bankenverband

Positionspapier

Handlungsfelder für eine bessere Nutzung der Cloud-Technologie

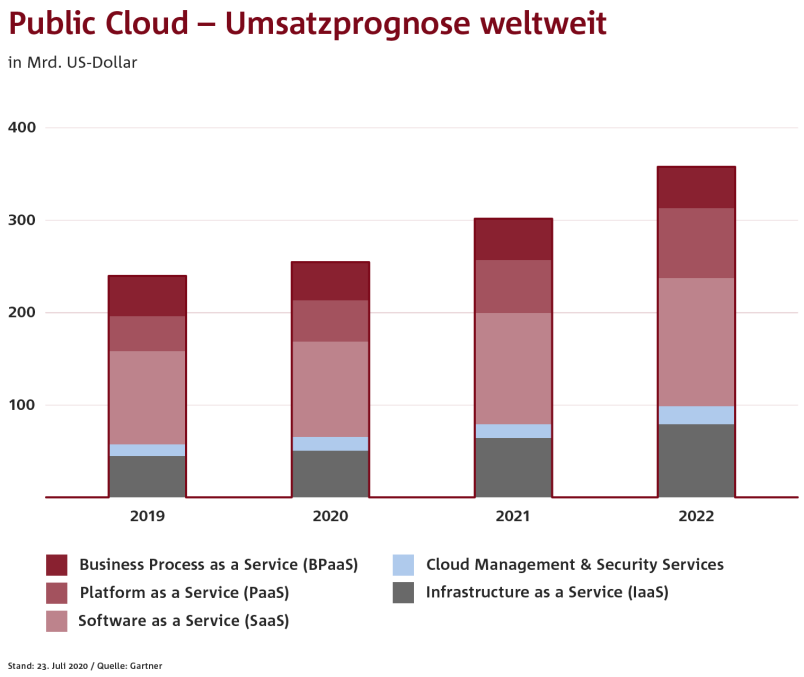
September 2021

Bundesverband deutscher Banken e. V.
Burgstraße 28
10178 Berlin
Telefon: +49 30 1663-0
Telefax: +49 30 1663-1399
www.bankenverband.de
USt.-IdNr. DE201591882

Inhaltsverzeichnis

1 Executive Summary

Die Gestaltung der digitalen Zukunft und die Sicherung der digitalen Wettbewerbsfähigkeit gehören zu den zentralen Herausforderungen der kommenden Jahre und rangieren auf der Agenda vieler Akteure weit oben. In ihrer Digitalstrategie formuliert die Europäische Kommission den Anspruch, Europa auf diesem Gebiet zu einem globalen Vorreiter zu entwickeln und den Nutzen digitaler Technologien zum Wohl der Menschen in den Mittelpunkt zu stellen. Seit Jahren ist die Digitalisierung ein Schwerpunktthema, dem sich auch der Bankenverband im Kontext zahlreicher Initiativen, Projekte, Veranstaltungen und Veröffentlichungen widmet. Dabei spielt das Cloud Computing als wesentliche technologische Grundlage der digitalen Zukunft immer wieder eine wichtige Rolle. Schließlich hat der Einsatz von Cloud Services in den letzten Jahren stark zugenommen, und auch für die kommenden Jahre wird ein Anhalten dieses Trends prognostiziert (siehe Abbildung).



Die Cloud-Technologie und die Auslagerung von Datenverarbeitungen in die Cloud gewinnen sektorenübergreifend immer mehr an Bedeutung. Dabei liegt der Fokus kaum noch darauf, **ob** Prozesse und Dienstleistungen ausgelagert werden sollen. Vielmehr geht es darum, **wie** die Cloud optimal genutzt werden kann, um die erwarteten Potentiale vollumfänglich auszuschöpfen.

Dieses Positionspapier dient dazu, bestehende Herausforderungen im Bankensektor zu identifizieren und mit konkreten Forderungen zu verknüpfen. Das Dokument richtet sich daher an Gesetzgeber, Standard- und Regelsetzer sowie Aufsichtsbehörden. Es soll den Dialog zwischen den beteiligten Akteuren intensivieren, um heutige Hürden so schnell wie möglich abzubauen und somit einen breiteren Einsatz der Cloud-Technologie in den Banken zu ermöglichen.

Ausgehend von vier Handlungsfeldern aus den Bereichen Anbieter-Konzentration, Regulatorik, Datenschutz/Drittstaatentransfer und Audits werden die folgenden 13 Forderungen erhoben:

1. Förderung von europäischen IT-Kooperationsprojekten und einer konkurrenzfähigen europäischen IT-Anbieterlandschaft im Cloud-Bereich.
2. Bewertung der in der GAIA-X-Initiative entwickelten Dienste für Finanzdienstleister hinsichtlich ihrer Tragfähigkeit durch Aufsichtsbehörden vor Veröffentlichung.
3. Intensivierung des gemeinsamen Dialoges zwischen Regulatoren, Aufsichtsbehörden und Kreditwirtschaft zu den von der Europäischen Kommission vorgeschlagenen freiwilligen Standardvertragsklauseln für Verträge zwischen Finanzdienstleistern und Cloud-Anbietern.
4. Entwicklung industrieübergreifender Standards inklusive geeigneter Sicherheitsstandards als Voraussetzung für eine grundsätzliche Übertragbarkeit von Daten zwischen Cloud-Anbietern und zur Verhinderung von Vendor Lock-in-Effekten.
5. Weitere Harmonisierung des Bankaufsichtsrechts insbesondere bei Anforderungen für das Reporting an Aufsichtsbehörden sowie für Ausstiegsstrategien, um die Komplexität aus einer Vielzahl an regulatorischen Vorgaben zu reduzieren.
6. Vereinheitlichung von abweichenden Begriffen und teils widersprüchlichen Definitionen aus den verschiedenen regulatorischen Vorgaben, die in der Praxis zu unterschiedlichen Interpretationen bei der Umsetzung führen.
7. Berücksichtigung eines risikobasierten Ansatzes bei der Definition von Anforderungen zur Cloud-Auslagerung, denn nicht jede Auslagerung in die Cloud führt zu einem erhöhten Risiko.
8. Entwicklung einer standardisierten elektronischen Übertragung für die Meldung von Outsourcing- und Drittanbietervereinbarungen, die heute europaweit unterschiedlich sind und auf manuellen Prozessen basieren.
9. Vermeidung nationaler Alleingänge, insbesondere bei Vorgaben bezüglich der Wahl des Datenspeicherortes, durch eine führende Rolle der EU-Aufsichtsbehörden im grenzüberschreitenden Dialog.
10. Intensivierung des Austausches zwischen Aufsichtsbehörden, Finanzinstituten und Cloud-Anbietern bezüglich der Bedeutung der Cloud-Nutzung und der Akzeptanz in der Risikobetrachtung und Prüfungspraxis.
11. Entwicklung einer Lösung durch den EU-Gesetzgeber für eine praxistaugliche Umsetzbarkeit der Anforderungen zur Gewährleistung des Datenschutzes beim Datentransfer in Drittstaaten. Insbesondere bei der Inanspruchnahme von US-basierten Cloud-Diensten und einer damit verbundenen Datenübermittlung in die USA bedarf es praxistauglicher standardisierter Instrumente, die den Cloud-Anbietern und Cloud-Nutzern Rechtssicherheit gewähren und belastbare Leitlinien für erforderliche Schutzmaßnahmen bieten.

12. Nutzung eines international standardisierten Kontrollkataloges für die Prüfung der Bank-Anforderungen bei der Auslagerung von Dienstleistungen zu Cloud-Anbietern.
13. Beauftragung eines externen (Cloud-)Prüfungsexperten zur Durchführung von Audits auf Basis eines einheitlichen, standardisierten Kontrollkataloges.

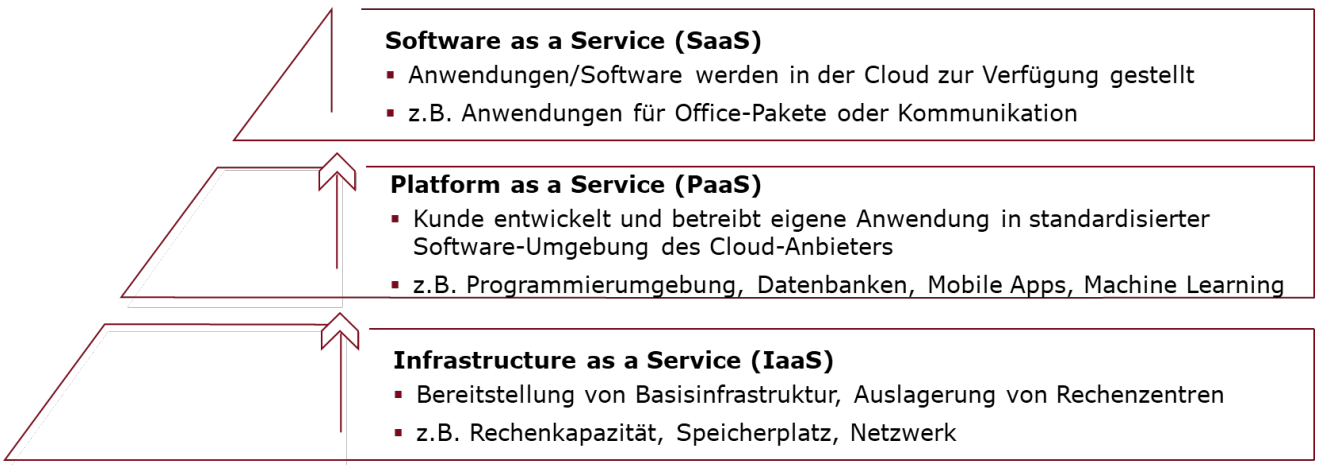
2 Ausgangssituation

Die Informationstechnologie (IT) vieler Banken unterliegt seit einigen Jahren einem Paradigmenwechsel. Angesichts des immer schnelleren Wandels von Markt- und Kundenbedürfnissen ist eine flexible und leistungsfähige IT-Infrastruktur inzwischen essenziell für die Wettbewerbsfähigkeit einer Bank. Von entscheidender Bedeutung ist dabei die Nutzung der Cloud-Technologie: Sie ermöglicht es, eine hochgradig flexible und Innovationen unterstützende IT-Infrastruktur zu überschaubaren Kosten zu betreiben.

Meist ergibt sich im Zielbild der IT-Architektur einer Bank ein hybrider Mix aus traditionellen IT-Systemen und Cloud-Anwendungen. Die gezielte Migration der Bankinfrastruktur von lokalen Systemen in die Cloud ist dabei ein wichtiger Baustein, die Wettbewerbsfähigkeit einer Bank zu sichern.

2.1 Cloud-Services im Überblick

Viele Banken setzen heute bereits öffentliche Cloud-Lösungen (Public Cloud) ein, d. h., sie nutzen Speicher- und Rechenkapazitäten in Rechenzentren von Cloud-Anbietern. Daneben existieren – je nach Art und Tragweite der Auslagerung – eine Reihe von Differenzierungen: von flexiblen Speicherkapazitäten (IaaS) über die Verwendung von Plattformdiensten (PaaS), die Nutzung von Tools zur Analyse von großen Datenmengen in der Cloud bis hin zu komplett aus der Cloud heraus ausgeführter Software (SaaS) (siehe Abbildung).



Bei der „Multi-Cloud" wiederum werden Dienstleistungen mehrerer Cloud-Anbieter genutzt, um deren unterschiedliche Angebote möglichst effizient zu bündeln.

2.2 Auswirkungen der Cloud auf den Finanzsektor

Der Einsatz von Cloud-Technologie in Banken wirkt sich, je nach Umfang, nicht nur auf die Bank-IT aus, sondern auf die gesamte Organisation, ihre Abläufe und Prozesse. Die erhöhte Agilität und Skalierbarkeit verbessern beispielsweise die Markteintrittsgeschwindigkeit („Time-to-Market") von Apps und IT-getriebenen Bankprodukten.

Daneben dient die Cloud als technologische Grundlage für die Analyse großer Datenmengen, wie beispielsweise beim Einsatz von künstlicher Intelligenz (KI). Sie macht zudem eine effizientere Nutzung von Ressourcen möglich, da zusätzliche Rechenkapazitäten für Spitzenlasten meist nicht mehr lokal vorgehalten werden müssen. Diese Reduzierung lokaler Rechenkapazitäten führt wiederum zu einem geringeren Kapitaleinsatz. Die Cloud-Services-Anbieter stehen dabei mit ihren Rechenzentren für eine hohe IT-Professionalisierung und standardisierte Betriebsabläufe.

2.3 Cloud-Initiativen

Es haben sich mittlerweile auf dem europäischen Markt verschiedene Initiativen gegründet, die spezifische Fragestellungen zur Cloud adressieren, beispielsweise GAIA-X, Switching Cloud Providers and Porting Data, die Collaborative Cloud Audit Group und die European Cloud User Coalition.

2.3.1 GAIA-X

GAIA-X basiert auf einer gemeinsamen Initiative der Wirtschaftsministerien Deutschlands und Frankreichs. Ziel ist es, gemeinsame Anforderungen an eine europäische Dateninfrastruktur zu entwickeln, um ein vertrauenswürdiges Ökosystem aus vernetzten dezentralen Infrastruktur-diensten zu schaffen. Auf Basis europäischer Werte sollen somit Daten sicher und vertrauensvoll verfügbar gemacht und geteilt werden können[1]. Im September 2020 gründeten hierfür 22 Mitglieder eine gemeinnützige Organisation nach belgischem Recht, die GAIA-X, European Association for Data and Cloud, AISBL[2]. Entsprechende Arbeiten zu Anwenderökosystemen und -anforderungen erfolgen in verschiedenen Domänen mit Branchenschwerpunkt. Die Domäne „Finanzwesen in Deutschland" wird dabei hauptsächlich durch das Projekt „Financial Big Data Cluster" unterstützt.

2.3.2 Switching Cloud Providers and Porting Data (SWIPO)

Die SWIPO AISBL[3] ist ein von der Europäischen Kommission unterstützter Verbund verschiedener Stakeholder, der freiwillige Verhaltenskodizes („Code of Conduct") für die ordnungsgemäße Anwendung der EU-Verordnung 2018/1807 über einen Rahmen für den freien

[1] https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html

[2] https://www.gaia-x.eu/#

[3] AISBL: Rechtsform für internationale Non Profit Organisationen nach belgischem Recht.

Verkehr nicht-personenbezogener Daten (Artikel 6 „Übertragung von Daten") entwickelt und verwaltet. Die Verhaltenskodizes sollen das Auftreten von Cloud Vendor Lock-in (die Abhängigkeit zu einem Anbieter) verhindern bzw. beheben. Die Kodizes und die zugehörigen Governance-Dokumente und -Verfahren wurden bereits finalisiert und veröffentlicht[4]. Die Organisation arbeitet ohne direkten Einfluss der Europäischen Kommission und besteht aus Cloud-Service-Anbietern und Cloud-Service-Nutzern.

2.3.3 Collaborative Cloud Audit Group (CCAG)

Die Collaborative Cloud Audit Group ist eine branchenweite Initiative zur kollektiven Durchführung von Audits bei wesentlichen Auslagerungen der Finanzinstitute und Versicherungsgesellschaften. Sie wurde durch die Deutsche Börse im Jahr 2017 gegründet. Die Gruppe reduziert den Aufwand rund um die Prüfung des Cloud-Anbieters dadurch, dass mehrere Finanzinstitute Teams bilden, deren Mitarbeiter gemeinsam die Cloud-Anbieter in sogenannten „Pooled Audits" prüfen.

2.3.4 European Cloud User Coalition (ECUC)

Im Januar 2021 wurde von zwölf europäischen Finanzinstituten die European Cloud User Coalition gegründet. Ziel ist es, die Nutzung von Public-Cloud-Systemen für die gesamte europäische Finanzbranche zu fördern. Hierfür haben die in der Initiative vertretenen Finanzinstitute Anforderungen an Cloud-Anbieter für gemeinsame Sicherheitsstandards und Best Practices erarbeitet. Auf dieser Grundlage sollen die hohen europäischen Regulierungs- und Datenschutzstandards auch bei außereuropäischen Cloud-Anbietern besser implementiert werden können und Finanzinstitute langfristig unabhängiger in der Technologieauswahl sein.

3 Handlungsfelder

3.1 Anbieter-Konzentration

3.1.1 Förderung einer konkurrenzfähigen europäischen Cloud-Infrastruktur

Die digitale Souveränität Europas ist von erheblicher Bedeutung für die Innovationsfähigkeit europäischer Unternehmen und Organisationen. Anwender von IT-Dienstleistungen und Nutzer erfolgskritischer digitaler Technologien sind darauf angewiesen, dass es einen hinreichenden Wettbewerb auf der Anbieterseite gibt. Dies spüren auch Banken als Anwender einer Vielzahl von IT-Dienstleistungen seit Jahren.

Eine konkurrenzfähige europäische IT-Anbieterlandschaft im Cloud-Bereich und europäische IT-Kooperationsprojekte wie z.B. die GAIA-X-Initiative sind von großer Bedeutung. Diese müssen nachhaltig gefördert werden. Die Initiativen zahlen auf die digitale Infrastruktursouveränität Europas ein und tragen zu einer größeren Unabhängig-

[4] www.swipo.eu

keit im Hinblick auf weltpolitische Risiken bei. Von Bedeutung ist hierbei ebenfalls die Gewährleistung des europäischen Datenschutzniveaus und das Betreiben vertrauenswürdiger Dienste.

3.1.2 Anerkennung aufsichtlicher Konformität von GAIA-X-Diensten durch Aufsichtsbehörden

Derzeit ist eine Konzentration auf einige wenige, sehr große globale Cloud-Infrastrukturanbieter zu beobachten. Um daraus resultierende Abhängigkeiten zu minimieren, sind Lösungen nötig, die die Zusammenarbeit mit diesen Anbietern weiterhin ermöglichen, aber gleichzeitig mehr Flexibilität bieten. Dieser Aspekt wird bereits von der GAIA-X-Initiative aufgegriffen. Für verschiedenste Sektoren – so auch für das Finanzwesen – wurden Anwendungsszenarien analysiert und bewertet, um die Anforderungen an eine europäische Dateninfrastruktur zu konkretisieren. Diese Anwendungsszenarien werden veröffentlicht und kommen in der Praxis ohne eine vorherige Bewertung durch zuständige Aufsichtsbehörden zum Einsatz.

Alle mit dem GAIA-X-Label versehenen Dienste für Finanzdienstleister sollten bereits vor Veröffentlichung von den Aufsichtsbehörden als tragfähig bewertet worden sein. GAIA-X könnte somit dazu beitragen, dass die Cloud-Regulierung den Anforderungen der Finanzbranche besser Rechnung trägt.

3.1.3 Standardisierung von Cloud-Service-Verträgen

Sowohl bankaufsichtsrechtlich als auch datenschutzrechtlich kommt dem zwischen dem Cloud-Anbieter und der Bank als Cloud-Nutzer zu schließenden Cloud-Service-Vertrag eine besondere Bedeutung zu, da die Vertragsinhalte entscheidenden Einfluss darauf haben, ob das jeweilige Institut aufsichtsrechtlich eine Auslagerung der Datenverarbeitung in die Cloud vornehmen darf. In der Vertragsverhandlungssituation muss der Cloud-Anbieter häufig erst ein Verständnis für die wesentlich höheren regulatorischen Anforderungen bei Cloud-Auslagerungen im Finanzsektor im Vergleich zu anderen Industrien erlangen. Gerade bei globalen Anbietern mit großer Marktmacht stellt die Akzeptanz bankspezifischer Vorgaben eine Herausforderung dar.

Eine Teil-Standardisierung von Cloud-Verträgen würde folglich zu Erleichterungen in den Verhandlungen zwischen Cloud-Dienstleistern und Kunden führen. Zugleich bietet diese Standardisierung den Aufsichtsbehörden eine einheitliche Basis bei der Evaluierung der Vertragsbeziehung von Cloud-Auslagerungen. Dabei sollte allerdings beachtet werden, dass sich Cloud-Projekte in vielen Punkten – etwa hinsichtlich Scope, Service-Level und Internationalität – stark voneinander unterscheiden. Vertragspartnern muss es deshalb weiterhin möglich sein, passgenau fallbezogene Vertragsvereinbarungen treffen zu können, was zu einem gewissen Spannungsfeld zwischen Standardisierung und Vertragsfreiheit führt.

Die EU-Kommission arbeitet bereits seit zwei Jahren an der Ausgestaltung von freiwilligen Klauseln für verschiedene Bereiche in Cloud-Verträgen. Die Empfehlungen der europäischen Kreditwirtschaft sollten dabei Berücksichtigung finden. Sinnvoll und notwendig wäre es, wenn die EU-Kommission ihren Vorschlag hinsichtlich der im Juni 2021 veröffentlichten neuen Datenschutz-Standardvertragsklauseln an die europäischen und nationalen Bankaufsichtsbehörden übermitteln würde. Das Ziel wäre dann ein gemeinsamer, weiterführender Dialog mit der europäischen Kreditwirtschaft über diese freiwilligen Standardvertragsklauseln. Die Standardvertragsklauseln sollten hinsichtlich ihrer aufsichtsrechtlichen Tragfähigkeit als Referenzklauseln durch die Aufsichtsbehörden wahrgenommen werden. Insbesondere den Vertragsbestandteilen zu Auditierungsrechten für Kunden und Informationspflichten zu Sub-Outsourcing des Cloud-Anbieters sollte dabei besondere Bedeutung zugemessen werden.

3.1.4 Datenportabilität zur Verhinderung von „Vendor Lock-in"

Bei einer Vielzahl der heute auf dem Markt angebotenen Cloud-Diensten setzen die Cloud-Anbieter auf die Verwendung von proprietären Technologien. Aus Anbietersicht geschieht dies aus Gründen der Differenzierung gegenüber Konkurrenzangeboten und dient der Kundenbindung. Allerdings sind damit die in der Cloud gespeicherten Daten bzw. die in der Cloud genutzten Dienste oftmals nicht an andere Anbieter übertragbar. Die Entwicklung industrieübergreifender Standards ist daher eine wichtige Voraussetzung, um eine grundsätzliche Übertragbarkeit von Daten zwischen Cloud-Anbietern sicherzustellen. Dies könnte ein Mittel sein, den Cloud-Markt transparenter zu gestalten und den Kreis der Cloud-Anbieter zu vergrößern.

Zudem verlangen die Richtlinien der Europäischen Bankenaufsichtsbehörde (EBA) zu Outsourcing-Vereinbarungen (EBA/GL/2019/02) von Finanzinstituten im Rahmen ihrer Risikobewertung, dass beim Auslagern kritischer oder wesentlicher Funktionen eine Ausstiegsstrategie vorhanden ist. Diese sieht unter anderem vor, dass ausgelagerte Funktionen und Daten dem Cloud-Anbieter entzogen werden können, um diese entweder an alternative Anbieter zu übertragen oder in die eigenen Systeme des Instituts einzugliedern.

Zur Verhinderung von Vendor Lock-in-Effekten sind automatisierte Prozesse nötig. Daher gilt es, Standards sowohl für Datenformate als auch für entsprechende Schnittstellen zur Datenübertragung inklusive geeigneter Sicherheitsvorgaben zu fördern. Cloud-Anbieter könnten zudem mit einer standardisierten Schnittstelle (Application Programming Interface, API) den Import und Export der gespeicherten Daten sowie Services zum Nachweis der Vollständigkeit des Imports/Exports bereitstellen.

3.2 Regulatorik

3.2.1 Harmonisierung des Bankaufsichtsrechts

Das aktuelle regulatorische Umfeld erlaubt es Banken bislang nur eingeschränkt, die Cloud-Technologie optimal einzusetzen, ist doch die heutige Bankenregulierung nicht ausreichend auf eine Bank-individuelle Cloud-Nutzung ausgelegt. Die Regelungen sind vielschichtig und in zahlreichen Vorgaben enthalten[5]. Eine eindeutige, widerspruchsfreie Ableitung der Anforderungen für eine Bank bedarf umfangreicher Analysen und Bewertungen. Ohne Angleichung und Vereinfachung bisheriger Regularien werden neue, zusätzliche Ansätze die Komplexität und damit die Kosten weiter erhöhen, ohne die Risiken signifikant zu senken.
Mit dem Digital Operational Resilience Act (DORA) hat die Europäische Kommission zwar nunmehr einen Entwurf für eine harmonisierte IT-(Sicherheits-)Regulierung für den Finanzsektor vorgelegt. DORA als „lex specialis" soll zukünftig als umfassende und somit einzige Regulierung für Finanzinstitute gelten. Damit wird eine Harmonisierung sowohl über die Vielzahl bisheriger Regulierungsansätze als auch im Sinne eines grenzübergreifend einheitlichen Regelsatzes – unter Vermeidung national abweichender Umsetzungen – beabsichtigt. Die Zielsetzung dieser Initiative ist richtig und im Interesse der Banken; aber das Ergebnis des Gesetzgebungsprozesses bleibt abzuwarten. DORA kann nur ein Teilbeitrag für eine weitere Harmonisierung des Bankaufsichtsrechts sein.

Wir sprechen uns weiterhin für eine Harmonisierung des Bankaufsichtsrechts – idealerweise auf EU-Ebene – und die Etablierung von Standards aus. Insbesondere müssen die Anforderungen für das Reporting an Aufsichtsbehörden sowie für Ausstiegsstrategien (z.B. Geschäftsfortführung bei Kündigung der Auslagerungsvereinbarung oder erheblichem Serviceausfall etc.) europaweit klar und einheitlich sein.

3.2.2 Vereinheitlichung von Begriffen und Definitionen

Die unterschiedlichen Vorgaben der Regulierungsbehörden führen zu abweichenden und teils widersprüchlichen Definitionen und Kriterien. So existieren beispielsweise unterschiedliche Definitionen für Outsourcing, Third Party Relationships, Information Technology Services und Cloud Services. Dies führt wiederum zu einer unnötigen Komplexität, erheblichen Kosten und zusätzlichen Zeitproblemen bei der Umsetzung der Anforderungen in einem globalen Umfeld.

Begriffe und Definitionen der unterschiedlichen Regulierungsvorgaben müssen vereinheitlicht werden, um unterschiedliche Interpretationen bei der Umsetzung von Vorgaben und späteren Prüfprozessen zu vermeiden. Schwellenwerte oder Kriterien für Kritikalität/Wesentlichkeit und Outsourcing müssen konsistent sein.

[5] u.a. EBA/ESMA-Guidelines on (Cloud-)Outsourcing; EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie); Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin; Bankaufsichtlichen Anforderungen an die IT (BAIT) der BaFin; BaFin-Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter; Datenschutz-Grundverordnung (DSGVO)

3.2.3 Unterstützung eines risikobasierten Ansatzes

Die heutigen Anforderungen bei Cloud-Auslagerungen sind zu wenig risikobasiert und daher oftmals nicht verhältnismäßig. Cloud-Dienste sollten aus unserer Sicht nicht automatisch als Outsourcing gelten, sondern erst dann, wenn eine Bewertung dies explizit ergeben hat. Nicht jede Auslagerung in die Cloud führt schließlich zu einem erhöhten Risiko im Bankgeschäft, dies gilt zum Beispiel dann nicht, wenn Kantinenpläne in der Cloud abgelegt werden oder Listen zu Anbietern von Büromaterial. Die pauschale Einstufung als Auslagerung liegt möglicherweise auch an mangelnden Erfahrungen seitens Aufsicht und Jahresabschluss-/IT-Prüfern, wie gut beziehungsweise schlecht die Cloud aus Sicht des Risikomanagements bewertet wird.

Die Regulierung und Beaufsichtigung von Cloud-Auslagerungen sollten immer auf Grundlage eines risikobasierten Ansatzes erfolgen. Dafür ist ein gemeinsames Verständnis zwischen Banken und Aufsichtsbehörden über die Risiken und die verfügbaren Kontrollmechanismen für Cloud-Services unerlässlich. Die Einschätzung der Risiko-dimension sollte anhand einheitlicher Kriterien, wie Grad der Verantwortungsübertragung und Kritikalität der ausgelagerten Daten und Funktionen, geschehen[6]. Wir sprechen uns hierbei für EU-weit einheitliche Regeln und der Etablierung von Standards aus.

3.2.4 Standardisierte elektronische Übermittlung von Meldeanforderungen

Die inhaltlichen Anforderungen sowie die Datenstandards für die Meldung von Outsourcing- und Drittanbietervereinbarungen sowie die Führung von Outsourcing-Registern sind in Europa fragmentiert. Sie basieren zudem auf manuellen und damit fehleranfälligen Systemen und Prozessen.

Wir regen an, dass das Reporting von Drittanbietervereinbarungen in Zusammenarbeit mit den Banken standardisiert wird, wobei gemeinsame Datenstandards und Schnittstellen (APIs) zur Norm werden sollten.

3.2.5 Abbau nationaler Vorgaben an den Ort der Datenspeicherung

Banken werden im internationalen Kontext oft mit nationalen Vorschriften konfrontiert, die eine lokale Speicherung oder Verarbeitung von Daten vorschreiben. Diese verursachen jedoch zusätzliche Kosten und Hürden für den Innovationsprozess, ohne dass die Erreichung der aufsichtsrechtlichen Ziele in angemessenem Umfang verbessert wird. Darüber hinaus wirken sich die Regeln zur lokalen Speicherung und Verarbeitung nachteilig auf die Fähigkeit der Finanzinstitute aus, die Cloud vollständig zu nutzen. Sie führen zu einer komplexeren IT-Architektur und schaffen gegebenenfalls neue Risiken in Bezug auf die Informationssicherheit.

[6] Siehe Kapitel 4.2 des Dokumentes „The use of Cloud Computing by Financial Institutions" der Europäischen Bankenvereinigung vom Juni 2020 (https://www.ebf.eu/wp-content/uploads/2020/06/EBF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf)

Europäische Aufsichtsbehörden sollten im weltweiten Kontext eine führende Rolle bei der Förderung eines umfassenderen Informationsaustauschs zwischen Regulierungs- und Aufsichtsbehörden einnehmen, um negative Auswirkungen bei nationalen Alleingängen zu vermeiden. Regeln zur lokalen Datenspeicherung oder Verarbeitung sollten vermieden werden. Insbesondere sollte ein direkter Zugriff der Aufsichtsbehörden auf Daten, die von Cloud-Dienstleistern im Namen von Banken gehalten werden, in einer Weise erfolgen, bei der die Einhaltung des Bankgeheimnisses und der Datenschutzvorschriften durch Banken gewährleistet bleibt.

3.2.6 Akzeptanz der Cloud-Nutzung bei Aufsichtsbehörden

Die Auslagerung von Dienstleistungen in der Bankenbranche ist nicht neu. Die Nutzung der Cloud ist jedoch eine besondere Form der Auslagerung und erfordert zum Teil spezifisches Know-how in der Risikobetrachtung und Prüfungspraxis. Dieses Know-how muss zum Teil erst noch aufgebaut werden.

So unterstützen zum Beispiel nicht alle nationalen und internationalen Aufsichtsbehörden den Ansatz unternehmensübergreifender Audits, obwohl diese bereits durch die EBA-Guidelines on Outsourcing ermöglicht werden (siehe hierzu auch die Initiative der Collaborative Cloud Audit Group zu Pooled Audits).

Der Austausch zwischen Aufsichtsbehörden, Finanzinstituten und Cloud-Anbietern sollte intensiviert werden, um die Vorteile und Risiken der Cloud angemessen bewerten zu können und die sichere Migration in die Cloud zu unterstützen. Insbesondere sollten die Initiativen der CCAG zu möglichen Pooled Audits in einer gemeinsamen Arbeit von Banken und Aufsichtsbehörden vorangetrieben werden, um bestmögliche Ansätze und Lösungen konkreter Prüfungshandlungen von Cloud-Services zu verfolgen.

3.3 Datenschutz und Drittstaatentransfer

Das Datenschutzrecht ist relevant, wenn in der Cloud personenbezogene Daten verarbeitet werden sollen. Dies sind Informationen über natürliche Personen. Daten, die keinen Personenbezug haben oder nur Informationen über juristische Personen enthalten, sind hiervon nicht erfasst. Bei Informationen über juristische Personen muss die Bank aber das Bankgeheimnis beachten.

Die Inanspruchnahme eines Cloud-Anbieters wird datenschutzrechtlich regelmäßig als Auftragsdatenverarbeitung eingeordnet. Nach Artikel 28 EU-Datenschutzgrundverordnung (DSGVO) muss zwischen Auftraggeber (Cloud-Nutzer) und Auftragnehmer (Cloud-Anbieter) ein Vertrag über die Auftragsverarbeitung geschlossen werden. Dieser muss insbesondere strenge Weisungsrechte des Auftraggebers gegenüber dem Auftragnehmer enthalten, damit Erstgenannter weiterhin „Herr der Daten" bleibt. Bei bestimmten Cloud-Anbietern kann eine solche Vorgabe bereits eine Herausforderung sein.

Die datenschutzrechtliche Komplexität und Schwierigkeit steigt deutlich, wenn der Cloud-Anbieter seinen Sitz in einem Drittstaat hat. Während es innerhalb des EU-/EWR-Raums egal ist, in welchem Staat der Anbieter die personenbezogenen Daten verarbeitet, sind bei einer Datenverarbeitung im Drittstaat besondere Vorgaben zu beachten. Nach der DSGVO ist die Übermittlung personenbezogener Daten an Staaten außerhalb der EU (= Drittstaaten) nur dann zulässig, wenn

- der Betroffene eingewilligt hat,
- dies zur Erfüllung eines Vertrags erforderlich ist (z.B. Ausführung eines Zahlungsauftrags in die USA) oder
- dort ein angemessenes Datenschutzniveau existiert.

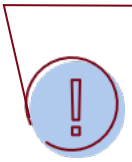
Nach EU-Recht wird ein angemessenes Datenschutzniveau im Drittstaat unter anderem in folgenden Fällen angenommen:

- Die EU-Kommission hat den Drittstaat als Land mit einem angemessenen Datenschutzniveau ausdrücklich anerkannt (Beispiele für „sichere Drittstaaten": Schweiz, Japan).
- Das übermittelnde Unternehmen in der EU hat mit dem im Drittstaat ansässigen Unternehmen die EU-Standardvertragsklauseln vereinbart (häufig genutzt bei Einschaltung von Rechenzentren im Drittstaat als Auftragsverarbeiter).
- Innerhalb von internationalen Unternehmen/Konzernen können Binding Corporate Rules (BCR) für unternehmensinterne Datentransfers das Datenschutzniveau sichern.
- Das US-Unternehmen als Datenempfänger hat sich zur Einhaltung des EU-US-Datenschutzschilds verpflichtet (früher „Safe-Harbor-Abkommen", das aber durch EuGH-Urteil „Schrems I" zu Fall gebracht wurde).

Allerdings hat sich die datenschutzrechtliche Situation bei Drittstaatenbezug im Sommer 2020 nochmals verschärft. Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 16. Juli 2020 (Rechtssache C-311/18, „Schrems II") den Angemessenheitsbeschluss der EU-Kommission zur Datenübermittlung in die USA (EU-US-Privacy-Shield) für ungültig erklärt. Die Datenschutzaufsichtsbehörden in der EU leiten aus dem EuGH-Urteil ab, dass eine Nutzung der von der EU-Kommission zur Absicherung des Drittstaatentransfers etablierten EU-Standardvertragsklauseln in bestimmten Ländern (z.B. USA) nur noch mit zusätzlichen Sicherheitsmaßnahmen zulässig sei. Wegen der vermeintlich extensiven Zugriffsrechte der US-Behörden (insbesondere US-Geheimdienste) auf Datenbanken in den USA bezweifeln einzelne Datenschutzbehörden, ob es in Bezug auf die USA überhaupt noch möglich ist, hinreichende Garantien mit dem Dienstleister zu vereinbaren. Faktisch besteht damit die Gefahr, dass eine Übermittlung von personenbezogenen Daten in die USA pauschal als rechtswidrig eingestuft werden könnte. Wirtschaftsverbände auf nationaler und europäischer Ebene (darunter der Bankenverband und die Europäische Bankenvereinigung) haben in Stellungnahmen auf Umsetzungsprobleme und ein unlösbares Dilemma hingewiesen und politischen Handlungsbedarf aufgezeigt.

Damit befinden sich Unternehmen in einer Sackgasse, denn die Datenübermittlung in die USA ist in der Praxis vielfach üblich, gerade bei der Inanspruchnahme von Cloud-Diensten. Zudem müssen die Unternehmen jetzt einzelfallbezogen mit ihren Geschäftspartnern verhandeln und könnten die eigentliche Generalwirkung der von der EU-Kommission etablierten EU-Standard-datenschutzklauseln nicht mehr ohne Weiteres für sich in Anspruch nehmen. Wichtig sind auch hier ein risikobasierter Ansatz und standardisierbare Lösungen. Die datenschutzrechtlich in Bezug auf bestimmte Drittstaaten zu ergreifenden Schutzmaßnahmen zur Gewährleistung des EU-Datenschutzniveaus sollten im Verhältnis zum jeweils ermittelten Risiko stehen. Die Maßnahmen sollten im Lichte der jeweiligen Anwendung und des möglichen Risikos erforderlich, geeignet und angemessen sein. Neben vertraglichen und organisatorischen Absicherungen kommt sicherlich auch technischen Schutzvorkehrungen (u.a. Verschlüsselung) eine erhebliche Bedeutung zu. Bei angemessenen Schutzmaßnahmen sollte es weiterhin möglich sein, dass sich die Unternehmen bei einem Drittstaatendatentransfer auf Basis der von der EU-Kommission herausgegebenen EU-Standardvertragsklauseln zum Datenschutz stützen können.

Derzeit ist noch nicht abzusehen, ob und wann es eine umsetzbare (politische) Lösung durch die Regulatoren geben wird. Ein guter Ansatz ist der von der EU-Kommission veröffentlichte Ange-messenheitsbeschluss zum BREXIT, mit dem das Datenschutzniveau im Vereinigten Königreich befristet auf 4 Jahre als angemessen bewertet wurde. Auch die Aufnahme von Verhandlungen zwischen der EU-Kommission und der US-Administration im März 2021 über ein Nachfolgemodell des EU-US-Datenschutzschilds ist ein wichtiger Schritt zur Wiederherstellung von Rechtssicherheit und praxistauglichen Instrumenten bezüglich der Gewährleistung des Datenschutzes.



Auch datenschutzrechtlich brauchen Banken, die Cloud-Dienste nutzen wollen, Planungs- und Rechtssicherheit. Diese Sicherheit haben bislang Instrumente wie u.a. das EU-US-Datenschutzschild oder die EU-Standardvertragsklauseln hergestellt. Diese konnten in der Praxis gut umgesetzt werden, nicht nur von Großunternehmen, sondern auch von kleinen und mittleren Unternehmen, die nur über begrenzte Ressourcen für die Rechtsberatung verfügen. Die derzeit zu beobachtende Tendenz, allein den Unternehmen eine detaillierte Datenschutzprüfung bei Drittstaatssachverhalten aufzubürden, ist ein Show-Stopper gerade für die Nutzung von in Drittstaaten angesiedelten Cloud-Diensten. Nach dem EuGH-Urteil "Schrems II" vom Juli 2020 ist es aus Sicht auch der gesamten Realwirtschaft dringend erforderlich, dass der Gesetzgeber auf EU-Ebene standardisierte Instrumente zur Verfügung stellt, die den Cloud-Anbietern und Cloud-Nutzern Rechtssicherheit gewähren und belastbare Leitlinien für bei bestimmten Drittstaaten erforderliche Schutzmaßnahmen bieten. Dabei ist ein risikobasierter Ansatz von herausragender Bedeutung. Die im Juni 2021 von der EU-Kommission etablierten neuen Standardvertragsklauseln zum Datenschutz sind hierbei ein wichtiger Fortschritt. Gleichwohl greift der Ansatz zu kurz, die Datenschutzadäquanzprüfung allein bei den Unternehmen und anderen Einrichtungen anzusiedeln, die auf einen Drittstaatendatentransfer angewiesen sind.

3.4 Effizienzsteigerung bei Audits von Cloud-Anbietern

Im Rahmen von Auslagerungen überprüfen Finanzinstitute ihre IT-Dienstleister hinsichtlich der an sie gerichteten Anforderungen. Im Falle von Cloud-Anbietern sind diese Prüfungen mit besonderen Herausforderungen verbunden. Die durch jedes Finanzinstitut bei jedem Cloud-Anbieter durchzuführenden Prüfungen sind zeit- und kostenaufwendig, binden Ressourcen, schaffen zusätzliche Risiken und erschweren letztendlich den Zugang von Finanzinstituten zu Cloud-Dienstleistungen. Zur Steigerung der Effizienz bei der Auditierung von Cloud-Anbietern könnten alternative Formen der Nachweiserbringung bezüglich der Erfüllung von Anforderungen dienen.

3.4.1 Standardisierter Anforderungskatalog

Im Rahmen von Auslagerungen definieren Finanzinstitute unterschiedliche Anforderungen an den Auslagerungsprozess. Dies betrifft bankspezifische Anforderungen für den Umgang mit dem Drittdienstleister, aber auch Anforderungen, die der IT-Dienstleister zu erfüllen hat. In Bezug auf IT-Sicherheitsanforderungen ist ein Großteil dieser Anforderungen bei vielen Banken gleich, da es sich um grundsätzliche Aspekte der IT- bzw. Informationssicherheit handelt.

Mit Hilfe eines auf international anerkannten Standards basierenden Kontrollkatalogs könnte der Teil der Anforderungen des Finanzinstitutes, der durch den Cloud-Anbieter zu erbringen ist, in einer einheitlichen und (auch qualitativ) gleichbleibenden Form geprüft und entsprechende Nachweise erbracht werden. Als Standard bietet sich die Cloud Control Matrix an. Darüber hinausgehende Anforderungen können weiterhin durch jedes Finanzinstitut individuell adressiert werden.

3.4.2 Nachweiserbringung durch zentralen Prüfer

Die Überprüfung der Umsetzung bzw. Einhaltung der im Kontrollkatalog festgelegten Anforderungen erfolgt durch das Finanzinstitut. Das Finanzinstitut fragt beim Cloud-Anbieter notwendige Nachweise (z.B. ISO-Zertifizierungen) an oder prüft selbst vor Ort, sofern es dazu in der Lage ist. Diese Nachweise werden zusammen mit den im eigenen Haus durchgeführten Prüfungen konsolidiert. Das Finanzinstitut stellt anschließend sowohl die Ergebnisse der hausinternen Prüfung als auch die Ergebnisse des Audits beim Cloud-Anbieter zusammen bzw. der Aufsichtsbehörde zur Verfügung. Die Prüfung des Cloud-Anbieters erfolgt derzeit durch jede Bank einzeln bzw. wird durch Pooled Audits durchgeführt (siehe Collaborative Cloud Audit Group). Letzteres ermöglicht eine Reduktion des Prüfaufwandes bei Banken und Cloud-Anbietern, der Aufwand ist aber weiterhin hoch. Eine Prüfung der gemeinsamen, über den Kontrollkatalog standardisierten Aspekte durch einen (zentralen) Prüfer für mehrere Banken würde eine Effizienzsteigerung bedeuten und Ergebnisse in hoher Qualität sicherstellen.

Für die Überprüfung der bankspezifischen Outsourcing-Anforderungen bei einem Cloud-Anbieter sollten die Institute die Möglichkeit haben, einen zentralen Prüfer für die in einem standardisierten Kontrollkatalog definierten Aspekte zu beauftragen. Dieser könnte die Ergebnisse des Audits dann mehreren Banken und – für die Institute – auch den zuständigen Aufsichtsbehörden zur Verfügung stellen. Die Anwendung eines einheitlichen, standardisierten Kontrollkatalogs und die Durchführung der Audits durch entsprechende (Cloud-)Prüfungsexperten verspricht qualitativ hohe (auf international anerkannten Sicherheitsstandards basierende) und langfristig vergleichbare Ergebnisse.

4 Ausblick

Der Trend zur Cloud-Nutzung wird sich auch in den kommenden Jahren weiter fortsetzen. Die Corona-Krise hat diesen Trend noch verstärkt. Die schnelle Umstellung auf Home-Office und die Nutzung digitaler Dienstleistungen wäre in der Kürze der Zeit ohne flexible Cloud-basierte Lösungen kaum machbar gewesen. Auch im Rahmen der weiteren Digitalisierung von Geschäftsprozessen werden zukünftig immer mehr Anwendungen aus der Cloud heraus betrieben.

Um von den Potentialen dieser Technologie bestmöglich zu profitieren, müssen heutige Hürden weiter abgebaut werden. So ist der Gesetzgeber gefordert, wenn es um einen rechtssicheren Datenaustausch mit Drittstaaten, der weiteren Harmonisierung des Bankaufsichtsrechts und der Definition von freiwilligen Standardvertragsklauseln geht. Zudem ist auch die Entwicklung und aufsichtsrechtliche Anerkennung von Standards von Bedeutung, zum Beispiel im Hinblick auf automatisierte Prozesse bei der Datenportabilität, bei der elektronischen Übertragung von Meldungen an Aufsichtsbehörden und der Überprüfung der bankspezifischen Outsourcing-Anforderungen bei Cloud-Anbietern.

Darüber hinaus sind Banken im Vergleich zu Technologieunternehmen jedoch immer noch Wettbewerbsnachteilen ausgesetzt. So richtet sich die derzeitige Bankenregulierung gesamthaft an Kreditinstitute und erfolgt demnach institutsbasiert. Sofern in einem Konzern mehr als die Hälfte bestimmter Kennzahlen (Eigenkapital, Vermögenswerte, Umsatz, Mitarbeiter, o.ä.) auf Banken oder Finanzinstitute entfallen, werden sämtliche Banken, Finanzinstitute aber auch Nebendienstleister der Bankenregulierung unterworfen, auch wenn die anderen Konzerneinheiten beispielweise als Nebendienstleister Technologiedienstleistungen anbieten. Bei Technologiekonzernen, die nur zu einem kleinen Teil Finanzdienstleistungen anbieten, trifft dies dagegen typischerweise nicht zu. Dies führt zu einem Ungleichgewicht, bezüglich der Verpflichtung, bestimmte Regularien einhalten zu müssen.

Erhöhte Anforderungen an Banken, die die Integration von externen Technologien und somit beispielsweise den Abbau von Alt-Systemen erschweren, hemmen weitere Digitalisierungs-initiativen und erschweren somit die gesamte Digitalisierung des Finanzsektors. Dadurch wird sowohl die Innovationskraft der Banken als auch ihr Beitrag für die digitale Souveränität Europas negativ beeinflusst.

Grundsätzlich sollten Regulierung und Aufsicht daher aktivitätenbezogen ausgerichtet werden. Dies entspräche einem, auch an den neuen Finanzmarktteilnehmern (Technologieunternehmen) ausgerichteten, risikobasierten Ansatz. Eine wirksame Regulierung muss deshalb den Fokus auf die aus Risikosicht besonders relevanten Prozesse richten und weniger auf die sie erbringenden Unternehmen.