LEITLINIEN

LEITLINIE (EU) 2021/1759 DER EUROPÄISCHEN ZENTRALBANK

vom 20. Juli 2021

zur Änderung der Leitlinie EZB/2012/27 über ein transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem (TARGET2) (EZB/2021/30)

DER EZB-RAT —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 127 Absatz 2 erster und vierter Gedankenstrich,

gestützt auf die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank, insbesondere auf die Artikel 3.1, 17, 18 und 22,

in Erwägung nachstehender Gründe:

(1) Am 26. April 2007 verabschiedete der EZB-Rat die Leitlinie EZB/2007/2 [1] zur Regelung von TARGET2 und zur Schaffung einer einheitlichen technischen Plattform, der „Gemeinschaftsplattform" („Single Shared Platform" – SSP). Diese Leitlinie wurde im Jahr 2012 als Leitlinie EZB/2012/27 der Europäischen Zentralbank neu gefasst [2].

(2) Für eine wirksame Regulierung ist es erforderlich, klarzustellen, dass TIPS-Geldkontoinhaber und T2S-Geldkontoinhaber ab November 2021 bzw. Juni 2022 über das Zugangsportal zur Finanzmarktinfrastruktur des Eurosystems (Eurosystem Single Market Infrastructure Gateway – ESMIG) an TARGET2 angeschlossen werden.

(3) Damit TARGET2 kontinuierlich weiterentwickelt wird, um den Bedrohungen der Cybersicherheit zu begegnen, müssen die Regeln zur Einhaltung der TARGET2-Endpunktsicherheitsanforderungen verdeutlicht und erweitert werden. Ebenso sollten die Begriffsbestimmungen geändert werden, um einen umfassenden und harmonisierten Rechtsrahmen zu gewährleisten.

(4) Um sicherzustellen, dass Instant Payments in der gesamten Union verfügbar sind, sollten PM-Kontoinhaber, ihre indirekten Teilnehmer und erreichbare BIC-Inhaber, die durch Zeichnung des SEPA Instant Credit Transfer Adherence Agreements dem SEPA Instant Credit Transfer Scheme (SCT Inst Scheme) beigetreten sind, auf der TIPS-Plattform über ein TIPS-Geldkonto ständig erreichbar sein und bleiben. Die Überweisungsdienste in Zentralbankgeld für Nebensysteme, die Instant Payments in ihren eigenen Büchern abwickeln, sollten über die TIPS-Plattform erbracht werden.

(5) Sobald das TARGET2/T2S-Konsolidierungsprojekt in die Betriebsphase übergeht, ist es im Sinne der Rechtssicherheit erforderlich, für Transparenz hinsichtlich der Modalitäten für die Übertragung von Salden von den Konten der TARGET2-Teilnehmer auf die entsprechenden Nachfolgekonten des künftigen TARGET-Systems zu sorgen.

(6) Um eine wirksame Anwendung zu gewährleisten, sind darüber hinaus einige weitere Bestimmungen der Leitlinie EZB/2012/27 zu verdeutlichen und zu aktualisieren.

(7) Die Umsetzung des TARGET2/T2S-Konsolidierungsprojekts erfordert zudem Änderungen der anwendbaren Regelungen für Verträge mit T2S-Netzwerkdienstleistern, die ab dem 13. Juni 2022 gelten sollen.

(8) Die Leitlinie EZB/2012/27 sollte daher entsprechend geändert werden —

[1] Leitlinie EZB/2007/2 der Europäischen Zentralbank vom 26. April 2007 über ein transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem (TARGET2) (ABl. L 237 vom 8.9.2007, S. 1).

[2] Leitlinie EZB/2012/27 der Europäischen Zentralbank vom 5. Dezember 2012 über ein transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem (TARGET2) (ABl. L 30 vom 30.1.2013, S. 1).

HAT FOLGENDE LEITLINIE ERLASSEN:

Artikel 1

Änderungen

Die Leitlinie EZB/2012/27 wird wie folgt geändert:

1. Artikel 1 Absatz 1 erhält folgende Fassung:

„(1) TARGET2 bietet Echtzeit-Brutto-Abwicklung (real-time gross settlement – RTGS) von Euro-Zahlungen in Zentralbankgeld über PM-Konten, über T2S-Geldkonten und über TIPS-Geldkonten an. TARGET2 wird auf der Grundlage der SSP eingerichtet und betrieben, über die – technisch in gleicher Weise – Zahlungsaufträge eingereicht und verarbeitet sowie schließlich Zahlungen empfangen werden. Was die technische Führung von T2S-Geldkonten betrifft, wird TARGET2 auf der T2S-Plattform eingerichtet und betrieben. Was die technische Führung von TIPS-Geldkonten und technischen TIPS-Nebensystemkonten betrifft, wird TARGET2 auf der TIPS-Plattform eingerichtet und betrieben."

2. Artikel 2 wird wie folgt geändert:

a) Nummer 58 wird gestrichen.

b) Nummer 62 erhält folgende Fassung:

„62. ‚Zahlungsauftrag' (‚payment order'): ein Überweisungsauftrag, ein Liquiditätsübertragungsauftrag, ein Lastschriftauftrag, ein Auftrag zur Liquiditätsübertragung von einem PM-Konto auf ein T2S-Geldkonto, ein Auftrag zur Liquiditätsübertragung von einem T2S-Geldkonto auf ein PM-Konto, ein Auftrag zur Liquiditätsübertragung von einem T2S-Geldkonto auf ein T2S-Geldkonto, ein Auftrag zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto, ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto, ein Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, ein Instant Payment-Auftrag oder eine positive Rückruf-Antwort;".

c) Nummer 78 wird gestrichen.

d) Nummer 81 erhält folgende Fassung:

„81. ‚Instant Payment-Auftrag' (‚instant payment order'): entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst Scheme) des European Payments Council (EPC) ein Zahlungsauftrag, der an jedem Kalendertag des Jahres rund um die Uhr ausgeführt werden kann, mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; hierzu zählen i) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein TIPS-Geldkonto, ii) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, iii) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto und iv) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein technisches TIPS-Nebensystemkonto;".

e) Die folgenden Nummern 87 bis 90 werden angefügt:

„87. ‚SEPA Instant Credit Transfer (SCT Inst) Scheme des European Payments Council' oder ‚SCT Inst Scheme' (‚European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme' or ‚SCT Inst scheme'): ein automatisiertes Verfahren mit offenen Standards, das ein Regelwerk für den Interbankenverkehr vorsieht, das von den SCT-Inst-Teilnehmern einzuhalten ist und es den im SEPA tätigen Zahlungsdienstleistern ermöglicht, ein automatisiertes, SEPA-weites Produkt für Euro-Echtzeitüberweisungen anzubieten;

88. ‚technisches TIPS-Nebensystemkonto' (‚TIPS ancillary system technical account (TIPS AS technical account)'): ein Konto, das von einem Nebensystem oder einer Zentralbank im Auftrag eines Nebensystems im TARGET2-Komponenten-System der Zentralbank zur Nutzung durch das Nebensystem zum Zwecke der Abwicklung von Instant Payments in seinen eigenen Büchern unterhalten wird;

89. ‚Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto' (‚TIPS DCA to TIPS AS technical account liquidity transfer order'): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu erhöhen;

90. ‚Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto' (‚TIPS AS technical account to TIPS DCA liquidity transfer order'): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu verringern."

3. Artikel 13 erhält folgende Fassung:

„*Artikel 13*

Nebensysteme

(1) Die Zentralbanken des Eurosystems stellen Überweisungsdienste in Zentralbankgeld für Nebensysteme innerhalb des PM, auf das über den TARGET2-Netzwerkdienstleister zugegriffen wird, zur Verfügung. Diese Dienste werden in bilateralen Vereinbarungen zwischen den Zentralbanken des Eurosystems und den jeweiligen Nebensystemen geregelt.

(2) Bilaterale Vereinbarungen mit Nebensystemen, die die Nebensystem-Schnittstelle (ASI) verwenden, müssen mit den in Anhang IV festgelegten Bestimmungen vereinbar sein. Darüber hinaus sehen die Zentralbanken des Eurosystems in diesen bilateralen Vereinbarungen vor, dass die folgenden, in Anhang II enthaltenen Bestimmungen entsprechend anwendbar sind:

a) Artikel 8 Absatz 1 (technische und rechtliche Anforderungen);

b) Artikel 8 Absätze 2 bis 5 (Antragsverfahren) mit der Ausnahme, dass das Nebensystem statt der Zugangsvoraussetzungen gemäß Artikel 4 die in der Begriffsbestimmung von ‚Nebensystem' in Anhang II Artikel 1 enthaltenen Zugangsvoraussetzungen erfüllen muss;

c) Anlage V (Öffnungszeiten und Tagesablauf);

d) Artikel 11 (Anforderungen an Zusammenarbeit und Informationsaustausch) außer Absatz 8;

e) Artikel 27 und 28 (Aufrechterhaltung des Geschäftsbetriebs (‚Business Continuity') und Notfallverfahren und Sicherheitsanforderungen und Kontrollverfahren), wobei als Grundlage für die Berechnung der Strafentgelte für die Nichteinhaltung der Sicherheitsanforderungen gemäß Anhang II Artikel 28 die in Anhang IV Nummer 18 Absatz 1 Buchstabe a genannte Gebühr herangezogen wird;

f) Artikel 31 (Haftungsregelung);

g) Artikel 32 (Nachweise);

h) Artikel 33 und 34 (Dauer, Beendigung und Suspendierung der Teilnahme) außer Artikel 34 Absatz 1 Buchstabe b;

i) Artikel 35 soweit einschlägig (Schließung von PM-Konten);

j) Artikel 38 (Vertraulichkeit);

k) Artikel 39 (Anforderungen der Union an Datenschutz, Geldwäschebekämpfung und damit zusammenhängende Aspekte);

l) Artikel 40 (Anforderungen an Mitteilungen);

m) Artikel 41 (Vertragsverhältnis mit dem TARGET2-Netzwerkdienstleister);

n) Artikel 44 (Anwendbares Recht, Gerichtsstand und Erfüllungsort);

o) Artikel 45a Absatz 1 (Übergangsbestimmung).

(3) Bilaterale Vereinbarungen mit Nebensystemen, die das PI verwenden, müssen mit den beiden folgenden Bestimmungen vereinbar sein:

a) Anhang II außer Titel V sowie Anlagen VI und VII; und

b) Anhang IV Nummer 18.

Für die Zwecke von Buchstabe a wird als Grundlage für die Berechnung der Strafentgelte für die Nichteinhaltung der Sicherheitsanforderungen gemäß Anhang II Artikel 28 die in Anhang IV Nummer 18 Absatz 1 Buchstabe a genannte Gebühr herangezogen.

(4) Abweichend von Absatz 3 müssen bilaterale Vereinbarungen mit Nebensystemen, die das PI verwenden, aber nur Zahlungen zugunsten ihrer Kunden abwickeln, mit den beiden folgenden Bestimmungen vereinbar sein:

a) Anhang II außer Titel V, Artikel 36 sowie Anlagen VI und VII; und

b) Anhang IV Nummer 18.

Für die Zwecke von Buchstabe a wird als Grundlage für die Berechnung der Strafentgelte für die Nichteinhaltung der Sicherheitsanforderungen gemäß Anhang II Artikel 28 die in Anhang IV Nummer 18 Absatz 1 Buchstabe a genannte Gebühr herangezogen.

(5) Die Zentralbanken des Eurosystems stellen Überweisungsdienste in Zentralbankgeld für Nebensysteme, die Instant Payments im Einklang mit dem SEPA Instant Credit Transfer Scheme in ihren eigenen Büchern abwickeln, ausschließlich über die TIPS-Plattform zur Verfügung. Bilaterale Vereinbarungen zur Erbringung solcher Überweisungsdienste müssen mit den in Anhang IVa festgelegten Bestimmungen vereinbar sein und dürfen die Abwicklung von Instant Payments nur im Einklang mit dem SEPA Instant Credit Transfer Scheme ermöglichen. In diesen bilateralen Vereinbarungen sind die folgenden, in Anhang IIb enthaltenen Bestimmungen entsprechend anwendbar:

a) Anlagen I, II und III;

b) Artikel 4 (Allgemeine Beschreibung von TARGET2);

c) Artikel 5 (Zugangsvoraussetzungen), wobei das Nebensystem die in der Begriffsbestimmung von ‚Nebensystem' in Anhang IIb Artikel 1 enthaltenen Zugangsvoraussetzungen erfüllen muss;

d) Artikel 6 Absatz 1 (technische und rechtliche Anforderungen), mit der Ausnahme, dass das Nebensystem nicht zu einem Beitritt zum SEPA Instant Credit Transfer Scheme durch Zeichnung des SEPA Instant Credit Transfer Adherence Agreements verpflichtet ist, sondern stattdessen zur Bekanntgabe der Einhaltung des SEPA Instant Credit Transfer Scheme;

e) Artikel 6 Absätze 2 bis 5 (Antragsverfahren), mit der Ausnahme, dass i) das Nebensystem statt der Zugangsvoraussetzungen gemäß Artikel 5 die in der Begriffsbestimmung von ‚Nebensystem' in Anhang IIb Artikel 1 enthaltenen Zugangsvoraussetzungen erfüllen muss, und ii) dass das Nebensystem nicht verpflichtet ist, einen Nachweis für den Beitritt zum SEPA Instant Credit Transfer Scheme vorzulegen, sondern stattdessen die Bekanntgabe der Einhaltung des SEPA Instant Credit Transfer Scheme nachweisen muss;

f) Artikel 7 (Zugriff auf die TIPS-Plattform);

g) Artikel 8 (Erreichbare Parteien);

h) Artikel 9 (Netzwerkdienstleister);

i) Artikel 11 (TIPS-Directory);

j) Artikel 11a (MPL-Verzeichnis);

k) Artikel 12 (Pflichten der Zentralbanken und der Kontoinhaber) außer Absatz 4;

l) Artikel 14 (Anforderungen an Zusammenarbeit und Informationsaustausch);

m) Artikel 16 (Arten von Zahlungsaufträgen);

n) Artikel 17 (Annahme und Zurückweisung von Zahlungsaufträgen);

o) Artikel 18 (Verarbeitung von Zahlungsaufträgen);

p) Artikel 19 (Rückruf-Anfrage);

q) Artikel 20 (Zeitpunkt der Einbringung; Zeitpunkt der Unwiderruflichkeit);

r) Artikel 21 (Sicherheitsanforderungen und Aufrechterhaltung des Geschäftsbetriebs);

s) Artikel 23 (Haftungsregelung);

t) Artikel 24 (Nachweise);

u) Artikel 25 und 26 (Bestandsdauer, Beendigung und Suspendierung der Teilnahme) außer Artikel 26 Absatz 1 Buchstabe b und Absatz 4 Unterabsatz 2;

v) Artikel 27 soweit einschlägig (Schließung von Konten);

w) Artikel 29 (Vertraulichkeit);

x) Artikel 30 (Anforderungen der Union an Datenschutz, Geldwäschebekämpfung und damit zusammenhängende Aspekte);

y) Artikel 31 (Anforderungen an Mitteilungen);

z) Artikel 34 (Anwendbares Recht, Gerichtsstand und Erfüllungsort);

aa) Artikel 35a (Übergangsbestimmung)."

4. Artikel 17 Absatz 4 erhält folgende Fassung:

„(4) Die Absätze 1 bis 3a dieses Artikels finden auch bei Suspendierung oder Beendigung der Nutzung der Nebensystem-Schnittstelle (ASI) oder der TIPS-Plattform durch Nebensysteme Anwendung."

5. Der folgende Artikel 27a wird eingefügt:

„*Artikel 27a*

Übergangsbestimmung

Die Zentralbanken des Eurosystems können bis zum 25. Februar 2022 Überweisungsdienste in Zentralbankgeld für Nebensysteme, die Instant Payments im Einklang mit dem SEPA Instant Credit Transfer Scheme in ihren eigenen Büchern abwickeln, unter Verwendung der Nebensystem-Schnittstelle (Ancillary System Interface – ASI) zur Verfügung stellen."

6. Anhang II der Leitlinie EZB/2012/27 wird gemäß Anhang I der vorliegenden Leitlinie geändert.
7. Anhang IIa der Leitlinie EZB/2012/27 wird gemäß Anhang II der vorliegenden Leitlinie geändert.
8. Anhang IIb der Leitlinie EZB/2012/27 wird gemäß Anhang III der vorliegenden Leitlinie geändert.
9. Anhang IV der Leitlinie EZB/2012/27 wird gemäß Anhang IV der vorliegenden Leitlinie geändert.
10. Ein neuer Anhang IVa der Leitlinie EZB/2012/27 wird gemäß Anhang V der vorliegenden Leitlinie eingefügt.

Artikel 2

Wirksamwerden und Umsetzung

(1) Die vorliegende Leitlinie wird am Tag ihrer Bekanntgabe an die nationalen Zentralbanken der Mitgliedstaaten, deren Währung der Euro ist, wirksam.

(2) Die nationalen Zentralbanken der Mitgliedstaaten, deren Währung der Euro ist, treffen die erforderlichen Maßnahmen zur Erfüllung der vorliegenden Leitlinie und wenden diese ab dem 21. November 2021 an, mit Ausnahme der im Zusammenhang mit Anhang II Nummer 1 Buchstabe c sowie Nummern 7 und 9 der vorliegenden Leitlinie zu treffenden Maßnahmen, die sie ab dem 13. Juni 2022 anwenden. Sie teilen der EZB die entsprechenden Rechtstexte und Umsetzungsmaßnahmen bis spätestens 9. September 2021 mit.

Artikel 3

Adressaten

Die vorliegende Leitlinie ist an alle Zentralbanken des Eurosystems gerichtet.

Geschehen zu Frankfurt am Main am 20. Juli 2021.

Für den EZB-Rat
Die Präsidentin der EZB
Christine LAGARDE

ANHANG I

Anhang II der Leitlinie EZB/2012/27 wird wie folgt geändert:

1. Artikel 1 wird wie folgt geändert:

   a) Buchstabe a der Begriffsbestimmung von „Gruppe“ erhält folgende Fassung:

   „a) eine Gruppe von Kreditinstituten, deren Jahresabschlüsse in den konsolidierten Abschluss bei einem Mutterunternehmen eingehen, sofern das Mutterunternehmen den konsolidierten Abschluss gemäß der Verordnung (EG) Nr. 1126/2008 der Kommission (*) nach dem International Accounting Standard (IAS) 27 erstellt, wobei die Gruppe sich wie folgt zusammensetzen muss: i) ein Mutterunternehmen und ein oder mehrere Tochterunternehmen oder ii) zwei oder mehr Tochterunternehmen desselben Mutterunternehmens, oder

   _____

   (*) Verordnung (EG) Nr. 1126/2008 der Kommission vom 3. November 2008 zur Übernahme bestimmter internationaler Rechnungslegungsstandards gemäß der Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates (ABl. L 320 vom 29.11.2008, S. 1).“;

   b) Die Begriffsbestimmung von „Instant Payment-Auftrag“ erhält folgende Fassung:

   „– ‚Instant Payment-Auftrag‘ (‚instant payment order‘): entsprechend dem SEPA Instant Credit Transfer (SCT Inst) Scheme des European Payments Council (EPC) ein Zahlungsauftrag, der an jedem Kalendertag des Jahres rund um die Uhr ausgeführt werden kann – mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; hierzu zählen i) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein TIPS-Geldkonto, ii) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, iii) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto und iv) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein technisches TIPS-Nebensystemkonto;“;

   c) Die folgenden Begriffsbestimmungen werden eingefügt:

   „— ‚SEPA Instant Credit Transfer (SCT Inst) Scheme des European Payments Council‘ oder ‚SCT Inst Scheme‘ (‚European Payments Council’s SEPA Instant Credit Transfer (SCT Inst) scheme‘ or ‚SCT Inst scheme‘): ein automatisiertes Verfahren mit offenen Standards, das ein Regelwerk für den Interbankenverkehr vorsieht, das von den SCT-Inst-Teilnehmern einzuhalten ist und es den im SEPA tätigen Zahlungsdienstleistern ermöglicht, ein automatisiertes, SEPA-weites Produkt für Euro-Echtzeitüberweisungen anzubieten;

   — ‚technisches TIPS-Nebensystemkonto‘ (‚TIPS ancillary system technical account (TIPS AS technical account)‘): ein Konto, das von einem Nebensystem oder einer Zentralbank im Auftrag eines Nebensystems im TARGET2-Komponenten-System der Zentralbank zur Nutzung durch das Nebensystem zum Zwecke der Abwicklung von Instant Payments in seinen eigenen Büchern unterhalten wird;

   — ‚Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto‘ (‚TIPS DCA to TIPS AS technical account liquidity transfer order‘): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu erhöhen;

   — ‚Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto‘ (‚TIPS AS technical account to TIPS DCA liquidity transfer order‘): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu verringern;

   — ‚erreichbare Partei‘ (‚reachable party‘): eine Stelle, die a) Inhaberin eines Business Identifier Code (BIC) ist, b) von einem TIPS-Geldkontoinhaber oder durch ein Nebensystem als erreichbare Partei bestimmt wird, c) Korrespondent, Kunde oder Zweigstelle eines TIPS-Geldkontoinhabers, oder Teilnehmer eines Nebensystems, oder Korrespondent, Kunde oder Zweigstelle eines Teilnehmers eines Nebensystems ist und d) entweder über den TIPS-Geldkontoinhaber oder das Nebensystem Instant Payment-Aufträge oder, falls eine entsprechende Genehmigung des TIPS-Geldkontoinhabers oder des Nebensystems erteilt wurde, direkt Instant Payment-Aufträge bei der TIPS-Plattform einreichen und über diese Zahlungen empfangen kann;“;

   d) Die Begriffsbestimmung von „TIPS-Netzwerkdienstleister“ wird gestrichen.

2. Artikel 3 wird wie folgt geändert:

   a) Absatz 2 Buchstabe fc erhält folgende Fassung:

   „fc) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto und Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto;“;

   b) In Absatz 2 wird folgender Buchstabe fd eingefügt:

   „fd) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto und Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, und“;

c) Absatz 3 erhält folgende Fassung:

„(3) TARGET2 bietet Echtzeit-Brutto-Abwicklung von Euro-Zahlungen in Zentralbankgeld über PM-Konten, über T2S-Geldkonten und über TIPS-Geldkonten an. TARGET2 wird auf der Grundlage der SSP eingerichtet und betrieben, über die – technisch in gleicher Weise – Zahlungsaufträge eingereicht und verarbeitet sowie schließlich Zahlungen empfangen werden. Was die technische Führung von T2S-Geldkonten betrifft, wird TARGET2 auf der T2S-Plattform eingerichtet und betrieben. Was die technische Führung von TIPS-Geldkonten und technischen TIPS-Nebensystemkonten betrifft, wird TARGET2 auf der TIPS-Plattform eingerichtet und betrieben."

3. Artikel 5 erhält folgende Fassung:

„Artikel 5

Direkte Teilnehmer

(1) PM-Kontoinhaber in TARGET2 [Zentralbank/Ländercode einfügen] sind direkte Teilnehmer und müssen die in Artikel 8 Absätze 1 und 2 festgelegten Anforderungen erfüllen. Sie müssen über mindestens ein PM-Konto bei der [Name der Zentralbank einfügen] verfügen. PM-Kontoinhaber, die durch Zeichnung des SEPA Instant Credit Transfer Adherence Agreements dem SEPA Instant Credit Transfer Scheme beigetreten sind, sind verpflichtet, jederzeit auf der TIPS-Plattform erreichbar zu sein und zu bleiben, sei es als TIPS-Geldkontoinhaber oder als erreichbare Partei über einen TIPS-Geldkontoinhaber.

(2) PM-Kontoinhaber können erreichbare BIC-Inhaber bestimmen, unabhängig von deren Ort der Niederlassung. PM-Kontoinhaber können erreichbare BIC-Inhaber, die durch Zeichnung des SEPA Instant Credit Transfer Adherence Agreements dem SEPA Instant Credit Transfer Scheme beigetreten sind, nur dann bestimmen, wenn diese Stellen auf der TIPS-Plattform erreichbar sind, sei es als TIPS-Geldkontoinhaber oder als erreichbare Partei über einen TIPS-Geldkontoinhaber.

(3) PM-Kontoinhaber können, sofern die Bedingungen nach Artikel 6 erfüllt sind, indirekte Teilnehmer im PM benennen. PM-Kontoinhaber können indirekte Teilnehmer, die durch Zeichnung des SEPA Instant Credit Transfer Adherence Agreements dem SEPA Instant Credit Transfer Scheme beigetreten sind, nur dann benennen, wenn diese Stellen auf der TIPS-Plattform erreichbar sind, sei es als TIPS-Geldkontoinhaber bei der [Name der Zentralbank einfügen] oder als erreichbare Partei über einen TIPS-Geldkontoinhaber.

(4) Multi-Adressaten-Zugang durch Zweigstellen kann wie folgt gewährt werden:

a) Ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 Buchstabe a oder b dieses Anhangs, das als PM-Kontoinhaber zugelassen wurde, kann einer oder mehreren seiner in der Union oder im EWR belegenen Zweigstellen zur direkten Einreichung von Zahlungsaufträgen und zum direkten Empfang von Zahlungen Zugang zu seinem PM-Konto gewähren, sofern die [Name der Zentralbank einfügen] darüber informiert wurde.

b) Wurde eine Zweigstelle eines Kreditinstituts als PM-Kontoinhaber zugelassen, so haben auch die anderen Zweigstellen derselben juristischen Person und/oder die Zentrale – vorausgesetzt, sie sind in der Union oder im EWR belegen – Zugang zum PM-Konto jener Zweigstelle, sofern die [Name der Zentralbank einfügen] darüber informiert wurde."

4. Artikel 12 Absatz 5 erhält folgende Fassung:

„(5) PM-Konten und deren Unterkonten werden entweder mit null Prozent oder zum Einlagesatz, je nachdem, welcher dieser Zinssätze niedriger ist, verzinst, sofern diese Konten nicht zur Haltung von Mindestreserven oder von Überschussreserven genutzt werden.

Im Falle von Mindestreserven werden die Berechnung und Zahlung der anfallenden Zinsen durch die Verordnung (EG) Nr. 2531/98 des Rates (*) und die Verordnung (EU) 2021/378 der Europäischen Zentralbank (EZB/2021/1) (**) geregelt.

Im Falle von Überschussreserven werden die Berechnung und Zahlung der anfallenden Zinsen durch den Beschluss (EU) 2019/1743 (EZB/2019/31) (***) geregelt.

(*) Verordnung (EG) Nr. 2531/98 des Rates vom 23. November 1998 über die Auferlegung einer Mindestreservepflicht durch die Europäische Zentralbank (ABl. L 318 vom 27.11.1998, S. 1).

(**) Verordnung (EU) 2021/378 der Europäischen Zentralbank vom 22. Januar 2021 über die Auferlegung einer Mindestreservepflicht (EZB/2021/1) (ABl. L 73 vom 3.3.2021, S. 1).

(***) Beschluss (EU) 2019/1743 der Europäischen Zentralbank vom 15. Oktober 2019 über die Verzinsung von Überschussreserven und bestimmten Einlagen (EZB/2019/31) (ABl. L 267 vom 21.10.2019, S. 12)."

5. Artikel 28 erhält folgende Fassung:

„*Artikel 28*

Sicherheitsanforderungen und Kontrollverfahren

(1) Die Teilnehmer führen zum Schutz ihrer Systeme vor unberechtigtem Zugriff und unbefugter Nutzung angemessene Sicherheitskontrollen durch. Der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Systeme obliegt der ausschließlichen Verantwortung der Teilnehmer.

(2) Die Teilnehmer informieren die [Name der Zentralbank einfügen] über alle sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern. Die [Name der Zentralbank einfügen] kann weitere Informationen über den Vorfall anfordern und erforderlichenfalls verlangen, dass der Teilnehmer angemessene Maßnahmen ergreift, um solche Ereignisse zukünftig zu vermeiden.

(3) Die [Name der Zentralbank einfügen] kann für alle Teilnehmer und/oder Teilnehmer, die von der [Name der Zentralbank einfügen] als systemkritisch angesehen werden, zusätzliche Sicherheitsanforderungen verlangen, insbesondere im Hinblick auf Cybersicherheit oder Betrugsbekämpfung.

(4) Teilnehmer i) gewähren der [Name der Zentralbank einfügen] dauerhaften Zugang zu ihrer Bescheinigung über die Einhaltung der Endpunktsicherheitsanforderungen des von ihnen gewählten TARGET2-Netzwerkdienstleisters und ii) übermitteln der [Name der Zentralbank einfügen] jährlich die auf der Website der [Name der Zentralbank einfügen] und der Website der EZB in englischer Sprache veröffentlichte TARGET2-Selbstzertifizierungserklärung.

(4a) Die [Name der Zentralbank einfügen] beurteilt anhand der Selbstzertifizierungserklärung(en) des Teilnehmers den Grad der Einhaltung jeder der in den TARGET2-Selbstzertifizierungsanforderungen festgelegten Anforderungen durch den Teilnehmer. Diese Anforderungen sind in Anlage VIII aufgeführt, die neben den in Artikel 2 Absatz 1 genannten Anlagen Bestandteil dieser Bedingungen sind.

(4b) Der Grad der Einhaltung der Anforderungen der TARGET2-Selbstzertifizierung durch den Teilnehmer wird, geordnet nach zunehmendem Schweregrad der Nichteinhaltung, wie folgt eingestuft: ‚vollständige Einhaltung', ‚geringfügige Nichteinhaltung', ‚gravierende Nichteinhaltung'. Die folgenden Kriterien finden Anwendung: Vollständige Einhaltung ist erreicht, wenn ein Teilnehmer 100 % der Anforderungen erfüllt; eine geringfügige Nichteinhaltung liegt vor, wenn ein Teilnehmer weniger als 100 %, aber mindestens 66 % der Anforderungen erfüllt, und eine gravierende Nichteinhaltung liegt vor, wenn ein Teilnehmer weniger als 66 % der Anforderungen erfüllt. Weist ein Teilnehmer nach, dass eine bestimmte Anforderung auf ihn nicht anwendbar ist, so wird für die Zwecke der Einstufung davon ausgegangen, dass er die Anforderungen erfüllt. Ein Teilnehmer, der die ‚vollständige Einhaltung' nicht erreicht, legt einen Maßnahmenplan vor, aus dem hervorgeht, wie er die vollständige Einhaltung zu erreichen beabsichtigt. Die [Name der Zentralbank einfügen] unterrichtet die betreffenden Aufsichtsbehörden über den Stand der Einhaltung durch den jeweiligen Teilnehmer.

(4c) Verweigert der Teilnehmer den dauerhaften Zugang zu seiner Bescheinigung über die Einhaltung der Endpunktsicherheitsanforderungen seines gewählten Netzwerkdienstleisters oder übermittelt er die TARGET2-Selbstzertifizierung nicht, so wird der Grad der Einhaltung der Anforderungen durch den Teilnehmer als ‚gravierende Nichteinhaltung' eingestuft.

(4d) Die [Name der Zentralbank einfügen] beurteilt jährlich erneut die Einhaltung der Anforderungen durch die Teilnehmer.

(4e) Die [Name der Zentralbank einfügen] kann Teilnehmern, deren Grad der Einhaltung der Anforderungen als geringfügige oder gravierende Nichteinhaltung eingestuft wurde, mit zunehmendem Schweregrad folgende Abhilfemaßnahmen auferlegen:

i) verstärkte Überwachung: Der Teilnehmer legt der [Name der Zentralbank einfügen] monatlich einen von einem leitenden Angestellten unterzeichneten Bericht über seine Fortschritte bei der Behebung der Nichteinhaltung vor. Darüber hinaus zahlt der Teilnehmer für jedes betroffene Konto ein monatliches Strafentgelt in Höhe seiner monatlichen Gebühr gemäß Anlage VI Nummer 1 ohne Transaktionsgebühren. Diese Abhilfemaßnahme kann auferlegt werden, wenn bei der Beurteilung der Einhaltung der Anforderungen durch den Teilnehmer zweimal in Folge eine geringfügige Nichteinhaltung oder eine gravierende Nichteinhaltung festgestellt wird;

ii) Suspendierung: Die Teilnahme an TARGET2-[Zentralbank/Ländercode einfügen] kann bei Vorliegen der in Artikel 34 Absatz 2 Buchstaben b und c dieses Anhangs beschriebenen Umstände suspendiert werden. Abweichend von Artikel 34 dieses Anhangs erfolgt die Suspendierung der Teilnahme mit einer Ankündigungsfrist von drei Monaten. Der Teilnehmer zahlt für jedes suspendierte Konto ein monatliches Strafentgelt in Höhe seiner doppelten monatlichen Gebühr gemäß Anlage VI Nummer 1 ohne Transaktionsgebühren. Diese Abhilfemaßnahme kann auferlegt werden, wenn bei der Beurteilung der Einhaltung der Anforderungen durch den Teilnehmer zweimal in Folge eine gravierende Nichteinhaltung festgestellt wird;

iii) Beendigung: Die Teilnahme an TARGET2-[Zentralbank/Ländercode einfügen] kann bei Vorliegen der in Artikel 34 Absatz 2 Buchstaben b und c dieses Anhangs beschriebenen Umstände beendet werden. Abweichend von Artikel 34 dieses Anhangs erfolgt die Beendigung der Teilnahme mit einer Ankündigungsfrist von drei Monaten. Der Teilnehmer zahlt für jedes im Rahmen der Beendigung der Teilnahme geschlossene Konto ein zusätzliches Strafentgelt in Höhe von 1 000 EUR. Diese Abhilfemaßnahme kann auferlegt werden, wenn der Teilnehmer die gravierende Nichteinhaltung nicht innerhalb von drei Monaten nach der Suspendierung zur Zufriedenheit der [Name der Zentralbank einfügen] behoben hat.

(5) Teilnehmer, die Dritten Zugang zu ihrem PM-Konto gemäß Artikel 5 Absätze 2, 3 und 4 gewähren, tragen dem mit der Erlaubnis eines solchen Zugangs verbundenen Risiko im Einklang mit den in den Absätzen 1 bis 4e dieses Artikels genannten Sicherheitsanforderungen Rechnung. In der in Absatz 4 genannten Selbstzertifizierung ist festgelegt, dass der Teilnehmer Dritte, die Zugang zu seinem PM-Konto haben, zur Einhaltung der Endpunktsicherheitsanforderungen des TARGET2-Netzwerkdienstleisters verpflichtet."

6. Artikel 39 Absatz 1 erhält folgende Fassung:

„(1) Es wird davon ausgegangen, dass sich die Teilnehmer ihrer gesetzlichen Pflichten zum Datenschutz bewusst sind, diese einhalten und in der Lage sind, die Einhaltung gegenüber den betreffenden zuständigen Behörden nachzuweisen. Sie sind sich ihrer gesetzlichen Pflichten zur Bekämpfung der Geldwäsche, der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst und halten diese ein; insbesondere treffen sie danach angemessene Vorkehrungen bei den Zahlungen, die auf ihren PM-Konten verbucht werden. Die Teilnehmer stellen vor Abschluss des Vertrags mit dem TARGET2-Netzwerkdienstleister sicher, dass sie mit den Regelungen des TARGET2-Netzwerkdienstleisters zur Wiederherstellung verloren gegangener Daten vertraut sind."

7. Der folgende Artikel 45a wird eingefügt:

„*Artikel 45a*

Übergangsbestimmungen

(1) Sobald das TARGET-System den Betrieb aufnimmt und der Betrieb von TARGET2 eingestellt wurde, werden PM-Kontosalden auf die entsprechenden Nachfolgekonten des Kontoinhabers im TARGET-System übertragen.

(2) Die Anforderung, dass PM-Kontoinhaber, indirekte Teilnehmer und erreichbare BIC-Inhaber, die dem SEPA Instant Credit Transfer Scheme beigetreten sind, gemäß Artikel 5 auf der TIPS-Plattform erreichbar sein müssen, gilt ab dem 25. Februar 2022."

8. Anlage I Nummer 8 Absatz 4 Buchstabe b erhält folgende Fassung:

„b) der User-to-Application-Modus (U2A)

Der U2A-Modus ermöglicht die direkte Kommunikation zwischen dem Teilnehmer und dem ICM. Die Informationen werden in einem Browser angezeigt, der auf einem PC-System (SWIFT Alliance WebStation oder eine andere von SWIFT vorgeschriebene Schnittstelle) läuft. Für den U2A-Zugriff muss die IT-Infrastruktur Cookies unterstützen. Weitere Einzelheiten sind im ICM-Benutzerhandbuch aufgeführt."

9. Anlage IV Nummer 6 Buchstabe g erhält folgende Fassung:

„g) Für die Abwicklung von Zahlungsaufträgen in der Notfallabwicklung stellen die Teilnehmer notenbankfähige Sicherheiten als Sicherheit bereit. Während der Notfallabwicklung können eingehende Notfallzahlungen zur Finanzierung von ausgehenden Notfallzahlungen verwendet werden. Die [Name der Zentralbank einfügen] wird die verfügbare Liquidität der Teilnehmer für die Zahlungsabwicklung im Rahmen der Notfallabwicklung nicht berücksichtigen."

10. Der Text des Anhangs VI der vorliegenden Leitlinie wird der Leitlinie EZB/2012/27 als neuer Anhang II Anlage VIII angefügt.

ANHANG II

Anhang IIa der Leitlinie EZB/2012/27 wird wie folgt geändert:

1. Artikel 1 wird wie folgt geändert:

   a) Die Begriffsbestimmung von „Instant Payment-Auftrag“ erhält folgende Fassung:

   „– ‚Instant Payment-Auftrag‘ (‚instant payment order‘): entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst Scheme) des European Payments Council (EPC) ein Zahlungsauftrag, der an jedem Kalendertag des Jahres rund um die Uhr ausgeführt werden kann – mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; hierzu zählen i) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein TIPS-Geldkonto, ii) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, iii) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto und iv) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein technisches TIPS-Nebensystemkonto;“

   b) Die folgenden Begriffsbestimmungen werden eingefügt:

   „— ‚technisches TIPS-Nebensystemkonto‘ (‚TIPS ancillary system technical account (TIPS AS technical account)‘): ein Konto, das von einem Nebensystem oder einer Zentralbank im Auftrag eines Nebensystems im TARGET2-Komponenten-System der Zentralbank zur Nutzung durch das Nebensystem zum Zwecke der Abwicklung von Instant Payments in seinen eigenen Büchern unterhalten wird;

   — ‚Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto‘ (‚TIPS DCA to TIPS AS technical account liquidity transfer order‘): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu erhöhen;

   — ‚Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto‘ (‚TIPS AS technical account to TIPS DCA liquidity transfer order‘): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu verringern;

   — ‚Netzwerkdienstleister (NSP)‘ (‚Network Service Provider (NSP)‘): ein Unternehmen, dem vom Eurosystem eine Konzession für die Erbringung von Verbindungsdiensten (auch ‚Konnektivitätsdienste‘ genannt) über das Zugangsportal zur Finanzmarktinfrastruktur des Eurosystems (ESMIG) erteilt wurde.“

   c) Die Begriffsbestimmung von „T2S-Netzwerkdienstleister“ wird gestrichen.

2. Artikel 4 Absatz 2 Buchstabe fc erhält folgende Fassung:

   „fc) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto und Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto;“.

3. In Artikel 4 Absatz 2 wird folgender Buchstabe fd eingefügt:

   „fd) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto und Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, und“.

4. Artikel 4 Absatz 3 erhält folgende Fassung:

   „(3) TARGET2 bietet Echtzeit-Brutto-Abwicklung von Euro- Zahlungen in Zentralbankgeld über PM-Konten, über T2S-Geldkonten und über TIPS-Geldkonten an. TARGET2 wird auf der Grundlage der SSP eingerichtet und betrieben, über die – technisch in gleicher Weise – Zahlungsaufträge eingereicht und verarbeitet sowie schließlich Zahlungen empfangen werden. Was die technische Führung von T2S-Geldkonten betrifft, wird TARGET2 auf der T2S-Plattform eingerichtet und betrieben. Was die technische Führung von TIPS-Geldkonten und technischen TIPS-Nebensystemkonten betrifft, wird TARGET2 auf der TIPS-Plattform eingerichtet und betrieben. Die [Name der Zentralbank einfügen] ist Erbringer der Dienstleistungen nach Maßgabe dieser Bedingungen. Handlungen und Unterlassungen der SSP-Anbieter-NZBen und der vier Zentralbanken gelten als Handlungen und Unterlassungen der [Name der Zentralbank einfügen], die für solche Handlungen und Unterlassungen gemäß Artikel 21 dieses Anhangs haftet. Die Teilnahme gemäß diesen Bedingungen begründet keine vertragliche Beziehung zwischen den T2S-Kontoinhabern und den SSP-Anbieter-NZBen oder den vier Zentralbanken, wenn eine der Letztgenannten in dieser Eigenschaft handelt. Weisungen/Anweisungen, Nachrichten oder Informationen, die ein T2S-Kontoinhaber im Rahmen der gemäß diesen Bedingungen erbrachten Dienste von der SSP oder der T2S-Plattform erhält oder an diese sendet, gelten als von [Name der Zentralbank einfügen] erhalten oder an diese gesendet.“

5. Artikel 8 Absatz 3 erhält folgende Fassung:

   „(3) Hat die [Name der Zentralbank einfügen] einem Antrag eines T2S-Geldkontoinhabers gemäß Absatz 1 stattgegeben, so wird davon ausgegangen, dass der T2S-Geldkontoinhaber dem/den teilnehmenden Zentralverwahrer (n) die Ermächtigung zur Belastung des T2S-Geldkontos mit den Beträgen erteilt hat, die bei den Wertpapierumsätzen auf diesen Wertpapierkonten anfallen.“

6. Artikel 28 Absatz 1 erhält folgende Fassung:

„(1) Es wird davon ausgegangen, dass sich die T2S-Geldkontoinhaber ihrer gesetzlichen Pflichten zum Datenschutz bewusst sind, diese einhalten und in der Lage sind, die Einhaltung gegenüber den betreffenden zuständigen Behörden nachzuweisen. Es wird davon ausgegangen, dass sie sich ihrer Pflichten zur Bekämpfung der Geldwäsche, der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst sind und diese einhalten; insbesondere treffen sie danach angemessene Vorkehrungen bei den Zahlungen, die auf ihren T2S-Geldkonten verbucht werden. Die T2S-Geldkontoinhaber stellen vor Abschluss des Vertrags mit dem Netzwerkdienstleister sicher, dass sie mit dessen Regelungen zur Wiederherstellung verloren gegangener Daten vertraut sind."

7. Artikel 30 erhält folgende Fassung:

„*Artikel 30*

Vertragsverhältnis mit einem Netzwerkdienstleister

(1) T2S-Geldkontoinhaber müssen entweder

a) einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abgeschlossen haben, um eine technische Verbindung zu TARGET2-[Name der Zentralbank einfügen] herzustellen, oder

b) die technische Verbindung über eine andere Stelle herstellen, die einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abgeschlossen hat.

(2) Das Rechtsverhältnis zwischen einem T2S-Geldkontoinhaber und dem Netzwerkdienstleister unterliegt ausschließlich den Bedingungen des mit einem Netzwerkdienstleister gemäß Absatz 1 Buchstabe a abgeschlossenen separaten Vertrags.

(3) Die vom Netzwerkdienstleister erbrachten Dienste sind nicht Bestandteil der Dienstleistungen, die die [Name der Zentralbank einfügen] im Rahmen von TARGET2 erbringt.

(4) Die [Name der Zentralbank einfügen] haftet daher weder für Handlungen, Fehler oder Unterlassungen des Netzwerkdienstleisters (einschließlich seiner Direktoren, Mitarbeiter und Zulieferer) noch für Handlungen, Fehler oder Unterlassungen von Dritten, die die Teilnehmer ausgewählt haben, um Zugang zum Netz des Netzwerkdienstleisters zu erhalten."

8. Der folgende Artikel 34a wird eingefügt:

„*Artikel 34a*

Übergangsbestimmungen

Sobald das TARGET-System den Betrieb aufnimmt und der Betrieb von TARGET2 eingestellt wurde, werden T2S-Geldkontoinhaber zu T2S-Geldkontoinhabern im TARGET-System."

9. Die Bezugnahmen auf „T2S-Netzwerkdienstleister" (Singular oder Plural) in Anhang IIa Artikel 6 Absatz 1 Buchstabe a Ziffer i, Artikel 9 Absatz 5, Artikel 10 Absatz 6, Artikel 14 Absatz 1 Buchstabe a, Artikel 22 Absätze 1, 2 und 3, Artikel 27 Absatz 5, Artikel 28 Absatz 1, Artikel 29 Absatz 1 und Anlage I Nummer 1 werden durch Bezugnahmen auf „Netzwerkdienstleister" ersetzt.

10. Anlage I Nummer 7 Absatz 1 Buchstabe b erhält folgende Fassung:

„b) User-to-Application-Modus (U2A)

Der U2A-Modus ermöglicht die direkte Kommunikation zwischen dem T2S-Geldkontoinhaber und der T2S GUI. Die Informationen werden in einem Browser angezeigt, der auf einem PC-System läuft. Für den U2A-Zugriff muss die IT-Infrastruktur Cookies unterstützen. Weitere Einzelheiten sind im T2S-Benutzerhandbuch aufgeführt."

ANHANG III

Anhang IIb der Leitlinie EZB/2012/27 wird wie folgt geändert:

1. Die Bezugnahmen auf „TIPS-Netzwerkdienstleister“ (Singular oder Plural) in Artikel 17 Absatz 1 Buchstabe a, Artikel 24 Absätze 1 und 2, Artikel 26 Absatz 2 Buchstabe d, Artikel 29 Absatz 6, Anlage I Nummer 1, Anlage I Nummer 6 Absatz 1 und Anlage II Nummer 3 Absatz 3 Buchstabe b werden durch Bezugnahmen auf „Netzwerkdienstleister“ ersetzt.

2. Artikel 1 wird wie folgt geändert:

   a) Die Begriffsbestimmung von „erreichbare Partei“ erhält folgende Fassung:

      „– ‚erreichbare Partei‘ (‚reachable party‘): eine Stelle, die a) Inhaberin eines Business Identifier Code (BIC) ist, b) von einem TIPS-Geldkontoinhaber oder durch ein Nebensystem als erreichbare Partei bestimmt wird, c) Korrespondent, Kunde oder Zweigstelle eines TIPS-Geldkontoinhabers, oder Teilnehmer eines Nebensystems, oder Korrespondent, Kunde oder Zweigstelle eines Teilnehmers eines Nebensystems ist und d) entweder über den TIPS-Geldkontoinhaber oder das Nebensystem Instant Payment-Aufträge oder, falls eine entsprechende Genehmigung des TIPS-Geldkontoinhabers oder des Nebensystems erteilt wurde, direkt Instant Payment-Aufträge bei der TIPS-Plattform einreichen und über diese Zahlungen empfangen kann;“

   b) Die Begriffsbestimmung von „Zahlungsauftrag“ erhält folgende Fassung:

      „– ‚Zahlungsauftrag‘ (‚payment order‘): mit Ausnahme der Verwendung in Artikel 16 bis 18 dieses Anhangs ein Instant Payment-Auftrag, eine positive Rückruf-Antwort, ein Auftrag zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto, ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto, ein Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto oder ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto;“

   c) Die Begriffsbestimmung von „Instant Payment-Auftrag“ erhält folgende Fassung:

      „– ‚Instant Payment-Auftrag‘ (‚instant payment order‘): entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst Scheme) des European Payments Council (EPC) ein Zahlungsauftrag, der an jedem Kalendertag des Jahres rund um die Uhr ausgeführt werden kann – mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; hierzu zählen i) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein TIPS-Geldkonto, ii) Instant Payment-Aufträge von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, iii) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto und iv) Instant Payment-Aufträge von einem technischen TIPS-Nebensystemkonto auf ein technisches TIPS-Nebensystemkonto;“

   d) Die folgenden Begriffsbestimmungen werden angefügt:

      „— ‚technisches TIPS-Nebensystemkonto‘ (‚TIPS ancillary system technical account (TIPS AS technical account)‘): ein Konto, das von einem Nebensystem oder der Zentralbank im Auftrag eines Nebensystems im TARGET2-Komponenten-System der Zentralbank zur Nutzung durch dieses Nebensystem zum Zwecke der Abwicklung von Instant Payments in seinen eigenen Büchern unterhalten wird;

      — ‚Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto‘ (‚TIPS DCA to TIPS AS technical account liquidity transfer order‘): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu erhöhen;

      — ‚Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto‘ (‚TIPS AS technical account to TIPS DCA liquidity transfer order‘): eine Weisung/Anweisung zur Übertragung eines bestimmten Geldbetrags von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto, um die Position des TIPS-Geldkontoinhabers (oder die Position eines anderen Teilnehmers des Nebensystems) in den Büchern des Nebensystems zu verringern;

      — ‚SEPA Instant Credit Transfer (SCT Inst) Scheme des European Payments Council‘ oder ‚SCT Inst Scheme‘ (‚European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme‘ or ‚SCT Inst scheme‘): ein automatisiertes Verfahren mit offenen Standards, das ein Regelwerk für den Interbankenverkehr vorsieht, das von den SCT-Inst-Teilnehmern einzuhalten ist und es den im SEPA tätigen Zahlungsdienstleistern ermöglicht, ein automatisiertes, SEPA-weites Produkt für Euro-Echtzeitüberweisungen anzubieten;

      — ‚Mobiler Proxy-Look-up-Dienst (MPL-Dienst)‘ (‚mobile proxy look-up (MPL) service‘): ein Dienst, der es TIPS-Geldkontoinhabern, Nebensystemen, die technische TIPS-Nebensystemkonten verwenden, und erreichbaren Parteien, die von ihren Kunden einen Auftrag zur Ausführung eines Instant Payment-Auftrags zugunsten eines über einen Proxy identifizierten Empfängers (z. B. Mobilfunknummer) erhalten, ermöglicht, die entsprechende IBAN und den entsprechenden BIC des Begünstigten, die zur Gutschrift des betreffenden Kontos in TIPS zu verwenden sind, vom zentralen MPL-Verzeichnis abzurufen;

      — ‚Netzwerkdienstleister (NSP)‘ (‚Network Service Provider (NSP)‘): ein Unternehmen, dem vom Eurosystem eine Konzession für die Erbringung von Verbindungsdiensten (auch „Konnektivitätsdienste“ genannt) über das Zugangsportal zur Finanzmarktinfrastruktur des Eurosystems erteilt wurde;

— ‚IBAN': die internationale Kontonummer (International Bank Account Number), die ein Einzelkonto bei einem bestimmten Finanzinstitut in einem bestimmten Land eindeutig identifiziert."

e) Die Begriffsbestimmung von „TIPS-Netzwerkdienstleister" wird gestrichen.

3. In Artikel 3 Absatz 1 wird die Bezugnahme auf „Anlage V: Technische Voraussetzungen für die TIPS-Anbindung" gestrichen.

4. Artikel 4 wird wie folgt geändert:

a) In Absatz 2 wird folgender Buchstabe ia eingefügt:

„ia) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto und Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto;";

b) Absatz 3 erhält folgende Fassung:

„(3) TARGET2 bietet Echtzeit-Brutto-Abwicklung von Euro-Zahlungen in Zentralbankgeld über PM-Konten, über T2S-Geldkonten und über TIPS-Geldkonten an. TARGET2 wird auf der Grundlage der SSP eingerichtet und betrieben, über die – technisch in gleicher Weise – Zahlungsaufträge eingereicht und verarbeitet sowie schließlich Zahlungen empfangen werden. Was die technische Führung von TIPS-Geldkonten und technischen TIPS-Nebensystemkonten betrifft, wird TARGET2 auf der TIPS-Plattform eingerichtet und betrieben. Was die technische Führung von T2S-Geldkonten betrifft, wird TARGET2 auf der T2S-Plattform eingerichtet und betrieben."

5. Artikel 6 Absatz 1 Buchstabe a Ziffer i erhält folgende Fassung:

„i) Installation, Verwaltung, Betrieb, Überwachung und Gewährleistung der Sicherheit der für die Anbindung an die TIPS-Plattform und zur Übermittlung von Zahlungsaufträgen an diese Plattform notwendigen IT-Infrastruktur. Dabei können die beantragenden TIPS-Geldkontoinhaber zwar Dritte mit einbeziehen, bleiben aber für deren Tun oder Unterlassen allein verantwortlich. Insbesondere ist – sofern keine einreichende Partei eingeschaltet wird – der beantragende TIPS-Geldkontoinhaber verpflichtet, mit einem oder mehreren Netzwerkdienstleistern eine Vereinbarung zu treffen, um die erforderliche Anbindung gemäß den technischen Spezifikationen in Anlage I zu erhalten, und".

6. Artikel 9 erhält folgende Fassung:

„*Artikel 9*

Vertragsverhältnis mit einem Netzwerkdienstleister

(1) Die Teilnehmer müssen entweder:

a) einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abschließen, um eine technische Verbindung zu TARGET2-[Zentralbank/Ländercode einfügen] herzustellen, oder

b) die technische Verbindung über eine andere Stelle herstellen, die einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abgeschlossen hat.

(2) Das Rechtsverhältnis zwischen einem Teilnehmer und dem Netzwerkdienstleister unterliegt ausschließlich den Bedingungen ihres separaten Vertrags gemäß Absatz 1 Buchstabe a.

(3) Die vom Netzwerkdienstleister erbrachten Dienste sind nicht Bestandteil der Dienstleistungen, die die [Name der Zentralbank einfügen] im Rahmen von TARGET2 erbringt.

(4) Die [Name der Zentralbank einfügen] haftet daher weder für Handlungen, Fehler oder Unterlassungen des Netzwerkdienstleisters (einschließlich seiner Direktoren, Mitarbeiter und Zulieferer) noch für Handlungen, Fehler oder Unterlassungen von Dritten, die die Teilnehmer ausgewählt haben, um Zugang zum Netz des Netzwerkdienstleisters zu erhalten."

7. Artikel 10 wird gestrichen.

8. Der folgende Artikel 11a wird eingefügt:

„*Artikel 11a*

MPL-Verzeichnis

(1) Das zentrale MPL-Verzeichnis enthält die Proxy-IBAN-Entsprechungstabelle für die Zwecke des MPL-Dienstes.

(2) Jeder Proxy darf nur mit einer IBAN verknüpft werden. Eine IBAN kann mit einem oder mehreren Proxys verknüpft werden.

(3) Artikel 29 findet Anwendung auf die im MPL-Verzeichnis enthaltenen Daten."

9. Artikel 12 Absatz 9 wird gestrichen.

10. Artikel 15 Absatz 5 erhält folgende Fassung:

„(5) TIPS-Geldkonten werden entweder mit 0 % oder zum Einlagesatz, je nachdem, welcher dieser Zinssätze niedriger ist, verzinst, sofern diese Konten nicht zur Haltung von Mindestreserven oder von Überschussreserven genutzt werden.

Im Falle von Mindestreserven werden die Berechnung und Zahlung der anfallenden Zinsen durch die Verordnung (EG) Nr. 2531/98 des Rates (*) und die Verordnung (EU) 2021/378 der Europäischen Zentralbank (EZB/2021/1) (**) geregelt.

Im Falle von Überschussreserven werden die Berechnung und Zahlung der anfallenden Zinsen durch den Beschluss (EU) 2019/1743 (EZB/2019/31) (***) geregelt.

_____

(*) Verordnung (EG) Nr. 2531/98 des Rates vom 23. November 1998 über die Auferlegung einer Mindestreservepflicht durch die Europäische Zentralbank (ABl. L 318 vom 27.11.1998, S. 1).

(**) Verordnung (EU) 2021/378 der Europäischen Zentralbank vom 22. Januar 2021 über die Auferlegung einer Mindestreservepflicht (EZB/2021/1) (ABl. L 73 vom 3.3.2021, S. 1).

(***) Beschluss (EU) 2019/1743 der Europäischen Zentralbank vom 15. Oktober 2019 über die Verzinsung von Überschussreserven und bestimmten Einlagen (EZB/2019/31) (ABl. L 267 vom 21.10.2019, S. 12).“

11. Artikel 16 erhält folgende Fassung:

„*Artikel 16*

Arten von Zahlungsaufträgen auf TIPS-Geldkonten

Im Rahmen des TIPS-Dienstes gelten als Zahlungsaufträge:

a) Instant Payment-Aufträge;

b) positive Rückruf-Antworten;

c) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto;

d) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto;

e) Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto.“

12. Artikel 18 Absatz 6 erhält folgende Fassung:

„(6) Wurde ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto, ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto oder ein Auftrag zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto wie in Artikel 17 beschrieben angenommen, prüft TARGET2-[Zentralbank/Ländercode einfügen], ob auf dem Konto des Zahlers ausreichend Mittel verfügbar sind. Sind keine ausreichenden Mittel verfügbar, wird der Auftrag zur Liquiditätsübertragung zurückgewiesen. Sind ausreichende Mittel verfügbar, wird der Auftrag zur Liquiditätsübertragung sofort abgewickelt.“

13. Artikel 20 Absatz 1 Buchstabe b erhält folgende Fassung:

„b) Aufträge zur Liquiditätsübertragung vom TIPS-Geldkonto auf das PM-Konto, positive Rückruf-Antworten und Aufträge zur Liquiditätsübertragung vom TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto in TARGET2-[Zentralbank/Ländercode einfügen] zu dem Zeitpunkt als eingebracht und sind zu dem Zeitpunkt unwiderruflich, zu dem das maßgebliche TIPS-Geldkonto belastet wird. Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto in TARGET2-[Zentralbank/Ländercode einfügen] gelten zu dem Zeitpunkt als eingebracht und sind zu dem Zeitpunkt unwiderruflich, zu dem das maßgebliche technische TIPS-Nebensystemkonto belastet wird.“

14. Artikel 30 Absatz 1 erhält folgende Fassung:

„(1) Es wird davon ausgegangen, dass sich die TIPS-Geldkontoinhaber ihrer gesetzlichen Pflichten zum Datenschutz bewusst sind, diese einhalten und in der Lage sind, die Einhaltung gegenüber den betreffenden zuständigen Behörden nachzuweisen. Es wird davon ausgegangen, dass sie sich ihrer gesetzlichen Pflichten zur Bekämpfung der Geldwäsche, der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst sind und diese einhalten; insbesondere treffen sie danach angemessene Vorkehrungen bei den Zahlungen, die auf ihren TIPS-Geldkonten verbucht werden. Die TIPS-Geldkontoinhaber stellen vor Aufnahme vertraglicher Beziehungen mit ihrem gewählten Netzwerkdienstleister sicher, dass sie mit den Regelungen dieses Netzwerkdienstleisters zur Wiederherstellung verloren gegangener Daten vertraut sind.“

15. Der folgende Artikel 35a wird eingefügt:

„*Artikel 35a*

Übergangsbestimmung

Sobald das TARGET-System den Betrieb aufnimmt und der Betrieb von TARGET2 eingestellt wurde, werden TIPS-Geldkontoinhaber zu TIPS-Geldkontoinhabern im TARGET-System.“

16. Die Tabelle in Anlage I Nummer 2 erhält folgende Fassung:

„Nachrichtentyp	Nachrichtenname
Pacs.002	FIToFIPayment Status Report
Pacs.004	PaymentReturn
Pacs.008	FIToFICustomerCreditTransfer
Pacs.028	FIToFIPaymentStatusRequest
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.011	ModifyLimit
camt.019	ReturnBusinessDayInformation
camt.025	Receipt
camt.029	ResolutionOfInvestigation
camt.050	LiquidityCreditTransfer
camt.052	BankToCustomerAccountReport
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.056	FIToFIPaymentCancellationRequest
acmt.010	AccountRequestAcknowledgement
acmt.011	AccountRequestRejection
acmt.015	AccountExcludedMandateMaintenanceRequest
reda.016	PartyStatusAdviceV01
reda.022	PartyModificationRequestV01“

17. Anlage I Nummer 6 Absatz 1 Buchstabe b erhält folgende Fassung:

„b) User-to-Application-Modus (U2A)

Der U2A-Modus ermöglicht die direkte Kommunikation zwischen dem TIPS-Geldkontoinhaber und der TIPS-GUI. Die Informationen werden in einem Browser angezeigt, der auf einem PC-System läuft. Für den U2A-Zugriff muss die IT-Infrastruktur Cookies unterstützen. Weitere Einzelheiten sind im TIPS-Benutzerhandbuch aufgeführt.“

18. In Anlage IV wird Nummer 2 gestrichen.

19. Anlage V wird gestrichen.

ANHANG IV

Anhang IV der Leitlinie EZB/2012/27 wird wie folgt geändert:

1. Nummer 14 Absatz 14 Buchstabe d erhält folgende Fassung:

   „d) SWIFT-Aufträge mittels MT 103-Nachricht dürfen nicht eingereicht werden."

2. In Nummer 18 Absatz 1 Buchstabe b erhält Zeile 1 der Tabelle folgende Fassung:

„Band-Band-breite	Von (Mio EUR/ Geschäftstag)	Bis (Mio. EUR/ Geschäftstag)	Jahresgebühr (EUR)	Monatsgebühr (EUR)"

3. In Nummer 18 Absatz 1 Buchstabe d wird der letzte Unterabsatz gestrichen.

ANHANG V

Der folgende Anhang IVa wird in die Leitlinie EZB/2012/27 eingefügt:

„*ANHANG IVa*

TIPS-DIENST FÜR NEBENSYSTEME, DIE INSTANT PAYMENTS ABWICKELN

1. **Begriffsbestimmungen**

In diesem Anhang gelten folgende Begriffsbestimmungen zusätzlich zu den in Anhang IIb Artikel 1 festgelegten:

1. ‚Nebensystem-Zentralbank' (‚ancillary system central bank (ASCB)'): die Zentralbank des Eurosystems, mit der das betreffende Nebensystem, das Instant Payments in seinen eigenen Büchern abwickelt, eine bilaterale Vereinbarung über die Abwicklung von Instant Payments des Nebensystems abgeschlossen hat.

2. ‚zugrunde liegendes Bruttovolumen' (‚underlying gross volume'): die Anzahl der in den eigenen Büchern des Nebensystems abgewickelten Instant Payments, die durch auf dem technischen TIPS-Nebensystemkonto gehaltene Mittel ermöglicht werden. Nicht inbegriffen sind Instant Payments an oder von TIPS-Geldkonten oder anderen technischen TIPS-Nebensystemkonten.

3. ‚einreichende Partei' (‚instructing party'): eine Stelle, die von einem Nebensystem als solche bestimmt wurde und die im Auftrag dieses Nebensystems oder einer erreichbaren Partei dieses Nebensystems Zahlungsaufträge an die TIPS-Plattform senden und/oder von der TIPS-Plattform erhalten kann.

2. **Einbringung von Zahlungsaufträgen in das System und deren Unwiderruflichkeit**

Die Anwendung von Anhang IIb Artikel 20 in Bezug auf den Zeitpunkt der Einbringung von Instant Payment-Aufträgen, positiven Rückruf-Antworten sowie Aufträgen zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto und Aufträgen zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto im betreffenden TARGET2-Komponenten-System hat keinen Einfluss auf Regeln von Nebensystemen, die einen Zeitpunkt für die Einbringung in das Nebensystem und/oder die Unwiderruflichkeit von bei diesem Nebensystem eingereichten Zahlungsaufträgen festlegen, der vor dem Einbringungszeitpunkt des jeweiligen Nebensystem-Zahlungsauftrags in das betreffende TARGET2-Komponenten-System liegt.

3. **Konten zur Unterstützung der Abwicklung von Instant Payments in den eigenen Büchern von Nebensystemen**

1. Zur Unterstützung der Abwicklung von Instant Payments im Zusammenhang mit Nebensystemen in TIPS ist ein technisches TIPS-Nebensystemkonto zu eröffnen.

2. Ein technisches TIPS-Nebensystemkonto erhält eine eindeutige, aus bis zu 34 Zeichen bestehende Kontonummer, die sich wie in der Tabelle dargestellt zusammensetzt:

	Bezeichnung	**Format**	**Inhalt**
Teil A	Kontoart	genau 1 Stelle	‚A' für AS Technical Account (technisches Nebensystemkonto)
	Ländercode der Zentralbank	genau 2 Stellen	Ländercode nach ISO-Norm 3166-1
	Währungscode	genau 3 Stellen	EUR
Teil B	Kontoinhaber	genau 11 Stellen	BIC
Teil C	Unterklassifizierung des Kontos	bis zu 17 Stellen	Vom Kontoinhaber frei gestalteter (alphanumerischer) Text.

3. Der Kontosaldo von technischen TIPS-Nebensystemkonten kann im Tagesverlauf nur null oder positiv sein. Technische TIPS-Nebensystemkonten können über Nacht einen positiven Saldo aufweisen. Ein Übernachtsaldo auf dem Konto unterliegt den gleichen Verzinsungsregeln, wie sie gemäß Artikel 11 dieser Leitlinie für Sicherungsguthaben gelten.

4. **Abwicklungsverfahren**

1. Das betreffende Nebensystem verwendet ein technisches TIPS-Nebensystemkonto, um die erforderliche, von seinen Verrechnungsmitgliedern bereitgestellte Liquidität zur Deckung ihrer Positionen zu sammeln.

2. Auf Wunsch wird das Nebensystem über Gutschriften und Belastungen auf seinem technischen TIPS-Nebensystemkonto informiert.

3. Ein Nebensystem kann Instant Payment-Aufträge und positive Rückruf-Antworten an einen TIPS-Geldkontoinhaber oder ein TIPS-Nebensystem senden. Ein Nebensystem empfängt und verarbeitet Instant Payment-Aufträge, Rückruf-Anfragen und positive Rückruf-Antworten von TIPS-Geldkontoinhabern oder TIPS-Nebensystemen.

5. **Benutzerschnittstelle**

1. Der Inhaber des technischen TIPS-Nebensystemkontos greift im A2A-Modus auf die TIPS-Plattform zu und kann darüber hinaus entweder direkt oder über eine oder mehrere einreichende Parteien eine Verbindung im U2A-Modus herstellen.

2. Der Zugang zur TIPS-Plattform ermöglicht den Inhabern technischer TIPS-Nebensystemkonten,

   a) Informationen über ihre Konten abzurufen und CMBs zu steuern,

   b) Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto zu erteilen und

   c) bestimmte Stammdaten zu verwalten.

6. **Gebührenverzeichnis und Rechnungsstellung**

1. Ein Nebensystem in TIPS hat Gebühren gemäß den beiden folgenden Posten zu entrichten:

   a) eine Transaktionsgebühr, die auf der Basis des für die TIPS-Geldkontoinhaber in Anhang IIb Anlage IV erstellten Gebührenverzeichnisses berechnet wird;

   b) eine Gebühr auf der Basis des zugrunde liegenden Bruttovolumens der auf der eigenen Plattform des Nebensystems abgewickelten Instant Payments, die durch die vorfinanzierten Positionen auf dem technischen TIPS-Nebensystemkonto ermöglicht werden. Die Gebühr beträgt 0,0005 EUR je Instant Payment.

2. Das zugrunde liegende Bruttovolumen der Instant Payments des Nebensystems wird von der Nebensystem-Zentralbank monatlich auf der Grundlage des auf 10 000 abgerundeten zugrunde liegenden Bruttovolumens des Vormonats berechnet und vom Nebensystem spätestens am dritten Geschäftstag des Folgemonats gemeldet. Das berechnete Bruttovolumen wird für die Berechnung der Gebühr im Folgemonat zugrunde gelegt.

3. Jedes Nebensystem erhält von seiner Nebensystem-Zentralbank eine auf den in Absatz 1 dieser Nummer genannten Gebühren beruhende Rechnung für den Vormonat spätestens am neunten Geschäftstag eines Monats. Die Zahlung hat spätestens bis zum vierzehnten Geschäftstag des Monats der Ausstellung der Rechnung auf das von der Nebensystem-Zentralbank angegebene Konto zu erfolgen oder wird von einem vom Nebensystem angegebenen Konto abgebucht.

4. Für die Zwecke der Gebührenverzeichnisse und der Rechnungsstellung gemäß diesem Anhang gilt Folgendes:

   a) Ein Nebensystem, das gemäß der Richtlinie 98/26/EG als System benannt wurde, wird als getrenntes Nebensystem behandelt, selbst wenn es von einer juristischen Person betrieben wird, die ein weiteres Nebensystem betreibt.

   b) Ein Nebensystem, das nicht gemäß der Richtlinie 98/26/EG als System benannt wurde, wird als getrenntes Nebensystem behandelt, wenn es folgende Kriterien erfüllt:

      i) es handelt sich um eine formelle Regelung auf vertraglicher oder regulatorischer Basis;

      ii) es hat mehr als [ein Mitglied]/[einen Teilnehmer], [ausgenommen den Systembetreiber dieses Systems];

      iii) es wurde für die Zwecke des Clearing, der Verrechnung und/oder der Abwicklung von Zahlungen und/oder Wertpapieren zwischen den Teilnehmern eingerichtet;

      iv) es wendet gemeinsame Bedingungen und standardisierte Regelungen auf das Clearing, die Verrechnung und die Abwicklung von Zahlungen und Wertpapieren zwischen den Teilnehmern an.

5. Für die Zwecke der Rechnungsstellung gemäß diesem Artikel belaufen sich die Gebühren für den Zeitraum vom 1. Dezember 2021 bis zum 28. Februar 2022 auf den Durchschnitt der für die Monate September, Oktober und November 2021 insgesamt in Rechnung gestellten Gebühren.“

ANHANG VI

Der folgende Anhang II Anlage VIII wird der Leitlinie EZB/2012/27 angefügt:

„Anlage VIII

Anforderungen an das Informationssicherheitsmanagement und das Business-Continuity-Management

Informationssicherheitsmanagement

Diese Anforderungen gelten für jeden einzelnen Teilnehmer, es sei denn, ein Teilnehmer weist nach, dass eine bestimmte Anforderung auf ihn nicht anwendbar ist. Bei der Festlegung des Anwendungsbereichs der Anforderungen innerhalb seiner Infrastruktur sollte der Teilnehmer die Elemente identifizieren, die Teil der Zahlungstransaktionskette sind. Die Zahlungstransaktionskette beginnt am Point of Entry (PoE), d. h. einem System, das an der Erstellung von Transaktionen beteiligt ist (z. B. Workstations, Front- und Back-Office-Anwendungen, Middleware), und endet beim System, das für die Übermittlung der Nachricht an SWIFT verantwortlich ist (z. B. SWIFT VPN Box) oder beim Internet (Letzteres trifft bei internetbasiertem Zugang zu).

Anforderung 1.1: Informationssicherheitsstrategie

Die Geschäftsführung legt einen klaren sicherheitspolitischen Kurs fest, der im Einklang mit den Geschäftszielen steht. Sie verpflichtet sich zur Informationssicherheit und fördert diese, indem sie eine Strategie für die Informationssicherheit formuliert, verabschiedet und aufrechterhält, die darauf abzielt, das Management von Informationssicherheit und Cyberresilienz innerhalb der gesamten Organisation in Bezug auf Identifikation, Bewertung und Behandlung von Risiken für die Informationssicherheit und die Cyberresilienz sicherzustellen. Die Strategie sollte mindestens folgende Abschnitte beinhalten: Ziele, Umfang (darunter Bereiche wie Organisation, Personal, Verwaltung der Informationswerte usw.), Grundsätze und Zuweisung von Verantwortlichkeiten.

Anforderung 1.2: Interne Organisation

Zur Umsetzung der Informationssicherheitsstrategie innerhalb der Organisation wird ein Informationssicherheitsrahmenwerk geschaffen. Die Geschäftsführung koordiniert und überprüft die Einrichtung des Informationssicherheitsrahmenwerks, damit die organisationsweite Umsetzung der Informationssicherheitsstrategie (gemäß der Anforderung 1.1), darunter auch die Zuteilung ausreichender Ressourcen und die Zuweisung entsprechender Sicherheitsverantwortlichkeiten, gewährleistet ist.

Anforderung 1.3: Externe Parteien

Wenn eine Organisation mit externen Parteien zusammenarbeitet bzw. deren Produkte oder Dienstleistungen in Anspruch nimmt und/oder von diesen abhängig ist, sollte dies nicht die Sicherheit ihrer Informationen und informationsverarbeitenden Einrichtungen beeinträchtigen. Der Zugang externer Parteien zu den informationsverarbeitenden Einrichtungen der Organisation ist in jedem Fall zu kontrollieren. Sofern externe Parteien oder Produkte/Dienstleistungen externer Parteien Zugang zu informationsverarbeitenden Einrichtungen der Organisation benötigen, ist eine Risikoprüfung durchzuführen, um die sicherheitsrelevanten Auswirkungen zu ermitteln und die Kontrollanforderungen zu bestimmen. Die Kontrollen werden mit der externen Partei jeweils einzeln vereinbart und vertraglich festgelegt.

Anforderung 1.4: Verwaltung von Informationswerten

Sämtliche Informationswerte, Geschäftsprozesse und zugrundeliegenden Informationssysteme entlang der Zahlungstransaktionskette, wie Betriebssysteme, Infrastrukturen, Fachsoftware, Standardprodukte, Dienste und von Nutzern entwickelte Anwendungen, sind zu erfassen und einem Eigentümer namentlich zuzuordnen. Zum Schutz der Informationswerte ist zudem festzulegen, wer für die Aufrechterhaltung und die Durchführung angemessener Kontrollen in den Geschäftsprozessen und den zugehörigen IT-Komponenten zuständig ist. Hinweis: Der Eigentümer kann soweit angemessen die Durchführung bestimmter Kontrollen delegieren; er ist jedoch weiterhin für den ordnungsgemäßen Schutz der Informationswerte verantwortlich.

Anforderung 1.5: Klassifizierung von Informationswerten

Die Informationswerte werden nach ihrer Kritikalität für den reibungslosen Betrieb durch den Teilnehmer klassifiziert. Aus der Klassifizierung muss ersichtlich sein, ob, mit welcher Priorität und in welchem Umfang Informationswerte zu schützen sind, während sie in den jeweiligen Geschäftsprozessen und durch die zugrunde liegenden IT-Komponenten verwendet werden. Mithilfe eines von der Geschäftsführung genehmigten Systems zur Klassifizierung von Informationswerten werden für die gesamte Lebensdauer der Informationswerte (einschließlich Löschung und Vernichtung der Informationswerte) angemessene Schutzkontrollen definiert und es wird die Notwendigkeit spezieller Maßnahmen im Umgang mit bestimmten Informationen kommuniziert.

Anforderung 1.6: Personelle Sicherheit

Die Verantwortlichkeiten bezüglich der Sicherheit werden bereits vor der Einstellung neuer Mitarbeiter in einer entsprechenden Stellenbeschreibung benannt und in den vertraglichen Beschäftigungsbedingungen festgehalten. Alle Bewerber, Vertragspartner und Drittanwender sind hinreichend zu überprüfen, besonders bei sensiblen Stellen bzw. Aufträgen. Mitarbeiter, Vertragspartner und Dritte, die informationsverarbeitende Einrichtungen nutzen, unterzeichnen eine Vereinbarung, in der ihre Sicherheitsrollen und Verantwortlichkeiten festgelegt sind. Es wird gewährleistet, dass alle Mitarbeiter, Vertragspartner und Dritte hinreichend für Sicherheitsaspekte sensibilisiert sind. Zur Minimierung möglicher Sicherheitsrisiken sind ihnen Fortbildungen und Schulungen zu Sicherheitsverfahren und dem korrekten Einsatz der informationsverarbeitenden Einrichtungen zu ermöglichen. Für Mitarbeiter ist ein formelles Disziplinarverfahren zu schaffen, das bei Verletzung von Sicherheitsbestimmungen zur Anwendung kommt. Durch Zuweisung entsprechender Verantwortlichkeiten ist zu gewährleisten, dass das Ausscheiden eines Mitarbeiters, Vertragspartners oder Dritten bzw. dessen Wechsel innerhalb der Organisation gesteuert wird sowie sämtliche Betriebsmittel zurückgegeben und alle Zugangsberechtigungen entzogen werden.

Anforderung 1.7: Physische und umgebungsbezogene Sicherheit

Kritische oder sensible informationsverarbeitende Einrichtungen werden in Sicherheitsbereichen untergebracht, die durch eine genau festgelegte Sicherheitszone sowie entsprechende Sicherheitsbarrieren und Zutrittskontrollen geschützt sind. Sie müssen physisch vor unrechtmäßigem Zutritt sowie Zerstörung und Manipulation geschützt sein. Der Zutritt ist nur Personen zu gewähren, die unter die Anforderung 1.6 fallen. Es werden Verfahren und Standards festgelegt, um physische Medien, auf denen Informationswerte gespeichert sind, auf Transportwegen zu schützen.

Die Betriebsmittel sind vor physischen und umgebungsbezogenen Bedrohungen zu schützen. Um das Risiko eines unerlaubten Zugriffs auf Informationen zu mindern sowie Schäden und Verluste in Bezug auf Betriebsmittel oder Informationen zu verhindern, ist es erforderlich, dass sämtliche (auch außerhalb des Standorts verwendete) Betriebsmittel geschützt und Vorkehrungen zum Schutz vor Entwendung von Eigentum getroffen werden. Zur Abwehr physischer Bedrohungen und zum Schutz der unterstützenden Infrastruktur wie der Stromversorgung und der Verkabelung können besondere Maßnahmen erforderlich sein.

Anforderung 1.8: Betriebsmanagement

Für die Verwaltung und den Betrieb von informationsverarbeitenden Einrichtungen, die durchgängig alle zugrunde liegenden Systeme der Zahlungstransaktionskette abdecken, werden Verantwortlichkeiten und Verfahren festgelegt.

Was die Betriebsprozesse einschließlich der technischen Administration der IT-Systeme betrifft, so ist soweit angemessen eine Aufteilung der Verantwortlichkeiten vorzunehmen, um das Risiko eines fahrlässigen oder vorsätzlichen Systemmissbrauchs zu verringern. Ist eine solche Aufteilung aus dokumentierten objektiven Gründen nicht möglich, sind im Anschluss an eine formale Risikoanalyse kompensierende Kontrollen zu implementieren. Es werden Kontrollen eingerichtet, um das Eindringen von Schadsoftware (Malware) in die Systeme der Zahlungstransaktionskette zu verhindern und aufzudecken. Es werden zudem Kontrollen (einschließlich der Nutzersensibilisierung) eingeführt, um Malware abzuwehren, aufzuspüren und zu entfernen. Mobiler Programmcode darf nur verwendet werden, wenn er aus vertrauenswürdigen Quellen stammt (z. B. signierte COM-Komponenten von Microsoft sowie Java Applets). Die Browsereinstellungen (z. B. Verwendung von Erweiterungen und Plug-ins) sind strengen Kontrollen zu unterziehen.

Es müssen Konzepte zur Datensicherung und -wiederherstellung von der Geschäftsführung umgesetzt werden. Hierzu zählt auch ein Wiederherstellungsplan, der in regelmäßigen Abständen, jedoch mindestens jährlich, zu testen ist.

Zudem werden die für die Sicherheit des Zahlungsverkehrs kritischen Systeme überwacht und relevante Informationssicherheitsvorfälle dokumentiert. Durch den Einsatz von Betreiberprotokollen ist sicherzustellen, dass Probleme im Bereich der Informationssysteme erkannt werden. Die Betreiberprotokolle werden in regelmäßigen Abständen – je nach der Kritikalität des Betriebsprozesses – stichprobenartig überprüft. Eine Systemüberwachung ist durchzuführen, um die Effizienz der als kritisch für die Sicherheit des Zahlungsverkehrs eingestuften Kontrollmechanismen zu überprüfen und die Einhaltung der Zugangsregelungen zu verifizieren.

Der Informationsaustausch zwischen Organisationen muss auf Basis einer formellen Austauschrichtlinie und im Rahmen von zwischen den betroffenen Parteien abgeschlossenen Austauschvereinbarungen erfolgen. Hierbei sind die einschlägigen Rechtsvorschriften einzuhalten. Werden Software-Komponenten von Drittanbietern im Informationsaustausch mit TARGET2 verwendet (z. B. wenn, wie im zweiten Anforderungsszenario der TARGET2-Selbstzertifizierung beschrieben, Software von einem Servicebüro bezogen wird), so muss hierfür eine formale Vereinbarung mit dem Dritten abgeschlossen werden.

Anforderung 1.9: Zugangskontrolle

Der Zugang zu Informationswerten ist durch die fachlichen Anforderungen (‚Kenntnis nur soweit nötig' [1]) und im Einklang mit dem bestehenden Regelungsrahmen der Organisation (einschließlich der Informationssicherheitsstrategie) zu begründen. Es sind eindeutige Regeln für die Zugriffskontrolle auf Basis des Grundsatzes der minimalen Rechtevergabe [2] festzulegen, die den Erfordernissen des jeweiligen Geschäftszwecks und der IT-Prozesse genau Rechnung tragen. Soweit relevant (z. B. zur Backup-Verwaltung), müssen die logischen mit den physischen Zugriffskontrollen übereinstimmen, es sei denn, es bestehen angemessene Ausgleichskontrollen (z. B. Verschlüsselung, Anonymisierung personenbezogener Daten).

Um die Zuweisung von Rechten zum Zugriff auf Informationssysteme und -dienste der Zahlungstransaktionskette zu kontrollieren, müssen formelle, dokumentierte Verfahren umgesetzt werden. Diese Verfahren müssen den gesamten Lebenszyklus des Nutzerzugangs abdecken – von der Erstregistrierung neuer Nutzer bis hin zur endgültigen Abmeldung von Nutzern, die keinen Zugang mehr benötigen.

Besondere Beachtung erfordert gegebenenfalls die Zuweisung von Zugriffsrechten, die so kritisch sind, dass ihr Missbrauch zu einer schwerwiegenden Beeinträchtigung der betrieblichen Prozesse des Teilnehmers führen kann (z. B. Zugriffsrechte im Zusammenhang mit der Systemadministration, dem Umgehen von Systemkontrollen oder dem direkten Zugriff auf Geschäftsdaten).

Es sind angemessene Kontrollen einzurichten, um die Nutzer an bestimmten Punkten des Netzwerks der Organisation, beispielsweise für den lokalen oder Fernzugang zu Systemen der Zahlungstransaktionskette, zu ermitteln, zu authentifizieren und zu berechtigen. Um die Zurechenbarkeit zu gewährleisten, dürfen persönliche Konten nicht geteilt werden.

Passwörter dürfen nicht einfach zu erraten sein. Deshalb müssen Regeln (z. B. für die Komplexität und zeitlich begrenzte Gültigkeit der Passwörter) festgelegt und durch spezielle Kontrollen durchgesetzt werden. Es ist ein Protokoll für die sichere Wiederherstellung bzw. Zurücksetzung von Passwörtern zu erstellen.

Es muss eine Leitlinie zur Anwendung kryptografischer Kontrollen entwickelt und umgesetzt werden, um die Vertraulichkeit, Authentizität und Integrität von Informationen zu schützen. Zur Unterstützung dieser Kontrollen muss die Verwaltung kryptografischer Schlüssel geregelt sein.

Ebenso sind Regelungen für das Lesen vertraulicher Informationen am Bildschirm oder auf Papier zu treffen, z. B. durch eine Strategie des leeren Bildschirms (Clear Screen Policy) oder des aufgeräumten Schreibtisches (Clear Desk Policy), um das Risiko eines unberechtigten Zugriffs zu reduzieren.

Bei Arbeit mit Fernzugriff muss das Risiko, das mit der Arbeit in einer ungeschützten Umgebung einhergeht, berücksichtigt werden, und es sind angemessene technische und organisatorische Kontrollen einzurichten.

Anforderung 1.10: Beschaffung, Entwicklung und Wartung von Informationssystemen

Vor der Entwicklung und/oder Implementierung von Informationssystemen sind die Sicherheitsanforderungen zu ermitteln und zu vereinbaren.

Zur Gewährleistung einer korrekten Verarbeitung müssen geeignete Kontrollen in die Anwendungen integriert werden, auch in solche, die von Nutzern entwickelt wurden. Die Validierung von Ein- und Ausgabedaten und intern verarbeiteten Daten ist Bestandteil dieser Kontrollen. Zusätzliche Kontrollen sind unter Umständen für Systeme erforderlich, die sensible, wertvolle oder kritische Informationen verarbeiten oder diese beeinflussen. Solche Kontrollen sind auf Basis der Sicherheitsanforderungen und einer Risikobewertung in Übereinstimmung mit den bestehenden Leitlinien und Konzepten (z. B. der Informationssicherheitsstrategie und der Leitlinie für kryptografische Kontrollen) zu bestimmen.

[1] Der Grundsatz ‚Kenntnis nur soweit nötig' bezieht sich auf die Ermittlung der Gesamtheit derjenigen Informationen, auf die eine einzelne Person Zugriff haben muss, um ihre Aufgaben zu erledigen.

[2] Nach dem Grundsatz der minimalen Rechtevergabe wird der Zugriff einer Person auf ein IT-System so gestaltet, dass er ihrer fachlichen Zuständigkeit entspricht.

Die betrieblichen Anforderungen an neue Systeme sind festzulegen, zu dokumentieren und vor ihrer Abnahme und Verwendung zu testen. Es müssen geeignete Kontrollen zur Gewährleistung der Netzwerksicherheit, einschließlich Segmentierung und sicherer Verwaltung, umgesetzt werden. Dies sollte in Abhängigkeit von der Kritikalität der Datenströme und vom Risikograd der Netzwerkbereiche in der Organisation erfolgen. Zum Schutz sensibler Daten, die über öffentliche Netzwerke geleitet werden, sind spezifische Kontrollmechanismen erforderlich.

Der Zugang zu Systemdateien und Quellcodes ist zu kontrollieren; IT-Projekte und Supportmaßnahmen sind in sicherer Form durchzuführen. Es ist dafür Sorge zu tragen, dass sensible Daten in Testumgebungen nicht frei zugänglich sind. Projekt- und Supportumgebungen sind einer strengen Kontrolle zu unterziehen. Dies gilt auch für Änderungen in der Produktionsumgebung. Bei wesentlichen Änderungen an der Produktionsumgebung ist eine Risikobewertung durchzuführen.

Zudem müssen regelmäßige Sicherheitstests der produktiven Systeme durchgeführt werden. Diese sind auf Grundlage der Ergebnisse einer Risikobewertung vorab zu planen und müssen mindestens Schwachstellenprüfungen umfassen. Sämtliche während der Sicherheitstests festgestellten Mängel sind zu prüfen. Maßnahmenpläne zur Schließung von ermittelten Sicherheitslücken müssen erstellt und zeitnah abgearbeitet werden.

Anforderung 1.11: Informationssicherheit bei Beziehungen zu Anbietern ([3])

Um den Schutz der den Anbietern zugänglichen internen Informationssysteme des Teilnehmers zu gewährleisten, sind Informationssicherheitsanforderungen zu dokumentieren und in einer formalen Vereinbarung mit dem Anbieter festzuhalten, durch welche die mit dem Zugang des Anbieters verbundenen Risiken begrenzt werden.

Anforderung 1.12: Umgang mit Informationssicherheitsvorfällen und diesbezügliche Verbesserungen

Um einen konsistenten und wirksamen Ansatz für den Umgang mit Informationssicherheitsvorfällen (wozu auch die Meldung von Sicherheitsereignissen und -schwachstellen zählt) sicherzustellen, sind sowohl auf fachlicher als auch auf technischer Ebene Rollen, Verantwortlichkeiten und Verfahren festzulegen und zu testen, damit nach Informationssicherheitsvorfällen eine rasche, wirksame und geordnete Wiederherstellung der Sicherheit erfolgen kann; dies schließt auch Szenarien im Zusammenhang mit Cybervorfällen ein (z. B. Betrug durch einen externen Angreifer oder einen Insider). Das in diese Verfahren eingebundene Personal ist angemessen zu schulen.

Anforderung 1.13: Überprüfung der Erfüllung technischer Anforderungen

Die internen Informationssysteme eines Teilnehmers (z. B. Back-Office-Systeme, interne Netzwerke und Verbindungen zu externen Netzwerken) sind regelmäßig darauf zu bewerten, ob sie dem bestehenden Regelungsrahmen der Organisation (z. B. der Informationssicherheitsstrategie und der Leitlinie für kryptografische Kontrollen) entsprechen.

Anforderung 1.14: Virtualisierung

Gast-VMs (virtuelle Maschinen) müssen sämtliche Sicherheitsanforderungen erfüllen, die auch für physische Hardware und Systeme gelten (z. B. Härten, Protokollierung). Als Anforderungen für Hypervisoren sind vorgeschrieben: Härten des Hypervisors und des Host-Betriebssystems, regelmäßige Patches und strikte Trennung der unterschiedlichen Umgebungen (z. B. Produktions- und Entwicklungsumgebung). Auf Basis einer Risikoanalyse sind eine zentralisierte Steuerung, Protokollierung, Überwachung und Verwaltung der Zugriffsrechte, insbesondere für Konten mit privilegierten Berechtigungen, zu implementieren. Verwaltet ein Hypervisor mehrere Gast-VMs, müssen diese ein ähnliches Risikoprofil haben.

Anforderung 1.15: Cloud Computing

Die Verwendung öffentlicher und/oder hybrider Cloud-Lösungen in der Zahlungstransaktionskette muss durch eine formale Risikoanalyse begründet sein, bei der die technischen Kontrollen und Vertragsbestimmungen der Cloud-Lösung geprüft werden.

Bei der Nutzung einer hybriden Cloud-Lösung wird davon ausgegangen, dass die Kritikalitätsstufe des Gesamtsystems der des angebundenen Systems mit der höchsten Kritikalität entspricht. Alle am Standort befindlichen Komponenten der Hybridlösung sind von den übrigen Standortsystemen zu trennen.

([3]) Als Anbieter ist in diesem Zusammenhang jede dritte Partei (einschließlich ihrer Mitarbeiter) zu verstehen, mit der das Institut eine vertragliche Vereinbarung zur Erbringung einer Dienstleistung abgeschlossen hat und die (einschließlich ihrer Mitarbeiter) im Rahmen des Dienstleistungsvertrags entweder direkt vor Ort oder über einen Fernzugang Zugriff auf Informationen und/oder Informationssysteme und/oder informationsverarbeitende Einrichtungen des Instituts im Anwendungsbereich oder in Verbindung mit dem Anwendungsbereich der TARGET2-Selbstzertifizierung erhält.

Business-Continuity-Management (gilt nur für kritische Teilnehmer)

Die folgenden Anforderungen (2.1 bis 2.6) beziehen sich auf das Business-Continuity-Management. Jeder TARGET2-Teilnehmer, der vom Eurosystem im Hinblick auf das reibungslose Funktionieren von TARGET2 als kritisch eingestuft wurde, muss über eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs verfügen, die folgende Elemente aufweist:

Anforderung 2.1: Pläne zur Aufrechterhaltung des Geschäftsbetriebs sind erstellt, und Verfahren zu deren Pflege sind umgesetzt.

Anforderung 2.2: Es muss ein Ausweichstandort vorhanden sein.

Anforderung 2.3: Das Risikoprofil des Ausweichstandorts muss sich von dem des Primärstandorts unterscheiden. Hierdurch soll vermieden werden, dass beide Standorte zeitgleich von derselben Störung betroffen sind. So sollte beispielsweise der Ausweichstandort an ein anderes Energieversorgungsnetz und eine andere Hauptfernmeldeleitung als der Primärstandort angeschlossen sein.

Anforderung 2.4: Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, muss der kritische Teilnehmer in der Lage sein, den normalen Betrieb vom Ausweichstandort aus wiederaufzunehmen und dort den Geschäftstag ordnungsgemäß abzuschließen und den/die folgenden Geschäftstag(e) zu beginnen.

Anforderung 2.5: Durch etablierte Verfahren muss eine Wiederaufnahme der Transaktionsverarbeitung am Ausweichstandort innerhalb einer angemessenen Zeitspanne nach der ursprünglichen Unterbrechung des Dienstes und verhältnismäßig zur Kritikalität des von der Unterbrechung betroffenen Geschäftsvorgangs gewährleistet werden.

Anforderung 2.6: Die Fähigkeit, Betriebsstörungen zu bewältigen, ist mindestens einmal jährlich zu überprüfen, und alle wichtigen Mitarbeiter sind in geeigneter Weise zu schulen. Der Abstand zwischen den Tests darf nicht länger als ein Jahr sein.“