German Banking Industry Committee

Die Deutsche
Kreditwirtschaft

Comments

On the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts

Register of Interest Representatives
Identification number in the register: **52646912360-95**

Our ref
Ref. DK: KI
Ref. DSGV:8528/01

Contact: Dr. Wiebke Lüke
Telephone: +49 30 20225- 5313
Telefax: +49 30 20225- 5345
E-Mail: wiebke.lueke@dsgv.de

Berlin, August 6, 2021

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent more than 1,700 banks.

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

1 Management Summary

The German Banking Industry Committee welcomes the efforts of the European legislator to create an innovation-friendly and legally robust framework for the use of artificial intelligence (hereinafter: AI) in a fair competitive environment to the benefit of consumers and businesses. AI is regarded as a key technology of the 21st century, which in the coming years and decades will influence business activities, but also the lives of consumers in many ways.

The draft regulation puts the protection of the fundamental rights of the citizens of the European Union centre stage. Citizens are to be protected in particular in key areas of their lives against the risks from the use of AI. Annex III of the draft regulation lists high-risk systems. We support the underlying approach in principle, as the areas of use stated in it (e.g. biometric identification, administering and operating critical infrastructures, access to education and training institutions etc.) impact fundamental areas of life and at the same time affect individual protection, the provision of essential goods and services and civic participation. This understanding reflects European values and is to be endorsed as such.

Nevertheless, the approach chosen in the regulation is misguided in our view, as selected use cases are sweepingly defined as high risk without there being a comprehensible criteria grid that explicitly names and objectively substantiates (quantifies) the risks and takes into account existing risk-mitigating (legal) requirements. We believe that when the risk mitigating facts are considered appropriately, it becomes apparent that there is no high risk for consumers in the context of creditworthiness assessment or credit scoring. It is also incomprehensible that a technology (AI) that embeds itself in existing processes and structures in credit institutions per se leads to a higher risk. This assumes that the existing risk mitigating requirements and institutions involved in the supervision and monitoring of credit institutions are inadequate and do not have sufficient impact, which is not the case.

If one merely assumes that the pertinent use case in question suffices for such categorisation due to its importance, then the approach would be a coherent one. We assume, however, that the nomination of risky use cases does not do justice to a dynamic, evolving risk landscape. There has instead to be an assessment of which risks exist or can arise and to what extent they actually occur, but above all can be mitigated or already have been.

Against this background, we feel that the draft regulation wrongly categorises credit assessments and credit scores as high-risk AI use cases. The financial sector, like hardly any other sector, is subject to numerous regulations as well as to appraisal and approval processes monitored by the supervisory bodies, which demand of it transparency, control and risk mitigation. Both the risk management systems installed for that purpose and the IT infrastructures have been subject to continuous monitoring and control for many years. These structures also ensure that even risks that are still unknown today, which may arise as a result of new technologies, can be identified as quickly as possible and addressed accordingly. The goals which are to be ensured in the demands on high-risk systems set forth in the regulation are already being achieved by credit institutions through their own risk management systems, in particular not only but especially also with respect to credit assessments and credit scores. This shows, in our opinion, that it is wrong to assume that this area is per se a high-risk one.

We therefore call upon the European legislator to remove credit institutions from the scope of Art. 2 of the regulation.

In addition, we are sceptical about the proposed definition of AI. We support the technology-neutral definition, but it should take particular account of the risk-relevant characteristics, so as to enable proportionate regulation. Hence the AI definition is in our opinion too broad and sweeping because it encompasses every rule-based procedure and thus goes well beyond the problematized aspects of AI.

We therefore call upon the European legislator to review the definition of AI. A concrete wording proposal can be found under item 5 "Regulation-specific comments on the proposed regulation".

2 Importance of AI applications for the financial sector

The financial sector in particular depends on AI. The sector's future is no longer imaginable without the use of AI but above all no longer conceivable. Banks are facing a steady increase in enormous data volumes, which they have to handle.

Over-zealous regulation would not only impede innovation, but, as a consequence, also fail to grasp that economic advantages, which inter alia affect financial market stability, could no longer be taken up. The objective of the regulation focuses in our opinion unilaterally on the protection of individuals without paying sufficient heed to the importance of financial market stability. The financial market regulation today already pays attention to aspects of consumer protection and financial market stability and is thus in our opinion already risk minimising and offers a proper balancing of interests. In addition, we fear that the current draft regulation can lead to contradictions and overlaps with existing regulations.

1. The focal points of AI use in the banking sector are inter alia real-time transaction analysis, algorithmic trading and AI-managed funds. There are as well more mundane processes such as personalising customer services, voice recognition, natural speech processing. Such systems are used, for example, to filter out the allocation of financial institutions' resources. Another example is the use of chatbots to automate routine customer interactions like opening bank accounts and general customer enquiries. AI is used in call centres to process and triage customer calls and to offer individualised service.

2. The use of AI thus offers benefits, above and beyond increasing efficiency, for customers, too. AI solutions give banks a more comprehensive picture of their customers and their sector-specific needs. This enables corporate customer advisors to be provided with company- and industry-specific know-how, enabling them to advise their customers more specifically on current developments or to submit needs-based offers.

   Thanks to AI, inflows and outflows of money can be analysed and so form the basis for forecasting further liquidity developments. If after combining a wide range of data points the AI algorithm predicts a financial bottleneck for a company, the bank can submit a suitable offer for a loan directly and in good time. These upstream processes will in future no longer be based solely on rule-based algorithms but also on machine learning. The reason for this lies in the greater precision offered by such models. Higher precision leads to a more sensitive, i.e. more accurate, assessment result. This in turn minimises the default probability, for example, of a loan. But if a machine-learning algorithm, which is used in preliminary creditworthiness assessments, is now classed as a high risk, this fails to see that the higher precision especially brings benefits for all parties to the process. Therefore, this is a good example of a risk-oriented regulatory approach that in our opinion is more reasonable than a sweeping categorisation of such procedures as high risk with the corresponding requirements. Apart from this, the final stage of every credit assessment is always human oversight. This is already the case today and is not doubted by institutions, either.

   Moreover, intelligent fraud detection no longer functions without AI. We are well aware that using AI for combatting financial crime is not subject to any requirements under the draft regulation. But we would like to point out that these areas are inter-connected and differing regulatory treatment could accordingly be contradictory. Neural networks use deep learning to process vast quantities of data and identify previously unknown patterns in the transaction data, which helps to detect and prevent fraud to a degree not previously possible. This has benefits for both banks and also for society, in particular as effectiveness is boosted, the risk of prosecution increased and the financial institution's reputation enhanced.[1]

   The convergence of skills within compliance, such as preventing money laundering and fraud through AI, enables significant cost savings. It is estimated that the overlap between data processing, system maintenance and administration of the legacy systems needed for independent support of these functions is about 80%. Criminals also frequently exploit the rigid infrastructure within the global financial system. Therefore, supervisory authorities encourage financial institutions to adopt new paths and methods.[2]

[1] https://www.capgemini.com/de-de/2020/04/invent-finanzkriminalitaet/.

[2] https://www.capgemini.com/de-de/2020/10/invent-ki-finanzkriminalitaetsbekaempfung-das-problem-der-holistischen-kundenueberwachung/.

New technologies always also entail new risks, which companies must address. In the development and use of AI systems, the following new risks inter alia are particularly noticeable:

- High complexity: The algorithms used in AI systems are far more complex than classic statistical processes, which makes plausibility and verifiability all the more difficult.
- Short recalibration cycles: The fact that AI systems independently process new and greater quantities of data and so constantly develop themselves makes the validation of any calibration increasingly more difficult.
- Bias: Due to biases and unbiased tendencies in big data, the risk of biased results and unfair treatment of natural persons increases.

However, the risks described are already known to financial institutions, and are addressed, mitigated and managed by the risk management processes.

3 Statutory and supervisory demands on the financial sector

3.1 European requirements

Scarcely a sector is subject to such strict regulatory requirements as the banking sector, whose compliance is closely monitored by sector-specific supervisory authorities at the national and European level.

3.1.1 Framework conditions score functions and classification methods

The score functions and classification methods developed on the basis of statistical processes are regularly reviewed by supervisory authorities. This applies for both processes based on internal rating systems ("IRB system") of IRB institutions, whose models were accepted for risk-oriented equity cover, and also for those institutions using a credit risk standard approach, whose classification methods for evaluating creditworthiness in Germany, for example, have to be reviewed and adjusted under Minimum Risk Management Requirements (MaRisk) at least annually and, where there indications of impairment also during the course of the year, within the scope of a comprehensive validation. In this context, IRB institutions are governed by the provisions of the Capital Requirements Regulation ("CRR") and related delegated regulations and guidelines. For institutions using credit risk standard approach processes, these IRB requirements are also applied by supervisory authorities during their reviews mutatis mutandis as a benchmark.

3.1.2 Analytical Credit Datasets

In addition to improving the capital adequacy of the financial sector, numerous banking regulation requirements are aimed at harmonizing sector-specific legislation and the supervisory regime in the European Union. For example, the European Central Bank introduced the AnaCredit Regulation (Analytical Credit Datasets) in 2016 in order to gather information at the level of individual borrowers and loans. The reports are to be filed with the national supervisory authorities. The AnaCredit Regulation also stipulates, which data must be collected and reported within the framework of a lending process. The regulation applies in all member states of the European Union.

3.1.3 Basel III

The most important pillar of banking regulation is Basel III. In its core, the reform strived to strike a balance between a more stable financial system and avoiding a credit squeeze, flanked by limiting and reducing the liability of the public sector and taxpayers. With the implementation of the banking package that implemented the Basel III requirements at the European level, the stability of the financial sector in Europe has improved since the beginning of the process to reform banking regulation. The new provision led to changes concerning inter alia:

- Capital Requirements Directive (CRD),
- Capital Requirements Regulation (CRR),
- Bank Recovery and Resolution Directive (BRRD) and
- Single Resolution Mechanism Regulation (SRMR).

3.1.4 Capital Requirements Regulation (CRR)[3]

Regulation 575/2013 (CRR) already makes comprehensive demands on rating systems, inter alia on the integrity of the process, models, documentation and data maintenance. Here too overlaps should be avoided. Credit institutions falling within the scope of the CRR should therefore be excluded from the requirements for high-risk AI systems so as to avoid overlaps and duplicated verifications.

3.1.5 Digital Operational Resilience Act (DORA)

On 24 September 2020, the EU Commission proposed the "Regulation on digital operational resilience for the financial sector [DORA]", COM 2020/0266. Dora is to ensure that all participants in the financial system have the necessary security measures in place to limit cyber-attacks and other risks. The financial supervisory authorities are to be given access to information on "ICT-related incidents" and ensure that

[3] Regulation (EU) 575/2013.

financial entities assess the effectiveness of their preventive and resilience measures and identify ICT-related vulnerabilities.

3.1.6 Directive on credit agreements for consumers (2008/48/EC) and Directive on credit agreements for consumers relating to residential immovable property (2014/17/EU)

The "Directive 2008/48/EC on credit agreements for consumers and Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property" already creates a harmonised EU framework for loans to consumers that ensures European consumers' fair and transparent access to loans and envisages an obligation to check the consumer's creditworthiness. Under this legislation, a loan may only be granted to consumers, if it is probable or to be expected that the obligations in conjunction with the loan can be met in the manner agreed in that contract. This is to ensure the consumer's protection against over-indebtedness and can give rise to liability claims for the consumer. In addition to the regulatory requirements for credit risk assessment, this also helps to ensure that the lending processes in the banks comply with the highest standards, also in the interests of the individual consumer. On 30 June 2021, the European Commission presented a revision of the Consumer Credit Directive, which inter alia takes into account the changes arising from digitalisation.

3.2 National requirements

It is undisputed that AI will continue to develop in the future, and that this will be accompanied by changes and/or new risks. So, it is all the more important that the regulation also focuses on the future. Looking at the regulatory requirements for banking IT that already exist today, we believe that the concerns to be addressed by the draft regulation are already sufficiently addressed today.

3.2.1 Second Act to Increase the Security of Information Technology Systems (IT Security Act)

The financial sector, across sectoral boundaries, as a critical infrastructure is subject to the scope of the "Second Act to Increase the Security of Information Technology Systems" (IT Security Act), which came into force at the end of May of this year Accordingly, the use of certain IT components by operators of critical infrastructures can now be prohibited, if it can be assumed that the use of these components is likely to impair Germany's public order or security. The detailed preconditions are determined by the "Regulation to Determine Critical Infrastructures". Every use of critical components in critical infrastructures is to be reported to and reviewed by the Federal Ministry of the Interior.

3.2.2 Regulations outside Banking Act

Outside the Banking Act inter alia

- the Solvency Regulation,
- the Large Exposures Regulation,
- the Liquidity Regulation and
- the Institutions' Remuneration Systems Regulation have been amended.

3.2.3 National implementation of the European Basel III rules

The European Basel III rules were implemented in Germany in 2013 above all

- through changes to the Banking Act (KWG) and
- the CRD IV Implementation Act.

3.2.4 Harmonisation of existing regulations with the requirements under Art. 9ff of the regulation

Credit assessments are already being comprehensively reviewed by the national supervisory authority. If further conformity assessments had to be carried out, as the regulation requires, there would be overlaps, as the same matters would be reviewed twice. This applies in particular for reviews conducted under the Supervisory Review and Evaluation Process (SREP).

To elucidate our argument that institutions already meet the goals of the requirements in the regulation or the risks expressed therein are sufficiently mapped in their risk management systems, there follows a presentation of the provisions valid in Germany. These have been implemented nationally on the basis of the European requirements. We therefore assume that the other member states have established corresponding / equivalent requirements for the financial sector.

The foundation for risk management systems is formed by the "Minimum Requirements for Risk Management" (MaRisk) issued by the Federal Financial Supervisory Authority (BaFin).

On the basis of their overall risk profile, credit institutions ensure that key risks facing the institution are documented in a risk inventory. The risks are determined at the level of the institution as a whole, regardless of which organisational unit or systems caused the risks.

These are covered on an ongoing basis by the risk coverage potential, which ensures risk-bearing capacity. Institutions have a process for ensuring risk-bearing capacity through which both the institution's ability to continue as a going concern and the protection of creditors against losses are adequately considered from an economic perspective. To safeguard the risk-bearing capacity, financial institutions have installed suitable risk management and risk monitoring processes.

Within the framework of that process, all the financial institution's possible risks are identified and addressed. The executive board is informed regularly and ad-hoc, as and when necessary, about the changing risk landscape and acute risks.

Thanks to a comprehensive internal control system, financial institutions are in a position to identify and monitor all risks and adopt risk-mitigating measures.

Concerning the use of information technology, the BaFin has also published the "Circular on the supervisory requirements for IT 10/2017" (BAIT), which set out the framework for the institutions' technical-organisational infrastructure – in particular for the management of IT resources and for IT risk management. The purpose of BAIT is to make the MaRisk more concrete with a particular focus on IT and information risks.

On the basis of BAIT, regulated institutions have to meet a number of requirements which ensure that their IT systems function adequately and IT risks are addressed. The protection objectives to be heeded in this context are: confidentiality, integrity, availability and authenticity (an example of different security levels concerning the confidentiality of information is: publicly accessible information, information known only to a company's employees, personal data etc.). These four protection objectives are used to define the need for protection and the risk class of the pertinent information (e.g. low risk, medium risk, high risk), which then each lead to related measures. The measures to be adopted thus address specifically those the risks to which the information is exposed. The IT systems deployed and the related IT processes with which the information is processed must meet the data's need for protection and its risk class.

Clear responsibilities and duties as well as monitoring and control processes for information risks are established. Furthermore, the risk-reducing measures are defined, which are then coordinated, documented, controlled and monitored.

Regular risks analyses are carried out to reflect the dynamic environment. The results of the risk analysis have to be communicated to and approved by the executive board before being incorporated in the process for managing operative risks.

Below, we present some examples to show that the requirements of Art. 9ff of the regulation are already largely fulfilled by credit institutions on the basis of regulatory or cross-sectoral requirements

Art. 9: Risk management system

The requirements listed in Article 9 correspond in almost all aspects to the CRR demands on credit institutions. The provisions can be found in numerous statutes, ordinances, directives, guideline, recommendations and opinions published by legislatures, standard setters (FSB, BCBS), regulators (ESA = EBA, ESMA, EIOPIA), supervisory bodies (ECB-SSM and also national supervisory bodies). In addition, many of the aforementioned requirements are individually implemented in every EU member state – often with numerous extensions of the requirements by the national supervisory authorities.

Furthermore, the banking sector has adopted the "three lines of defence" principle. Application of this principle ensures that an institute-specific risk management system is designed, implemented, lived, monitored and modified as and when required. A key feature is that changes in products, customers, markets and also in organisation, processes and ICT are analysed for the pertinent risk. Before the changes are released, it must be clarified in the case of high-risk aspects what are the risks and how can they be mitigated.

The risk management system in banks thus goes well beyond the requirements of Article 9.

Art. 11: Technical documentation

Pursuant to BAIT 6 (40), the functionality of all of a financial institution's applications and also their development have to be clearly documented in a way that is plausible for third parties. This includes at least user documentation, technical system documentation and operating documentation.
Annex IV Technical documentation: Not necessary: 1. d), f), 2. c), f), 4., 8.

Beside the above, there are comprehensive statutory requirements with which banks have to comply. These can be found, for example, in German law texts, pursuant to Section 25a KWG. For example, Section 25a stipulates that there has to be "a complete documentation of business operations". These provisions apply for all companies listed in Article 22 of Regulation (EU) no. 575/2013.

Art. 12: Record-keeping requirements

These are already covered by BAIT (29, 30), therefore the technical preconditions for the logging of activities defined as events are in place. This is already done with "robotic process automation" or technical users (as with audit logs).

Art. 14 Human oversight (Art. 14)

Article 22 (3) GDPR already provides for the additional protection through human oversight required by the regulation. This stipulates that the controller of automated processing has to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Incidentally, the idea of human oversight is in principle embodied in the "three lines of defence model", see the remarks on Art. 9 Risk management system above.

Art. 15: Accuracy, robustness and cybersecurity

The information and IT systems in the institutions are adequately protected, and thus the intention of the European legislator is met with respect to Art. 15. Concerning cybersecurity, we already commented on DORA above under para. 3.1.5. Furthermore, the European Banking Authority (EBA) has published new directives on ICT and security risk management – the "EBA Guidelines on ICT and Security Risk Management" – [4], which came into force for national supervisory authorities on 30 June 2020. Following a change to BAIT most recently in 2018, these were already adapted to the EBA Guidelines and comprehensively updated. Publication of the amended BAIT is expected in 2021. The IT-specific requirements for information security are comprehensively laid down in it.

At the national level, the KRITIS Regulation and the 2nd Act to Increase the Security of Information Technology Systems also entered into force, see para. 3.2.1.

The aforementioned regulations show what strong regulation and supervision the sector already stands concerning the requirements in Art. 9ff of the draft regulation. The increasing use of AI will in our opinion make no difference to this. Credit institutions are well positioned to address and adequately manage current and future risks. If, on the other hand, the AI Regulation now establishes regulations that are already largely regulated, at least for the financial sector, this may not only lead to unnecessary duplication, but also to contradictory requirements that will cause enormous difficulties for both the supervisory authority and the institutions.

This applies in particular to similar requirements that are comparable in terms of their objectives but different in detail, and for which it can only be determined after an extensive detailed analysis exactly how they differ in detail from the solutions currently used by credit institutions and are therefore in line with the objectives of the proposed regulation but do not fully comply with its requirements. For example, this is particularly true for the data-related requirements. Consequently, a high additional effort would have to be expected in order to fully comply with these requirements, without this being offset by any additional benefit for consumers. The envisaged grandfathering of existing processes would change little in this respect, as it would no longer apply in the case of new developments and significant changes, and the data-related requirements, for example, would also apply immediately with the use of the new process.

As an example, significant changes and new developments of procedures for the assessment of creditworthiness may become necessary if the forecasting quality of the models decreases over time and would no longer find acceptance by the supervisory authorities. In this case, it would not be in the interest of the consumer to be evaluated with procedures whose predictive power can no longer be

[4] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.

described as satisfactory compared to a new development. Consumers should be able to benefit here from the best available procedures for assessing their creditworthiness. This is the best way to ensure that those consumers who are creditworthy receive credit on favourable terms.

4. German Banking Industry Committee calls and suggestions

4.1 Exception from the scope in Art. 2 and dispensation with para. 5b) in Annex III

Due to the already existing comprehensive sector-specific regulations, the German Banking Industry Committee calls upon the European legislator to remove the financial sector from the scope of Art. 2 of the regulation. By dint of the present banking regulatory requirements, any such risks are adequately addressed. This applies in our opinion for all and any kind of risk, but especially also for high-risk applications.

A specific suggested wording for the sector-specific exception can be found in para. 5.1.
Hence, deleting Annex III 5 b) would be the logical step.

The European legislator subsumes credit assessment and credit scoring under the high risks listed in Annex III, as there is in particular a risk of discrimination through bias in data records.

In our view, however, these concerns have already been adequately addressed and the assumed risks have already been minimized to such an extent that a high risk in this area cannot be assumed per se.

On the basis of the already existing regulatory requirements listed above, existing risks are continuously monitored, new risks regularly identified and added to the risk inventory before being classified as per their impact and measures developed on that basis. IT risks in particular are handled in accordance with the protection goals of availability, integrity, confidentiality and authenticity of the data to be protected.. As a result, financial institutions are extremely well positioned to meet the changing requirements and risks of new technologies.

On the basis of this approach, credit assessment of natural persons cannot be classified as a high-risk activity per se. Rather, it is important to identify and address the risks associated with a credit assessment and credit scoring. The risk management processes of financial institutions are already set up accordingly and capable of doing so.

4.2 Inclusion of sector-specific references in the regulation

Should the legislator not accept our suggestion of excluding the financial sector from the scope of Article 2, we suggest as an alternative including sector-specific references in Art. 9ff of the regulation, as was done in Art. 17 – Quality management system with the reference in paragraph 3 to Directive 2013/36/EU.

There is no denying that there are contexts that may pose a particular risk to people, society and its democratic values. We also believe that such risks should be addressed in order to prevent any dangers that may result from the use of AI.

In our view, companies should be able to address the risks inherent in the Annex III use cases. This is already the case for financial institutions with regard to credit assessments and credit scores due to previous regulations and their risk management systems.

Credit assessment in banks is already subject to a strict supervisory regime. The competent authorities constantly monitor those procedures. This not only protects consumers and investors but also ensures financial stability. The use of statistical processes to determine an evaluation function, possibly extended by a Bayes function, has been standard practice in credit institutions since 2005 at the latest, after they had already been increasingly used since the mid-1990s and then, in line with banking practice, were also allowed to be used for risk-oriented capital backing of credit risks under Basel II. Accordingly, the banking sector has decades of experience. The supervisory authorities also already have around 15 years of experience through their audits of corresponding procedures. Additional demands on the loan granting are therefore not required.

Consumers also benefit from receiving a quick and uncomplicated loan approval. This has helped to increase the supply of credit to consumers in recent years. In addition, under the data protection law requirements, there is a right to information, so that the loan decision can be reviewed and corrected if a loan is refused. We therefore see no increased risk for natural persons suffering a biased loan decision compared to manual decision-making processes.

5 Regulation-specific comments on the draft regulation

5.1 Art. 2, inclusion of a new paragraph (3):

"For high-risk systems developed and / or used by companies subject to the provisions of Regulation (EU) no. 575/2013 (CRR), only Art. 84 of that regulation shall apply.

5.2 Art. 3: Definitions

The German Banking Industry Committee calls upon the European legislator to reconsider the definition of AI given in the draft regulation and move more to the international understanding of AI, which is defined far more narrowly than the draft regulation envisages, see for example the OECD definition.

Under this definition, an AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.[5] The definition of the regulation clearly goes beyond this, in that it states that every rule-based procedure is to fall under the AI concept, regardless of the extent to which autonomy is given at all. With a legally secure framework, companies must be able to design risk strategies and corresponding mitigation processes that can be sustained in the long-term.

Score cards for natural persons developed on the basis of statistical processes should be explicitly excluded from this regulation. These processes have proven themselves over decades in some cases and are successfully used by institutions. For nearly 15 years, they have also been reviewed by authorities and have a demonstrably high benefit for the consumers in that they support fast, uncomplicated and low process-cost granting of loans.

The German banking supervisory authority, BaFin, points out that the current definitions of artificial intelligence do not permit sharp distinction between classic statistical processes and deployed algorithms and further development of the definition constitutes one of the challenges facing supervisory authorities, regulators and above standard setters.[6]

Due to its breadth, the definition in the proposed regulation now basically covers every kind of software developed with one or more of the techniques and concepts listed in Appendix I. This makes the definition very rigid and not dynamic, which is not useful or future-proof for a dynamic technology like AI. Too little distinction is made as to which characteristics of a technology, such as AI, give rise to certain risks and need to be mitigated. To classify an entire technology as risky across the board - i.e., irrespective of its specific characteristics, e.g., the degree of autonomy - is misguided, because it does not take into account the extent, to which a real risk can actually be realized by the AI used.

The definition in our opinion covers different kinds of technical methods, which against the background of the regulation's actual risk-based approach, but also the pertinent method as such, does not seem appropriate.

[5] OECD Council „Recommendation of the Council on Artificial Intelligence", retrievable at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[6] https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl_Prinzipienpapier_BDAI.html?nn=9021442.

With respect to the financial sector, the suggested definition means that the use of traditional statistical processes, as used in credit institutions in part for decades, but at the latest since Basel II, leads to an undifferentiated categorisation as AI. From the perspective of the Deutsche Kreditwirtschaft, this seems unnecessary over-regulation. Rather, the aspiration of a modern regulatory framework should be to enable companies to develop and deploy under risk-based considerations.

It is therefore surprising that rule-based procedures, which have been in use at banks for a long time and have been monitored and approved by the supervisory authorities, are now to be covered by the regulation. In the case of rule-based procedures, statistical procedures, mathematical functions or classification assignments, the banks clearly specify, for example, which classification results are to be derived from certain data constellations. They are (further) developed by humans with the help of statistical procedures and are unable to do this themselves. Independent working is not immanent in these processes and methods. Therefore, they have nothing in common with the general understanding of AI. Risks of these methods are already adequately included in the financial institutions' risk management systems and addressed pursuant to their impact.

Even with new technologies, such as machine learning, no additional risks arise which financial institutions cannot adequately address in their installed systems.

Too strict regulations are not in the interest of consumers either, as demonstrated by a European Consumer Organisation survey. Consumers consider that AI can be useful. The respondents seem to hope that AI will help to resolve some fundamental problems of human life. In all participating countries, people find the following services based on machine calculations somewhat or very useful:

- Predicting traffic accidents (91%)
- Predicting their health problems (87%)
- Predicting their financial problems (81%)[7].

According to the survey, consumers have concerns regarding their privacy protection, AI manipulating their decisions, the risks of discrimination, the reliability and safety of AI, and the allocation of responsibility and liability[8].

Those concerns are rightly plausible and must be adequately taken into consideration – as intended in the regulation - in order to create strong protection for consumers and ensure their trust in this technology. However, this can only be implemented in a meaningful way, if it is based on the respective purpose of the AI: The regulation of AI must be be proportionate to the risk that it is intended to minimise.

[7] https://www.beuc.eu/publications/beuc-x-2020-078_artificial_intelligence_what_consumers_say_report.pdf, pg.4.

[8] https://www.beuc.eu/publications/beuc-x-2020-078_artificial_intelligence_what_consumers_say_report.pdf, pg. 9.

Against this background, we suggest the following definition for AI:

- '**artificial intelligence system'** (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with *under the overall condition that the system, to a significant degree, works autonomously.*

It is also suggested that the criteria for classifying a technique as AI be put down more specifically in a delegated act, because the use of the techniques listed in Appendix I, in particular concerning the use of statistical approaches including Bayes estimators, is too far-reaching and would thus also cover traditional statistical approaches already used for decades.

Furthermore, we submit further suggestions for revising the definitions made in Art. 3 so as to eliminate ambiguities and avoid misunderstandings:

- '**provider**': the definition of 'provider' is not clear and precise enough, as it embraces not only the developer as such but also those who have AI systems developed. The definitions do not do justice to the frequent triad of IT provider, financial institution and customer which is frequently encountered. A provider should only develop. White-label providers should also be included.

  Suggestion: "'provider' means a natural or legal person, public authority, agency or other body that develops an AI system ~~or that has an AI system developed~~ with a view to placing it on the market or putting it into service ~~under its own name or trademark~~, whether for payment or free of charge"

- '**operator'**: The definition is not clear, as it can mean all and anything.

  Suggestion: Remove this definition.

- '**placing on the market'**, '**making available on the market'** and '**putting into service'** are very similar and very unclearly separated from each other.

  Suggestion: Remove (9) and (11), and leave only (10).

- **'remote biometric identification system'**: First of all, the term **'**remote**'** has to be defined, as it can give rise to differing interpretations. In addition, it is unclear whether know-your-customer processes or biometric authentication processes used are included.
  Moreover, it sounds as if remote biometric identification systems ("RBI") are not named as such if people know they are being identified. This aspect also requires clarification. In addition, it is unclear to what extent an RBI system is considered high risk if it is used in public. A uniform

definition of "public" or "public space" must also be given here, as this is defined differently in the member states.

5.3 Art. 10: Data and data governance (Art. 10):

Overall, the article seems overridden due to the existing regulation of the GDPR. There is also no reference to the Basel Committee's BCBS 239 "principles for the effective aggregation of risk data and risk reporting". It has been implemented nationally in MaRisk AT 4.3.4.

- Art 10 para. 3: "Training, validation and testing data sets shall be relevant, representative, free of errors and complete." That is far from praxis. The criteria are not measurable, especially completeness. The requirements do not reflect the necessities and practice for developing valid and well calibrated scoring functions / score cards for private customers. These scorecards are developed with a view to achieving high forecasting quality. This is also in the interest of consumers in order to determine their creditworthiness as accurately as possible. For this purpose, e.g. in the development of score cards based on variance and regression analytical approaches, all data are included in a function which multivariate, i.e. in their interaction make a high contribution to an accurate assessment of the creditworthiness. This does not necessarily require the filling of a data field, because already the specification or non-specification of an information in interaction with further information can contribute to the improvement of the forecast quality. Omitting such data because of the completeness requirement would result in the adjustment of score maps and degraded forecast quality due to the omission of significantly explainable information. As a result, higher risk costs would have to be borne by borrowers via the interest rate on loans, or a more restrictive underwriting policy would have to be expected, which would tend to exclude borrowers with a somewhat weaker credit rating from receiving loans. That surely cannot be in the interest of customers.

- "free of errors": This phrase is unrealistic in our opinion. Possible errors, in so far as these are not clearly outliers that are eliminated, are usually implicitly taken into consideration in the data during development. Since an individual information point only makes a limited contribution to evaluating creditworthiness and it depends more on the interaction of a number of information points, which taken together enable an optimum and time-stable assessment of borrowers, the processes are to a certain degree error-tolerant.

5.4 Art. 13: Transparency and provision of information to users

Art. 13 (1): The requirement pursuant to Art. 13 (1) 2nd sentence, that operation of the high-risk systems has to be adequately transparent, so that users can adequately interpret and use the results of the systems, is welcomed in principle.

However, in our opinion what exactly is meant by transparency and what is expected of companies concerning the explainability of algorithms is too vaguely worded. The question about the explainability of algorithms can namely be answered quite diversely, because the algorithms themselves are diverse.
It should therefore suffice if an algorithm's mode of action is explicable and validatable. This is from our understanding also the view of the High-Level Expert Group on Artificial Intelligence:

"[…] Technical explainability presumes that the decisions taken by an AI system can be understood by people and are traceable. Furthermore, compromises between enhanced explainability of a system (which can impair precision) and more precision (at the expense of explainability) may have to be made"[…][9].

The BaFin said much the same in a discussion paper published on 15 July 2021:

"The more complex and higher-dimensional the hypothesis space that can be represented by the model is, the more difficult it becomes to describe the functional relationship between input and output (i.e., the hypothesis concretized in the training) verbally or by mathematical formulas, and the less comprehensible the calculations are in detail by modelers, users, validators and supervisors. This leads to a more difficult comprehensibility of the modeling and possibly also to a more difficult verification of the validity of the model results."[10].

The requirements in Art. 13 of the regulation must in particular must enable users to fulfill information and transparency obligations under other legal requirements, such as the GDPR, vis-à-vis end users. At the same time, it has to be ensured that the information depth does not unduly impair protection the provider's intellectual property and that statutory provisions, in particular business secrets legislation, are not breached.

5.5 Art. 53ff.: Sandboxes

We welcome the installation of regulatory accompanied sandboxes to promote AI innovation. However, we see a further need for sharpening this section. The definition of a "regulatory sandbox" is not clear. The draft regulation should be supplemented accordingly.

Moreover, the goal of the sandboxes is unclear, e.g. development of new applications, implementation of use cases, scaling of already implemented applications.

[9] Retrievable at: https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai, see 4 HLEG, para. 75ff.

[10] „Maschinelles Lernen in Risikomodellen – Charakteristika und aufsichtliche Schwerpunkte", retrievable at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2021/meldung_2021_07_15_Konsultation_Maschinelles_Lernen.html, pg. 14, point 3.

In addition, it is not apparent which regulatory requirements are to apply in the sandboxes, as on the one hand it reads that an improved environment would be provided, but on the other hand all participants would have to follow all regulatory requirements. Furthermore, it is not defined according to which criteria companies gain access. The provisions need to be made more precise. Moreover, there is a lack of clarity regarding the question of whether data protection facilitations with regard to the processing of personal data could also come into play in the context of the use of sand-boxes, e.g., in the event of a change in the purpose of processing.

In particular, we see a risk of unfair competitive conditions, as only selected companies will have access to the sandboxes. All market participants must be given the opportunity of regulatory accompaniment in their innovations, so that the usefulness of investments can be checked as early as possible and money and time are not spent unnecessarily.

Moreover, we suggest that the report on the work in the sandboxes, which is provided to the European AI Board and the EU Commission, is accessible for all companies in the EU, so that experiences about the development and use of AI can be shared and thus innovation is promoted. If the report will contain confidential information, a summary of key lessons learned from the sandboxes should be publicly available, unless confidential.

5.6 Art. 73: Exercise of the delegation

In discussions with the Commission, it became clear that there will be a two-year transition phase for implementing the requirements for AI systems newly categorised as high risk – this should be added here in writing.

Suggestion adding a paragraph 6 to Art. 73:
"(6) *Any delegated act adopted pursuant to Article 7(1) shall foresee an application date of at least two years after entry into force*."

5.7 Art. 83: AI systems already on the market or put into service

Grandfathering only applies to the extent that high-risk AI systems already placed on the market or in use are within scope only if they undergo significant changes in their "de-sign" or intended use after the application date (24 months after entry into force) (see Article 83 (2)). In addition, it is questionable what is meant by significant changes in design.

In any case, processes with significant changes in design in the sense of a further development, which objectively leads to an improved assessment quality, should also be given a two-year implementation period after the end of the implementation period under Art. 85 (2) so that the requirements of this regulation concerning the processes and the demands on the data can be fully implemented. This avoids a situation in which significant further developments to improve the quality of the assessment are not implemented simply because not all the requirements of the Regulation have been fully implemented at this point in time.

5.8 Access to data / level playing field / promotion

PricewaterhouseCoopers has conducted a survey about using AI with banks and insurance companies in the DACH (German-speaking) region. 69% of the companies cite a lack of available data as an obstacle to adaption. 67% of the respondent companies are also struggling with budget restrictions and a shortage of funding for such projects, 64 % of the companies have a lack of competent employees to answer questions about establishing AI, such as which business unit offers an appropriate interface for establishing AI projects in operational business or which department will finance the integration process.[11]

Even though this survey was only limited to banks and insurance companies in the DACH region, it can be assumed that the difficulties presented apply across all sectors and throughout Europe.

From the perspective of the Deutsche Kreditwirtschaft, the draft regulation does not go far enough in the issues of "access to data, level playing field and promotion of AI" and correlating expertise. It is not enough to rely on regulatory sandboxes and data pools based on GaiaX; a reform of the current regulation on data exchange and data protection is also called for. Otherwise, there is a risk that innovators will turn to national legislators to obtain more flexibility, e.g. with respect to the General Data Protection Regulation (GDPR), which ultimately could thwart the purpose of such regulations, namely creating a harmonised level playing field throughout the EU. An investment plan must also be presented, including the criteria under which investment projects are selected. If this is not the case, companies will have the will to use AI but not the capabilities. Initiatives to strengthen knowledge, skills and research projects must be launched.

5.9 Biometric identification of natural persons

We have understood that under the new rules, all AI systems which are to be used for remote biometric identification of persons will be classified as high-risk and subject to ex-ante third party conformity assessment, including the demands on documentation and human oversight. We anticipate that financial service providers and their vendors which rely on biometric identification to support customers remotely and meet the Know-You-Customer-requirements do not fall within the scope of the complete requirements of the AI regulation. In this regard, we ask for clarification as a precautionary measure.

[11] https://www.pwc.de/de/finanzdienstleistungen/kuenstliche-intelligenz-im-finanzsektor.html.

6 Closing remarks

We support the Commission in its efforts to create a clear legal framework for AI that promotes innovation and at the same time offers certainty for all market participants. In particular, we support the approach of fostering "digitalisation with a human face". We believe that ethically programmed AI in conjunction with human expertise will be of great value for the European Community. A core point in this context was implemented in the draft: responsibility for an activity always lies with a person. To ensure that, the development of an AI system has to be documented in a traceable manner and all AI system's activities have to be recorded so that decisions can be traced and audited. It also has to be ensured that an AI system's assessment can be overturned by a person at any time.

AI constitutes an enormous potential for the European economy. AI experts have made great progress in their research. Today, the EU is second only to China in the publication of research results. However, too few of those research results are being implemented in products and services. But to make that possible, the EU has to become an attractive location for companies, one in which a propensity for risk is highly regarded and innovative minds will find attractive conditions as well as a supportive ecosystem. For innovation cannot be transferred from the political level to the economy, it originates in the companies themselves under good framework conditions.

We therefore appeal to the European legislator to first and foremost promote the development and use of AI technology with its regulation and merely regulate those use cases in which risks can actually arise that have not already identified and adequately mitigated the sector in question. In that way, we will establish an active, successful and sustainable AI ecosystem in the EU.

We are of the opinion that the current scope of the draft regulation is too broad. Scorecards for natural persons developed on statistical processes should be explicitly excluded from this regulation. These processes have proven themselves over decades in some cases and are successfully used by institutions. For nearly 15 years, they have also been reviewed by authorities and have a demonstrably high benefit for the consumers in that they support fast, uncomplicated and low process-cost granting of loans. Other circumstances in which AI in the actual sense is used in conjunction with creditworthiness assessments are fully addressed by existing requirements imposed on credit institutions, so that the risks assumed by the legislator do not come into play in practice.

***