STELLUNGNAHME DER EUROPÄISCHEN ZENTRALBANK

vom 11. April 2022

zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Einleitung und Rechtsgrundlage

Am 16. Dezember 2020 verabschiedete die Europäische Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 ([1]) (nachfolgend der „Richtlinienvorschlag"). Am 3. Dezember 2021 hat der Rat der Europäischen Union seine allgemeine Ausrichtung in Bezug auf den Richtlinienvorschlag ([2]) festgelegt. Die Zuständigkeit der Europäischen Zentralbank (EZB) zur Abgabe einer Stellungnahme beruht auf Artikel 127 Absatz 4 Unterabsatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), da der Richtlinienvorschlag Bestimmungen enthält, die in den **Zuständigkeitsbereich** der EZB fallen; hierzu gehören insbesondere die Förderung des reibungslosen Funktionierens der Zahlungssysteme, die Mitwirkung bei der reibungslosen Durchführung der von den zuständigen Behörden auf dem Gebiet der Stabilität des Finanzsystems ergriffenen Maßnahmen und die Aufgaben der EZB im Zusammenhang mit der Aufsicht über die Kreditinstitute gemäß Artikel 127 Absatz 2 vierter Gedankenstrich sowie Artikel 127 Absatz 5 und Artikel 127 Absatz 6 AEUV. Diese Stellungnahme wurde gemäß Artikel 17.5 Satz 1 der Geschäftsordnung der Europäischen Zentralbank vom EZB-Rat verabschiedet.

Allgemeine Anmerkungen

Die EZB begrüßt ausdrücklich die im Richtlinienvorschlag festgelegten Ziele, das Cyberresilienzniveau in allen relevanten Sektoren zu erhöhen, eine einheitliche Resilienz im Binnenmarkt zu fördern und die Lageerfassung und kollektive Vorsorge und Reaktionsfähigkeit zu verbessern, indem eine effiziente Zusammenarbeit in der Union gewährleistet wird.

Die EZB erkennt an, wie wichtig es ist, enge Verbindungen zwischen dem Richtlinienvorschlag und dem Finanzsektor aufrechtzuerhalten, der weiterhin Teil des Ökosystems der Netz- und Informationssysteme (NIS) bleiben sollte, um die einheitliche Bewertung der Risiken im Zusammenhang mit der Informations- und Kommunikationstechnologie (IKT) in der gesamten Union sowie die Wirksamkeit des Informationsaustauschs und der Zusammenarbeit zwischen den einzelnen Sektoren beim Umgang mit Cyberbedrohungen zu fördern. Zu diesem Zweck sollten die gemäß dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors ([3]) (nachfolgend die „DORA-Verordnung") zuständigen Behörden die Möglichkeit haben, sich an den strategischen politischen Diskussionen und der technischen Arbeit der NIS-Kooperationsgruppe zu beteiligen und mit den im Richtlinienvorschlag genannten zentralen Anlaufstellen und nationalen Reaktionsteams für IT-Sicherheitsvorfälle (Computer Security Incident Response Teams – CSIRTs) Informationen auszutauschen und weitergehend zusammenzuarbeiten ([4]).

1. Anwendungsbereich des Richtlinienvorschlags

1.1 Die EZB geht davon aus, dass die DORA-Verordnung in Bezug auf Einrichtungen des Finanzsektors als sektorspezifischer Rechtsakt betrachtet wird, mit dem Anforderungen an das Cybersicherheitsrisikomanagement und die Meldung von Sicherheitsvorfällen eingeführt werden, die den im Richtlinienvorschlag festgelegten Anforderungen zumindest gleichwertig sind ([5]). Die Bestimmungen des Richtlinienvorschlags, die sich auf das Cybersicherheitsrisikomanagement, die Meldepflichten, den Informationsaustausch sowie die Aufsicht und Durchsetzung beziehen, gelten daher nicht für Finanzunternehmen, die unter die DORA-Verordnung fallen ([6]). Wie in den Erwägungsgründen des

([1]) COM(2020) 823 final.
([2]) Abrufbar auf der Website des Rates unter www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Siehe Nummer 1.5 der Stellungnahme CON/2021/20 der Europäischen Zentralbank vom 4. Juni 2021 zu einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (ABl. C 343 vom 26.8.2021, S. 1). Sämtliche Stellungnahmen der EZB sind auf EUR-Lex abrufbar. Artikel 17 Absatz 5 und Artikel 42 der DORA-Verordnung; Artikel 11 des Richtlinienvorschlags.
([5]) Artikel 2 Absatz 6 des Richtlinienvorschlags.
([6]) Erwägungsgrund 13 und Artikel 2 Absatz 6 des Richtlinienvorschlags.

Richtlinienvorschlags klargestellt, sollten die Bestimmungen der DORA-Verordnung, die sich auf IKT-Risikomanagementmaßnahmen, das Management und die Meldung von IKT-bezogenen Vorfällen, die Prüfung der digitalen Betriebsstabilität, Vereinbarungen über den Informationsaustausch und Risiken durch IKT-Drittanbieter beziehen, anstelle der Bestimmungen des Richtlinienvorschlags gelten ([7]).

1.2 Die EZB stellt ferner fest, dass der Rat in seiner allgemeinen Ausrichtung in Bezug auf den Richtlinienvorschlag eine Änderung vorschlägt, um „Einrichtungen, die Tätigkeiten in den Bereichen der Justiz, der Parlamente oder der Zentralbanken ausüben" ([8]), vom Anwendungsbereich des Richtlinienvorschlags auszunehmen. Die EZB geht davon aus, dass sich die vorgeschlagene Änderung auf alle grundlegenden Aufgaben und Zuständigkeiten des Europäischen Systems der Zentralbanken (ESZB) gemäß Artikel 127 Absatz 2 AEUV und Artikel 3.1 der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank (nachfolgend die „ESZB-Satzung"), wie etwa die Förderung des reibungslosen Funktionierens der Zahlungssysteme, erstrecken würde. In diesem Zusammenhang wird davon ausgegangen, dass im Besitz des Eurosystems befindliche und von ihm betriebene Finanzmarktinfrastrukturen wie TARGET2 und TARGET2-Securities unter den vom Rat vorgeschlagenen Ausschluss der Zentralbanken vom Anwendungsbereich des Richtlinienvorschlags fallen.

2. **Überwachungszuständigkeiten des ESZB und des Eurosystems**

2.1 Neben dem vorrangigen Ziel des ESZB, die Preisstabilität zu gewährleisten, besteht gemäß Artikel 127 Absatz 2 AEUV eine der grundlegenden Aufgaben des ESZB darin, das reibungslose Funktionieren der Zahlungssysteme zu fördern ([9]). Im Rahmen der Wahrnehmung dieser grundlegenden Aufgabe können die EZB und die nationalen Zentralbanken Einrichtungen zur Verfügung stellen und kann die EZB Verordnungen erlassen, um effiziente und zuverlässige Verrechnungs- und Zahlungssysteme innerhalb der Union und im Verkehr mit dritten Ländern zu gewährleisten ([10]). In Ausübung ihrer Aufsichtsfunktion hat die EZB die Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank (EZB/2014/28) ([11]) (nachfolgend die „SIPS-Verordnung") verabschiedet, mit der die CPSS-IOSCO-Prinzipien für Finanzmarktinfrastrukturen ([12]) in unmittelbar anwendbares Recht umgesetzt werden. Die SIPS-Verordnung enthält Anforderungen für Großbetrags- und Massenzahlungsverkehrssysteme mit systemischer Bedeutung, ob öffentlich oder in privatem Besitz. Die Anforderungen der SIPS-Verordnung umfassen bereits unter anderem die Steuerung des operationellen Risikos und die Schaffung eines Rahmens für die Cyberresilienz ([13]).

2.2 Neben systemrelevanten Zahlungsverkehrssystemen umfasst die Überwachung durch das Eurosystem auch nicht als systemrelevant eingestufte Zahlungsverkehrssysteme, elektronische Zahlungsinstrumente, -verfahren und -mechanismen sowie andere Infrastrukturen und kritische Dienstleister gemäß dem Überwachungsrahmen des Eurosystems ([14]). Zahlungsverkehrssysteme und andere Mechanismen, die der Überwachung durch das Eurosystem unterliegen, sind nicht ausdrücklich in den Anwendungsbereich des Richtlinienvorschlags einbezogen ([15]). Da es sich beim Richtlinienvorschlag um ein Instrument zur Mindestharmonisierung ([16]) handelt, könnten sich die von den Mitgliedstaaten erlassenen Durchführungsvorschriften schließlich mit der Aufsichtskompetenz des Eurosystems überschneiden. Um dies zu vermeiden, sollten die Zuständigkeiten des ESZB gemäß dem AEUV und der ESZB-Satzung sowie die Zuständigkeiten des Eurosystems gemäß der SIPS-Verordnung und allgemein gemäß dem Überwachungsrahmen des Eurosystems in den Erwägungsgründen des Richtlinienvorschlags ausdrücklich anerkannt werden.

([7]) Erwägungsgrund 13 des Richtlinienvorschlags.

([8]) Artikel 2 Absatz 3a Unterabsatz 1 Buchstabe b der allgemeinen Ausrichtung des Rates in Bezug auf den Richtlinienvorschlag.

([9]) Artikel 127 Absatz 2 AEUV und entsprechende Regelung in Artikel 3.1 der ESZB-Satzung.

([10]) Artikel 22 der ESZB-Satzung.

([11]) Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank vom 3. Juli 2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (EZB/2014/28) (ABl. L 217 vom 23.7.2014, S. 16).

([12]) Siehe die Prinzipien für Finanzmarktinfrastrukturen des Ausschusses für Zahlungsverkehrs- und Abrechnungssysteme (Committee on Payment and Settlement Systems – CPSS) und des Technischen Ausschusses der Internationalen Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions – IOSCO), April 2012, abrufbar auf der Website der Bank für Internationalen Zahlungsausgleich unter www.bis.org. Die darin enthaltene Verantwortlichkeit D bedeutet, dass von allen CPSS- und IOSCO-Mitgliedern erwartet wird, dass sie die Prinzipien so weit auf die betreffenden Finanzmarktinfrastrukturen in ihren Rechtsordnungen anwenden, wie es nach den nationalen Rechtsrahmen möglich ist.

([13]) Artikel 15 der Verordnung (EU) Nr. 795/2014 (EZB/2014/28).

([14]) Eurosystem oversight policy framework, überarbeitete Fassung (Juli 2016), abrufbar auf der Website der EZB unter www.ecb.europa.eu

([15]) Artikel 2 des Richtlinienvorschlags und Anhänge I und II des Richtlinienvorschlags.

([16]) Artikel 3 des Richtlinienvorschlags.

3. Risiken durch IKT-Drittanbieter, Management massiver Sicherheitsvorfälle und Krisen, Informationsaustausch und nationale Cybersicherheitsstrategie

3.1 *Management von Risiken durch IKT-Drittanbieter*

3.1.1 Gemäß dem Richtlinienvorschlag sind die zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wesentliche Einrichtungen befugt, verbindliche Anweisungen oder Anordnungen zu erteilen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen die im Richtlinienvorschlag festgelegten Verpflichtungen zu beheben ([17]). Gleichzeitig kann die gemäß der DORA-Verordnung benannte „federführende Aufsichtsinstanz" Empfehlungen an kritische IKT-Drittanbieter abgeben, um die potenziellen Systemrisiken zu bewältigen, die mit der Auslagerung und der Konzentration der Abhängigkeiten von IKT-Drittanbietern verbunden sind ([18]).

3.1.2 Da eine wesentliche Einrichtung im Sinne des Richtlinienvorschlags auch als kritischer IKT-Drittanbieter gemäß der DORA-Verordnung bezeichnet werden kann, betont die EZB ([19]), dass Empfehlungen und verbindliche Anweisungen, die einander widersprechen, vermieden werden sollten. In diesem Zusammenhang begrüßt die EZB die allgemeine Ausrichtung des Rates in Bezug auf den Richtlinienvorschlag. Gemäß dieser Ausrichtung müssen die zuständigen Behörden das gemäß der DORA-Verordnung eingerichtete „Aufsichtsforum" bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse in Bezug auf wesentliche Einrichtungen, die gemäß der DORA-Verordnung als kritischer IKT-Drittanbieter benannt wurden, unterrichten ([20]).

3.2 *Management massiver Sicherheitsvorfälle und Krisen*

3.2.1 Gemäß dem Richtlinienvorschlag ([21]) müssen die Mitgliedstaaten eine oder mehrere für das Management massiver Sicherheitsvorfälle und Krisen zuständige Behörden benennen. Wie in den Erwägungsgründen des Richtlinienvorschlags klargestellt wird, sollte der Begriff „Sicherheitsvorfall großen Ausmaßes" einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Sicherheitsvorfälle großen Ausmaßes können sich zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern ([22]).

3.2.2 Während die gemäß der DORA-Verordnung benannten zuständigen Behörden weiterhin für das Management von Cybersicherheitsvorfällen, die Finanzunternehmen betreffen, verantwortlich sind, wird die Zusammenarbeit mit den gemäß dem Richtlinienvorschlag eingerichteten Strukturen und Behörden von entscheidender Bedeutung sein, um eine koordinierte Reaktion in der gesamten Union zu gewährleisten. Zu diesem Zweck würde die EZB die Beteiligung der gemäß der DORA-Verordnung benannten zuständigen Behörden, einschließlich der EZB, am Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network – EU-CyCLONe) ([23]) begrüßen, wenn massive Cybersicherheitsvorfälle und -krisen den Finanzsektor betreffen.

3.3 *Informationsaustausch*

3.3.1 Wie bereits erwähnt, befürwortet die EZB ausdrücklich die Zusammenarbeit zwischen den gemäß der DORA-Verordnung benannten zuständigen Behörden und den gemäß dem Richtlinienvorschlag eingerichteten Strukturen und Behörden. Insbesondere kann der Informationsaustausch zwischen den Behörden sektorübergreifende Erkenntnisse ermöglichen, zur Verhinderung und wirksamen Bewältigung von Cyberangriffen beitragen und die einheitliche Bewertung IKT-bezogener Risiken in der gesamten Union fördern. Dennoch betont die EZB, dass der Informationsaustausch nur dann stattfinden sollte, wenn klar festgelegte Verfahren für die Klassifizierung und den Austausch von Informationen vorhanden sind, die mit angemessenen Garantien zur Gewährleistung der Vertraulichkeit einhergehen ([24]). Die EZB begrüßt die allgemeine Ausrichtung des Rates in Bezug auf den Richtlinien-

([17]) Artikel 29 Absatz 4 Buchstabe b des Richtlinienvorschlags.
([18]) Artikel 31 der DORA-Verordnung.
([19]) Siehe Nummer 1.2 der Stellungnahme CON/2021/20.
([20]) Artikel 29 Absatz 10 der allgemeinen Ausrichtung des Rates in Bezug auf den Richtlinienvorschlag.
([21]) Artikel 7 Absatz 1 des Richtlinienvorschlags.
([22]) Erwägungsgrund 27 des Richtlinienvorschlags.
([23]) Artikel 14 des Richtlinienvorschlags.
([24]) Siehe Nummer 1.5 der Stellungnahme CON/2021/20.

vorschlag, wonach ein regelmäßiger Austausch relevanter Informationen zwischen Behörden ([25]), der Abschluss von Kooperationsvereinbarungen zur Festlegung eines Mechanismus für den Informationsaustausch ([26]) und die automatische und direkte Weiterleitung der Meldungen zu Sicherheitsvorfällen ([27]) vorgeschlagen werden. In diesem Zusammenhang sollte sichergestellt werden, dass Informationen, die gemäß den Bestimmungen zum Berufsgeheimnis nach der DORA-Verordnung ([28]) oder den einschlägigen sektorspezifischen Rechtsvorschriften ([29]) vertraulich sind, nur dann mit den im Richtlinienvorschlag genannten zuständigen Behörden ausgetauscht werden können, wenn dieser Austausch für die zuständigen Behörden erforderlich ist, um die Bestimmungen des Richtlinienvorschlags anzuwenden ([30]).

3.4 *Nationale Cybersicherheitsstrategie*

3.4.1 Gemäß dem Richtlinienvorschlag müssen die Mitgliedstaaten nationale Cybersicherheitsstrategien verabschieden, in denen die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden ([31]). Wie in den Erwägungsgründen des Richtlinienvorschlags klargestellt, sollten die Mitgliedstaaten den Finanzsektor weiterhin in ihre jeweiligen Cybersicherheitsstrategien einbeziehen ([32]). Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Cybersicherheitsstrategien beispielsweise Konzepte zur Cybersicherheit in der Lieferkette für IKT-Produkte und -Dienste annehmen, die von Einrichtungen für die Erbringung ihrer Dienste genutzt werden. Was den Finanzsektor betrifft, so sollten die nationalen Cybersicherheitsstrategien mit dem Rechtsrahmen, der sich aus der DORA-Verordnung ergibt, im Einklang stehen. In diesem Zusammenhang ist die EZB der Auffassung, dass weitere Klarstellungen erforderlich sind, um sicherzustellen, dass die nationalen Cybersicherheitsstrategien mit den sektorspezifischen Rechtsvorschriften im Einklang stehen.

Insofern die EZB eine Änderung des Richtlinienvorschlags empfiehlt, sind spezielle Redaktionsvorschläge mit Begründung in einem separaten technischen Arbeitsdokument aufgeführt. Das technische Arbeitsdokument steht in englischer Sprache auf EUR-Lex zur Verfügung.

Geschehen zu Frankfurt am Main am 11. April 2022.

Die Präsidentin der EZB
Christine LAGARDE

([25]) Artikel 11 Absatz 5 der allgemeinen Ausrichtung des Rates in Bezug auf den Richtlinienvorschlag.
([26]) Erwägungsgrund 23a der allgemeinen Ausrichtung des Rates in Bezug auf den Richtlinienvorschlag.
([27]) Erwägungsgrund 13 der allgemeinen Ausrichtung des Rates in Bezug auf den Richtlinienvorschlag.
([28]) Artikel 49 der DORA-Verordnung.
([29]) Artikel 53 bis 62 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).
([30]) Artikel 2 Absatz 5 und Artikel 11 Absatz 4 des Richtlinienvorschlags.
([31]) Artikel 5 des Richtlinienvorschlags.
([32]) Erwägungsgrund 13 des Richtlinienvorschlags.