Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union

Unsere Zeichen
AZ DK: KI
AZ DSGV: 8528/01

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

Berlin, 06.08.2021

Federführer:
Deutscher Sparkassen- und Giroverband e. V.
Charlottenstraße 47 | 10117 Berlin
Telefon: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

1 Management Summary

Die Deutsche Kreditwirtschaft begrüßt das Bestreben des europäischen Gesetzgebers, einen innovationsfreundlichen und rechtssicheren Rahmen für den Einsatz künstlicher Intelligenz (im Folgenden: KI) in einem fairen Wettbewerbsumfeld schaffen zu wollen, von dem Verbraucher und die Wirtschaft profitieren. KI wird als Schlüsseltechnologie des 21. Jahrhunderts angesehen, die in den kommenden Jahren und Jahrzehnten unternehmerisches Handeln, aber auch das Leben von Verbrauchern in vielfacher Hinsicht beeinflussen wird.

Der Verordnungsentwurf stellt den Schutz der Grundrechte der Bürger der Europäischen Union in den Vordergrund. Die Bürger sollen insbesondere in grundlegenden Bereichen des Lebens vor den Risiken des Einsatzes von KI geschützt werden. Dafür wurden in Annex III des Verordnungsentwurfs hochrisikoreiche Systeme genannt. Wir unterstützen den zugrundeliegenden Ansatz grundsätzlich, da die dort genannten Einsatzbereiche (z. B. biometrische Identifizierung, Verwaltung und Betrieb kritischer Infrastrukturen, Zugang zu Einrichtungen des Bildungswesens etc.) grundlegende Lebensbereiche berühren und zugleich und den individuellen Schutz, die Versorgung mit lebenswichtigen Gütern und die Teilhabe am Gemeinwesen betreffen. Dieses Verständnis spiegelt die europäischen Werte wider und ist entsprechend zu befürworten.

Dennoch greift der in der Verordnung gewählte Ansatz aus unserer Sicht fehl, da ausgewählte Anwendungsfälle pauschal als hoch risikoreich definiert werden, ohne dass es hierfür ein nachvollziehbares Kriterienraster gibt, welches die Risiken explizit benennt und objektiv belegt (quantifiziert) und dabei bereits bestehende risikomitigierende (gesetzliche) Anforderungen berücksichtigt. Wir meinen, dass bei Berücksichtigung der risikomitigierenden Fakten erkennbar wird, dass kein hohes Risiko für Verbraucher im Rahmen der Kreditwürdigkeitsprüfung oder für das Kreditscoring besteht. Unverständlich ist zudem, dass eine Technologie (KI) die, sich in bestehende Prozesse und Strukturen in den Kreditinstituten einbettet, per se zu einem höheren Risiko führt. Dies unterstellt, dass die existierenden risikomitigierenden Anforderungen und Institutionen, die mit der Beaufsichtigung und Überwachung von Kreditinstituten befasst sind, unzulänglich sind und nicht hinreichend Wirkung entfalten. Dies ist unzutreffend.

Geht man lediglich davon aus, dass der jeweils betroffene Anwendungsfall aufgrund seiner Bedeutung für eine solche Zuordnung ausreicht, wäre der Ansatz folgerichtig. Wir gehen jedoch davon aus, dass die Nennung von risikoreichen Anwendungsfällen einer dynamischen, sich weiter entwickelnden Risikolandschaft nicht gerecht wird. Es muss vielmehr bewertet werden, welche Risiken bestehen bzw. entstehen können und inwieweit diese tatsächlich eintreten, vor allem aber auch mitigiert werden können bzw. bereits werden.

Vor diesem Hintergrund erfolgt in dem Verordnungsentwurf die Einordnung der Kreditwürdigkeitsprüfung und der Kreditpunktebewertung als Hoch-Risiko-KI-Anwendungsfall nach unserer Auffassung zu Unrecht.

Die Finanzbranche unterliegt, wie kaum eine andere Branche, zahlreichen Regulierungen, aufsichtlich begleiteten Prüfungs- und Genehmigungsprozessen, welche von ihr Transparenz, Kontrolle und Risikomitigierung einfordern. Sowohl die hierfür eingerichteten Risikomanagementsysteme als auch die IT-Infrastrukturen unterliegen seit vielen Jahren einer kontinuierlichen Überwachung und Kontrolle. Diese Strukturen gewährleisten zudem, dass auch heute noch unbekannte Risiken, welche aufgrund neuer Technologien entstehen können, schnellstmöglich identifiziert und entsprechend adressiert werden können. Die Ziele, die die in der Verordnung geforderten Anforderungen an Hoch-Risiko-Systeme sicherstellen sollen, werden bereits von Kreditinstituten durch ihre eigenen Risikomanagementsysteme erreicht, insbesondere nicht nur, aber gerade auch im Bereich der Kreditwürdigkeitsprüfung und Kreditpunktebewertung. Daraus folgt, dass die Annahme, dieser Bereich sei per se ein Hoch-Risiko-Bereich, aus unserer Sicht fehlschlägt. Wir fordern daher den Europäischen Gesetzgeber auf, Kreditinstitute aus dem Anwendungsbereich des Art. 2 der Verordnung auszunehmen.

Des Weiteren sehen wir die vorgeschlagene Definition von KI kritisch. Wir unterstützen zwar eine technologieneutrale Definition, diese sollte aber insbesondere den risikorelevanten Charakteristika Rechnung tragen, um eine verhältnismäßige Regulierung zu ermöglichen. Daher fällt die KI-Definition aus unserer Sicht zu weit und zu pauschal aus, da sie jedes regelbasierte Verfahren erfasst und damit weit über die problematisierten Aspekte von KI hinausgeht.

Wir fordern daher den europäischen Gesetzgeber auf, die Definition von KI noch einmal zu prüfen und zu erneuern. Ein konkreter Formulierungsvorschlag findet sich unter Ziffer 5 „Regelungsspezifische Anmerkungen zum Verordnungsvorschlag".

2 Bedeutung von KI-Anwendungen für die Finanzbranche

Insbesondere die Finanzbranche ist auf KI angewiesen. Die Zukunft der Branche ist ohne die Nutzung von KI nicht mehr vorstellbar, vor allem aber auch nicht mehr darstellbar. Banken sehen sich mit einer stetigen Zunahme von enormen Datenmengen konfrontiert, mit denen umgegangen werden muss. Eine übermäßige Regulierung würde nicht nur Innovationen hemmen, sondern in der Folge auch verkennen, dass volkswirtschaftliche Vorteile ungenutzt bleiben, die u. a. die Finanzmarktstabilität betreffen. Die Zielsetzung der Verordnung stellt aus unserer Sicht einseitig auf den Schutz des Einzelnen ab und denkt nicht ausreichend an die Bedeutung der Finanzmarktstabilität. Die Finanzmarktregulierung berücksichtigt bereits heute Aspekte des Verbraucherschutzes wie auch zugleich der Finanzmarkstabilität und ist aus unserer Sicht somit bereits risikominimierend und interessengerecht ausbalanciert. Wir befürchten zudem, dass der derzeitige Verordnungsentwurf zu Widersprüchen und Überschneidungen mit den bereits existierenden Regelungen führen kann.

1. Schwerpunkte der Nutzung von KI im Bankensektor sind u. a. die Echtzeit-Transaktionsanalyse, algorithmisches Trading und KI-verwaltete Fonds. Hinzukommen aber auch einfache Vorgänge wie z. B.

Personalisierung von Kundendienstleistungen, Spracherkennung, natürliche Sprachverarbeitung. Solche Systeme werden z. B. eingesetzt, um die Allokation von Ressourcen von Finanzinstituten herauszufiltern. Ein weiteres Beispiel ist der Einsatz von Chatbots zur Automatisierung von Routine-Kundeninteraktionen, wie bei der Kontoeröffnung und allgemeinen Kundenanfragen. KI wird in Call-Centern eingesetzt, um Kundenanrufe zu bearbeiten, zu triagieren und individuellen Service zu bieten.

2. Die Nutzung von KI bietet zudem Vorteile, die über Effizienzsteigerungen hinausgehen – auch für Kunden. Banken erhalten durch KI-Lösungen ein umfangreicheres Bild über ihre Kunden und deren branchenspezifische Bedürfnisse. Dadurch können Firmenkundenbetreuer mit firmen- und branchenspezifischen Know-how versorgt werden, wodurch sie ihre Kunden gezielter zu aktuellen Entwicklungen beraten bzw. bedarfsorientierte Angebote unterbreiten können.

   Mittels KI lassen sich z. B. Geldeingänge und -ausgänge analysieren und darauf aufbauend eine Prognose für die weitere Liquiditätsentwicklung ableiten. Sagt der KI-Algorithmus durch Zusammenführung unterschiedlicher Datenpunkte einen finanziellen Engpass für ein Unternehmen voraus, kann die Bank direkt und frühzeitig ein passendes Kreditangebot unterbreiten. Diese vorgeschalteten Verfahren werden in Zukunft nicht mehr nur auf regelbasierten Algorithmen basieren, sondern auf Basis maschinellen Lernens. Der Grund hierfür liegt in der genaueren Trennschärfe, die solche Modelle hervorbringen. Eine höhere Trennschärfe führt zu einem sensitiveren, also genaueren Prüfergebnis. Das wiederum minimiert die Ausfallwahrscheinlichkeit beispielsweise eines Kredits. Wird nun aber ein maschinell lernender Algorithmus, der bei einer Vorprüfung zur Kreditwürdigkeit eingesetzt wird, unter High-Risk subsumiert, wird verkannt, dass die höhere Trennschärfe für alle an dem Vorgang Beteiligten vor allem Vorteile bringt. Daher ist dies ein gutes Beispiel für einen risikoorientierten Regelungsansatz, der aus unserer Sicht sinnvoller ist als eine pauschale Einordnung solcher Vorgänge unter High-Risk mit den entsprechenden Anforderungen. Abgesehen davon steht am Ende einer Kreditwürdigkeitsprüfung immer der Human Oversight. Dies ist bereits heute der Fall und wird durch die Institute auch nicht in Frage gestellt.

   Weiterhin funktioniert intelligente Betrugserkennung nicht mehr ohne KI. Wir sind uns darüber bewusst, dass der Einsatz von KI zum Zwecke der Bekämpfung der Finanzkriminalität gemäß dem Verordnungsvorschlag keinen Anforderungen unterliegt. Wir möchten aber darauf hinweisen, dass diese Bereiche miteinander verknüpft sind und entsprechend eine unterschiedliche regulatorische Behandlung widersprüchlich sein könnte. Neuronale Netze werten riesige Datenmengen mithilfe von Deep Learning aus und identifizieren vorher unbekannte Muster in den Transaktionsdaten. Das hilft in einem bisher nicht möglichen Maß, Betrug zu erkennen und diesem vorzubeugen. Dies hat sowohl Vorteile für Banken als auch für die Gesellschaft, insbesondere da die Effektivität erhöht, das Risiko strafrechtlicher Verfolgung gesteigert und die Reputation des Finanzinstituts gesteigert wird.[1]

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

Die Konvergenz von Fähigkeiten innerhalb der Compliance, etwa die Verhinderung von Geldwäsche und Betrug durch KI, ermöglicht wesentliche Kosteneinsparungen. Es wird geschätzt, dass die Überschneidung der Datenverarbeitung, der Systemwartung und der Verwaltung der Legacy Systeme, die zur unabhängigen Unterstützung dieser Funktionen benötigt wird, etwa 80% beträgt. Kriminelle nutzen zudem häufig die starre Infrastruktur innerhalb des globalen Finanzsystems. Daher ermutigen Aufsichtsbehörden Finanzinstitute, neue Wege und Methoden einzugehen.[2]

Neue Technologien bergen immer auch neue Risiken, die Unternehmen adressieren müssen. Bei der Entwicklung und dem Einsatz von KI-Systemen fallen unter anderem folgende neue Risiken besonders auf:

- Hohe Komplexität: Die in KI-Systemen eingesetzten Algorithmen weisen eine deutlich höhere Komplexität als klassische statistische Verfahren auf, welche die Nachvollziehbarkeit und Überprüfbarkeit deutlich erschwert.
- Kurze Rekalibrierungszyklen: Aufgrund der Tatsache, dass KI-Systeme immer neue und größer werdende Datenmengen selbstständig verarbeiten und sich dadurch konstant weiterentwickeln, wird die Validierung einer Kalibrierung zunehmen schwerer
- Bias: Aufgrund von Vorurteilen und unvorteilhaften Tendenzen in großen Datenmengen steigt das Risiko eines verzerrten Ergebnisses sowie einer unfairen Behandlung von natürlichen Personen.

Die hier genannten Risiken sind den Finanzinstituten jedoch bereits bekannt und werden durch die Risikomanagementprozesse adressiert, mitigiert und gesteuert.

3 Gesetzliche und aufsichtsrechtliche Anforderungen an die Finanzbranche

3.1 Europäische Anforderungen

Kaum eine Branche unterliegt so starken regulatorischen Vorgaben wie die Kreditwirtschaft, deren Einhaltung durch sektorspezifische Aufsichtsbehörden auf nationaler und europäischer Ebene streng überwacht wird.

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

3.1.1 Rahmenbedingungen Score--Funktionen und Klassifikationsverfahren

Die auf Basis statistischer Verfahren entwickelten Score-Funktionen und Klassifikationsverfahren werden regelmäßig von den Aufsichtsbehörden überprüft. Dies gilt sowohl für die auf internen Ratings basierenden Verfahren („IRB-Verfahren") von IRB-Instituten, deren Modelle für die risikoorientierte Eigenkapitalunterlegung abgenommen wurden als auch für die Institute, die den Kreditrisikostandansatz („KSA-Institute") anwenden und deren Klassifikationsverfahren zur Bewertung der Kreditwürdigkeit z. B. in Deutschland nach den Mindestanforderungen für das Risikomanagement (MaRisk) mindestens jährlich und bei Hinweisen auf eine Beeinträchtigung auch unterjährig im Rahmen einer umfassenden Validierung zu überprüfen und anzupassen sind. Hierfür gelten für IRB-Institute bereits die Vorschriften der Capitil Requirements Regulation („CRR") und dazugehöriger delegierter Verordnungen und Leitlinien. Für KSA-Institute, die solche Verfahren einsetzen, werden diese IRB-Vorgaben bei aufsichtlichen Prüfungen ebenfalls sinngemäß als Benchmark von den Aufsichtsbehörden herangezogen.

3.1.2 Analytical Credit Datasets

Neben der besseren Ausstattung der Finanzbranche mit Eigenkapital zielen bei der Bankenregulierung zahlreiche Vorgaben auf die Vereinheitlichung der sektorspezifischen Gesetzgebung und des Aufsichtsregimes in der Europäischen Union ab. So bezweckt beispielsweise die 2016 von der Europäischen Zentralbank eingeführte Regulierung zu AnaCredit (Analytical Credit Datasets), Informationen auf Ebene der einzelnen Kreditnehmer und der einzelnen Kredite zu erheben. Die Meldungen sind an die nationalen Aufsichtsbehörden zu liefern. Die AnaCredit-Regulierung gibt zudem vor, welche Daten im Rahmen eines Kreditvergabeprozesses erhoben und gemeldet werden müssen. Die Regulierung gilt in allen Mitgliedsstaaten des Euro-Raums der Europäischen Union.

3.1.3 Basel III

Der wichtigste Eckpfeiler der Bankenregulierung ist Basel III. Im Kern der Reform stand das Ziel einer Balance zwischen einem stabileren Finanzsystem und der Vermeidung einer Kreditverknappung, außerdem die Begrenzung und Reduzierung der Haftung der öffentlichen Hand und der Steuerzahler. Mit der Umsetzung des Bankenpakets, das Vorgaben von Basel III auf europäischer Ebene umsetzt, hat sich die Stabilität des Finanzsektors in Europa seit Beginn des Reformprozesses zur Bankenregulierung verbessert. Aus den Neuregelungen gingen unter anderem Änderungen hervor im Hinblick auf:

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

3.1.4 Capital Requirements Regulation (CRR)3

Mit der Verordnung 575/2013 (CRR) werden bereits umfassende Anforderungen an Rating-Systeme gestellt, u. a. zur Integrität des Prozesses, der Modelle, der Dokumentation, sowie der Datenpflege. Auch hier sollten Überschneidungen vermieden werden. Kreditinstitute, die unter die CRR fallen, sollten daher von den Anforderungen für High-Risk KI-Systeme ausgenommen werden, um so Überschneidungen und Doppelprüfungen zu vermeiden.

3.1.5 Digital Operational Resilience Act (DORA)

Am 24. September 2020 hat die EU-Kommission die „Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors [DORA]", COM 2020/0266 vorgeschlagen. Dora soll sicherstellen, dass alle Teilnehmer des Finanzsystems über die notwendigen Sicherheitsvorkehrungen verfügen, um Cyber-Angriffe und andere Risiken einzudämmen. Finanzaufsichtsbehörden sollen Zugang zu Informationen über "IKT-bezogene Vorfälle" bekommen und sicherstellen, dass Finanzunternehmen die Wirksamkeit ihrer Präventiv- und Belastbarkeitsmaßnahmen bewerten und Schwachstellen identifizieren.

3.1.6 Richtlinie über Verbraucherkreditverträge (2008/48/EG) und Richtlinie über Wohnimmobilienkreditverträge (2014/17/EU)

Mit der Richtlinie 2008/48/EG über Verbraucherkreditverträge und der Richtlinie 2014/17/EU über Wohnimmobilienkreditverträge wurde bereits ein harmonisierter EU-Rahmen für Kredit an Verbraucher geschaffen, der einen fairen und transparenten Zugang der europäischen Verbraucher zu Krediten gewährleistet und eine Verpflichtung zur Prüfung der Kreditwürdigkeit des Verbrauchers vorsieht. Danach darf eine Kreditvergabe an Verbraucher nur dann erfolgen, wenn wahrscheinlich bzw. zu erwarten ist, dass die Verpflichtungen im Zusammenhang mit dem Kreditvertrag in der gemäß diesem Vertrag vorgeschriebenen Weise erfüllt werden können. Damit soll dem Schutz des Verbrauchers vor Überschuldung Sorge getragen werden und es können hieraus Haftungsansprüche des Verbrauchers entstehen. Auch dies trägt ergänzend zu den aufsichtsrechtlichen Maßgaben an die Kreditrisikoprüfung dazu bei, dass die Kreditvergabeprozesse in den Banken auch im Interesse des einzelnen Verbrauchers höchsten Standards folgen. Am 30. Juni 2021 hat die Europäische Kommission eine Überarbeitung der Verbraucherkreditrichtlinie vorgelegt, unter anderem um den Veränderungen, welche die Digitalisierung mit sich gebracht hat, Rechnung zu tragen.

---

[3] Verordnung (EU) 575/2013.

3.2 Nationale Anforderungen

Unbenommen ist, dass sich KI in Zukunft weiterentwickeln wird und damit einhergehend auch veränderte und / oder neue Risiken auftreten werden. Umso wichtiger ist es, dass die Verordnung die Zukunft im Blick hat. Betrachtet man die bereits heute existierenden regulatorischen Anforderungen für die Banken-IT, so sind wir der Auffassung, dass den Bedenken, denen mit dem Verordnungsentwurf Rechnung getragen werden soll, bereits heute genügend begegnet wird.

3.2.1 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Branchenübergreifend unterliegt der Finanzsektor als sogenannte kritische Infrastruktur dem Anwendungsbereich des „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz), welches zu Ende Mai dieses Jahres in Kraft getreten ist. Hiernach soll eine Verwendung bestimmter IT-Komponenten durch Betreiber kritischer Infrastrukturen nunmehr untersagt werden können, wenn anzunehmen ist, dass der Einsatz dieser Komponenten die öffentliche Ordnung oder Sicherheit Deutschlands voraussichtlich beeinträchtigt. Die genauen Voraussetzungen werden durch die „Verordnung zur Bestimmung Kritischer Infrastrukturen" weiter konkretisiert. Jeder Einsatz kritischer Komponenten kritischer Infrastrukturen ist beim Bundesministerium des Innern anzuzeigen und wird von diesem geprüft.

3.2.2 Regelungen außerhalb des Kreditwesensgesetzes

Außerhalb des Kreditwesengesetzes wurden unter anderem

- die Solvabilitätsverordnung,
- die Großkredit- und Millionenkreditverordnung,
- die Liquiditätsverordnung und
- die Institutsvergütungsverordnung angepasst.

3.2.3 Nationale Umsetzung der europäischen Basel III-Regeln

Die nationale Umsetzung der europäischen Basel III-Regeln erfolgte in Deutschland 2013 vor allem

- durch Änderungen des Kreditwesengesetzes (KWG) und
- durch das CRD IV-Umsetzungsgesetz.

3.2.4 Abgleich bestehender Regelungen mit den Anforderungen aus den Art. 9ff der Verordnung

Kreditwürdigkeitsprüfungen werden bereits umfangreich von der nationalen Aufsicht geprüft. Würden weitere Conformity Assessments durchgeführt werden müssen, wie es die Verordnung fordert, gäbe es Überschneidungen, da der gleiche Sachverhalt doppelt geprüft würde. Dies gilt insbesondere für die Prüfungen, die im Rahmen des Supervisory Review and Evaluation Process (SREP) durchgeführt werden.

Zur Verdeutlichung unseres Arguments, dass die Institute bereits die Ziele der Anforderungen aus der Verordnung erfüllen bzw. die dort adressierten Risiken ausreichend in ihren Risikomanagementsystemen abbilden, stellen wir nachfolgend die in Deutschland geltenden Vorschriften dar. Diese sind aufgrund der europäischen Vorgaben national umgesetzt worden. Wir gehen daher davon aus, dass die anderen Mitgliedstaaten für die Finanzbranche entsprechende / gleichwertige Vorgaben aufgestellt haben.

Die Basis für Risikomanagementsysteme bilden die „Mindestanforderungen an das Risikomanagement" (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Auf der Grundlage ihres Gesamtrisikoprofils stellen Kreditinstitute sicher, dass wesentliche Risiken des Instituts in einem Risikoinventar dokumentiert werden. Die Risiken werden auf der Ebene des gesamten Instituts erfasst, unabhängig davon, in welcher Organisationseinheit oder welchem System die Risiken verursacht wurden.

Durch das Risikodeckungspotenzial werden diese laufend abgedeckt, wodurch die Risikotragfähigkeit gegeben ist. Institute verfügen über einen Prozess zur Sicherstellung der Risikotragfähigkeit, durch den sowohl die Fortführung des Instituts als auch der Schutz der Gläubiger vor Verlusten aus ökonomischer Sicht angemessen berücksichtigt werden. Zur Gewährleistung der Risikotragfähigkeit haben Finanzinstitute geeignete Risikosteuerungs- und Risikoüberwachungsprozesse eingerichtet.

Im Rahmen dieses Prozesses werden alle möglichen Risiken eines Finanzinstitutes identifiziert und adressiert. Der Vorstand wird regelmäßig und bei Bedarf über die sich verändernde Risikolandschaft sowie akute Risiken informiert.

Durch ein umfassendes internes Kontrollsystem sind Finanzinstitute in der Lage, alle Risiken zu identifizieren, zu überwachen und risikomitigierende Maßnahmen einzurichten.

Hinsichtlich des Einsatzes von Informationstechnologie hat die BaFin zusätzlich das "Rundschreiben zu bankaufsichtlichen Anforderungen an die IT 10/2017" (BAIT) herausgegeben, in dem der Rahmen für die

technisch-organisatorische Ausstattung der Institute – insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement – vorgegeben werden. Die BAIT dienen als Konkretisierung der MaRisk und fokussieren sich speziell auf IT- und Informationsrisiken.

Auf Basis der BAIT haben regulierte Institute eine Reihe von Anforderungen zu erfüllen, die sicherstellen, dass ihre IT-Systeme angemessen funktionieren und IT-Risiken adressiert werden. Die in diesem Zusammenhang zu beachtenden Schutzziele sind: Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität (Ein Beispiel für verschiedene Sicherheitsniveaus hinsichtlich der Vertraulichkeit von Informationen ist: öffentlich zugängliche Informationen, nur den Mitarbeitern eines Unternehmers bekannte Informationen, personenbezogene Daten etc.). Anhand dieser vier Schutzziele werden der Schutzbedarf und die Risikoklasse der jeweiligen Information definiert (z.B. low risk, medium risk, high risk), die zu jeweils davon abhängigen Maßnahmen führen. Die zu ergreifende Maßnahmen adressieren somit konkret die Risiken, denen die Informationen ausgesetzt sind. Die eingesetzten IT-Systeme und zugehörigen IT-Prozesse, durch die die Informationen verarbeitet werden, müssen dem Schutzbedarf und der Risikoklasse der Daten gerecht werden.

Es werden klare Verantwortlichkeiten und Pflichten sowie Überwachungs- und Steuerungsprozesse für Informationsrisiken eingerichtet. Weiterhin werden die risikoreduzierenden Maßnahmen definiert, die anschließend koordiniert, dokumentiert, gesteuert und überwacht werden.

Um einem dynamischen Umfeld gerecht zu werden, werden regelmäßig Risikoanalysen durchgeführt. Die Ergebnisse der Risikoanalyse sind an den Vorstand zu kommunizieren, von diesem zu genehmigen und in den Prozess des Managements der operationellen Risiken zu überführen.

Nachfolgend zeigen wir exemplarisch anhand einiger Beispiele, dass die Anforderungen der Art. 9ff der Verordnung bereits weitestgehend aufgrund aufsichtsrechtlicher oder sektorübergreifender Vorgaben von Kreditinstituten erfüllt werden.

<u>Art. 9: Risikomanagementsystem</u>
Die in Artikel 9 aufgeführten Anforderungen entsprechen in nahezu allen Aspekten den Anforderungen an Kreditinstitute gemäß CRR. Die Regelungen finden sich in zahlreichen Gesetzen, Verordnungen, Direktiven, Leitlinie (Guidelines), Empfehlungen (Recommendations) und Meinungen (Opinions) wieder, welche von Gesetzgebern, Standardsetzern (FSB, BCBS), Regelsetzern (ESA = EBA, ESMA, EIOPIA), Aufsehern (ECB-SSM sowie nationale Aufseher) publiziert werden. Zudem werden viele der vorgenannten Anforderungen in jedem EU-Mitgliedstaat individuell umgesetzt – hierbei kommt es in Teilen zu zahlreichen Erweiterungen der Anforderungen durch die nationalen Aufsichtsbehörden.

Darüber hinaus besteht in der Kreditwirtschaft das Prinzip der „Three-Lines-Of-Defense". Die Anwendung des Prinzips gewährleistet, dass ein institutsspezifisches Risikomanagementsystem entworfen, implementiert, gelebt, überwacht und bei Bedarf angepasst wird. Ein Wesensmerkmal ist es, dass Veränderungen bei Produkten, Kunden, Märkten sowie an Organisation, Prozessen und der IKT auf das jeweilige Risiko bezogen, analysiert werden. Hierbei muss vor Freigabe der Veränderungen, im Falle von Hoch-Risiko-Aspekten, klar dargestellt werden, welche Risiken bestehen und wie diese mitigiert werden können.

Das Risikomanagementsystem in Banken geht somit deutlich über die Anforderungen des Artikel 9 hinaus.

Art. 11: Technische Dokumentation

Gemäß BAIT 6 (40) werden die Funktionsweisen aller Anwendungen eines Finanzinstitutes sowie deren Entwicklung übersichtlich und für Dritte nachvollziehbar dokumentiert. Dies schließt mindestens eine Anwenderdokumentation, technische Systemdokumentation sowie eine Betriebsdokumentation ein.
Annex IV Technical documentation: Nicht notwendig: 1. d), f), 2. c), f), 4., 8.

Hierneben bestehen umfangreiche gesetzliche Vorgaben, welche Banken einzuhalten haben. Diese finden sich beispielsweise im Deutschen Gesetzestext, gemäß §25a KWG. So ist dem §25a zu entnehmen, dass „eine vollständige Dokumentation der Geschäftstätigkeit" vorzuliegen hat. Diese Regelungen gelten für alle in Artikel 22 der Verordnung (EU) Nr. 575/2013 genannten Unternehmen.

Art. 12: Aufzeichnungspflichten

Diese sind bereits abgedeckt durch BAIT (29, 30), daher bestehen die technischen Voraussetzungen für die Protokollierungen von als Handlungen definierten Aktivitäten. Dies wird bereits bei „robotic process automation" oder technischen Usern gemacht (wie bei Audit Logs).

Art. 14 Human Oversight (Art. 14)

§ 22 Abs. 3 DSGVO bietet bereits den von der Verordnung geforderten zusätzlichen Schutz des Human Oversight. Danach hat derjenige, der für eine automatisierte Verarbeitung verantwortlich ist, angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört Im Übrigen ist der Gedanke des Human Oversight im Prinzip des „Three-Lines-Of-Defense-Modell" grundsätzlich angelegt, siehe oben Ausführungen zu Art. 9 Risikomanagementsystem.

Art. 15: Genauigkeit, Robustheit und Cyber-Sicherheit

Die Informationen und IT-Systeme sind in den Instituten hinreichend gesichert, die Intention des europäischen Gesetzgebers ist in Bezug auf Art. 15 damit erfüllt. Hinsichtlich der Cyber-Sicherheit haben wir

oben unter Ziffer 3.1.5 bereits Ausführungen zu DORA gemacht. Überdies hat die European Banking Authority (EBA) neue Leitlinien zu IKT und Sicherheitsrisikomanagement – die „EBA Guidelines on ICT and security risk management" – veröffentlicht4, die am 30. Juni 2020 für die nationalen Aufsichtsbehörden in Kraft traten. Nachdem eine Anpassung der BAIT letztmalig im Jahr 2018 erfolgte, wurden diese bereits an die EBA-Leitlinien angepasst und umfassend aktualisiert. Eine Veröffentlichung der BAIT-Novelle wird zeitnah in 2021 erwartet. Die IT-spezifischen Anforderungen Informationssicherheit sind in diesen umfassend geregelt.

Auf nationaler Ebene trat zudem die KRITIS-Verordnung und das 2. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in Kraft, siehe hierzu Ziffer. 3.2.1.

Die vorgenannten Regelungen zeigen auf, unter welch starker Regulierung und Aufsicht die Branche bereits hinsichtlich der Anforderungen in den Art. 9ff des Verordnungsvorschlages steht. Hieran ändert nach unserer Auffassung auch die zunehmende Verwendung von KI nichts. Kreditinstitute sind angemessen aufgestellt, um aktuelle sowie zukünftigen Risiken zu adressieren und angemessen zu steuern. Werden hingegen über die KI-Verordnung nun Regelungen aufgestellt, die zumindest für die Finanzbranche bereits weitestgehend reguliert sind, kann es nicht nur zu unnötigen Dopplungen kommen, sondern vielmehr noch zu widersprüchlichen Anforderungen, die sowohl die Aufsicht als auch die Institute vor enorme Schwierigkeiten stellen.

Dies gilt insbesondere für ähnliche von ihrer Zielsetzung zwar vergleichbare, im Detail aber unterschiedliche Anforderungen, von denen erst nach einer umfangreichen Detailanalyse genau festgestellt werden kann, wie diese sich im Detail von den heute von Kreditinstituten eingesetzten Lösungen unterscheiden und damit zwar im Einklang mit den Zielen des Verordnungsvorschlags stehen, aber nicht mit dessen Anforderungen vollständig übereinstimmen. Beispielsweise gilt dies für besonders für die Daten-bezogenen Anforderungen. Um diese Anforderungen vollständig zu erfüllen, wäre folglich mit einem hohen zusätzlichen Aufwand zu rechnen, ohne dass diesem ein zusätzlicher Nutzen für die Verbraucher gegenüberstünde. Daran ändert auch die vorgesehene Bestandsschutzregelung für die bestehenden Verfahren nur wenig, da diese bei Neuentwicklungen und wesentlichen Änderungen nicht mehr greift und z.B. auch die Daten bezogenen Anforderungen unmittelbar mit dem Einsatz des neuen Verfahrens gelten würden.

Als Beispiel kann gelten, dass wesentliche Änderungen und Neuentwicklungen von Verfahren zur Bewertung der Kreditwürdigkeit erforderlich werden können, wenn im Laufe der Zeit die Prognosegüte der Modelle abnimmt und diese dann auch keine Akzeptanz der Aufsichtsbehörden mehr finden würden. Hier läge es nicht im Interesse des Verbrauchers, mit Verfahren bewertet zu werden, deren Prognosekraft im Vergleich zu einer Neuentwicklung nicht mehr als zufriedenstellend zu bezeichnen ist. Verbraucher sollten

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.

hier von den besten verfügbaren Verfahren zur Beurteilung ihrer Kreditwürdigkeit profitieren können. Dies stellt am besten sicher, dass diejenigen Verbraucher, die kreditwürdig sind, auch einen Kredit zu günstigen Konditionen erhalten.

4 Forderungen und Vorschläge der Deutschen Kreditwirtschaft

4.1 Ausnahme vom Anwendungsbereich in Art. 2 und Verzicht auf Ziffer 5b) in Annex III

Die Deutsche Kreditwirtschaft fordert aufgrund der bereits existierenden umfangreichen bereichsspezifischen Regulierungen den europäischen Gesetzgeber auf, die Finanzbranche aus dem Anwendungsbereich des Art. 2 der Verordnung auszunehmen. Aufgrund der vorliegenden bankaufsichtsrechtlichen Vorgaben sind etwaige Risiken ausreichend adressiert. Dies gilt nach unserer Auffassung für jedwedes Risiko, insbesondere aber auch für Hoch-Risiko-Anwendungen.

Ein konkreter Formulierungsvorschlag für die sektorspezifische Ausnahme findet sich hierzu in Ziffer 5.1. In der Folge wäre eine Streichung des Annex III 5 b) folgerichtig.

Der europäische Gesetzgeber subsumiert die Kreditwürdigkeitsprüfung sowie die Kreditpunktebewertung unter die in Annex III aufgeführten hohen Risiken, da insbesondere die Gefahr einer Diskriminierung durch in Datensätzen vorhandenen Vorurteile (bias) bestünde.

Aus unserer Sicht ist diesen Bedenken aber schon heute ausreichend Rechnung getragen und die angenommenen Risiken sind bereits so weit minimiert, dass nicht per se ein hohes Risiko in diesem Bereich unterstellt werden kann.

Auf Grundlage der oben aufgeführten bereits existierenden regulatorischen Vorgaben werden bestehende Risiken kontinuierlich überwacht, regelmäßig neue Risiken identifiziert, in das Risikoinventar aufgenommen, gemäß ihrer Tragweite klassifiziert und auf dieser Basis Maßnahmen entwickelt. Insbesondere IT-Risiken werden gemäß der Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der zu schützenden Daten behandelt. Somit sind Finanzinstitute ausgesprochen gut aufgestellt, um den geänderten Anforderungen und Risiken neuer Technologien zu begegnen.

Legt man diesen Ansatz zugrunde, kann die Kreditwürdigkeitsprüfung natürlicher Personen nicht per se als Hoch-Risiko-Tatbestand klassifiziert werden. Vielmehr gilt es, die mit einer Kreditwürdigkeitsprüfung und Kreditpunktebewertung im Zusammenhang stehenden Risiken zu identifizieren und zu adressieren. Die Risikomanagementprozesse der Finanzinstitute sind bereits entsprechend aufgestellt und in der Lage, dies zu tun.

4.2 Aufnahme sektorspezifischer Verweise in die Verordnung

Sollte der Gesetzgeber unserem Vorschlag eine Ausnahme der Finanzbranche aus dem Anwendungsbereich des Artikel 2 nicht folgen, schlagen wir ersatzweise vor, in die Verordnung sektorspezifische Verweise in die Art. 9ff aufzunehmen, wie dies in Art. 17 – Qualitätsmanagementsystem mit dem Verweis in Absatz 3 auf die Richtlinie 2013/36/EU vorgenommen wurde.

Es ist unbenommen, dass es Kontexte gibt, die ein besonderes Risiko für Menschen, die Gesellschaft und ihre demokratischen Werte darstellen können. Auch wir vertreten die Auffassung, dass solche Risiken adressiert werden sollten, um etwaigen Gefahren vorzubeugen, die aus der Verwendung von KI resultieren können.

Nach unserer Ansicht sollten Unternehmen in der Lage sein, den Risiken zu begegnen, die in den Anwendungsfällen von Annex III immanent enthalten sind. Das ist bei Finanzinstituten hinsichtlich Kreditwürdigkeitsprüfungen und Kreditpunktebewertungen aufgrund der bisherigen Regulierungen und ihrer Risikomanagementsysteme bereits der Fall.

Die Kreditwürdigkeitsprüfung in Banken unterliegt bereits einem strengen Aufsichtsregime. Die zuständigen Behörden überwachen diese Vorgänge fortlaufend. So werden nicht nur Verbraucher und Anleger geschützt, sondern auch die Finanzstabilität gewährleistet. Der Einsatz statistischer Verfahren zur Ermittlung einer Bewertungsfunktion, ggf. erweitert um eine Bayes-Funktion, ist spätestens seit 2005 Standard in den Kreditinstituten, nachdem diese bereits seit Mitte der 90er Jahre zunehmend eingesetzt und dann der Bankpraxis entsprechend auch zur risikoorientierten Eigenkapitalunterlegung der Kreditrisiken nach Basel II genutzt werden durften. Insofern bestehen in der Kreditwirtschaft Jahrzehnte lange Erfahrungen. Auch die Aufsichtsbehörden verfügen durch die Prüfung entsprechender Verfahren bereits über rund 15 Jahre Erfahrung. Zusätzliche Anforderungen an die Kreditvergabe sind daher nicht erforderlich.

Die Verbraucher profitieren zudem davon, dass sie schnell und unkompliziert eine Kreditzusage erhalten können. Dies hat dazu beigetragen, die Kreditversorgung der Verbraucher in den letzten Jahren zu steigern. Zudem besteht nach den datenschutzrechtlichen Vorgaben ein Auskunftsrecht, so dass bei einer Kreditablehnung eine Überprüfung und Korrektur der Kreditentscheidung erfolgen kann. Wir sehen deshalb, verglichen mit manuellen Entscheidungsprozessen, kein erhöhtes Risiko für natürliche Personen einer diskriminierenden Kreditentscheidung zu unterliegen.

5 Regelungsspezifische Anmerkungen zum Verordnungsvorschlag

5.1 Art. 2, Einfügung eines neuen Absatzes (3):

„Für Hoch-Risiko-Systeme, die von Unternehmen entwickelt und / oder eingesetzt werden, die den Vorschriften der Verordnung (EU) Nr. 575/2013 (CRR)
unterliegen, gilt nur Art. 84 dieser Verordnung.

5.2 Art. 3: Definitionen

Die Deutsche Kreditwirtschaft ruft den europäischen Gesetzgeber dazu auf, die in dem Verordnungsentwurf vorgenommene Definition von KI noch einmal zu überdenken und sich dem internationalen Verständnis von KI anzunähern, welches deutlich enger gefasst ist, als es der Verordnungsvorschlag vorsieht, siehe beispielhaft die Definition der OECD.

Danach ist ein KI-System ein maschinenbasiertes System, das für menschlich definierte Ziele Vorhersagen, Empfehlungen oder Entscheidungen treffen kann, die reale oder virtuelle Umgebungen beeinflussen. KI-Systeme sind so konzipiert, dass sie mit unterschiedlichem Grad an Autonomie arbeiten[5]. Die Definition der Verordnung geht deutlich darüber hinaus, indem jedes regelbasierte Verfahren unter den KI-Begriff fallen soll, unabhängig davon, inwieweit Autonomie überhaupt gegeben ist. Unternehmen müssen mit rechtssicheren Rahmenbedingungen in der Lage sein, Risikostrategien und entsprechen Mitigationsprozesse zu gestalten, die längerfristig Bestand haben können.

Auf statistischen Verfahren entwickelte Score-Karten für natürliche Personen sollten von dieser Verordnung explizit ausgenommen werden. Diese Verfahren sind bereits zum Teil seit Jahrzehnten bewährt haben und werden erfolgreich von den Instituten eingesetzt. Seit beinahe 15 Jahren werden sie auch von den Aufsichtsbehörden geprüft und haben einen nachweislich hohen Nutzen für die Verbraucher, um eine schnelle, unkomplizierte und mit niedrigen Prozesskosten verbundene Kreditgewährung zu unterstützen.

Die deutsche Bankenaufsicht, BaFin, verweist ihrerseits darauf, dass die aktuellen Definitionen von künstlicher Intelligenz keine trennscharfe Abgrenzung von klassischen statistischen Verfahren und dabei verwendeten Algorithmen ermöglichen und die Weiterentwicklung der Definition zu den Herausforderungen zählt, vor denen Aufsicht, Regulierung und vor allem Standardsetzer stehen.[6]

---

5 OECD Council „Recommendation of the Council on Artificial Intelligence“, abrufbar unter: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

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

Aufgrund der Weite der Definition des Verordnungsvorschlags ist nun im Grunde jede Art von Software erfasst, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist. Damit ist die Definition sehr starr und nicht dynamisch, was bei einer dynamischen Technologie wie KI nicht sinnvoll und zukunftssicher ist. Es wird zu wenig unterschieden, durch welche Charakteristika einer Technologie, wie KI, bestimme Risiken entstehen und zu mitigieren sind. Eine gesamte Technologie pauschal – d.h. unabhängig von ihrer konkreten Ausprägung z.B. dem Grad der Autonomie - als risikoreich einzustufen, greift fehl, da nicht berücksichtigt wird, in welchem Ausmaß sich ein wirkliches Risiko durch die eingesetzte KI überhaupt realisieren kann.

Die Definition umfasst aus unserer Sicht unterschiedliche Arten von technischen Methoden, was vor dem Hintergrund des eigentlich risikobasierten Ansatzes der Verordnung, aber auch der jeweiligen Methode selbst, nicht angemessen erscheint.

In Bezug auf die Finanzbranche bedeutet der Definitionsvorschlag, dass undifferenziert der Einsatz traditioneller statistischer Verfahren, wie sie zum Teil bereits seit Jahrzehnten, spätestens aber seit Basel II in Kreditinstituten eingesetzt werden, zur Einstufung als KI führt. Dies erscheint aus Sicht der Deutschen Kreditwirtschaft eine unnötige Überregulierung. Vielmehr sollte es der Anspruch eines modernen Regulierungsrahmens sein, Unternehmen zu befähigen, unter risikoorientierten Gesichtspunkten zu entwickeln und einzusetzen.

Daher verwundert es, dass auch regelbasierte Verfahren, die schon lange bei Kreditinstituten im Einsatz und von den Aufsichtsbehörden überwacht werden und genehmigt sind, nun von der Verordnung erfasst werden sollen. Bei regelbasierten Verfahren, statistischen Verfahren, mathematischen Funktionen oder Klassifikationszuordnungen wird seitens der Banken eindeutig vorgegeben, z.B. welche Klassifikationsergebnisse aus bestimmten Datenkonstellationen abzuleiten sind. Sie werden von Menschen mit Hilfe statistischer Verfahren (weiter-)entwickelt und vermögen dies nicht selbst zu tun. Eigenständiges Arbeiten ist diesen Verfahren und Methoden nicht immanent. Daher haben sie mit dem gängigen Verständnis von KI nichts gemein. Risiken dieser Methoden werden bereits in den Risikomanagementsystemen der Finanzinstitute angemessen aufgenommen und gemäß ihrer Tragweite adressiert.

Auch bei neuen Technologien, wie z.B. dem sogenannten maschinellen Lernen, entstehen keine zusätzlichen Risiken, die die Finanzinstitute nicht angemessen in ihren bestehenden Systemen adressieren können.

Zu strenge Regelungen sind auch nicht im Interesse der Verbraucher, wie eine Umfrage des Europäischen Verbraucherverbands gezeigt hat. Verbraucher sehen auch das Nützliche in KI. Die Befragten scheinen zu hoffen, dass KI helfen wird, einige grundlegende Probleme des menschlichen Lebens zu lösen. In allen an der Umfrage beteiligten Ländern befanden die Teilnehmer folgende Dienstleistungen, die auf maschinellen Berechnungen basieren, etwas oder sogar sehr nützlich:

- Die Vorhersage von Verkehrsunfällen (91%)
- Vorhersage von Gesundheitsproblemen (87%)
- Vorhersage ihrer finanziellen Probleme (81%)[7].

Laut der Umfrage haben Verbraucher Bedenken hinsichtlich des Schutzes ihrer Privatsphäre, der Manipulation ihrer Entscheidungen durch KI, der Risiken von Diskriminierung, der Zuverlässigkeit und Sicherheit von KI sowie der Verteilung von Verantwortung und Haftung[8].

Diese Bedenken sind zu Recht nachvollziehbar und müssen – wie in der Verordnung bezweckt - angemessen berücksichtigt werden, um einen starken Schutz für Verbraucher zu schaffen und deren Vertrauen in diese Technologie zu gewährleisten. Dies kann aber nur sinnvoll umgesetzt werden, wenn auf den jeweiligen Einsatzzweck der KI abgestellt wird: Die Regulierung von KI muss proportional zu dem Risiko sein, das sie minimieren soll.

Vor diesem Hintergrund schlagen wir folgende Definition für KI vor:

- **'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.*

Es wird ferner vorgeschlagen, die Kriterien für die Einstufung eines Verfahrens als KI in einem delegierten Rechtsakt näher zu spezifizieren, da die Verwendung der in Anhang I genannten Techniken insbesondere im Hinblick auf die Verwendung statistischer Ansätze einschließlich Bayes-Schätzungen zu weitgehend ist und damit auch traditionelle statistische Ansätze, wie sie bereits seit Jahrzehnten verwendet werden, umfasst würden.

Darüber hinaus unterbreiten wir nachfolgend weitere Vorschläge zur Überarbeitung der in Art. 3 vorgenommenen Definitionen, um Unklarheiten auszuräumen und Missverständnissen vorzubeugen:

- '**provider**': Definition von 'Provider' ist nicht klar genug gefasst, da hiervon der Entwickler selbst, aber auch derjenige erfasst wird, der KI-Systeme entwickeln lässt. Die Definitionen werden dem häufigen Dreiklang aus IT-Provider, Finanzinstitut, und Kunde nicht gerecht, der oft vorliegt. Ein provider sollte nur entwickeln. Auch white-label-Anbieter sollten miteingeschlossen werden.

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.

Vorschlag: *„'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'**: Die Definition ist nicht klar, da alles damit gemeint sein kann.

  Vorschlag: Diese Definition herauszunehmen.

- `**placing on the market'**, `**making available on the market'** und `**putting into service'** sind sehr ähnlich und sehr unklar voneinander getrennt.
  Vorschlag: (9) und (11) herausnehmen, und nur (10) bestehen lassen.

- **`remote biometric identification system'**: Zunächst muss der Begriff **`**remote**`** definiert werden, da es hier unterschiedliche Auslegungen geben kann. Des Weiteren ist unklar, ob Know-Your-Customer-Prozesse oder biometrische Authentifizierungsverfahren eingesetzt werden, eingeschlossen werden. Weiterhin klingt es so, dass Remote Biometric Identification-Systeme („RBI") nicht als solche benannt werden, wenn Personen wissen, dass sie identifiziert werden. Auch dieser Umstand bedarf einer Klarstellung. Zudem ist unklar, inwieweit ein RBI-System als high risk gilt, wenn es in der Öffentlichkeit eingesetzt wird. Hier muss auch eine einheitliche Definition von „Öffentlichkeit" bzw. „public space" gegeben werden, da dies in den Mitgliedstaaten unterschiedlich definiert wird.

5.3 Art. 10: Daten und Daten-Governance (Art. 10):

Insgesamt scheint der Artikel übersteuert aufgrund der bestehenden Regelung der GDPR. Es fehlt zudem der Verweis auf BCBS 239 „Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung" des Basler Ausschuss. Die nationale Umsetzung ist in MaRisk AT 4.3.4 erfolgt.

- Art 10 Ziffer 3: „Training, validation and testing data sets shall be relevant, representative, free of errors and complete." Das ist praxisfern. Die Kriterien sind nicht messbar, insbesondere Vollständigkeit. Die Anforderungen entsprechen nicht den Notwendigkeiten und der Praxis für die Entwicklung valider und gut kalibrierter Scoring-Funktionen / Score-Karten für Privatkunden. Die Entwicklung dieser Score-Karten ist darauf fokussiert, eine hohe Prognosegüte zu erreichen. Dies liegt auch im Interesse der Verbraucher, um deren Kreditwürdigkeit möglichst zutreffend zu ermitteln. Dazu werden z. B. bei der Entwicklung von Score-Karten auf Basis varianz- und regressionsanalytischer Ansätze alle Daten in eine Funktion einbezogen, die multivariat, d. h. in ihrem Zusammenspiel einen hohen Beitrag zu einer zutreffenden Bewertung der Kreditwürdigkeit leisten. Das setzt nicht unbedingt die Befüllung eines Datenfeldes voraus, weil bereits die

Angabe oder Nichtangabe einer Information im Zusammenspiel mit weiteren Informationen einen Beitrag zur Verbesserung der Prognosegüte leisten kann. Der Verzicht auf solche Daten wegen der Vollständigkeitsanforderung würde die Anpassung von Score-Karten und eine verschlechterte Prognosegüte aufgrund des Verzichts signifikant erklärungsfähiger Informationen zur Folge haben. Infolgedessen wäre mit höheren Risikokosten, die von den Kreditnehmern über den Kreditzins zu tragen wären, oder mit einer restriktiveren Annahmepolitik zu rechnen, die Kreditnehmer mit einer etwas schwächeren Bonität eher von einer Kreditvergabe ausschließen würden. Das kann nicht im Interesse der Kunden sein.

- „free of errors": Diese Formulierung ist aus unserer Sicht praxisfern. Mögliche Fehler, sofern es sich nicht um offensichtliche Ausreißer handelt, die eliminiert werden, werden in den Daten üblicherweise bei der Entwicklung implizit berücksichtigt. Da eine einzelne Information nur einen begrenzten Beitrag zur Bewertung der Kreditwürdigkeit liefert und es hier auf das Zusammenspiel einer Reihe von Informationen ankommt, die zusammen genommen eine optimale und im Zeitablauf stabile Bewertung der Kreditnehmer ermöglichen sollen, sind die Verfahren bis zu einem gewissen Grad fehlertolerant.

5.4 Art. 13: Transparenz und Bereitstellung von Informationen für die Nutzer

Art. 13 Ziffer 1: Die Anforderung gem. Art. 13 (1) S. 2, dass der Betrieb der Hoch-Risiko-Systeme hinreichend transparent zu sein hat, damit die Nutzer die Ergebnisse des Systems angemessen interpretieren und verwenden können, ist grundsätzlich zu begrüßen.

Allerdings ist aus unserer Sicht zu unscharf formuliert, was genau mit Transparenz gemeint ist und welche Erwartungshaltung an die Unternehmen gestellt wird im Hinblick auf die Erklärbarkeit von Algorithmen. Die Frage nach der Erklärbarkeit von Algorithmen kann nämlich durchaus vielschichtig beantwortet werden, weil die Algorithmen selbst vielschichtig sind.

Es sollte daher genügen, wenn die Wirkweise eines Algorithmus erklärbar und validierbar ist. So nach unserem Verständnis auch die High-level expert group on artificial intelligence:

„[…] Technische Erklärbarkeit setzt voraus, dass die von einem KI-System getroffenen Entscheidungen vom Menschen verstanden und rückverfolgt werden können. Darüber hinaus müssen möglicherweise Kompromisse zwischen einer verbesserten Erklärbarkeit eines Systems (was die Präzision beeinträchtigen kann) und mehr Präzision (auf Kosten der Erklärbarkeit) eingegangen werden"[…][9].

Die Bafin hat hierzu in einem am 15. Juli 2021 veröffentlichten Diskussionspapier ähnlich ausgeführt:

[9] Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai, dort: Ziffer 4 HLEG, RN 75ff.

„Je komplexer und höherdimensional der vom Modell abbildbare Hypothesenraum ist, desto schwieriger wird es, den funktionalen Zusammenhang zwischen Input und Output (d. h. die im Training konkretisierte Hypothese) verbal oder durch mathematische Formeln zu beschreiben, und desto weniger sind die Berechnungen durch Modellierer, Anwender, Validierer und Aufseher im Detail nachvollziehbar. Dies führt zu einer erschwerten Nachvollziehbarkeit der Modellierung und ggf. auch zu einer erschwerten Überprüfung der Validität der Modellergebnisse."[10]

Insbesondere müssen die Anforderungen aus Art. 13 der Verordnung den Nutzer in die Lage versetzen, Auskunfts- und Transparenzverpflichtungen aus anderen rechtlichen Vorgaben, wie z.B. der GDPR, gegenüber dem Endnutzer zu erfüllen. Gleichzeitig muss gewährleistet sein, dass die Informationstiefe den Schutz des geistigen Eigentums des Anbieters nicht ungebührlich beeinträchtigt und die gesetzlichen Bestimmungen, insbesondere des Geschäftsgeheimnisgesetzes, wahrt bleiben.

5.5 Art. 53ff.: Sandboxes

Wir begrüßen die Einrichtung regulatorisch begleiteter Sandboxes zur Förderung von KI-Innovation. Allerdings sehen wir in diesem Abschnitt noch Nachschärfungsbedarf. Die Definition von „Regulatory Sandbox" ist nicht klar. Der Verordnungsentwurf sollte entsprechend ergänzt werden.

Weiterhin ist das Ziel der Sandboxes unklar, z. B. Entwicklung neuer Anwendungen, Umsetzung von Use Cases, Skalierung von schon umgesetzten Anwendungen.

Zudem ist nicht ersichtlich, welche regulatorischen Anforderungen in den Sandboxes gelten sollen, da es einerseits heißt, es würde eine verbesserte Umgebung bereitgestellt, andererseits müssten sich alle Teilnehmer an alle regulatorischen Anforderungen halten. Darüber hinaus ist nicht definiert, nach welchen Kriterien Unternehmen Zugang hierzu erhalten. Hier bedarf es einer Konkretisierung der Vorschriften. Hinzukommt, dass Unklarheit in Bezug auf die Frage besteht, ob im Rahmen der Nutzung von Sandboxes auch datenschutzrechtliche Erleichterungen hinsichtlich der Verarbeitung personenbezogener Daten zum Tragen kommen könnten, z. B. bei Änderung des Verarbeitungszweckes.

Insbesondere sehen wir die Gefahr von unfairen Wettbewerbsbedingungen, da nur ausgewählte Unternehmen Zugang zu den Sandboxes erhalten. Es muss allen Marktteilnehmern die Möglichkeit gegeben werden, bei Innovationen regulatorisch begleitet zu werden, damit sich die Sinnhaftigkeit von Investitionen möglichst frühzeitig überprüfen lässt und nicht unnötig Geld und Zeit aufgewandt wird.

10 „Maschinelles Lernen in Risikomodellen – Charakteristika und aufsichtliche Schwerpunkte", abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2021/meldung_2021_07_15_Konsultation_Maschinelles_Lernen.html, S. 14, Ziffer 3.

Weiterhin fordern wir, dass der Bericht über die Arbeit in den Sandboxes, welcher dem European AI Board und der EU-Kommission zur Verfügung gestellt wird, für alle Unternehmen der EU einsehbar ist, so dass Erfahrungen über die Entwicklung und den Einsatz von KI weitergegeben werden können und so Innovation gefördert wird. Falls der Bericht vertrauliche Informationen beinhalten wird, sollte eine Zusammenfassung mit den wichtigsten Erfahrungen aus den Sandboxes öffentlich verfügbar sein, soweit diese nicht vertraulich sind.

5.6 Art. 73: Ausübung der Befugnisübertragung

In Gesprächen mit der Kommission wurde deutlich, dass für die Umsetzung der Anforderungen für neu als high risk eingestufte KI-Systeme eine Übergangsphase von zwei Jahren gelten soll – dies sollte hier schriftlich ergänzt werden.

Vorschlag zur Ergänzung von Art. 73 durch einen zusätzlichen Absatz 6:
"(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: Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme

Bestandsschutz ist nur insofern gegeben, als dass bereits auf den Markt gebrachte oder im Einsatz befindliche Hoch-Risiko-KI-Systeme sich nur dann im Anwendungsbereich befinden, wenn sie nach dem Anwendungszeitpunkt (24 Monate nach Inkrafttreten) wesentliche Änderungen in ihrem „Design" oder dem Verwendungszweck erfahren (siehe Artikel 83 (2)). Zudem ist fraglich, was unter wesentlichen Designveränderungen zu verstehen ist.

In jedem Fall sollte für Verfahren mit wesentlichen Designveränderungen im Sinne einer Weiterentwicklung, die objektiv zu einer Verbesserung der Bewertungsqualität führen, auch nach Ablauf des Umsetzungszeitraums nach Art. 85 Abs. 2 ein zweijähriger Umsetzungszeitraum eingeräumt werden, um die Anforderungen dieser Verordnung im Hinblick auf das Verfahren und die Anforderungen an die Daten vollständig umzusetzen. Damit kann vermieden werden, dass wesentliche Weiterentwicklungen zur Verbesserung der Bewertungsqualität nur deshalb nicht umgesetzt werden, weil zu diesem Zeitpunkt noch nicht alle Anforderungen der Verordnung vollständig umgesetzt sind.

5.8 Zugang zu Daten / Level-Playing-Field / Förderung

Die Unternehmensberatung PricewaterhouseCoopers hat Banken und Versicherungsunternehmen aus der DACH-Region über den Einsatz von KI befragt. 69% der Unternehmen machen einen Mangel an verfügbaren Daten als Hindernis für eine Adaption aus. 67% der befragten Unternehmen kämpfen außerdem

mit Budgetrestriktionen und unzureichender Finanzierung für entsprechende Projekte, 64% der Unternehmen mangelt es an Mitarbeitern mit Kompetenz, um Fragen zur Etablierung von KI zu beantworten wie z. B. welcher Geschäftsbereich einen angemessenen Anknüpfungspunkt für die Etablierung von KI-Projekten im operativen Geschäft bietet oder welche Abteilung die Finanzierung des Integrationsprozesses sicher stellt.[11]

Auch, wenn es sich um eine auf den DACH-Bereich begrenzte Umfrage nur bei Banken und Versicherern handelte, ist davon auszugehen, dass die dargestellten Schwierigkeiten branchenübergreifend und europaweit vorhanden sind.

Aus Sicht der Deutschen Kreditwirtschaft geht der Verordnungsvorschlag bei den Themen „Zugang zu Daten, Level-Playing-Field und Förderung von KI" nebst korrelierendem Know-how nicht weit genug. Es ist nicht ausreichend, auf regulatorische Sandkästen und Datenpools auf der Basis von GaiaX zu setzen, sondern nötig ist auch eine Reform der aktuellen Regulierung von Datenaustausch und Datenschutz. Sonst besteht die Gefahr, dass sich Innovatoren an die nationalen Gesetzgeber wenden, um mehr Flexibilität zu erlangen, z. B. bei der Datenschutzgrundverordnung (GDPR), was letztendlich den Zweck solcher Regelungen, nämlich die Schaffung eines harmonisierten Level-Playing-Fields in der gesamten EU, zunichtemachen könnte. Auch muss ein Investitionsplan vorgelegt werden, inklusive Kriterien, nach denen Investitionsvorhaben ausgewählt werden. Ist dies nicht der Fall, werden Unternehmen zwar den Willen zum Einsatz von KI haben, aber nicht die Möglichkeiten. Auch Initiativen zur Stärkung von Wissen, Skills und Forschungsvorhaben müssen angestoßen werden.

5.9 Biometrische Identifizierung von natürlichen Personen

Wir haben verstanden, dass nach den neuen Regeln alle KI-Systeme, die für die biometrische Identifizierung von Personen aus der Ferne eingesetzt werden sollen, als risikoreich eingestuft werden und von vornherein einer Konformitätsbewertung durch Dritte unterliegen, einschließlich der Anforderungen an die Dokumentation und die menschliche Aufsicht. Wir gehen davon aus, dass die Finanzdienstleister und ihre Anbieter, die sich auf die biometrische Identifizierung verlassen, um Kunden aus der Ferne zu betreuen und die Know-You-Customer-Anforderungen zu erfüllen, nicht in den Anwendungsbereich der vollständigen Anforderungen der KI-Verordnung fallen. Diesbezüglich bitten wir vorsorglich um Klarstellung.

6 Schlussbemerkung

Wir unterstützen die Kommission in ihren Bemühungen, einen klaren Rechtsrahmen für KI zu schaffen, der Innovationen fördert und gleichzeitig Sicherheit für alle Marktteilnehmer bietet. Besonders unterstützen wir den Ansatz, die "Digitalisierung mit menschlichem Antlitz" zu fördern. Wir glauben, dass ethisch

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

programmierte KI in Zusammenarbeit mit menschlicher Expertise von großem Wert für die europäische Gesellschaft sein wird. Ein Kernpunkt in diesem Zusammenhang wurde mit dem Entwurf umgesetzt: Die Verantwortung einer Handlung liegt immer bei einem Menschen. Um dies sicherzustellen, muss die Entwicklung eines KI-Systems nachvollziehbar dokumentiert sein und alle Handlungen des KI-Systems aufgezeichnet werden, so dass Entscheidungen rückverfolgt und revidiert werden können. Auch muss garantiert sein, dass eine Bewertung eines KI-Systems jederzeit von einem Menschen außer Kraft gesetzt werden kann.

KI stellt ein enormes Potenzial für die europäische Wirtschaft dar. KI-Experten haben große Fortschritte in der Forschung gemacht. Heute steht die EU – nach China – an zweiter Stelle bei der Veröffentlichung von Forschungsergebnissen. Allerdings werden zu wenige dieser Forschungsergebnisse in Produkte und Dienstleistungen umgesetzt. Um das aber möglich zu machen, muss die EU ein attraktiver Standort für Unternehmer werden, an dem Risikobereitschaft geschätzt wird und Innovationsgeist auf entsprechende Bedingungen und ein unterstützendes Ökosystem trifft. Denn Innovation lässt sich nicht von der politischen Ebene auf die Wirtschaft übertragen, sie entsteht unter guten Rahmenbedingungen in den Unternehmen selbst.

Wir appellieren daher an den europäischen Gesetzgeber, die Entwicklung und Anwendung von KI-Technologie mit ihrer Regulierung zuvorderst zu fördern und lediglich die Anwendungsfälle zu regulieren, bei denen sich tatsächlich Risiken realisieren können, die nicht bereits durch die betroffenen Branchen identifiziert und hinreichend mitigiert werden (können). Auf diese Weise werden wir ein aktives, erfolgreiches und nachhaltiges KI-Ökosystem in der EU aufbauen.

Wir sind der Meinung, dass der aktuelle Anwendungsbereich des Verordnungsvorschlages zu weit gefasst ist. Auf statistischen Verfahren entwickelte Score-Karten für natürliche Personen sollten von dieser Verordnung explizit ausgenommen werden. Diese Verfahren sind bereits zum Teil seit Jahrzehnten bewährt und werden erfolgreich von den Instituten eingesetzt. Seit beinahe 15 Jahren werden sie auch von den Aufsichtsbehörden geprüft und haben einen nachweislich hohen Nutzen für die Verbraucher, um eine schnelle, unkomplizierte und mit niedrigen Prozesskosten verbundene Kreditgewährung zu unterstützen. Auch andere Fallgestaltungen, bei denen KI im eigentlichen Sinne im Zusammenhang mit der Bewertung der Kreditwürdigkeit eingesetzt wird, sind durch bestehende Anforderungen an Kreditinstitute vollumfänglich adressiert, so dass die vom Verordnungsgeber unterstellten Risiken in der Praxis nicht zum Tragen kommen.

***