

Aktuelle regulatorische Entwicklungen im Zahlungsverkehr sowie in der Wertpapier- und Derivateabwicklung

Der Zahlungsverkehr und die Finanzmarktinfrastuktur haben sich in den letzten Jahren deutlich weiterentwickelt. Das Eurosystem hat dazu mit TARGET2 und TARGET2-Securities wichtige Beiträge geleistet, über die im Monatsbericht Dezember 2017 umfassend berichtet wurde. Gleichzeitig hat aber auch die Regulierung einen wesentlichen Einfluss auf die Entwicklungen. Ausgangspunkt ist dabei, dass widerstandsfähige Finanzmarktinfrastrukturen aufgrund ihrer zentralen Funktionen für das Finanzsystem und die Realwirtschaft erhebliche Bedeutung haben. Zur Gewährleistung einer sicheren Abwicklung des Zahlungsverkehrs und der Wertpapier- und Derivategeschäfte wurden bereits im Jahr 2012 von den G20-Ländern die Prinzipien für Finanzmarktinfrastrukturen (PFMI) verabschiedet. Entsprechend lag der Schwerpunkt in den letzten Jahren darauf, diese Prinzipien für Zahlungssysteme, Zentralverwahrer und zentrale Gegenparteien verbindlich zu verankern. Gegenstand der aktuellen Diskussion ist insbesondere die Überarbeitung des seit 2012 existierenden Aufsichts- und Regulierungsrahmens für zentrale Gegenparteien. Der aktuell diskutierte Rahmen in der Europäischen Union sieht eine stärkere Rolle der Notenbanken und der Europäischen Wertpapier- und Marktaufsichtsbehörde (European Securities and Markets Authority: ESMA) vor sowie insbesondere ein strafferes Regime für die Beaufsichtigung von zentralen Gegenparteien in Drittstaaten. Dieser Aspekt hat durch den bevorstehenden Austritt des Vereinigten Königreichs aus der Europäischen Union eine besondere Bedeutung erlangt. Für die Bewertung möglicher Handlungsoptionen steht dabei für die Bundesbank vor allem die Sicherheit des Zahlungsverkehrs und der Abwicklung von Wertpapier- und Derivategeschäften im Vordergrund. Zudem soll künftig die Sanierung und Abwicklung von zentralen Gegenparteien durch die Umsetzung internationaler Vereinbarungen europaweit vereinheitlicht werden. Die Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme wurden verschärft, um unter anderem der gestiegenen Bedrohung aus dem Cyber-Raum zu begegnen und den überwachenden Notenbanken neue Prüfungskompetenzen einzuräumen. Gerade im Hinblick auf die gestiegene Bedrohungslage sind im Bereich der Finanzmarktinfrastrukturen, aber auch im Finanzsektor insgesamt, nachhaltige Anstrengungen erforderlich, um die Cyber-Widerstandsfähigkeit zu verbessern. Im EU-Zahlungsverkehr werden mit der zweiten Zahlungsdiensterichtlinie (Payment Services Directive 2: PSD2) die Regelungen deutlich geändert. Zielsetzung ist dabei vor allem die Vertiefung der Marktintegration innerhalb der Europäischen Union und die Stärkung des Wettbewerbs. Insbesondere die Möglichkeit von Kontoinhabern, Drittparteien einen Zugang zum Konto zu gewähren, was auch unter dem Stichwort „open banking“ diskutiert wird, kann erhebliche Strukturveränderungen im Markt für Zahlungsdienste herbeiführen.

Finanzmarktinfrastrukturen und Zahlungsdienste

Als Lektion aus der Finanzkrise wurde die Regulierung der Finanzmärkte in den vergangenen Jahren maßgeblich verschärft. Neben einer Fortentwicklung der Bankenregulierung wurden auch die Regeln zur Abwicklung des Zahlungsverkehrs und der Wertpapier- und Derivategeschäfte überarbeitet und strenger gefasst. Als Grundlage hierzu dienen die im Jahr 2012 von den G20-Ländern international vereinbarten Prinzipien für Finanzmarktinfrastrukturen¹⁾ (PFMI), die auch weit über diese Länder hinaus Beachtung finden. Diese stellen einheitliche Anforderungen an das Risikomanagement, die Verwaltungsstrukturen und die Transparenz von Finanzmarktinfrastrukturen. Letztere nehmen eine wichtige Stellung im Finanzsystem ein, denn sie dienen unter anderem der Abwicklung von Finanztransaktionen. Sie konzentrieren Risiken und können aufgrund ihrer zentralen Funktion im eng geflochtenen Netzwerk der Finanzwirtschaft zu einem erheblichen Ansteckungskanal in Krisensituationen werden. Zu den Finanzmarktinfrastrukturen (vgl. Schaubild auf S. 45) zählen unter anderem:

– Zahlungsverkehrssysteme

Über diese wickeln die Teilnehmer ihre Zahlungen ab. In einigen Fällen werden die Zahlungsverkehrssysteme auch von anderen Finanzmarktinfrastrukturen zur geldlichen Verrechnung genutzt.

– Zentralverwahrer (Central Securities Depositories: CSDs)

Wertpapiere werden heute fast ausnahmslos bei Zentralverwahrern hinterlegt. Anleger erhalten die damit verbundenen Eigentumsrechte über ein Depot, welches ihre Bank bei einem Zentralverwahrer unterhält.

– Wertpapierabwicklungssysteme

Diese werden von Zentralverwahrern betrieben, um Wertpapiere beispielsweise beim Kauf buchmäßig von einem Depot zu einem anderen zu übertragen und die Transaktion endgültig durchzuführen.

– Zentrale Gegenparteien (Central Counterparties: CCPs)

Sie übernehmen das Clearing – also die Übermittlung, Abstimmung und Aufrechnung sowie das Risikomanagement – von noch schwebenden Wertpapier- und Derivategeschäften bis zu deren Fälligkeit und schalten sich dabei zwischen zwei Handelspartner. Die mit dem Clearing verbundenen Risikopositionen werden durch die zentrale Gegenpartei zeitnah und fortlaufend berechnet und durch die Einforderung von Sicherheiten von den Vertragsparteien besichert.

– Transaktionsregister²⁾

Sie erlauben eine zentralisierte und standardisierte Erfassung der Transaktions- und Positionsdaten von Derivategeschäften.

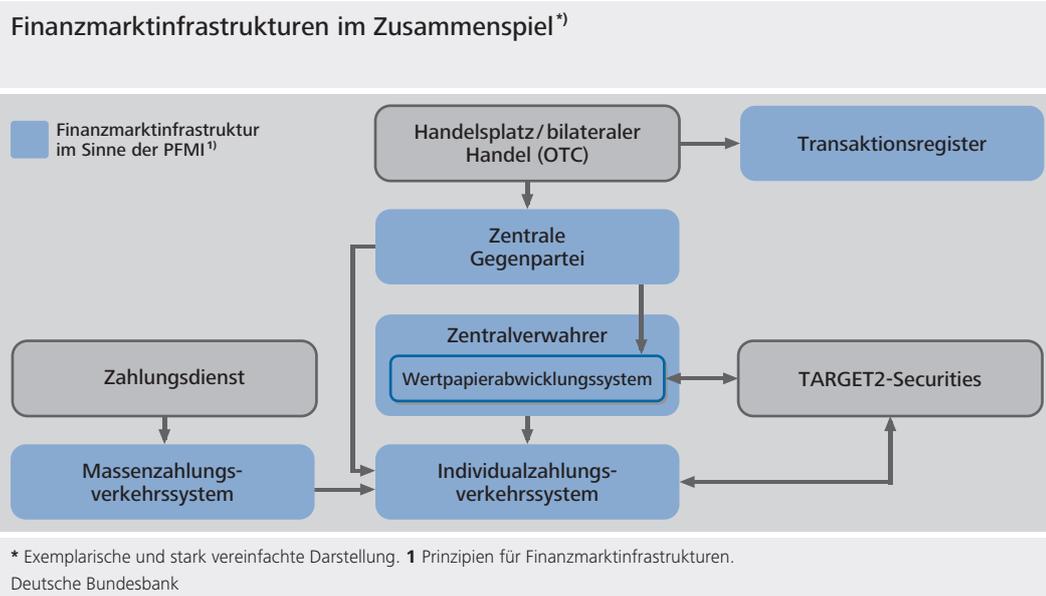
Innerhalb der EU haben die PFMI durch konsequente Umsetzung in Form europäischer Rechtsakte für bestimmte Finanzmarktinfrastrukturen (z. B. für CCPs, CSDs und systemrelevante Zahlungsverkehrssysteme) bindende Wirkung erlangt. Der so geschaffene Rechtsrahmen wird laufend weiterentwickelt, um aktuellen Entwicklungen und Erkenntnissen Rechnung zu tragen.

Neben der Stärkung der Sicherheit und Effizienz der Finanzmarktinfrastrukturen zum Schutz vor Krisen wird auch das gesetzliche Rahmenwerk

*Zahlungsdienste
im Binnenmarkt*

¹ Vgl. hierzu: Deutsche Bundesbank, Die neuen CPSS-IOSCO-Prinzipien für Finanzmarktinfrastrukturen, Monatsbericht, Juli 2012, S. 39–51 und <https://www.bis.org/cpmi/publ/d101a.pdf>

² Transaktionsregister sind nicht Gegenstand dieses Aufsatzes.



für das Angebot von Zahlungsdiensten grundlegend zur Förderung von Innovationen und Verbraucherrechten mit dem Ziel überarbeitet, die Konvergenz im europäischen Binnenmarkt für Zahlungsverkehr zu unterstützen.

■ Zentrale Gegenparteien

Funktion und Bedeutung von zentralen Gegenparteien

CCPs sind ein zentraler Bestandteil der Finanzmarktinfrastruktur und dienen unter anderem dazu, Risiken im Finanzsystem abzumildern und die Abwicklung von Geschäften zu erleichtern. Als zentrale Gegenpartei schalten sie sich zwischen die Parteien von Finanzgeschäften, die an einem Handelsplatz (z. B. einer Börse) oder auch außerhalb (sog. Over-the-Counter-Geschäfte: OTC-Geschäfte) gehandelt werden. Eine zentrale Gegenpartei tritt für den Käufer an die Stelle des Verkäufers und für den Verkäufer an die Stelle des Käufers und übernimmt somit gegenüber beiden die Vertragserfüllung. CCPs haben deshalb im normalen Geschäftsbetrieb immer ein ausgeglichenes Buch, das heißt, für jede Position, die von einer CCP gegenüber einem Marktteilnehmer übernommen wird, gibt es eine entsprechende gegenläufige Position bei einem anderen Marktteilnehmer. In diesem Sinne sind sie Risikomanager für ihre Clearingmitglieder und nur nachrangig Risikoträger.³⁾ Beim Risikomanagement bedient sich die CCP

nur in geringerem Umfang ihres Eigenkapitals, sondern nutzt vor allem die Mittel ihrer Clearingmitglieder. Diese müssen für die jeweils getätigten Geschäfte Sicherheiten hinterlegen (sog. Initial Margins) und zum Schutz des Gesamtsystems als ergänzende Solidarhaftung in einen sogenannten Ausfallfonds einzahlen. Die Nutzung einer CCP dient den Marktteilnehmern nicht nur zur Reduktion ihrer Kreditrisiken gegenüber ihren Geschäftspartnern, sondern erlaubt ihnen, über sogenannte Nettingeffekte bei gegenläufigen Transaktionen in ihrem Gesamtportfolio ihre Finanzierungs- und Kapitalkosten zu senken.

CCPs verfügen üblicherweise über Quasi-Monopolstellungen in Teilmärkten und sind als systemrelevante Finanzmarktinfrastrukturen nicht leicht ersetzbar. Seit die G20-Länder im Jahr 2009 in Pittsburgh vereinbart haben, alle standardisierten OTC-Derivate-Geschäfte über CCPs abzuwickeln, ist die Bedeutung der CCPs für die Funktionsfähigkeit des Finanzsystems weiter gestiegen.⁴⁾ Deshalb wird auf nationaler, europäischer und internationaler Ebene und auch

³ Diese Feststellung gilt zumindest für Verluste, die sich im Zusammenhang mit dem Ausfall eines Clearingmitglieds ergeben können.

⁴ Vgl.: Deutsche Bundesbank, Bedeutung zentraler Gegenparteien gestiegen, Finanzstabilitätsbericht 2016, S. 83–94.

seitens der Bundesbank ein besonderes Augenmerk auf CCPs gelegt.

Überarbeitung des regulatorischen Rahmenwerks

EMIR

Für CCPs wurden die internationalen Anforderungen mit der am 16. August 2012 in Kraft getretenen Verordnung über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (European Market Infrastructure Regulation: EMIR⁵⁾) sowie mit ergänzenden technischen Regulierungsstandards (Regulatory Technical Standards: RTS) auf EU-Ebene in ein rechtlich bindendes Regime überführt. Mit EMIR wurden die CCPs in der EU erstmals einem einheitlichen Aufsichts- und Überwachungsrahmen unterworfen. So wurden die deutschen CCPs Eurex Clearing AG und European Commodity Clearing AG im April beziehungsweise Juni 2014 nach EMIR zugelassen. Neben aufsichtlichen Anforderungen an CCPs werden in EMIR unter anderem auch die Aufgaben und Zusammenarbeit der Behörden bei der Aufsicht und Zulassung von CCPs, die Pflicht zur Abwicklung bestimmter OTC-Derivate über CCPs (sog. Clearing-Pflicht), sowie Meldepflichten zu Derivatekontrakten gesetzlich verankert. EMIR sieht ferner Anerkennungsregelungen für CCPs mit Sitz in Drittstaaten vor, die Dienstleistungen in der EU anbieten möchten. Voraussetzung für die Anerkennung solcher CCPs ist unter anderem die Gleichwertigkeit des Aufsichts- und Regulierungsrahmens des Drittstaates mit EMIR.

EMIR-Review
und REFIT

Bereits im Jahr 2015 begann die Europäische Kommission – wie in EMIR vorgesehen – mit einer Überprüfung des Regulierungsrahmens. Diese Überprüfung ist auch Bestandteil des regulatorischen Eignungs- und Leistungsprogramms der Europäischen Kommission (Regulatory Fitness and Performance Programme: REFIT), mit welchem eine Vereinfachung europäischer Rechtsakte, insbesondere zur Reduzierung von Bürokratie und zur Senkung gesamtgesellschaftlicher Kosten, erzielt werden soll.

Nach dem Abschluss dieser Überprüfung legte die Europäische Kommission im Mai 2017 einen entsprechenden Verordnungsvorschlag zur Änderung von EMIR vor.⁶⁾ Im Ergebnis sieht dieser Verordnungsvorschlag lediglich kleinere Änderungen vor. So sollen zum Beispiel die bisherigen Regelungen zur Aussetzung der Clearingpflicht vereinfacht werden und deren Anwendung im Bedarfsfall schneller als bisher möglich sein. Außerdem sollen Anreize zum zentralen Clearing geschaffen und der Zugang zu CCPs verbessert werden. Der Vorschlag verfolgt zudem das Ziel, eine größere Transparenz hinsichtlich der Berechnung der Sicherheitsanforderungen durch CCPs sicherzustellen.

Vorschläge zur Aufsicht über Drittstaaten-CCPs und zur Änderung des CCP-Aufsichtsregimes über EU-CCPs

Des Weiteren hat sich die Bedeutung des CCP-Geschäftes – unter anderem aufgrund der Clearingpflicht von standardisierten OTC-Geschäften über CCPs – stark erhöht. Aufgrund der globalen Marktstruktur ist dabei eine Konzentration bei CCPs in Drittstaaten, das heißt außerhalb der EU, nicht ausgeschlossen. Dem trägt das bisherige Anerkennungsverfahren nicht mehr genügend Rechnung. Die Problematik der Beaufsichtigung und Überwachung von Drittstaaten-CCPs in Europa wird vor allem durch den bevorstehenden Austritt des Vereinigten Königreichs aus der EU („Brexit“) akzentuiert, da derzeit ein Großteil der außerbörslich gehandelten Zins- und Kreditderivate über CCPs in London geclart wird.

EMIR II

⁵ Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister.

⁶ Vorschlag vom 4. Mai 2017 für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 648/2012 in Bezug auf die Clearingpflicht, die Aussetzung der Clearingpflicht, die Meldepflichten, die Risikominderungstechniken für nicht durch eine zentrale Gegenpartei geclarte OTC-Derivatekontrakte, die Registrierung und Beaufsichtigung von Transaktionsregistern und die Anforderungen an Transaktionsregister.

Noch unterliegen die britischen CCPs dem Aufsichts- und Regulierungsrahmen, der durch EMIR vorgegeben wird. Nach dem wirksamen Austritt des Vereinigten Königreichs aus dem europäischen Binnenmarkt könnte eine Situation entstehen, in der britische CCPs automatisch zu Drittstaaten-CCPs erklärt werden, sofern es keine Anschlussregelungen gibt. Die dort getätigten Geschäfte würden dann außerhalb des gemeinsamen europäischen Aufsichts- und Regulierungsrahmens stattfinden. Dies war einer der Gründe, weshalb die Europäische Kommission im Juni 2017 einen weiteren Vorschlag zur Überarbeitung von EMIR (EMIR II) vorlegte.⁷⁾

Drittstaaten- CCPs

Als Maßstab für die künftige Aufsicht über Drittstaaten-CCPs durch EU-Behörden schlägt die Europäische Kommission die Systemrelevanz einer CCP vor. So sollen zukünftig die Anforderungen an eine Drittstaaten-CCP je nach Grad ihrer systemischen Relevanz für die Finanzstabilität der EU insgesamt oder eines oder mehrerer Mitgliedstaaten unterschiedlich hoch sein. Bei nicht systemrelevanten CCPs („Tier 1“-CCPs) soll das gegenwärtig gültige Verfahren der Prüfung der Gleichwertigkeit des Aufsichts- und Regulierungsrahmens mit EMIR weiterhin Anwendung finden. Systemrelevante CCPs („Tier 2“-CCPs) müssten jedoch wesentliche Anforderungen von EMIR erfüllen und sich weitgehenden Informations- und Kontrollrechten der Europäischen Wertpapier- und Marktaufsichtsbehörde (European Securities and Market Authority: ESMA) unterwerfen. Dabei ist durch Rechtsgutachten zu belegen, dass diese Einräumung rechtswirksam erfolgt. Bei sogenannten substanziiell systemrelevanten CCPs könnte die Europäische Kommission zudem auf Empfehlung der ESMA einen Durchführungsrechtsakt erlassen, wonach eine solche CCP ihre Dienstleistungen innerhalb der EU nur dann anbieten dürfte, wenn sie innerhalb der EU zugelassen und damit auch niedergelassen ist („Lokationserfordernis“). Dies kann vor allem dann erforderlich sein, wenn die Risiken einer substanziiell systemrelevanten Drittstaaten-CCP für die Finanzstabilität in der EU oder einem EU-Mit-

gliedstaat selbst durch Einhaltung strenger aufsichtlicher Vorschriften nicht hinreichend gemindert würden. Aus Sicht der Bundesbank bietet der dreistufige Ansatz der Europäischen Kommission grundsätzlich einen zweckmäßigen Rahmen, um der unterschiedlichen systemischen Bedeutung von CCPs Rechnung zu tragen.

Auch hinsichtlich der Organisation der inner-europäischen Aufsicht schlägt die Europäische Kommission zwei wesentliche Änderungen vor: die Stärkung der ESMA bei der Aufsicht über EU-CCPs und die stärkere Einbindung der betroffenen währungsemittierenden Zentralbank (Central Bank of Issue: CBI). So müssten die national zuständigen Behörden für CCPs – in Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) – für wesentliche Entscheidungen im Zusammenhang mit der Aufsicht über CCPs künftig die Zustimmung der ESMA einholen. Zudem wird vorgeschlagen, innerhalb der ESMA einen sogenannten CCP-Exekutiv Ausschuss zu schaffen, der für allgemeine Aufgaben im Zusammenhang mit CCPs sowie die Aufsicht über EU-CCPs und Drittstaaten-CCPs zuständig sein soll. Aus Sicht der Bundesbank sind diese Vorschläge kritisch einzustufen, weil sich der bisherige Ansatz, zumal erst seit kurzer Zeit in Kraft, im Großen und Ganzen bewährt hat und die Neuerungen nicht zu einer Vereinfachung, sondern zu einer Verkomplizierung des Aufsichtsregimes führen dürften.

Anders ist der Vorschlag der Europäischen Kommission zu bewerten, der währungsemittierenden Zentralbank künftig bei der Autorisierung und laufenden Aufsicht einen größeren Stellenwert einzuräumen. Da negative Auswirkungen auf das reibungslose Funktionieren der Zahlungssysteme, auf das Liquiditätsmanagement

*Stärkung von
ESMA kritisch zu
sehen*

⁷ Vorschlag vom 13. Juni 2017 für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 1095/2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde) sowie der Verordnung (EU) Nr. 648/2012 hinsichtlich der für die Zulassung von zentralen Gegenparteien anwendbaren Verfahren und zuständigen Behörden und der Anforderungen für die Anerkennung zentraler Gegenparteien aus Drittstaaten.

der Clearingteilnehmer und auf die allgemeine Liquiditätslage am Geldmarkt verhindert werden sollten, wäre durch das so erweiterte Mitspracherecht der CBI ein stärkerer Einfluss auf das Risikomanagement der CCP gegeben. Das Eurosystem nimmt schon jetzt die Rolle der CBI für den Euro wahr, und zwar im Wesentlichen durch die Teilnahme an den bestehenden EMIR-Aufsichtskollegien für CCPs. Bei CCPs mit Sitz innerhalb des Euroraums wird das Eurosystem in der Regel durch die nationale Zentralbank im Sitzland der CCP vertreten; außerhalb des Euroraums übernimmt die Europäische Zentralbank (EZB) diese Aufgabe. Die Willensbildung der CBI für den Euro wird in beiden Fällen über die Beschlussorgane des Eurosystems vollzogen, an deren Votum der jeweilige Vertreter gebunden ist. Die Bundesbank vertritt dementsprechend das Eurosystem als CBI gegenüber den deutschen CCPs Eurex Clearing AG und European Commodity Clearing AG.

Rechte des Eurosystems und der EZB

Damit das Eurosystem seine Rolle als währungs-emittierende Zentralbank gemäß der vorgeschlagenen Überarbeitung von EMIR rechtsicher wahrnehmen kann, hat der EZB-Rat beschlossen, dem Europäischen Parlament und dem Rat der Europäischen Union eine Änderung der Satzung des Europäischen Systems der Zentralbanken (ESZB) und der EZB zu empfehlen,⁸⁾ um eine klare Rechtsgrundlage für Regulierungsbefugnisse im Bereich des zentralen Clearings für Finanzinstrumente zu schaffen.

Sanierung und Abwicklung von CCPs

Sanierung und Abwicklung von CCPs

Aufgrund der gestiegenen Bedeutung von CCPs ist es umso wichtiger, dass CCPs sicher und in Krisensituationen widerstandsfähig sind. Die in EMIR vorgegebenen Mindeststandards für das CCP-Risikomanagement sollen grundsätzlich dafür sorgen, dass eine CCP die Verluste aus dem gleichzeitigen Ausfall der beiden Clearingmitglieder mit den größten Risikopositionen unter extremen, aber plausiblen Marktbedingungen abdecken kann. Hierfür halten CCPs

vorfinanzierte Mittel in Form von Einschusszahlungen (Margins) und einem Ausfallfonds bereit. Für darüber hinausgehende Stresssituationen gibt es bisher nur internationale Standards und Leitlinien, nach denen solche Verluste abgedeckt, aber nicht vorfinanziert werden müssen. Gesetzliche EU-Vorgaben gibt es jedoch nicht. Eine EU-Verordnung über ein Sanierungs- und Abwicklungsregime soll diese Regelungslücke schließen.⁹⁾ Sowohl Sanierung als auch Abwicklung einer CCP dienen der Sicherung der Finanzstabilität und der Fortführung der kritischen Funktionen der CCP, wobei der Rückgriff auf staatliche Mittel zum Schutz der Steuerzahler möglichst vermieden werden soll. Ein reguläres Insolvenzverfahren könnte dagegen diese Ziele gefährden, da es vorrangig der Befriedigung der Insolvenzgläubiger dienen würde.

Die Risiken für den Bestand einer CCP können zwei Ursachen haben, nämlich zum einen Verluste aus dem Ausfall von Clearingmitgliedern, die ihren finanziellen Verpflichtungen nicht nachkommen (sog. Default Losses), zum anderen sonstige Verluste zum Beispiel aufgrund von operationellen Risiken oder Investitionsrisiken (sog. Non-Default Losses).

Bei einem Ausfall eines Clearingmitglieds würde ein Ungleichgewicht in dem unter normalen Umständen ausgeglichenen Buch der CCP entstehen.¹⁰⁾ Grundsätzlich sind deshalb Instrumente zur Glattstellung des Buches (Position Allocation Tools) sowie Instrumente zur Ver-

Bestandsbedrohende Risiken für CCPs

⁸ Empfehlung für einen Beschluss des Europäischen Parlaments und des Rates zur Änderung des Art. 22 der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank (EZB/2017/18).

⁹ Vorschlag vom 28. November 2016 für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für die Sanierung und Abwicklung zentraler Gegenparteien und zur Änderung der Verordnungen (EU) Nr. 1095/2010, (EU) Nr. 648/2012 und (EU) Nr. 2015/2365. Am 19. Dezember 2017 wurde ein Kompromissvorschlag des Europäischen Rates veröffentlicht: <http://data.consilium.europa.eu/doc/document/ST-15432-2017-INIT/en/pdf>

Am 31. Januar 2018 wurde ein Bericht des Europäischen Parlaments veröffentlicht: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0015+0+DOC+XML+V0//DE>

¹⁰ Für Verluste, die nicht Folge des Ausfalls eines Clearingmitglieds sind, können CCPs häufig nur auf ihr Eigenkapital zurückgreifen.

Wasserfallprinzip und beispielhafte Sanierungsmaßnahmen einer zentralen Gegenpartei (CCP)

Wasserfallprinzip (vorgegeben durch EMIR)	Instrumente zum Glattstellen des Buchs einer CCP: – Hedging von Positionen – Auktionen und freihändiger Verkauf von Positionen Instrumente zur Verlustallokation: – Einschusszahlungen des ausgefallenen Clearingmitglieds – Beitrag des ausgefallenen Clearingmitglieds zum Ausfallfonds – Zugeordnete Eigenmittel der CCP – Beiträge der nicht ausgefallenen Clearingmitglieder zum Ausfallfonds
Darüber hinausgehende Maßnahmen aus dem Sanierungsplan (von einer CCP mit den Clearingmitgliedern vereinbart)	Instrumente zum Glattstellen des Buchs einer CCP: – Beendigung von Positionen (Termination, full/partial Tear-up) Instrumente zur Verlustallokation: – Nachschusszahlungen der Clearingmitglieder – Beschneidung von Zahlungsverpflichtungen der CCP (Haircut)

Deutsche Bundesbank

lustallokation (Loss Allocation Tools) erforderlich. Zu den Instrumenten der Glattstellung können Auktionen oder bilaterale Verkäufe der Positionen des ausgefallenen Clearingmitglieds gehören. Als weiteres, zwangsweises Glattstellungsinstrument ist zum Beispiel das Fälligstellen von Positionen nicht ausgefallener Clearingmitglieder, die Gegenpositionen zu dem ausgefallenen Clearingmitglied halten (Tear-up, Termination), möglich. Bei diesen Glattstellungsoperationen können Verluste entstehen, die nicht durch die vom ausgefallenen Clearingmitglied gestellten Sicherheiten¹¹⁾ beziehungsweise zusätzliche Eigenmittel der CCP gedeckt sind. Bereits heute sind im Rahmen des regulären Ausfallmanagements bestimmte Instrumente zur Glattstellung sowie zur Verlustallokation vorgesehen, insbesondere die Nutzung der Mittel aus dem vorfinanzierten Ausfallfonds.¹²⁾ Im Verordnungsentwurf der Europäischen Kommission werden weitere Instrumente vorgeschlagen. So können zur Verlustallokation zum Beispiel auch Barnachschüsse (Cash Calls, Assignments) durch die verbliebenen Clearingmitglieder oder die Kürzung der laufend zu berechnenden und auszugleichenden Bewertungsgewinne derjenigen Clearingteilnehmer, die von der CCP Ausgleichszahlungen erhalten (Variation Margin Gains Haircutting, Gains Based Haircutting), zur Anwendung kommen.

Die oben stehende Übersicht gibt einen Überblick über die Mittel, die einer CCP für die Deckung der mit einem Teilnehmerausfall verbundenen Verluste gemäß EMIR zur Verfügung stehen, sowie mögliche Maßnahmen zur Sanierung, falls sich diese Mittel als unzureichend erweisen.

Der Verordnungsentwurf sieht vor, dass die europäischen CCPs künftig Sanierungspläne vorlegen müssen, die insbesondere die Identifizierung kritischer Funktionen, die Stressszenarien, die Beschreibung der Sanierungsinstrumente sowie die Voraussetzungen für ihren Einsatz enthalten sollen.

Während das normale Management des Ausfalls eines Clearingmitglieds noch in weitgehender Selbstverantwortung als Teil des Risikomanagements einer CCP erfolgen kann, erfordern die zwar weiterhin in Eigenverantwortung durchgeführten weitergehenden Maßnahmen einer Sanierung eine stärkere behördliche Begleitung. Für die Sanierungsplanung ist die Einbindung der CCP-Aufsichtsbehörde und eines Kollegiums vorgesehen, in welchem unter anderem die Beteiligung von Aufsichts- und Ab-

Sanierungspläne und Rolle der Behörden

¹¹ Initial Margin und Beitrag des Clearingmitglieds zum Ausfallfonds.

¹² Sog. Wasserfallprinzip nach der EMIR-VO.

wicklungsbehörden wichtiger Clearingmitglieder avisiert ist. Damit sollen einerseits die Interessen und die Leistungsfähigkeit der Clearingmitglieder berücksichtigt und andererseits die Verantwortung der Clearingmitglieder und der jeweils zuständigen Behörden für eine adäquate eigene Risikovorsorge betont werden.

Abwicklung einer CCP

Die Abwicklung einer CCP würde demgegenüber durch die zuständige Abwicklungsbehörde durchgeführt. Die entsprechenden Instrumente sind dabei teilweise mit denen im Sanierungsfall identisch. Den Abwicklungsbehörden sollen ergänzend noch weitere Instrumente, wie etwa die Veräußerung der CCP in Teilen oder als Ganzes sowie die Etablierung einer Brücken-CCP, zur Verfügung stehen.

■ Zentralverwahrer

Central Securities Depositories Regulation

Zentralverwahrer (Central Securities Depositories: CSDs) erbringen wichtige Dienstleistungen für Banken bei der Verwahrung, Abwicklung und Verwaltung von Wertpapieren, die mittelbar den Kunden der Banken zugute kommen. In der Europäischen Union gibt es 28 nationale und zwei internationale Zentralverwahrer. Der durch die internationalen Anforderungen vorgegebene Überwachungsrahmen für Zentralverwahrer befindet sich aufgrund der im September 2014 in wesentlichen Teilen in Kraft getretenen Verordnung über Zentralverwahrer (Central Securities Depositories Regulation: CSDR¹³) sowie ergänzender Rechtsakte auf europäischer Ebene aktuell in einem tief greifenden Umbruchprozess. Vergleichbar mit EMIR dient die CSDR der Überführung der Prinzipien für Finanzmarktinfrastrukturen in ein einheitliches europäisches Aufsichts- und Überwachungsregime für Zentralverwahrer. In einigen Punkten, insbesondere im Bereich der Abwicklungsdisziplin, geht die CSDR inhaltlich sogar über die internationalen Vorgaben hinaus.

Zulassungen nach CSDR

Wie bereits für zentrale Gegenparteien unter EMIR sieht nun auch die CSDR einen einheitlichen europäischen Zulassungsprozess für Zen-

tralverwahrer vor, bei dem die in der CSDR definierten Dienstleistungen der Zentralverwahrer unter Risikogesichtspunkten geprüft und bewertet werden. Nachdem die entsprechenden europäischen Sekundärrechtsakte am 30. März 2017 in Kraft getreten sind, waren Zulassungsanträge der Zentralverwahrer bis zum 30. September 2017 zu stellen. In Deutschland hat die Clearstream Banking AG Frankfurt (CBF) die Zulassung fristgemäß bei der BaFin als zuständiger nationaler (Wertpapier-)Aufsichtsbehörde beantragt. Formal hat die BaFin sämtliche Unterlagen nach Abschluss der Prüfung auf Vollständigkeit an die Überwachungsfunktion der Bundesbank weiterzuleiten, die dann innerhalb von drei Monaten ihren Standpunkt dazu mitteilen kann. Dabei besteht in der Praxis ein enges Kooperationsverhältnis zwischen der BaFin und der Bundesbank, das sich auf Vorbereitung, Vollständigkeitsprüfung und inhaltliche Prüfung des Zulassungsantrags erstreckt. Da die CBF auch über eine Banklizenz verfügt, ist die Bundesbank zusätzlich in ihrer Bankenaufsichtsfunktion in dieses kooperative nationale Aufsichts- und Überwachungsregime eingebunden.

Da der Euro für die im Euroraum angesiedelten nationalen Zentralverwahrer eine der wichtigsten Währungen darstellt, in denen Abwicklungen vollzogen werden, ist im Fall der CBF neben der Bundesbank auch das Eurosystem als CBI in die Zulassungs- und Genehmigungsverfahren einzubeziehen. Analog zur Handhabung der CBI-Rolle bei der CCP-Aufsicht wird die Bundesbank das Eurosystem als CBI im Außenverhältnis gegenüber der CBF vertreten. Im Innenverhältnis wird die Bundesbank insoweit jedoch an die Vorgaben der Beschlussorgane des Eurosystems gebunden sein. Die Stellung des Eurosystems als CBI hat eine über den Zulassungsprozess hinausgehende Bedeutung. Da alle geldpolitischen Geschäfte zwischen Banken und

Eurosystem als CBI

¹³ Verordnung Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012.

dem Eurosystem besichert werden müssen und die marktfähigen Sicherheiten bei einem Zentralverwahrer gelagert oder umgebucht werden, ist das Eurosystem ein wichtiger Nutzer der von Zentralverwahrern angebotenen Abwicklungsdienstleistungen. Bisher führte das Eurosystem aus der Nutzersicht heraus eigenständige Prüfungen und Bewertungen der von Zentralverwahrern betriebenen Wertpapierabwicklungssysteme durch. Diese sollen in absehbarer Zeit aufgegeben werden, da sie sich inhaltlich in weiten Teilen mit den Vorgaben der CSDR überschneiden. Zukünftig sollen dann die aus der CBI-Rolle des Eurosystems heraus gewonnenen Erkenntnisse über die Risikolage genutzt werden, um die Eignung der betreffenden Zentralverwahrer für die geldpolitischen Geschäfte des Eurosystems sicherzustellen.¹⁴⁾

end hat das EPTF vom 23. August bis zum 15. November 2017 eine öffentliche Marktkonsultation durchgeführt, um Trends im Nachhandelsbereich zu identifizieren, Marktbarrieren aufzubrechen und bestehende Risiken besser beherrschen zu können. Alle diese Anstrengungen verfolgen letztlich das übergeordnete Ziel, die europäische Nachhandelslandschaft in Zukunft noch effizienter, wettbewerbsorientierter und vor allem sicherer zu machen. Das EPTF beschäftigt sich darüber hinaus auch mit der Frage, wie sich neue Technologien (z. B. Blockchain) und Angebote von innovativen FinTechs auf die Wertpapierabwicklung auswirken.

Systemrelevante Zahlungsverkehrssysteme

CSDR und T2S

Die durch das Eurosystem betriebene Plattform TARGET2-Securities (T2S)¹⁵⁾ ist bei rechtlicher Betrachtung weder als Zentralverwahrer noch als Wertpapierabwicklungssystem einzuordnen und fällt daher nicht in den unmittelbaren Anwendungsbereich der CSDR. Als technische Plattform für die Wertpapierabwicklung in Zentralbankgeld erbringt T2S jedoch zentrale Dienstleistungen für die teilnehmenden Zentralverwahrer. Daraus ergibt sich eine mittelbare Betroffenheit in der Form, dass T2S den teilnehmenden Zentralverwahrern eine vollständige Einhaltung der Vorgaben der CSDR ermöglichen muss.

EPTF

Eine wichtige Rolle bei der Beseitigung von im Nachhandelsbereich verbliebenen Hindernissen bei der Integration der europäischen Finanzmärkte sowie der vollumfänglichen Realisierung einer europäischen Kapitalmarktunion soll dem im Jahr 2016 von der Europäischen Kommission etablierten europäischen Forum für den nachbörslichen Handel (European Post-Trade Forum: EPTF) zukommen.¹⁶⁾ In einem Bericht vom 15. Mai 2017 setzt sich diese Expertengruppe näher mit den sogenannten Giovannini-Barrieren¹⁷⁾ auseinander und gibt einen Überblick zu weiterhin bestehenden und neu identifizierten Hürden. Auf diesem Bericht aufbau-

Im Juli 2014 machte die EZB erstmalig von ihrer Verordnungsermächtigung im Bereich der Zahlungsverkehrsüberwachung¹⁸⁾ Gebrauch. Die Verordnung zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (Regulation on the oversight requirements for systemically important payment sys-

SIPS-Verordnung

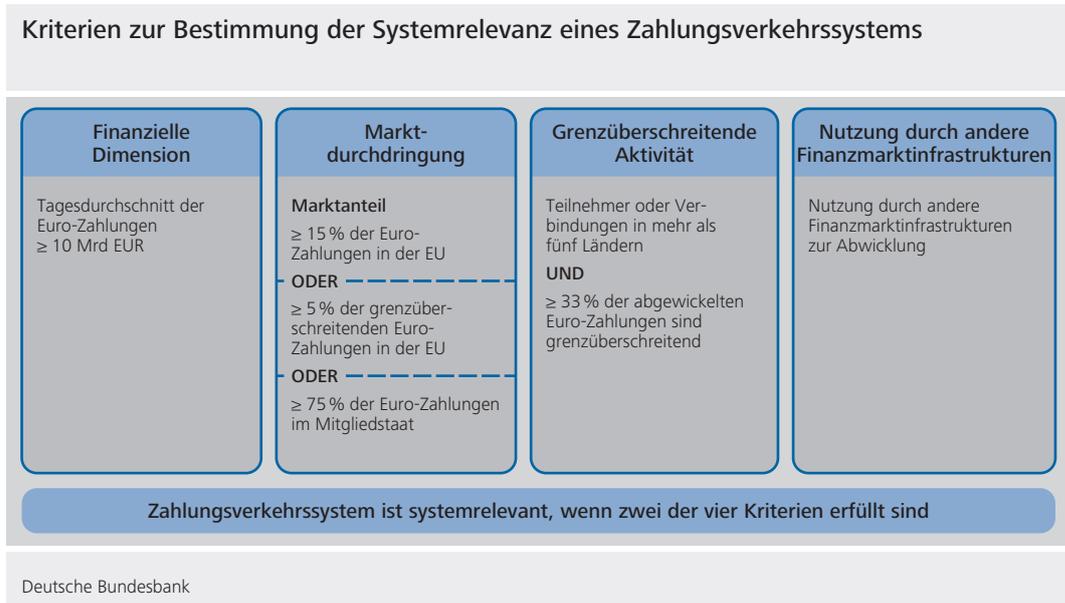
¹⁴ In diesem Zusammenhang waren auch Aktualisierungen der Leitlinien über die Durchführung der Geldpolitik des Eurosystems erforderlich, die seit dem 18. April 2018 zur Anwendung kommen, vgl. Art. 2 der Leitlinie EZB/2018/3 vom 7. Februar 2018.

¹⁵ Vgl. hierzu: Deutsche Bundesbank, Die Finanzmarktinfrastruktur des Eurosystems – Rückblick und zukünftige Ausrichtung des Leistungsangebots, Monatsbericht, Dezember 2017, S. 69–88.

¹⁶ Dem ESZB kommt beim EPTF lediglich eine Beobachterrolle zu. Teilnehmer am EPTF sind insbesondere Vertreter aus Interessenverbänden und unabhängige Experten.

¹⁷ Der Begriff geht auf die nach ihrem Vorsitzenden Alberto Giovannini benannte Giovannini-Gruppe zurück, die in den Jahren 2001 und 2003 Berichte zu grenzüberschreitenden Clearing- und Abwicklungsvereinbarungen an den EU-Wertpapiermärkten veröffentlichte und verschiedene Barrieren identifizierte (https://ec.europa.eu/info/publications/giovannini-reports_en).

¹⁸ Die Überwachung (Oversight) von Zahlungsverkehr und Abwicklungssystemen ist eine Zentralbankaufgabe zur Förderung der Sicherheit und Effizienz. Dabei werden bestehende und geplante Systeme beobachtet, in Hinblick auf ihre Sicherheit und Effizienz überprüft und ggf. Veränderungen herbeigeführt. Vgl. hierzu: Deutsche Bundesbank, Zahlungsverkehrsüberwachung – ein Beitrag zur Stabilität des Finanzsystems und zur Effizienz des Zahlungsverkehrs, Monatsbericht, Januar 2004, S. 29–46.



tems: SIPS-Verordnung¹⁹⁾) regelt Zuständigkeiten, Rechte und Pflichten bei der Überwachung systemrelevanter Zahlungsverkehrssysteme. Die SIPS-Verordnung geht in ihren Anforderungen – wie auch die CSDR – über die internationalen Anforderungen hinaus. So sind systemrelevante Zahlungsverkehrssysteme dazu verpflichtet, den finalen Zahlungsausgleich am Tagesende in Zentralbankgeld vorzunehmen.

Im August 2014 identifizierte das Eurosystem vier Zahlungsverkehrssysteme als systemrelevant (vgl. Tabelle auf S. 53): das vom Eurosystem betriebene Zahlungsverkehrssystem TARGET2 sowie die kommerziellen Systeme EURO1, STEP2-T und CORE(FR). Als zuständige Behörde wurde für das letztgenannte System die Banque de France, für die übrigen Systeme die EZB benannt. Die Bundesbank beteiligt sich an diesen Überwachungsaktivitäten der EZB im Eurosystem. Das von der Bundesbank betriebene Massenzahlungsverkehrssystem Elektronischer Massenzahlungsverkehr erfüllt demgegenüber nicht die oben genannten Kriterien und gilt somit als sonstiges Massenzahlungsverkehrssystem, das nur in Teilbereichen ausgewählten Prinzipien Rechnung tragen muss.

Systemrelevanz wird dabei bemessen an einer Kombination aus unterschiedlichen Kriterien, nämlich der Höhe der abgewickelten Beträge, der Marktdurchdringung, dem Umfang der grenzüberschreitenden Aktivitäten sowie der Nutzung durch andere Finanzmarktinfrastrukturen (vgl. oben stehendes Schaubild). Einmal jährlich überprüft das Eurosystem, welche Zahlungsverkehrssysteme systemrelevant im Sinne der SIPS-Verordnung sind und benennt für jedes System, welches die Voraussetzungen erfüllt, eine zuständige Überwachungsbehörde aus dem Kreis des Eurosystems. Diese ist für die Überprüfung des Zahlungsverkehrssystems in Bezug auf die Einhaltung der SIPS-Verordnung zuständig und hat dann das Recht, Auskünfte vom Systembetreiber einzuholen und bei Notwendigkeit Korrekturmaßnahmen anzuordnen. Sollten Verstöße gegen die Verordnung festgestellt werden, so darf die EZB Sanktionen gegen den Systembetreiber verhängen.

Im November 2017 verabschiedete der EZB-Rat Änderungen an der SIPS-Verordnung.²⁰⁾ Diese umfassen im Wesentlichen eine strengere Würdigung von Kredit- und Liquiditätsrisiken, neue Anforderungen an die Cyber-Widerstandsfähig-

Überarbeitung der SIPS-Verordnung

Systemrelevanz und Aufgaben der Überwachungsbehörden

¹⁹ Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank vom 3. Juli 2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (EZB/2014/28).

²⁰ Verordnung (EU) 2017/2094 der Europäischen Zentralbank vom 3. November 2017 zur Änderung der Verordnung (EU) Nr. 795/2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (EZB/2017/32).

keit und neue Kompetenzen der für die Überwachung zuständigen Behörden. So kann der Überwacher künftig eine unabhängige Überprüfung des Systems anordnen. Einzelne Aspekte des Systems können dann im Detail von Experten geprüft werden, zum Beispiel wenn die zuständige Behörde selbst nicht über die hierzu notwendige Expertise verfügt. Zum anderen kann die zuständige Behörde auch Vor-Ort-Prüfungen durchführen.

Cyber-Widerstandsfähigkeit

Mit der Überarbeitung trägt das Eurosystem auch insbesondere der gestiegenen Bedrohung durch Cyber-Risiken in den letzten Jahren Rechnung. Dabei wird jedoch auf genaue Vorgaben, wie die Cyber-Widerstandsfähigkeit im Einzelnen zu erreichen ist, verzichtet. Allerdings wurde hierzu bereits im Juni 2016 vom Committee on Payments and Market Infrastructures (CPMI) und der International Organization of Securities Commissions (IOSCO) eine „Guidance on cyber resilience for financial market infrastructures“²¹⁾ veröffentlicht. Hierin werden allgemein gehaltene Ziele für die Stärkung der Cyber-Widerstandsfähigkeit formuliert, wobei die Wege zum Erreichen dieser Ziele individuell von der jeweiligen Finanzmarktinfrastruktur bestimmt werden können. Die wichtigsten Aspekte der Guidance sind dabei:

- Der Cyber-Widerstandsfähigkeit soll auch auf Vorstandsebene Aufmerksamkeit geschenkt werden.
- Der Fähigkeit, nach einem erfolgreichen Cyber-Angriff den Betrieb schnell und sicher wieder aufnehmen zu können, soll oberste Priorität eingeräumt werden.
- Die Cyber-Widerstandsfähigkeit soll regelmäßig getestet und Informationen zur Bedrohungslage ausgewertet werden.
- Die Bedeutung der Cyber-Widerstandsfähigkeit soll sich in der Unternehmenskultur widerspiegeln.

Zahlungsvolumen in systemrelevanten Zahlungsverkehrssystemen²⁾

2016, insgesamt

SIPS	Stückzahlen (in Millionen)	Umsatz (in Mrd €)
TARGET2	89,0	485 811,8
EURO1	53,3	41 103,6
STEP2-T	10 419,0	13 169,3
CORE(FR)	14 432,2	5 513,0
Gesamt	24 993,5	545 597,7

* Quelle: Statistical Data Warehouse der EZB.

Deutsche Bundesbank

- Die Stärkung der Cyber-Widerstandsfähigkeit bedarf gemeinschaftlicher Anstrengungen der gesamten Industrie.

Zwischenzeitlich hat das Eurosystem konkrete Überwachungsanforderungen erarbeitet, um die Guidance im Euroraum anzuwenden. Diese Anforderungen werden derzeit mit dem Markt²²⁾ konsultiert. Dabei sollen sie nicht nur die Überprüfung der Finanzmarktinfrastrukturen durch die Überwachungsbehörden erleichtern, sondern den Infrastrukturbetreibern detaillierte Schritte zur Verbesserung der Cyber-Widerstandsfähigkeit aufzeigen und den Dialog zwischen Betreibern und Überwachungsbehörden zum Erreichen dieses Zieles in enger Zusammenarbeit fördern.

Zahlungsdienste

Mit der sogenannten Zahlungsdiensterichtlinie (Payment Services Directive: PSD) aus dem Jahr 2009 wurde ein einheitlicher Rechtsrahmen für die Abwicklung von Zahlungen in der EU geschaffen. Ihre Überarbeitung zur sogenannten PSD2 ...

²¹ Siehe auch: <https://www.bis.org/cpmi/publ/d146.htm>
²² Siehe: Pressenotiz der EZB vom 10. April 2018, ECB launches public consultation on cyber resilience oversight expectations.

PSD 2²³⁾ dürfte nunmehr zu tief greifenden Veränderungen am Markt für Zahlungsdienste führen.

Mit ihrer Neufassung soll die PSD2 zum einen die Marktintegration innerhalb der Europäischen Union weiter vertiefen und zu einer Stärkung des Wettbewerbs und der Verbraucherrechte beitragen. Zum anderen sollen neue Regelungen die Sicherheit im Massenzahlungsverkehr insbesondere bei der Nutzung innovativer Bezahlförmlichkeiten, wie zum Beispiel beim Bezahlen mittels Mobiltelefon, weiter erhöhen.

... seit Januar 2018 in nationales Recht umgesetzt

Die PSD2 war bis zum 13. Januar 2018 in nationales Recht umzusetzen. In Deutschland geschah dies unter anderem durch Änderungen im Bürgerlichen Gesetzbuch und dem Zahlungsdienstenaufsichtsgesetz (ZAG) durch das Gesetz zur Umsetzung der Zweiten Zahlungsdiensterrichtlinie vom 17. Juli 2017, das am 13. Januar 2018 in Kraft trat.

Neue Zahlungsdienstleister ...

Eine wesentliche Neuerung der PSD2 ist die Aufnahme von Zahlungsauslösediensten (ZAD) und Kontoinformationsdiensten (KID) in die Liste der Zahlungsdienste. Während die Anbieter von ZAD insbesondere im Zusammenhang mit der Bezahlung von Käufen im „e-commerce“ den Überweisungsauftrag eines Kunden bei dessen Institut auslösen, stellen Anbieter von KID konsolidierte Informationen über ein oder mehrere Zahlungskonten ihrer Kunden bereit, die bei anderen Zahlungsdienstleistern geführt werden. Mit der PSD2 wird das Zusammenspiel von kontoführenden Kreditinstituten und diesen sogenannten Drittanbietern, die sich bereits seit Mitte der 2000er Jahre am Markt befinden, nunmehr gesetzlich geregelt.

... erfordern neue Regelungen

Da bei der Erbringung von ZAD und KID ein zusätzlicher Dienstleister tätig wird, der sich in der Prozesskette zwischen Kunde und kontoführendem Institut einfügt, waren sowohl bestehende Regelungen anzupassen als auch neue Vorgaben einzuführen. Die hieraus resultierenden Änderungen betreffen sowohl spezifische Rechte und Pflichten der neuen Anbieter ihren

Kunden gegenüber, wie etwa beim Umgang mit vertraulichen Kundendaten, als auch Regelungen, die ihr Verhältnis zu den kontoführenden Instituten betreffen, vor allem im Hinblick auf die Identifizierungspflicht und sichere Kommunikation. Die bislang geltenden Transparenzanforderungen und Informationspflichten für Zahlungsdienstleister bleiben hingegen weitestgehend unverändert.

Schließlich enthält die PSD2 neben einer Stärkung von Verbraucherrechten auch eine Reihe von Neuregelungen, um die Sicherheit im Massenzahlungsverkehr zu erhöhen und einen besseren Schutz der Finanzdaten von Kunden zu erreichen. Die vielleicht wichtigste Neuerung regelt die Verpflichtung des Zahlungsdienstleisters zur Nutzung der sogenannten starken Kundenauthentifizierung.²⁴⁾ Diese ist immer dann erforderlich, wenn erstens, ein Kunde online, das heißt per Internet oder mobil, auf sein Konto zugreift, zweitens, er einen elektronischen Zahlungsvorgang auslöst oder, drittens, über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs oder anderen Missbrauchs birgt. Für elektronische Fernzahlungen muss die starke Kundenauthentifizierung außerdem Elemente umfassen, die die Zahlung dynamisch mit dem jeweiligen Betrag und Empfänger verknüpfen.

In wichtigen Bereichen enthält die PSD2 nur allgemeine Regelungen, die der Konkretisierung bedürfen. Hierzu wurden der Europäischen Bankenaufsichtsbehörde (European Banking Authority: EBA) in Zusammenarbeit mit der EZB in der PSD2 drei Mandate für die Erarbeitung von technischen Regulierungsstandards (Regu-

Mehr Sicherheit im Massenzahlungsverkehr

Mandate für die Europäische Bankenaufsichtsbehörde

²³ Siehe auch: Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG.

²⁴ Gemäß Art. 4 (30) PSD2 bzw. § 1 (24) ZAG erfordert starke Authentifizierung die Nutzung von mindestens zwei voneinander unabhängigen Faktoren aus zwei der drei Kategorien Wissen (= etwas, das nur der Nutzer weiß, wie z. B. ein Passwort), Besitz (= etwas, das nur der Nutzer besitzt, wie z. B. eine Zahlungskarte) oder Inhärenz (= etwas, das der Nutzer ist, wie z. B. ein Fingerabdruck).

latory Technical Standards, RTS) und Leitlinien erteilt.²⁵⁾

*Technische
Regulierungs-
standards zur
starken Kunden-
authentifizierung
und sicheren
Kommunikation*

Besondere Aufmerksamkeit erlangte die Diskussion um die RTS der EBA zur starken Kundenauthentifizierung und sicheren Kommunikation. Diese RTS entwickelte die EBA in Zusammenarbeit mit der EZB und mehreren Zentralbanken aus dem Europäischen Wirtschaftsraum, darunter auch der Bundesbank. Am 13. März 2018 wurden sie von der Europäischen Kommission als delegierter Rechtsakt veröffentlicht. Sie konkretisieren unabhängig von der jeweils genutzten Technologie und dem jeweiligen Geschäftsmodell die Anforderungen an die Form der Authentifizierung, die Zahlungsdienstleister von ihren Kunden fordern müssen, sowie mögliche Ausnahmen von der starken Authentifizierung (vgl. nebenstehende Übersicht). Darüber hinaus enthalten sie Regelungen zum Schutz personalisierter Sicherheitsmerkmale und zur Ausgestaltung von gemeinsamen und sicheren Standards für die Kommunikation zwischen den verschiedenen Anbietern von Zahlungsdiensten sowie zwischen Zahlungsdienstleistern und ihren Kunden.

Kern dieses zweiten Teils der Standards ist die Verpflichtung für die kontoführenden Institute, für Anbieter von ZAD und KID mindestens eine Schnittstelle zum Kundenkonto bereitzustellen. Diese Öffnung des Bankkontos für andere Anbieter von Zahlungsdiensten kann über die bestehende Online-Banking-Schnittstelle des Kunden oder über eine neue dedizierte Schnittstelle, ein sogenanntes Application Programming Interface (API), erfolgen und erfordert jeweils eine Identifizierung des Drittanbieters gegenüber dem kontoführenden Institut. Wenn sich kontoführende Institute für das Angebot einer dedizierten Schnittstelle entscheiden, muss diese die gleiche Verfügbarkeit und Leistungsfähigkeit aufweisen wie der direkte Zugang der Kunden zu ihrem Konto. Weiterhin haben die kontoführenden Institute bei Vorhal-

²⁵ Weitere acht Mandate sind rein bankaufsichtlicher Natur und ausschließlich an die EBA gerichtet.

Starke Kundenauthentifizierung

Anforderungen an eine starke Authentifizierung

- Generierung eines Authentifizierungscodes aus mindestens zwei voneinander unabhängigen Elementen unterschiedlicher Kategorien (Wissen, Besitz, Inhärenz)
- Bei Fernzahlungen dynamische Bindung des Authentifizierungscodes an Betrag und Zahlungsempfänger

Ausnahmen von der starken Authentifizierung

- Kontozugang ohne Zugriff auf sensitive Zahlungsdaten
- Kontaktlose Transaktionen am Point of Sale bis 50 €
- Beförderungsentgelte und Parkgebühren an unbedienten Terminals
- Elektronische Fernzahlungen an vertrauenswürdige Empfänger/als wiederkehrende Zahlungen (gleicher Zahlungsempfänger und Betrag)/an den Zahler selbst/bis zu 30 €
- Unternehmenszahlungen auf Basis sicherer Prozesse und Protokolle
- Zahlung mit niedrigem Risiko gemäß Echtzeit-Transaktionsrisikoanalyse

Maßnahmen zum Schutz der persönlichen Sicherheitsmerkmale

- Sicherstellung von Vertraulichkeit und Integrität der Authentifizierungscodes während des gesamten Authentifizierungsvorgangs
- Sicherstellung von Vertraulichkeit und Integrität der Sicherheitsmerkmale über ihren gesamten Lebenszyklus

ten einer API eine Rückfalllösung für Notfälle bereitzustellen, über welche die Anbieter von ZAD und KID, ebenfalls nach vorheriger Identifikation gegenüber dem kontoführenden Institut, auf das Kundenkonto zugreifen können. Von dieser Verpflichtung können kontoführende Institute allerdings unter bestimmten Voraussetzungen von ihrer nationalen Aufsichtsbehörde entbunden werden. Die RTS treten 18 Monate nach ihrer Veröffentlichung in Kraft. Damit wird dann auch die aktuelle Praxis von ZAD- und KID-Anbietern, ohne vorherige Identifizierung auf Kundenkonten zuzugreifen, für alle der PSD2 unterliegenden Zahlungskonten verboten.

Leitlinien zum Management von operationellen und sicherheitsrelevanten Risiken

Bereits im Dezember 2017 verabschiedete die EBA Leitlinien über Sicherheitsmaßnahmen und Kontrollmechanismen zur Eindämmung von operationellen und sicherheitsrelevanten Risiken, die sich aus dem Angebot von Zahlungsdiensten ergeben. Unter Beachtung des Grundsatzes der Proportionalität entwickelten EBA und EZB – in Anlehnung an die bereits bestehenden EBA-Leitlinien zur Sicherheit von Internetzahlungen und andere Standards und Rahmenwerke – Anforderungen unter anderem zu Governance, Risikobewertung, dem Schutz von Daten und Systemen, Business Continuity und der Durchführung von Tests. Die neuen Regelungen haben einen weiteren Anwendungsbereich als die bisherigen EBA-Leitlinien, da sie für alle der PSD2 unterliegenden Anbieter und Zahlungsdienste gelten. Sie sind von den nationalen Aufsichtsbehörden in ihre jeweilige Aufsichtspraxis umzusetzen.

Leitlinien für die Meldung von schwerwiegenden Sicherheitsvorfällen

Die Leitlinien für die Meldung von schwerwiegenden Sicherheitsvorfällen sind seit dem 13. Januar 2018 in Kraft. Sie verpflichten Anbieter von Zahlungsdiensten, relevante Zwischenfälle an die für sie zuständige Aufsichtsbehörde zu melden. In Deutschland ist dies die BaFin. Diese leitet die Meldungen an Bundesbank, EBA und EZB weiter, sowie bei entsprechender Relevanz des Vorfalls auch anonymisiert an andere nationale Behörden.

Neben der PSD2 und ihren nachgeordneten Rechtsakten üben weitere europäische Regelungen und Vorhaben erheblichen Einfluss auf die Erbringung von Zahlungsdiensten aus. Hierzu gehören zum Beispiel die sogenannte Vierte Geldwäscherichtlinie sowie die neue Geldtransferverordnung, die im Einklang mit derzeit geltenden internationalen Standards und Empfehlungen den Rechtsrahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung modernisieren.²⁶⁾

Bekämpfung von Geldwäsche und Terrorismusfinanzierung ...

Daraus resultieren unter anderem Neuerungen bei der Kundenidentifizierung, beispielsweise zur Eröffnung eines Zahlungskontos durch Verbraucher auf elektronischem Wege. So werden im deutschen Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie zur Authentifizierung bei Online-Diensten unter bestimmten Voraussetzungen auch elektronische Identifizierungsmittel im Sinne der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen²⁷⁾ anerkannt. Dies kann zum Beispiel ein elektronischer Personalausweis oder eine Chipkarte sein, auf denen Daten gespeichert sind, die zur Identifizierung einer Person genutzt werden. Darüber hinaus wird auch die Nutzungsmöglichkeit von sogenannten Video-Ident-Verfahren erwähnt, welche die BaFin für in Deutschland tätige Institute bereits geregelt hat. Diese Entwicklungen können zur besseren Etablierung vollständig

... fördert Unterstützung digitaler Geschäftsprozesse durch elektronische Identifizierung

²⁶ Siehe auch: Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission sowie Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006.

²⁷ Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Laut Art. 3 Ziffer 12 der Verordnung ist ein elektronisches Identifizierungsmittel „eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird“.

digitaler Geschäftsprozesse beitragen und damit helfen, das Potenzial der Digitalisierung noch besser auszuschöpfen.

*„Aktionsplan
Finanzdienst-
leistungen für
Verbraucher:
bessere Pro-
dukte, mehr
Auswahl“*

Im März 2017 schließlich hat die Europäische Kommission den „Aktionsplan Finanzdienstleistungen für Verbraucher: bessere Produkte, mehr Auswahl“ veröffentlicht. Konkret hat die Europäische Kommission am 28. März 2018 einen Vorschlag vorgelegt, mit dem künftig in der gesamten EU die Gebühren für grenzüberschreitende Euro-Zahlungen auf das Niveau für inländische Zahlungen angeglichen würden. Bislang gilt diese Regelung nur für den Euro-Raum. Zudem soll die Transparenz im Hinblick auf die Währungsumrechnung bei Zahlungen in Fremdwährung verbessert und damit der Wettbewerb gestärkt werden.²⁸⁾

■ Fazit

Widerstandsfähige Finanzmarktinfrastrukturen sind aufgrund ihrer zentralen Funktion für die Abwicklung von Finanztransaktionen sowohl für das Finanzsystem als auch für die Realwirtschaft von überragender Bedeutung. Störungen in diesen kritischen Komponenten können erhebliche Implikationen für die teilnehmenden Banken, für die Finanzmärkte sowie für die Aufgabenerfüllung durch das Eurosystem entfalten. Denn Zentralbanken sind zum Beispiel in starkem Maße auf die Dienste von Zentralverwahrern angewiesen, um Sicherheiten für geldpolitische Kredite an Geschäftspartner entgegenzunehmen oder Wertpapiere im Rahmen der derzeitigen Ankaufprogramme zu verwahren. Neben einer wirkungsvollen Aufsicht und Überwachung ist auch das Angebot von Abwicklungsleistungen in hochliquidem und hochsicherem Zentralbankgeld aus Gründen der Risikoreduktion und der Finanzstabilität von großer Bedeutung.

Angesichts der gestiegenen Bedrohungslage hat die Stärkung der Cyber-Widerstandsfähigkeit der Finanzmarktinfrastrukturen für die Aufsicht und die Überwachung eine besonders

hohe Priorität. In diesem Zusammenhang ist zu berücksichtigen, dass die fortschreitende Digitalisierung neben Effizienzgewinnen neue Angriffsflächen bietet und die Risikolage für die Betreiber von Marktinfrastrukturen verändert. Dabei ist es in erster Linie in der Verantwortung der Systembetreiber und Marktteilnehmer, selbst Maßnahmen zu ergreifen, um das Schutzniveau zu erhöhen. Dies ist nicht nur eine Frage von technischen Vorrichtungen, sondern auch der Unternehmenskultur. Angesichts der hohen Dynamik kommt dabei vonseiten der Überwachung ein neuer Ansatz zur Anwendung, bei dem nicht die Erfüllung von konkreten Vorgaben überprüft wird, sondern der Reifegrad der Abwehrmaßnahmen analysiert und auf dessen Steigerung hingearbeitet wird. Einen wichtigen Beitrag hat das Eurosystem zudem mit der Errichtung des European Cyber Resilience Boards (ECRB) geleistet. Hierdurch soll der Dialog zwischen europäischen Finanzmarktinfrastrukturen und Notenbanken sowie weiteren Regulatoren auf dem Gebiet der Cyber-Widerstandsfähigkeit gefördert werden.

Weitere wichtige Weichenstellungen stehen im Bereich der zentralen Gegenparteien an. Nachdem das zentrale Clearing in den letzten Jahren zunehmend an Bedeutung gewonnen hat, kommt es nunmehr darauf an, die Arbeiten am europäischen Sanierungs- und Abwicklungsregime für CCPs bald zu vollenden. Ziel muss sein, ein glaubwürdiges Regime zu etablieren, das die Finanzstabilität gewährleistet und im Ernstfall möglichst ohne Rückgriff auf staatliche Mittel auskommt. Mit Blick auf das zukünftige Aufsichtsregime für zentrale Gegenparteien in Drittstaaten kommt aus Sicht der Bundesbank einer funktionierenden Aufsicht durch die Behörden der EU-Mitgliedstaaten unter Einhaltung der in der EU geltenden Regulierung entscheidende Bedeutung zu. Entsprechend muss sich die Bewertung konkreter Handlungsoptionen

²⁸ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 924/2009 in Bezug auf Entgelte für grenzüberschreitende Zahlungen in der Union und Entgelte für Währungsumrechnungen SWD (2018)84.

vor allem an der Sicherheit des Zahlungsverkehrs und der Abwicklung von Wertpapier- und Derivategeschäften und weniger an den Kosten orientieren. In jedem Fall sollte das Eurosystem wegen der vielfältigen Wechselwirkungen mit seinen Aufgaben in angemessener Weise an der Aufsicht beteiligt werden.

Durch die PSD2 werden die Regeln im EU-Zahlungsverkehr deutlich geändert. Insbesondere durch die Möglichkeit für Drittparteien, Kunden innovative Dienste auf Basis eines Zugangs zu ihren Konten anzubieten (sog. „open banking“), wird erwartet, dass etablierte Strukturen im Markt für Zahlungsdienste aufgebrochen werden. Die Regelungen der PSD2 sowie der zugehörigen RTS bieten aus Sicht der Bundesbank eine gute Ausgangsbasis für die weitere Digitalisierung des Zahlungsverkehrs, insbesondere durch mehr Wettbewerb bei einem gleichzeitig erhöhten Sicherheitsniveau. Um flächendeckend für eine zunehmende Wettbewerbs-

intensität in der EU zu sorgen und die Fragmentierung in nationale Märkte zu überwinden, ist die konsistente Umsetzung der PSD2 und die Anwendung der RTS in allen Mitgliedstaaten eine wichtige Voraussetzung. Zudem muss darauf geachtet werden, dass die Bereitstellung von kreditwirtschaftlichen dedizierten Schnittstellen (APIs), auf die sowohl Drittdienstleister als auch andere Kreditinstitute zugreifen können, ausreichend standardisiert erfolgt. Nur dann können sich neue für den Verbraucher attraktive Angebote im einheitlichen Euro-Zahlungsverkehrsraum entwickeln. Ob diese neuen Produkte stärker von traditionellen Kreditinstituten, Start-ups oder bereits bestehenden Internetplattformen auf den Markt gebracht werden, ist derzeit nur schwer abzuschätzen. Allerdings scheinen die marktführenden Kreditinstitute erkannt zu haben, dass die PSD2 durchaus Chancen bietet, das Serviceniveau des Zahlungskontos für die eigenen Kunden und damit auch die eigene Attraktivität zu erhöhen.