018.

Consumers should have freedom of choice

Consumers in Germany have a choice between different routes for accessing insurance cover. They can take out a policy directly with the insurer. However – and most people do this – they can also use an insurance intermediary who receives a commission. Or they choose an insurance consultant who works on a fee basis. The coexistence of these options is an important asset and no remuneration system should be discriminated against.

Digitalisation is accompanied by a new diversity. That is the actual business challenge because, on the one hand, there is a recognisable trend towards standardisation. At the same time, however, there is also an evident trend towards increasingly bespoke solutions. Digitalisation makes both of these possible and makes them both ever better. It appears to be paradoxical in this respect, but it is and is likely to remain reality: particularly in this world of diversity, direct customer contact will play an important role, both when insurance contracts are entered into and when good relationships with customers are being developed and, above all, maintained.

3 New technologies: Artificial Intelligence, cloud and blockchain

Technological advances open up opportunities for the insurance industry

The focus now will be above all on the opportunities: technical progress offers a wide variety of possibilities for improving the provision of insurance products. This affects all parts of the value chain. The potential rewards are substantial; additional data sources are available; there are new analysis methods for risk assessment and rate setting; the automation of business processes is in full swing; young talent and its start-up culture are shaping innovative marketing and distribution strategies. All this is fuelling a fiercely competitive innovation climate that aims to provide efficient, cost-effective processes, improved product solutions and services, and customer access that is as optimised as possible.

Key areas of AI are process automation, risk analysis and customer contact

The insurance industry is particularly suitable for deploying AI because it processes large volumes of data and the processes are characterised, in part, by both repetitions and specific semantic features. AI is expected to play an important role in three key areas: first, AI will help automate insurance processes. Second, AI will make a valuable contribution in the area of risk analysis. And third, AI will make customer contact more efficient.

AI is already helping today: customers can now receive their insurance benefits not within days, but within hours. Robo-advice and language assistants provide customers with high-quality advice around the clock.⁷ Losses can be reduced or even prevented, for example by sending severe weather alert data to customers in good time. Insurers can use data linkage to better inform their customers in new life situations, such as marriage and birth, about duplicate policies or gaps in their insurance cover. Address changes or archiving processed insurance claims can be handled in the background by intelligent systems,

cutting administrative expenses and hence also saving customers money.

As well as optimising the insurance process and claims settlement, AI will also improve data processing and analytics – in light of the data volumes becoming available from the Internet of Things (IoT), for example, this represents tremendous progress. The outcome will be an increase in customers' understanding of risk, with insurers being able to offer innovative, bespoke services more quickly.

Cloud computing gaining ground in the insurance industry

Cloud computing continues to make tremendous advances, producing attractive opportunities for optimisation and cost reduction programmes. Cloud service providers offer various service models: one service level is "Infrastructure as a Service" (IaaS), meaning that virtualised computer hardware such as computers, storage devices and networks are used in an external data centre. Another is "Platform as a Service" (PaaS), denoting the cloud as a development environment. Users can use PaaS to develop their own software applications or test them in an environment provided by the cloud provider. In the case of "Software as a Service" (SaaS), the application itself is delivered from the cloud. All three variants and any subcategories must be accessible to companies in regular business operations and protected by a high level of security – if the companies are to survive in the competitive international environment.

Blockchain offers enormous potential in the field of e-government

Interest in blockchain technology is continuing unabated, albeit from a different perspective. After the initial market hype, triggered in particular by the rise of the bitcoin cryptocurrency, attention is now focused increasingly on concrete applications and the need to adapt the legal framework. This is because blockchain is the technology and bitcoin only one of many possible applications.

Distributed ledger technology (DLT) has considerable potential, particularly for the insurance industry – this is always the case when a series of partners has

⁷ See GDV, Hey, Computer, was geht ab? (Hey computer, what's up?), <https://www.gdv.de/de/themen/positionen-magazin/hey--computer--was-geht-ab--39074>, retrieved on 5 December 2018.

a legitimate interest in the end-to-end, authoritative history of a thing or person at different times over a longer period of time and can demonstrate this. Examples of this include the structural condition of a house and building insurance, or the mileage of a car and motor insurance, or also a pension insurance contract that may run for several decades, such as the German “Riester” pension. Especially in e-government, blockchain offers an opportunity to network private and state agencies such as land registries, vehicle registration offices and pension benefits agencies cost-effectively, reliably and securely. Intelligently designed blockchain solutions would allow the contract and inventory systems of all partners involved to be smarter and the process chains to be simpler.

A state-of-the-art legal framework for applying new technologies in a global competitive environment

There is a need for a state-of-the-art regulatory and supervisory framework to allow opportunities offered by digital technologies to be leveraged. Regulation must be innovation-friendly. This means that it must be technology-neutral, principle- and risk-based, and stripped of excessive requirements.

That is why there are repeated calls for an “algorithm TÜV”, i.e. a standards-based inspection and validation of algorithms. A criticism voiced by consumer protection experts is that the decisions, for example by a simple AI engine, are not understandable or transparent, basically taking place in a black box. Already today, customers are able to find out about the criteria and require a manual review if there is a negative or unfavourable decision by a fully automated system. The calls for an “algorithm TÜV” may come as a surprise because the use of algorithms in the insurance industry is basically nothing new. What is innovative today is the use of partially and fully automated process chains that also use AI. These can manage address changes or archiving processes centrally via intelligent systems, for example.

Despite all the euphoria, there is a need for responsible handling of AI technology. It is important in this respect for all players to subscribe to a broad social dialogue about the use of AI. It must be ensured that

the interests of both the affected consumers and the companies are adequately reflected. Nevertheless, the use of new technologies cannot be allowed to be inhibited by premature calls for regulation. Additionally, regulation that is limited to the national level could lead to disadvantages for German companies facing international competition.

Blockchain: The need for government involvement

In an exploratory study, insurers – under the umbrella of the German Insurance Association (GDV) – identified and analysed suitable deployment scenarios for blockchain. One key outcome: for blockchain to gain acceptance, government has to get involved, because it is still not clear how the potential blockchain applications can be reconciled with the existing legal framework. The “right to be forgotten” that is enshrined in the General Data Protection Regulation (GDPR), which was incorporated into European law with so much effort, is diametrically opposed to the underlying technical design of blockchain. In addition, there must be no legal uncertainty in blockchain solutions in the area of insurance regarding the recognition of transactions and identities.

4 Creative destruction: new business models and products

The revolution in mobility is a prime example of the upheavals that lie ahead in technology, society and also, of course, in politics and the economy. The insurance industry is addressing this issue in great detail, not least because, of course, it is also directly affected by it economically (motor vehicle insurance). In November 2018, the association discussed reality and vision intensively at a congress in Berlin. The foundation for the use of automated driving systems was laid by the federal government with its reform of the German Road Traffic Act in 2017. During the congress, a representative of the federal government emphasised that the country where the car was invented should also strive to be at the forefront of autonomous driving.

Digital transformation in road traffic

In fact, almost all the car manufacturers are working intensely on solutions that can handle driving tasks

without any driver intervention. Looking ahead to the future of assisted, automated and – in the final stage of its evolution – autonomous driving, one might come to the conclusion that many insurance policies will become superfluous one day: for example if error-free technology delivers the dream of accident-free road transportation. So “Vision Zero” – no fatalities and serious injuries involving road traffic – would become reality. Really?

This is the background to an interdisciplinary project group consisting of engineers, mathematicians, insurance experts and accident researchers established by the GDV. Its mission was to carry out a realistic, well-founded assessment of the expected impact of assisted and automated driving. The in-depth analysis by the experts and the consequent prediction of the impact on claims trends up to 2035 show that:



State-of-the-art driver assistance systems and automated driving functions

- make driving safer, but prevent significantly fewer claims in practice than in theory,
- are only catching on with a strong time lag and are therefore only slowly reducing claims,
- lead to higher repair costs in the event of a claim, and
- have a greater impact on motor vehicle third-party liability claims than on claims under partially and fully comprehensive cover.

The GDV study proves that, by 2035, the new systems will only reduce compensation payments by motor insurers by between seven and a maximum of 15 per cent.⁸ The new technology, which is far from perfect, makes repairs more expensive, prevents fewer claims in practice than expected and reaches its limits in the case of damage caused by stones and rocks, hail or rodent bites. Even in a digital era, insurance protection will therefore remain indispensable.

The intelligent house itself becomes a risk

The same applies to smart homes and the increasing use of intelligent household appliances: if you believe the promises of the manufacturers, damage will be a thing of the past in intelligent homes, burglars won't stand a chance and the refrigerator will replenish itself. None of this is even remotely close to reality, at least today.

A look at the bigger picture will help to show where we actually are: before the supposedly new technology found its way into our homes, practically all of its components were already being used in industrial/commercial applications. Examples: building surveillance using cameras and motion sensors, electronic locks, fire alarms and leakage sensors. They have helped to keep a check on the claims burden even though the value of assets keeps rising. But they have not succeeded in completely freeing the world from insurance claims,

although these components were designed for a challenging working environment and are therefore expensive to buy and maintain across their life cycle. So is insurance superfluous? Hard to believe.

And that is not all: unfortunately, today's technology all too often serves as a gateway for additional dangers. This is because the cybersecurity offered by many products for private users is already highly dubious. Short device life cycles, a lack of updates, backdoor access – the list of problematic components could be continued indefinitely.

This has implications for anybody who buys unsafe products and for third parties. 21st century burglars no longer have to hide behind the bushes and scout out a house; now all they have to do is access the hacked surveillance camera, which has also conveniently recorded the PIN code of the smart door lock. And while you are happy with the convenience of the intelligent shutter control, it attacks your employer unnoticed as part of a botnet. At the latest the example of the Mirai botnet⁹ should make clear to everybody how easy it is to use Internet of Things (IoT) devices as an attack route – for example for distributed denial of service (DDoS) attacks¹⁰.

Identifying and containing risks

Combining intelligent, secure home technology with residential building and household contents insurance concepts can, of course, also offer tremendous opportunities. Damage such as leaking tap water can be detected and contained earlier, for example by automatically shutting off the main water supply. Corresponding product developments by the insurers are being vigorously driven forward. The problem here is that it is not clear at present, either to consumers or to insurers, which devices are worth recommending when it comes to security and support. Nobody has an

8 See GDV, Automatisiertes Fahren – Weniger Unfälle, teurere Reparaturen (Automated driving – Fewer accidents, more expensive repairs), <https://www.gdv.de/de/medien/aktuell/weniger-unfaelle--teurere-reparaturen-8286>, retrieved on 28 January 2019.

9 Symantec Corporation, Mirai Botnet, <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks>, retrieved on 24 January 2019.

10 Symantec Corporation, Distributed Denial of Service Attack, <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html>, retrieved on 24 January 2019.

overview about which devices deliver benefits in the sense of a security gain and which do not.

For this reason, the insurance industry published specific requirements for the Smart Home and Internet of Things device category as far back as 2017.¹¹ If the risks associated with these devices are to be tolerable in the long term, there must be a radical change in the manufacturers' product and support philosophy. If not, the exponential growth of intelligent and networked devices means that we are heading for an unparalleled security worst case scenario. In the next two years alone, the number of these devices will double – to around 20 billion worldwide (see Figure 1).

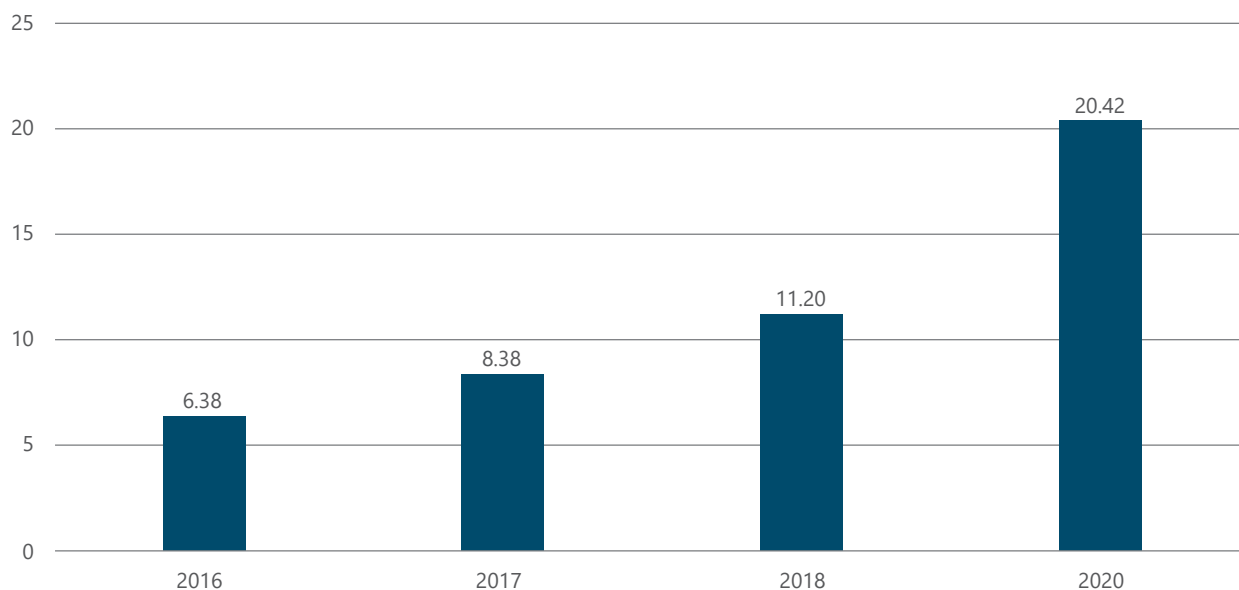
The insurance industry therefore expressly welcomes the publication of the "Secure Broadband Router"

Technical Guideline (TR-03148)¹² by the Federal Office for Information Security (BSI), as broadband routers are the central security hub in all private households. If the router is compromised, the smart home and data of the owner are exposed to the cybercriminal. A key goal of the Technical Guideline is to make the security features transparent for all users – and hence also insurers. Manufacturers can support this by labelling the device appropriately. The Technical Guideline is therefore an important step in the direction of an IT security label, as intended by the federal government in its 2016 Cyber Security Strategy and in the coalition agreement. The insurance industry supports the BSI's plans to also develop minimum requirements for IT security for other devices associated with the Internet of Things and the Smart Home.

11 GDV, Smart Home – Versicherer warnen vor Cyberrisiken im digitalen Zuhause (Smart homes – Insurers warn of cyber risks in the digital home), <https://www.gdv.de/de/medien/aktuell/versicherer-warnen-vor-cyberrisiken-im-digitalen-zuhause-8258>, retrieved on 5 December 2018.

12 Federal Office for Information Security, BSI TR-03148 Secure Broadband Router, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.html>, retrieved on 5 December 2018.

Figure 1: The Internet of Things – more than 20 billion units installed in 2020



Source: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>

New products and business models

Digitalisation not only transforms individual market segments, it even creates entirely new ones: the GDV has developed non-binding model terms and conditions for cyber insurance policies that can specifically protect small and medium-sized enterprises.¹³ They are addressed to medical practices or law firms as well as craft businesses and industrial suppliers. The insurance not only covers data theft and business interruptions, but also costs for IT forensic specialists or crisis communication.

The information to be provided by customers so that the cyber risk can be determined is different from the information needed to take out a conventional operating liability or building insurance policy. The GDV has also developed non-binding risk questions so that insurers can better assess a customer's individual risk of becoming a victim of a cyber attack before entering into a contract, and so that the company to be insured can more easily identify possible vulnerabilities in its IT security. The number and content of the questions depend on the company's risk category and business fields, and whether, for example, it handles sensitive data, manufactures in a network or operates e-commerce.

If necessary, new types of risk coverage are also possible: short-term insurance, for example, that can be taken out based on the on-demand principle depending on the particular circumstances. Examples are adding drivers to a motor vehicle insurance policy on a day-by-day basis or an accident insurance specifically for skiing holidays.

At the same time, many innovative approaches for extending the business model can be seen at insurers: in addition to cash benefits for an insured event, customers are being increasingly supported in dealing with risks or are receiving direct assistance. This includes information about improving driving behaviour and swift assistance

in the event of an accident in motor vehicle insurance, or help with managing chronic illnesses in health insurance. This will make insurers even more of a risk management partner than before. Insurers will generate quotes that reward low-risk behaviour with particularly low-cost rates. To do this, they are already collecting data on a voluntary basis, for example on an insured's driving behaviour and how much physical exercise they get. Insurers reward careful driving and active exercise – as a key contribution to modern loss prevention.¹⁴

Perhaps one of the most far-reaching innovations made possible by digital technologies is the “sharing economy” – direct, peer-to-peer transactions between private individuals via Internet portals, which act solely as intermediaries. In some areas, such portals have already achieved a high level of market penetration, for example for short-term rentals of homes and rooms. Peer-to-peer platforms are also becoming more important in the area of credit intermediation.

In insurance, on the other hand, peer-to-peer platforms are still in their early days. There are concepts for some property/casualty insurance classes in the German market, for example, that cover small claims within small groups of insureds. If there are no claims, the customers receive a premium refund. Larger losses continue to be covered by insurers as risk carriers.

However, there are no indications to date that peer-to-peer cover is being extended to higher risks in the retail insurance business – and certainly not in the commercial insurance business. In the course of the further race to innovate, however, it is possible that new product offerings that integrate peer-to-peer elements could be launched in the German insurance market.

¹³ See GDV, Medieninformation – GDV stellt Musterbedingungen für Cyberversicherung vor (Media release – GDV presents model terms and conditions for cyber insurance), <https://www.gdv.de/de/medien/aktuell/gdv-stellt-musterbedingungen-fuer-cyberversicherung-vor-8270>, retrieved on 5 December 2018.

¹⁴ For information about extending the business model and new product approaches, see, for example, Wiener, Theis, Vier Gründe, warum die Versicherungswirtschaft wichtiger wird, (Four reasons why the insurance industry is becoming more important) in: GDV Makro und Märkte kompakt (GDV Macro and markets compact), no. 15, <https://www.gdv.de/resource/blob/26204/b0ce16220de8b51d62f31e6f54fdeebe/makro-und-maerkte-kompakt--vier-gruende--warum-die-versicherungswirtschaft-wichtiger-wird-data.pdf>, retrieved on 6 December 2018.



One possible competitive advantage of these products could be that a sense of community arises in the small group that engenders a significantly lower tendency to commit fraud and can therefore have a positive effect on claims trends. Nevertheless, it is unlikely that more or even all insurance risks will be assumed on a peer-to-peer basis. This runs counter to the characteristics of the insurance business, which include a high loss potential, for example in liability insurance. Moreover, the long-term nature of many personal insurance contracts in particular should be remembered. This is linked to the necessary guarantee of the promised benefits, including in the event of unfavourable developments, so that the insurance fulfils its purpose for the individual (“potential commitment to provide additional funds”). Correspondingly, the peer-to-peer concept also raises a number of legal questions.

To be able to leverage the potential of the concepts described above productively, insurers must have the freedom to innovate as well as legal certainty. For example, they must be permitted to agree that risk-relevant data from networked devices can be used, at the customer’s discretion, for insurance and service offerings. The data sovereignty of policyholders, for example in the case of automated driving, is a prerequisite for effective competition for the best solutions.

Plea for a new risk culture

A fundamental plea on the issue of internet security: society needs nothing less than a new risk culture for cyberspace: firstly, and most fundamentally, the willingness of industry to take these risks seriously and act accordingly; secondly, a common understanding of a level of IT security that reliably protects a company but does not overstretch it financially; and thirdly, of course, insurance policies that cover the remaining risk and provide companies not only with money, but also with expertise, in a crisis. It is to be hoped that the publication by the GDV of the non-binding model terms and conditions for these new products will help this young market see rapid growth. Every company must take the first step itself, however – identifying the risk and taking it seriously – if it does not want to become a victim of the current criminal gold rush on the world wide web.

Consequently, providing cover for risks will remain a core business model for the insurers, although digitalisation will help make insurance policies more personal and more customised. New data and analysis techniques will allow a more precise risk assessment and extended insurance coverage.

5 The process revolution

High level of automation in the insurance industry

Standardised and automated processes are a core pillar of the digitalisation of the insurance business. If insurance customers expect personalised, smart responses from their insurer within seconds, insurance undertakings can only achieve this by systematically and continuously automating and accelerating their processes. This applies to all the undertakings' lines of business, departments and business processes.

Programs generate records automatically, convert scanned letters into machine-readable text, verify invoices or trigger payments autonomously.¹⁵ Whereas only just on one customer issue in eight was processed fully automatically from start to finish in non-life insurance in 2013, today it is already one in four. The proportion of fully automated processing also rose in life insurance, from four to eleven per cent (see Figure 2). The industry invested a total of 4.45 billion euros in information technology in 2017.

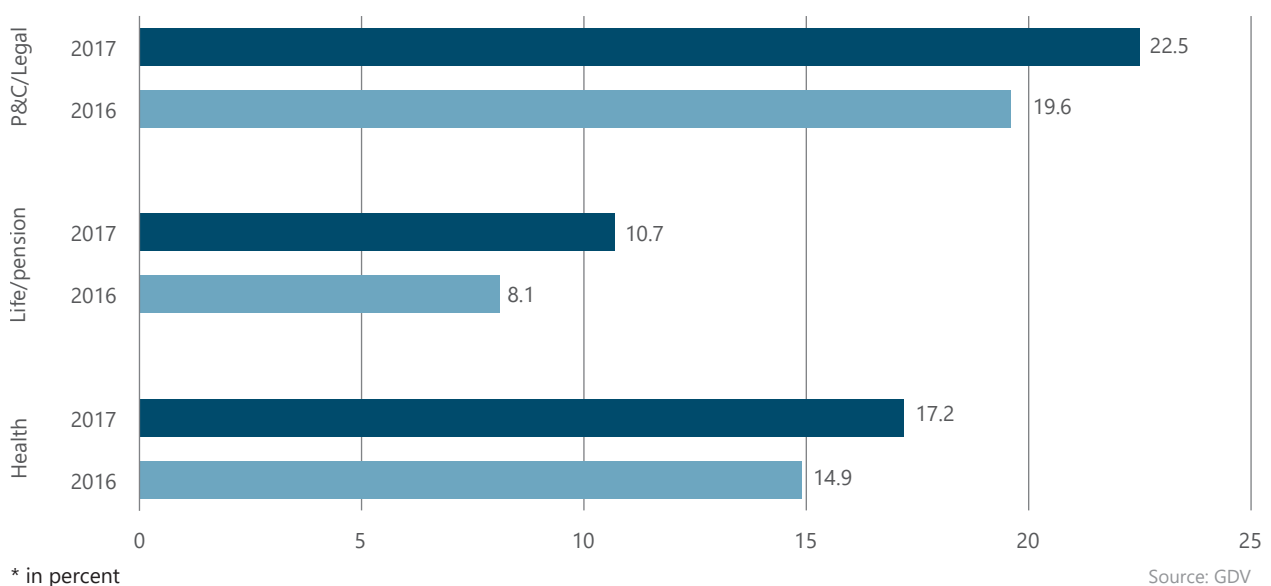
Even Capgemini's World Insurance Report 2018 attests that German insurers are setting an example in using digital technologies for automation.¹⁶ This is particularly evident in the area of robotic process automation (RPA) across all three insurance classes (property and casualty, life and health insurance). The vast majority of German insurers (89 per cent) have at least piloted RPA systems (36 per cent) or have already fully deployed them (53 per cent). Capgemini also believes that German insurers are among the pioneers compared with their international peers when it comes to implementing other automation technologies (including Artificial Intelligence, machine learning/deep learning and blockchain).¹⁷

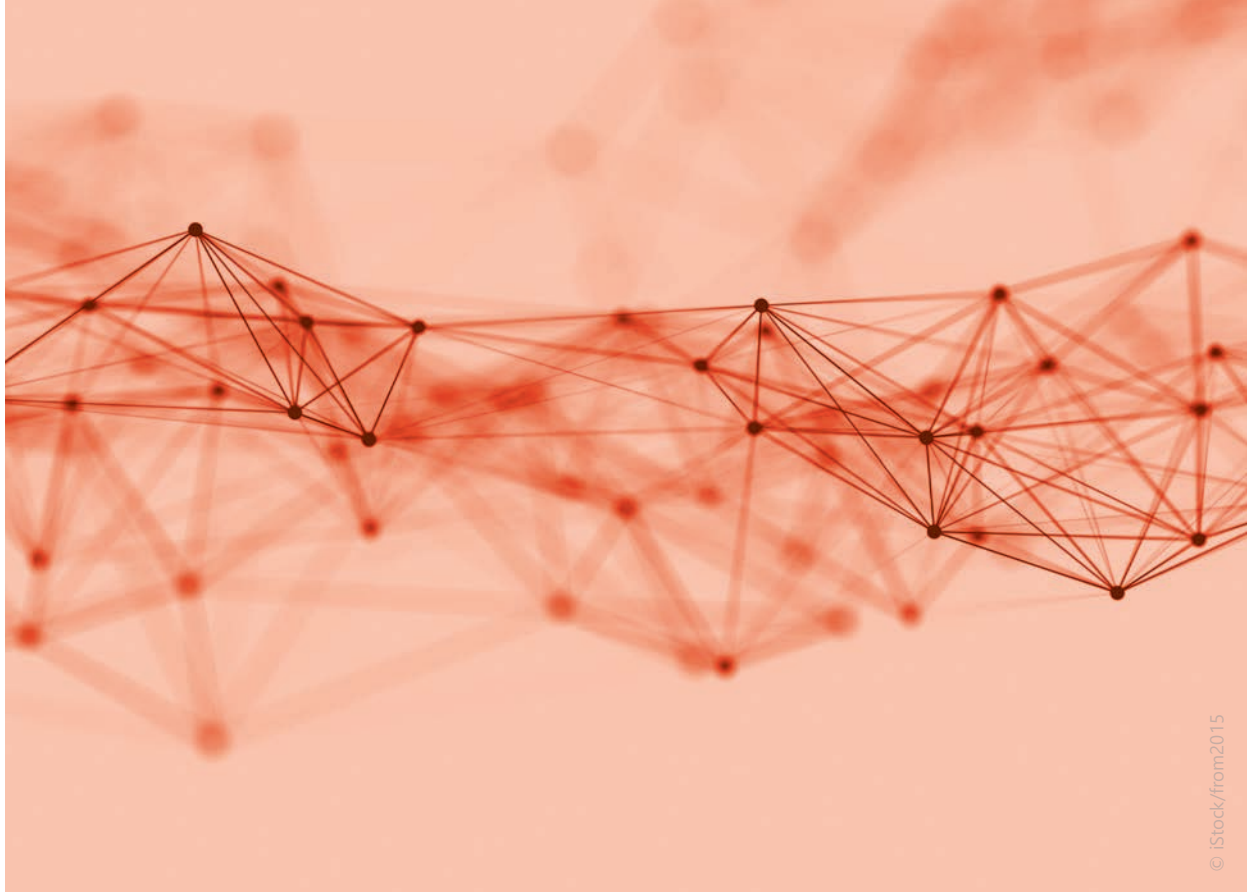
15 See GDV, Digitale Schadenbearbeitung – Feinjustiert (Digital claims processing – Fine-tuned), <https://www.gdv.de/de/themen/positionen-magazin/feinjustiert-38876>, retrieved on 5 December 2018.

16 See Capgemini, World Insurance Report 2018, <https://worldinsurancereport.com/>, retrieved on 6 December 2018.

17 See IT Finanzmagazin, Deutsche Versicherer bei Automatisierungstechnologien über dem weltweiten Durchschnitt (German insurers ahead of the global average when it comes to automation technologies), <https://www.it-finanzmagazin.de/deutsche-versicherer-bei-automatisierungstechnologien-ueber-dem-weltweiten-durchschnitt-71261/>, retrieved on 5 December 2018.

Figure 2: Fully automated processing by class of insurance*





© iStock/From2015

AI as a driver of the process revolution

AI solutions offer tremendous potential for improving business processes and are therefore essential tools in the business process revolution. However, AI systems are only ever as good as the data and information they are fed with and trained on. Powerful AI solutions should therefore be capable of being supplied with all the information that an insurer has collected to date. And of course with all the other facts, for example about the products the undertaking offers. This input management ultimately decides how good the results will be that AI can deliver when used in an insurance context. In the end, both consumers and undertakings stand to gain from the fair and responsible use of these processes, such as those used in chatbots.¹⁸ The new GDV pension calculator is another example: like a game, and with mathematical accuracy, the tool calculates possible benefit gaps inside one minute.¹⁹

The example of character recognition and analysis using AI shows that this is certainly a time-consuming process: it requires paper and digital documents such as emails, signed paper contracts, web forms, faxes or PDFs, for example for claims settlement, to be fed into

the AI system. Before AI can generate information and knowledge from such a data mix, all the facts must be processed into a machine-accessible format using Natural Language Processing (NLP). In the next step, the system has to learn the meanings and contexts of the technical terms in order to be able to associate and interpret them correctly in the future.

The system can only understand the context, interpret texts correctly and derive options for action from them through this conceptual enrichment of the facts and the definition of the rules for the processing algorithms. The AI system can then read the information from the unstructured and distributed texts. This training phase is decisive for the quality of the information when the system is subsequently used. The learning phase must be didactically designed and rationally structured by humans, because the system will only autonomously become more intelligent and, by applying its knowledge, itself derive and apply patterns and rules if this learning phase is well organised.

State-of-the-art payment service providers as partners in the process revolution

In the same way as for e-commerce, the processes involved in payments and payouts are critical success factors for digitalisation in the insurance industry. Customers expect the highest possible ease of payment for their premiums and for payouts of benefits, ideally paired with comprehensive flexibility and maximum security. However, the industry is still cautious about

¹⁸ See GDV, loc. cit. (footnote 7), retrieved on 6 December 2018.

¹⁹ See GDV, Neuer Rentenrechner – In 60 Sekunden zur individuellen Altersvorsorge (New pension calculator – A customised pension in 60 seconds), <https://www.gdv.de/de/medien/aktuell/in-60-sekunden-zur-individuellen-altersvorsorge-32892>, retrieved on 5 December 2018.



offering alternative payment methods. This is due not least to the fact that payment service providers active on the market – be they traditional credit institutions or newly arrived payment service providers – have primarily geared their offerings so far to the needs of e-commerce. But the insurance industry and its product range are not readily comparable with other industries. For example, paying for an e-commerce item ordered online is different from paying for recurring premiums under an insurance contract. In addition, insurers expect more than just payments processing from a state-of-the-art payment service provider. They also seek to combine of the payment process with additional process-related added value in order to support the digitalisation processes in the undertakings and to lift the level of automation (for example: secure customer identification/authentication, e-invoicing services with a linked payment function, issuing a legally watertight electronic direct debit mandate). This can help payment service providers to become strong partners in process automation and digitalisation at insurers.

The Second Payment Services Directive (PSD2) and its open banking approach laid the foundations for this development. Banks, savings banks and new payment service providers now have the same opportunity to become payment service providers in the true sense of the word. The resulting open API (application programming interface) ecosystems are enabling the creation of innovative value added offerings for

everything to do with accounts and payments and the transformation into a digital banking platform. This trend towards digital payment ecosystems is being monitored closely and welcomed by the German insurance industry. It also offers insurers an opportunity to make their own payment and settlement processes more efficient, more digital and more customer-friendly.

Security and standards critical for interoperability and business success

Customer trust is the critical success factor: customers' data is an essential resource in the core business. Its security and integrity are the top priority. Regardless of whether data and algorithms are processed internally or externally, for example through cloud computing, appropriate security measures must be adopted to safeguard IT security.

To safeguard the undertaking's future ability to act, interoperability and security must be factored in right from the start and integrated into IT systems and business processes according to the motto "security by design". This is because especially fully automated end-to-end processing still offers substantial potential for cost-efficiency in all classes of insurance. The optimisation measures already initiated must continue to be driven forward with a high level of commitment and, ideally, flanked by technology-neutral, modern legislation.

6 New competitors, greater diversity of providers

Market positions are shifting

In recent years, a large number of new competitors such as the insurtech start-ups have entered the German insurance market. The large majority of these new players are limited to parts of the value chain, such as distribution or IT services.²⁰ However, some insurtechs have now also received an insurance licence. There is speculation that large technology groups or other groups outside the industry could enter the market to a more significant extent. These potential new competitors are fuelling competition and innovation and increasing the pressure on traditional insurers to adapt.

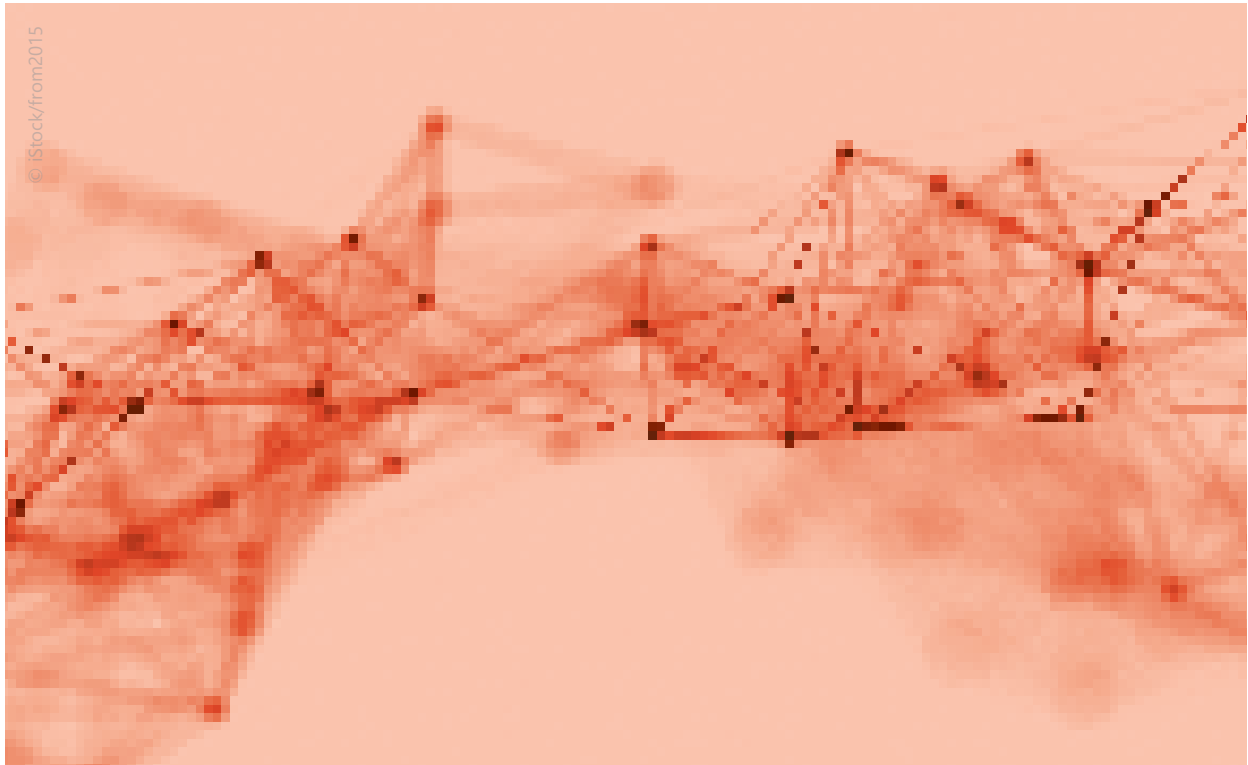
The various types of provider – established insurers, insurtech start-ups and newcomers from other sectors such as tech companies – each have their own individual strengths. Insurtechs can fully tailor their offerings to the digital world without a legacy burden. The bigtechs are characterised by their expertise in handling new technologies and their extensive data pools. Traditional insurers, on the other hand, benefit from their mature customer relationships and their comprehensive insurance and regulatory expertise. However, they face the challenge of adapting their strategy and business activities to the new reality.

Market entries and exits will increase, and so will M&A transactions

A number of entirely different strategic options are now emerging for competitors to compete successfully in the market. It is evident that insurers are taking very different strategic routes, and this is further fragmenting the traditionally very diverse provider landscape in the German insurance market. It is being reinforced

²⁰ See e.g. Institute of Insurance Economics, University of St. Gallen, The Current InsurTech Landscape: Business Models and Disruptive Potential, Institute of Insurance Economics, University of St. Gallen, https://www.iww.unisg.ch/~media/internet/content/dateien/instituteundcenters/iww/studien/ab-insurtech_2017.pdf, retrieved on 5 December 2018.





by the increasing importance of alliances – both between insurers and companies in other sectors and between multiple insurers. In this competitive process, considerable shifts in market positions are expected in the next few years. Not all insurers will be able to maintain their position in the market. Market entries and exits will increase, and so will M&A transactions.

Extreme changes in the provider landscape not realistic in the mid-term

In light of this, a GDV project group has examined how these far-reaching changes could transform the provider landscape in the German insurance market in the mid-term – i.e. up to around 2025.²¹

Based on the available information, five extreme scenarios can be identified as theoretically possible long-term trends for the provider landscape:

- Innovative insurers (insurtechs or the insurance subsidiaries of tech companies) oust the existing providers.

- Traditional insurers adapt successfully and maintain their dominant market position.
- Insurers become pure risk carriers and the customer interface is serviced by other companies – such as internet platforms.
- The new opportunities offered by digital networking will fragment the value chain.
- Insurers will be disintermediated as risk carriers, for example by peer-to-peer portals.

Although there is a lot of uncertainty about future trends and the potential different development paths, the conclusion of the GDV's study is that none of the extreme scenarios is likely to occur. Instead, it can be expected that elements of all scenarios will be found in the future provider structure in the insurance market. In the mid-term, however, the various extreme scenarios are likely to have very different impacts (see Figure 3, page 105).

There is a lot of evidence suggesting that established insurers will preserve a strong market position in the next few years because they will adapt successfully to the new world. At the same time, however, it can also be expected that a number of innovative insurers will gain a foothold in the market. In light of the increasing importance of alliances and internet portals at the interface to the customer, insurers could assume the role of pure risk carriers more frequently in the future than at present. By contrast, there are likely to be tight constraints on disintermediation – the substitution of insurers in their

²¹ See GDV, Volkswirtschaftliche Themen und Analysen Nr. 8, Anbieterlandschaft am Versicherungsmarkt: Ein Ausblick (Economic Issues and Analysis No. 8, Provider landscape in the insurance market: A look ahead), <https://www.gdv.de/resource/blob/33376/29aaed518cba2d28d01aba3906c18f81/anbieterlandschaft-download-data.pdf>, retrieved on 6 December 2018.

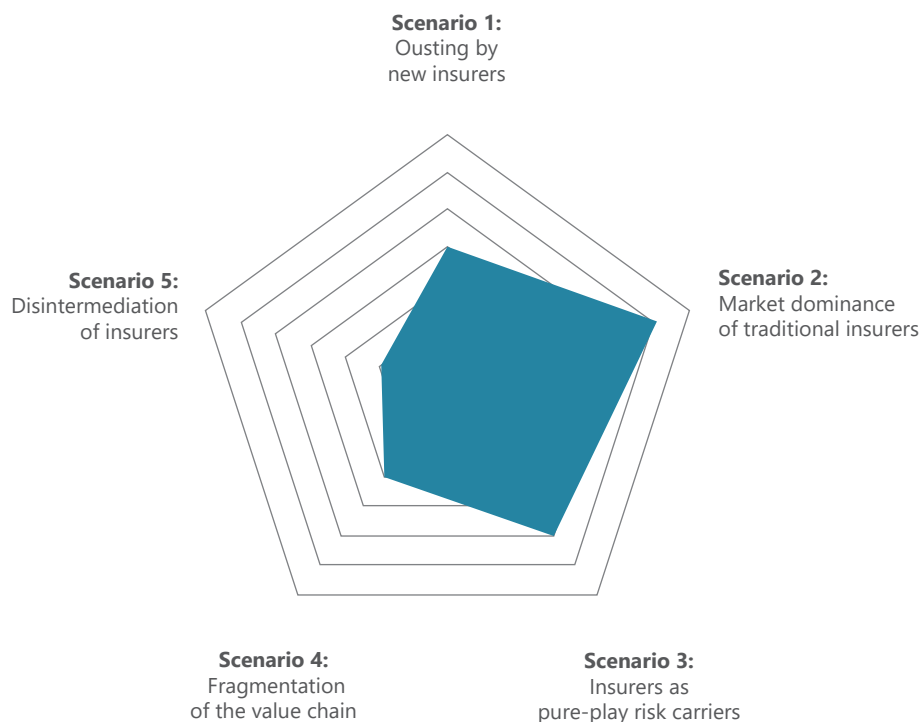
role as risk carriers by other risk assumption models – for the foreseeable future. And in light of the economies of scale that exist in many areas, any heavy fragmentation of the value chain does not seem realistic either.

As things stand today, there are very strong indications that the German insurance market will continue to be distinguished by a broad range of offerings and providers in the medium term. This is clear from both market entries and realignments within the group of established suppliers. However, the competitive process and continuous adaptation by the providers cannot by themselves guarantee high productivity in all segments of the insurance market under the conditions prevailing in the future. Government and supervisors will also be called on to act. An effective competition policy and an appropriate regulatory framework must safeguard fair competition between traditional and new business models and all groups of providers, including across industry boundaries. Monopolies must be prevented.

The core principles underlying the regulatory framework are ensuring a level playing field for all providers and the systematic application of the principle of proportionality in supervisory activities.²² Regulation must be efficient and effective and may not unnecessarily prejudice the ability to leverage opportunities available in the new world, for example through requirements that are no longer appropriate. Only then can competition in the insurance market act as a constant discovery process for the best solutions in the interests of customers and society, even in times of sweeping change.

²² See GDV, Solvency II – Wer soll das stemmen ?, <https://www.gdv.de/de/themen/positionen-magazin/wer-soll-das-stemmen--39638>, (Solvency II – Who is supposed to manage it?), retrieved on 5 December 2018.

Figure 3: Range of realistic mid-term trends – Ranking of expected relevance of extreme scenarios



7 Competition for talent

IT-savvy employees as a key to the digital company

Customers quite rightly expect insurers to leverage the opportunities offered by digitalisation and to continuously enhance their products and services: more user-friendly, simpler, more innovative, faster, cheaper. If the insurers do not do this, new competitors will – and they are more agile than ever before, including in the labour market.

It is not exactly news that employee skills are an important factor, especially in times of huge technological advances. Questions are therefore being increasingly asked about the negative impact of digitalisation on the number of jobs in the insurance industry. Traditional clerical work or customer service centres will probably be affected first. The effects of process optimisation or the use of robotics, Artificial Intelligence and blockchain are already being seen here. But digitalisation also triggers opposite effects, and there is already a need for new employees with new skills. For insurance undertakings to be able to recruit these digital natives, they must transform themselves into digital companies. It is likely to be less the will to embark on digitalisation as the availability

of IT-savvy employees that will be a bottleneck in the insurance undertaking's process of renewal.

The industry faces a major challenge in this respect. A current GDV study demonstrates that although the number of IT jobs is still on the rise, there is still a long way to go before the increased need for skilled internal IT staff can be met. In turn, this increases the pressure to systematically shut down old IT systems and replace them with new ones, which increases the value of the qualified digital natives needed to do this.

Digital companies need well-qualified people who can think outside the box and find the insurance industry inspiring. The digitalisation of insurers requires a balancing act in this respect: helping staff with experience into the new working environment and, at the same time, being attractive for new staff with new qualifications. Anyone who chooses this route into the future has to think in terms of multimedia; they must be at home in both social networks and the traditional insurance business; and above all they must want cultural change. And the speed of this cultural change



© iStock/From2015



is accelerating: more trial and error, co-working spaces, even an in-house basketball court – the new working environment also reflects an industry in the midst of a digital revolution.²³

Permitting and encouraging modern working environments

Working time models must reflect digitalisation and become even more flexible than they already are, because the more flexible the people in the industry are as far as location and time are concerned, the more they increase their job opportunities in the digitalised working environment. However, the German Working Time Act (*Arbeitszeitgesetz*) imposes tight limits on any future, more flexible working environment. National and European lawmakers must therefore ensure that both the German Working Time Act and the European

Working Time Directive are fundamentally revised and adapted to meet the requirements of the current production conditions.

Collective agreements for the private insurance industry are very widespread. This is mainly because they give the partners to the agreements (companies and works councils) significant scope for agreeing individual options, including working time arrangements. However, not all aspects of flexible working time arrangements have been exhausted. In addition, the scope of the collective agreements is extremely broad and also includes salaried employees who are paid well above the collective pay scales but are not senior executives as defined by the law. It is now time for the industry's collective bargaining partners to ensure more flexibility in this area. The aim must be to make work covered by collective agreements sufficiently flexible that in particular the new competitors in the market, such as insurtechs, view national and regional collective agreements as a sensible instrument for agreeing working conditions in the industry and seek to join them.

²³ See GDV, Karriere – Ziemlich geile Aufgaben (Career – Pretty cool jobs, <https://www.gdv.de/de/themen/positionen-magazin/ziemlich-geile-aufgaben-39582>, retrieved on 5 December 2018.

8 Agile supervisors

Regulatory objectives and supervisory practice are mainly technology-neutral, although they have been shaped by the analogue world for decades. Agile companies in highly regulated branches of industry need equally agile supervisors so they can keep up on the journey into the digital future – with customer expectations, with other industries and with their international competitors. Being agile means responding quickly to change.²⁴ Being agile means being flexible, having a distinct ability to adapt and being inherently nimble. Only a supervisor that is digitally on a level with the undertakings it supervises can enable them to transform their business processes and products as quickly as necessary without any negative effects on consumer protection standards or financial stability.

Openness to new technologies and systematic application of the principle of proportionality

So what do insurers expect from an agile, digital supervisory authority? Of course, being open to new technologies, not blindly and unconditionally, but always with an eye on the opportunities and not just focused on potential threats. We hope for the systematic avoidance of duplicate regulation and redundant reporting obligations, as well as the systematic application of the principle of proportionality.²⁵ Essentially, this means creating the freedom to individually adapt digital business and IT based on risk and business-related criteria.

It is therefore encouraging to see that the Federal Financial Supervisory Authority (BaFin) – both in its current form and those of its predecessors – did not act as systematically and quickly, even agilely, in any of the processes of change in the past 50 years as it is doing today with regard to the technological transformation. With its study “Big data meets artificial intelligence – Challenges and implications for the supervision and

regulation of financial services”²⁶, BaFin has produced a thorough analysis of the challenges and implications for the supervision and regulation of financial services. BaFin has thus assumed a pioneering role not only nationally, but also at European and international levels.

BaFin’s digitalisation strategy – A step in the right direction

Just like the undertakings, BaFin is working agilely on its own digitalisation strategy. This is to be welcomed, as it facilitates communication between undertakings and the supervisor. In essence, from the perspective of the undertakings BaFin will have to ask itself four questions about its strategy:

- How does it approach market changes caused by technological advances in products and processes?
- What is BaFin’s position on the issue of “IT supervision and security”, in particular in light of the functions of the BSI?
- How is BaFin planning its journey into the digital world, its transformation into a digital supervisory authority?
- How can digitalisation make reporting by insurance undertakings to supervisors more efficient?

The establishment of the Financial Technology Innovation division and the IT Supervision/Payments/Cybersecurity directorate are certainly the right steps and signals at BaFin, as is the planned appointment of a Chief Digital Officer. Close dialogue between BaFin and the supervised undertakings is pivotal.

24 See Agile Unternehmen, Was ist agil und evolutionär im Kontext von Unternehmen? (What is agile and evolutionary in the corporate context?), <https://agile-unternehmen.de/was-ist-agil-definition/>, retrieved on 6 December 2018.

25 See GDV, Solvency II – Wer soll das stemmen? (Solvency II – Who is supposed to manage it?), loc. cit. (footnote 22).

26 BaFin, Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services, www.bafin.de/dok/11250046, retrieved on 6 December 2018.

9 Summary

The seven game changers mentioned here are only some of the challenges linked to the digital revolution, because the digital agenda is global, it is all-encompassing and it affects all sectors of the economy. For the highly regulated insurance industry, this means, of course, that it also has to ensure that the right basic conditions are in place: for data protection and copyright, for digital infrastructure and technical standards. And, of course, it also needs fair, agile regulation – to name just a few of the crucial aspects.

But it is not just about the hard issues. If the industry wishes to be at the forefront of digitalisation, above all it needs a transformation that unleashes creative potential.

But this is primarily a question of corporate culture. A technocratic management approach that is first and foremost concerned with risk minimisation and process control will be unable to steer this change. On the

contrary: digital transformation requires a search and learning process in which trial and error, planning and execution run more or less in parallel. There is therefore a need for a corporate culture that encourages personal initiative, self-organisation, creativity, teamwork and interdisciplinary work. The industry needs this not just because it will allow it to develop better solutions for the digital world, but above all as an employer who can win over the most innovative minds. To do this, the industry must make attractive offers and open up career opportunities that fit the new understanding of work, personal responsibility, dynamism and teams that embody diversity. The insurance industry needs a corporate culture that fosters free and new ways of thinking. That is certainly a culture that no money can buy. Rather, it has to be developed in a sometimes arduous process of change. And that is perhaps the biggest task facing the insurance industry today.



Imprint

Publisher

Federal Financial Supervisory Authority
(Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin)
Directorate K: Communications
Graurheindorfer Straße 108 | 53117 Bonn
Marie-Curie-Straße 24 – 28 | 60439 Frankfurt am Main
www.bafin.de

Editing and layout

BaFin, Public Relations and Speeches
Editor: Ursula Mayer-Wanders (Head of Division)
Tel.: +49 (0)228 4108-2978
Jens Valentin
Tel.: +49 (0)228 4108-2363

E-mail: perspektiven@bafin.de

Design

werksfarbe.com | konzept + design
Humboldtstraße 18, 60318 Frankfurt
www.werksfarbe.com

Bonn and Frankfurt am Main | February 2019
ISSN 2625-5952

Access

BaFinPerspectives is published on BaFin's website in German and English. The German edition is published under the title "BaFinPerspektiven". If you sign up to the BaFin-Newsletter, you will be informed by e-mail when a new edition is published. The BaFin-Newsletter can be found at:
www.bafin.de » [Newsletter](#).

Disclaimer

Please note that great care has been taken in compiling all of the information contained herein. However, BaFin accepts no liability for the completeness and accuracy of this information.

The articles and interviews in BaFinPerspectives are subject to copyright. Reprinting and distribution is only permitted with BaFin's written consent, which may also be issued by e-mail.

Typesetting

Naumilkat – Agentur für Kommunikation und Design
Jahnstraße 84
40215 Düsseldorf

Printed by

W. Kohlhammer Druckerei GmbH & Co. KG
Augsburger Straße 722
70329 Stuttgart

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Federal Financial Supervisory Authority
Communications (Directorate K)
Graurheindorfer Straße 108, 53117 Bonn
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main
www.bafin.de