OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

**Änderungen der Geschäftsbestimmungen der Oesterreichischen Nationalbank per 21.11.2021**

**(Diese Liste dient der Information, rechtsverbindlich sind nur die Geschäftsbestimmungen, wie auf der Website der OeNB veröffentlicht.)**

| Regelung | Aktuelle Version | **Änderung ab 21.11.2021** |
|---|---|---|
| **Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und die Inanspruchnahme von Innertageskrediten (GB ASTI)** | | |
| § 4 Abs 13 | (13) Bei der Verzinsung von Forderungen im Rahmen der Haftung gelangt der EONIA Zinssatz zur Anwendung. | (13) Bei der Verzinsung von Forderungen im Rahmen der Haftung gelangt der Marktzinssatz für täglich fällige Einlagen zur Anwendung. |
| § 10 Abs 2<br>entfernt | (2) Für Geschäftspartner, die unmittelbar vor Inkrafttreten dieser Geschäftsbestimmungen Inhaber eines Girokontos aufgrund der „Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und die Inanspruchnahme von Innertageskrediten (gültig ab 30.11.2018)“ der OeNB waren, entfällt das Erfordernis der Antragstellung | --- |
| § 12<br>(Sprachliche Neufassung, keine materielle Änderung der Negativverzinsung) | § 12 Kontoführung<br><br>(1) Die Girokonten sind grundsätzlich in Euro denominiert. Die Führung eines Girokontos in einer anderen Währung als Euro bedarf einer schriftlichen Vereinbarung zwischen OeNB und Kontoinhaber.<br><br>(2) Das Girokonto bei der OeNB dient der Durchführung des Zahlungsverkehrs über die OeNB und/oder der Haltung der Mindestreserve. Die Verwendung von Girokonten zwecks Durchführung von Kapitalerhöhungen von Kreditinstituten bleibt unberührt. Jegliche weitere Verwendung, wie z. B. Haltung von Einlagen, Vermögensverwaltung, Treuhand etc., bedarf der schriftlichen Zustimmung der OeNB.<br><br>(3) Die OeNB kann ein auf dem Girokonto ständig zu belassendes Mindestguthaben festsetzen. | § 12 Kontoführung<br><br>(1) Die Girokonten sind grundsätzlich in Euro denominiert. Die Führung eines Girokontos in einer anderen Währung als Euro bedarf einer schriftlichen Vereinbarung zwischen OeNB und Kontoinhaber.<br><br>(2) Das Girokonto bei der OeNB dient der Durchführung des Zahlungsverkehrs über die OeNB und/oder der Haltung der Mindestreserve. Die Verwendung von Girokonten zwecks Durchführung von Kapitalerhöhungen von Kreditinstituten bleibt unberührt. Jegliche weitere Verwendung, wie z. B. Haltung von Einlagen, Vermögensverwaltung, Treuhand etc., bedarf der schriftlichen Zustimmung der OeNB.<br><br>(3) Die OeNB kann ein auf dem Girokonto ständig zu belassendes Mindestguthaben festsetzen. |

| | | |
|---|---|---|
| | (4) Guthaben, die aufgrund einer gesetzlichen Verpflichtung auf einem Girokonto gehalten werden müssen oder aufgrund eines geldpolitischen Geschäftes im Rahmen des Eurosystems entstanden sind, können positiv verzinst werden. Auf Guthaben auf sämtlichen anderen Girokonten leistet die OeNB – unbeschadet der Sonderregelungen für Girokonten von öffentlichen Haushalten in Abs. 5 und Abs. 6 – keine Verzinsung. Beträgt der Einlagesatz jedoch weniger als null Prozent, kann die OeNB die Guthaben ebenfalls mit dem negativen Einlagezinssatz belasten.<br><br>(5) Der Gesamtbetrag aller täglich fälligen Einlagen und Termineinlagen öffentlicher Haushalte auf Girokonten bei der OeNB, insoweit als dieser den höheren Betrag aus:<br><br>i) 200 Mio. EUR oder<br><br>ii) 0,04 % des österreichischen Bruttoinlandsprodukts<br><br>(Schwellenwert) übersteigt, wird nicht verzinst. Zur Bestimmung dieses Schwellenwerts ist das Bruttoinlandsprodukt gemäß der auf der Website der Europäischen Kommission veröffentlichten Herbstprognose des Vorjahres heranzuziehen. Ist der Einlagesatz an einem Tag, an dem dieser Schwellenwert überschritten wird, negativ, findet ein Zinssatz Anwendung, der nicht höher als der Einlagesatz ist. Der den oben genannten Schwellenwert unterschreitende Gesamtbetrag kann, soweit dies den diesbezüglichen Vorgaben der EZB entspricht, positiv verzinst werden. Die Aufteilung erfolgt einmal jährlich nach den Durchschnittssalden der Konten. Liegt jedoch an einem beliebigen Kalendertag der Einlagesatz bei null Prozent oder niedriger, aber über dem Marktzinssatz für unbesicherte täglich fällige Einlagen bzw. dem Marktzinssatz für besicherte Einlagen, werden alle Einlagen öffentlicher Haushalte zum jeweiligen Marktzinssatz (täglich fällige Einlagen mit dem Marktzinssatz für unbesicherte täglich fällige Einlagen, Termineinlagen mit dem Marktzinssatz für besicherte Einlagen mit einer vergleichbaren Laufzeit oder, sofern nicht verfügbar, ebenfalls mit dem Marktzinssatz für unbesicherte täglich fällige Einlagen) verzinst. Nicht in Euro denominierte Einlagen öffentlicher Haushalte werden ggf. vergleichbar verzinst. | (4) Guthaben, die aufgrund einer gesetzlichen Verpflichtung auf einem Girokonto gehalten werden müssen oder aufgrund eines geldpolitischen Geschäftes im Rahmen des Eurosystems entstanden sind, können positiv verzinst werden. Auf Guthaben auf sämtlichen anderen Girokonten leistet die OeNB keine positive Verzinsung. Beträgt der Einlagesatz jedoch weniger als null Prozent, kann die OeNB die Guthaben ebenfalls mit dem negativen Einlagezinssatz belasten.<br><br>(5) Guthaben, die für den Kontoinhaber nicht frei verfügbar sind (Kontosperre gem. § 18), werden gemäß Art 3 Abs 1 lit d der Verordnung (EU) 2021/378 der EZB nicht in die Haltung der Mindestreserve und den damit verbundenen Sonderregelungen hinsichtlich der Verzinsung einbezogen.<br><br>(6) Ist ein Guthaben auf einem Girokonto negativ verzinst, entsteht eine Zahlungsverpflichtung des Geschäftspartners gegenüber der OeNB. Die OeNB wird das Girokonto entsprechend belasten.<br><br>(7) Eine unbesicherte Überziehung eines Girokontos ist nicht gestattet.<br><br>(8) Girokonten werden bei der Hauptanstalt der OeNB in Wien geführt.<br><br>(9) Sämtliche die Girokonten betreffende Kommunikation erfolgt in deutscher oder englischer Sprache. |

| | | |
|---|---|---|
| | (6) Die Einlagen öffentlicher Haushalte iSd Leitlinie EZB/2019/7 idgF in Zusammenhang mit finanziellen Hilfsprogrammen der Europäischen Union/des Internationalen Währungsfonds und anderen vergleichbaren Hilfsprogrammen, die auf Girokonten bei der OeNB gehalten werden, werden nicht verzinst; sie werden jedoch nicht auf den in Abs. 4 genannten Schwellenwert angerechnet.<br><br>(7) Sämtliche anderen Guthaben auf Girokonten werden nicht verzinst.<br><br>(8) Ist ein Guthaben auf einem Girokonto negativ verzinst, entsteht eine Zahlungsverpflichtung des Geschäftspartners gegenüber der OeNB. Die OeNB wird das Girokonto entsprechend belasten.<br><br>(9) Eine unbesicherte Überziehung eines Girokontos ist nicht gestattet.<br><br>(10) Girokonten werden bei der Hauptanstalt der OeNB in Wien geführt.<br><br>(11) Sämtliche die Girokonten betreffende Kommunikation erfolgt in deutscher oder englischer Sprache. | |
| § 12a<br>Eingefügt<br>(Sprachliche Neufassung, keine materielle Änderung der Negativverzinsung) | --- | § 12a Negativverzinsung des Guthabens öffentlicher Haushalte iSd Leitlinie (EU) 2019/671 der EZB<br><br>(1) Eine positive Verzinsung von Guthaben öffentlicher Haushalte findet nicht statt.<br><br>(2) Jedem Kontoinhaber, der dem öffentlichen Haushalt zuzurechnen ist, wird zum Zwecke der Negativverzinsung jährlich ein individueller Schwellenbetrag zugewiesen, der sich aus dem Verhältnis seines durchschnittlichen Guthabens zum Guthaben aller öffentlichen Haushalte bei der OeNB in der Vorperiode (jeweils Juli – Juni) sowie der Obergrenze gemäß Art 4 Abs 1 lit b der Leitlinie (EU) 2019/671 der EZB idgF ergibt.<br><br>(3) Liegt der Einlagesatz bei 0 % oder höher und ist der Marktzinssatz für unbesicherte täglich fällige Einlagen an einem beliebigen Kalendertag negativ, wird das Gesamtguthaben mit diesem Marktzinssatz negativ verzinst. |

| | | |
|---|---|---|
| | | (4) Ist der Einlagesatz an einem beliebigen Kalendertag negativ und liegt der Marktzinssatz für unbesicherte täglich fällige Einlagen bei null Prozent oder höher, wird das Guthaben bis zum Schwellenwert nicht verzinst und das über dem Schwellenwert liegende Guthaben mit dem Einlagesatz negativ verzinst.<br><br>(5) Sind sowohl der Einlagesatz als auch Marktzinssatz für unbesicherte täglich fällige Einlagen an einem beliebigen Kalendertag negativ, und ist der Einlagesatz gleich oder höher als der Marktzinssatz für unbesicherte täglich fällige Einlagen, wird das Gesamtguthaben mit dem Marktzinssatz für unbesicherte täglich fällige Einlagen negativ verzinst.<br><br>(6) Sind sowohl der Einlagesatz als auch Marktzinssatz für unbesicherte täglich fällige Einlagen an einem beliebigen Kalendertag negativ, und ist der Einlagesatz niedriger als der Marktzinssatz für unbesicherte täglich fällige Einlagen, wird das Guthaben bis zum Schwellenwert mit dem Marktzinssatz für unbesicherte täglich fällige Einlagen negativ verzinst und das über dem Schwellenwert liegende Guthaben mit dem Einlagesatz negativ verzinst.<br><br>(7) Nicht in Euro denominierte Einlagen öffentlicher Haushalte werden ggf. vergleichbar verzinst. |
| § 14 Abs 1 lit d | d) Mittels schriftlichen Auftrags: Sofern nicht anderweitig vereinbart, sind ausschließlich die von der OeNB aufgelegten Vordrucke zu verwenden. Schriftlich erteilte Zahlungsaufträge müssen alle für die Durchführung notwendigen Angaben enthalten und sind entsprechend dem bei der OeNB hinterlegten Unterschriftsprobenblatt giromäßig zu fertigen. Der Geschäftspartner haftet sowohl der OeNB als auch Dritten gegenüber, dass Urschrift und Durchschriften des jeweiligen Zahlungsauftrags übereinstimmen. | d) Mittels schriftlichen Auftrags: Sofern nicht anderweitig vereinbart, sind ausschließlich die von der OeNB aufgelegten Vordrucke zu verwenden. Schriftlich erteilte Zahlungsaufträge müssen alle für die Durchführung notwendigen Angaben enthalten und sind entsprechend dem bei der OeNB hinterlegten Unterschriftsprobenblatt giromäßig zu fertigen. Der Geschäftspartner haftet sowohl der OeNB als auch Dritten gegenüber, dass Urschrift und Durchschriften des jeweiligen Zahlungsauftrags übereinstimmen. Schriftliche Aufträge bedürfen der Rückbestätigung per Telefon oder E-Mail. |
| § 21 | § 21 Kontoauskünfte<br><br>(1) In Ermangelung anderslautender gesetzlicher Vorschriften werden Auskünfte über das Girokonto nur dem Geschäftspartner oder den von ihm ermächtigten Personen erteilt. | § 21 Kontoauskünfte und Informationsregime<br><br>(1) In Ermangelung anderslautender gesetzlicher Vorschriften werden Auskünfte über das Girokonto nur dem Geschäftspartner oder den von ihm ermächtigten Personen erteilt. |

| | | |
|---|---|---|
| | (2) Abweichend von Abs. 1 erklärt der Geschäftspartner hiermit seine Zustimmung zur Weiterleitung von zahlungsbezogenen, technischen oder organisatorischen Informationen an Aufsichts- und Überwachungsbehörden und –stellen Österreichs oder der Europäischen Union, soweit dies für die Erfüllung ihrer öffentlichen Aufgaben erforderlich ist.<br><br>(3) Der Geschäftspartner erklärt sich damit einverstanden, von der OeNB unabhängig von der Nutzung der Funktion „E-Konto“ gemäß § 14 Abs. 1 lit. d) und § 15 dieser Geschäftsbestimmungen Zusendungen auch auf elektronischem Weg (via E-Mail) zu erhalten. Solche Zusendungen umfassen Informationen, welche im Zusammenhang mit dem Zahlungsverkehr der OeNB stehen, (z. B. Kontoauszüge, Informationen zur Kontoführung, sonstige Hinweise u. ä.). | (2) Abweichend von Abs. 1 erklärt der Geschäftspartner hiermit seine Zustimmung zur Weiterleitung von zahlungsbezogenen, technischen oder organisatorischen Informationen an Aufsichts- und Überwachungsbehörden und –stellen Österreichs oder der Europäischen Union, soweit dies für die Erfüllung ihrer öffentlichen Aufgaben erforderlich ist.<br><br>(3) Die OeNB (Zahlungsverkehrsabteilung) wird ermächtigt, von den zuständigen Aufsichtsbehörden, insbesondere der Finanzmarktaufsicht sowie von an der Ausübung der Aufsicht gesetzlich beteiligten Stellen und Einrichtungen, alle für sie in Bezug auf den Zahlungsverkehr, zur Wahrnehmung der in den gegenständlichen Geschäftsbestimmungen geregelten Rechte und Pflichten sowie zur Sicherstellung des Funktionierens des Zahlungsverkehrssystems maßgeblichen Informationen zum Geschäftspartner einzuholen; sie ist dazu aber nicht verpflichtet.<br>(4) Der Geschäftspartner erklärt sich damit einverstanden, von der OeNB unabhängig von der Nutzung der Funktion „E-Konto“ gemäß § 14 Abs. 1 lit. d) und § 15 dieser Geschäftsbestimmungen Zusendungen auch auf elektronischem Weg (via E-Mail) zu erhalten. Solche Zusendungen umfassen Informationen, welche im Zusammenhang mit dem Zahlungsverkehr der OeNB stehen, (z. B. Kontoauszüge, Informationen zur Kontoführung, sonstige Hinweise u. ä.). |
| § 40 Abs 1 | (1) § 2, § 12 Abs 5 und Abs 6 sind bereits mit 1. Oktober 2019 in Kraft getreten (vgl. § 40 der „Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und die Inanspruchnahme von Innertageskrediten gültig ab 01.10.2019“). § 35 Abs 2 lit b) tritt mit 17. November 2019 in Kraft. Im Übrigen bleiben die „Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und die Inanspruchnahme von Innertageskrediten (gültig ab 30.11.2018)“ bis 31. Dezember 2019 in Kraft. | (1) Diese Geschäftsbestimmungen treten am 21. November 2021 in Kraft. |
| § 40 Abs 3 | (3) Mit 1. Jänner 2020 verlieren die „Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und die Inanspruchnahme von Innertageskrediten (gültig ab 30.11.2018)“ sowie die | (3) Mit 21. November 2021 verlieren die „Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und |

| | | |
|---|---|---|
| | „Geschäftsbestimmungen der OeNB für die Führung von Girokonten, die Teilnahme am OeNB-Zahlungssystem ASTI und die Inanspruchnahme von Innertageskrediten (gültig ab 1.10.2019)“ ihre Gültigkeit. | die Inanspruchnahme von Innertageskrediten (gültig ab 17. November 2019)“ ihre Gültigkeit. |
| **Geschäftsbestimmungen der OeNB für die Teilnahme an TARGET2-OeNB (GB TARGET2-OeNB)** | | |
| Art. 1<br>Definition „Gruppe” | […]<br>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. 2238/20041 nach dem International Accounting Standard (IAS) 27 erstellt, wobei die Gruppe sich wie folgt zusammensetzen muss:<br>i) ein Mutterunternehmen und ein oder mehrere Tochterunternehmen oder[…] | […]<br>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 nach dem International Accounting Standard (IAS) 27 erstellt, wobei die Gruppe sich wie folgt zusammensetzen muss:<br>i) ein Mutterunternehmen und ein oder mehrere Tochterunternehmen oder ii) zwei oder mehr Tochterunternehmen desselben Mutterunternehmens oder[…] |
| Art. 1<br>Definition „Instant Payment-Auftrag” | — „Instant-Payment-Auftrag“ (instant payment order): entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst) des European Payments Council (EPC) eine Zahlungsanweisung, die an jedem Kalendertag des Jahres rund um die Uhr ausgeführt werden kann – mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; | – „Instant-Payment-Auftrag“ (instant payment order): entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst) 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; |
| Art 1<br>Eingefügte Definitionen | --- | – „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“ oderr „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;<br><br>– „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;<br><br>– „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;<br><br>– „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;<br><br>– „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; |
| Art 1<br>Definition „TIPS-Netzwerkdienstleister” entfernt | — „TIPS-Netzwerkdienstleister“ (TIPS network service provider):<br>Ein Unternehmen, das:<br>a) im Einklang mit den in Anhang IIb Anlage V der Leitlinie EZB/2012/27 festgelegten Regeln und Verfahren alle für die technische Anbindung an die TIPS-Plattform erforderlichen Voraussetzungen erfüllt und eine technische Verbindung hergestellt hat und<br>b) die TIPS connectivity hosting terms and conditions unterzeichnet hat, die auf der Website der EZB abgerufen werden können; | --- |
| Art. 3 Abs 2 lit fc) | fc) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto und Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto, | fc) Aufträge zur Liquiditätsübertragung von einem TIPS- Geldkonto auf ein PM-Konto und Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto”; |
| Art. 3 Abs 2 lit fd)<br>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 |
| Art. 3 Abs 3 | 3. TARGET2 ist ein Echtzeit-Brutto-Zahlungsverkehrssystem in Euro, über das Zahlungen von und auf PM-Konten, T2S-Geldkonten und TIPS-Geldkonten in Zentralbankgeld abgewickelt werden. TARGET2 wird auf der Grundlage der SSP 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 betrifft, wird TARGET2 auf der TIPS-Plattform eingerichtet und betrieben. | 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. |
| Art 5 | Artikel 5 – Direkte Teilnehmer | Artikel 5 – Direkte Teilnehmer<br>1. PM-Kontoinhaber in TARGET2-OeNB sind direkte Teilnehmer und müssen die in Artikel 8 Absätze 1 und 2 festgelegten Anforderungen erfüllen. Sie müssen über mindestens |

| | | |
|---|---|---|
| | 1. Direkte Teilnehmer an TARGET2-OeNB müssen die in Artikel 8 Absätze 1 und 2 festgelegten Anforderungen erfüllen. Sie müssen über mindestens ein PM-Konto bei der OeNB verfügen.<br><br>2. PM-Kontoinhaber können erreichbare BIC-Inhaber bestimmen, unabhängig von deren Ort der Niederlassung.<br><br>3. PM-Kontoinhaber können, sofern die Bedingungen nach Artikel 6 erfüllt sind, indirekte Teilnehmer im PM benennen.<br><br>4. Multi-Adressaten-Zugang durch Zweigstellen kann wie folgt gewährt werden:<br><br>a) Ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 lit a oder b, das als PM-Kontoinhaber zugelassen wurde, kann einer oder mehreren seiner in der Union oder im EWR gelegenen Zweigstellen zur direkten Einreichung von Zahlungsaufträgen und zum direkten Empfang von Zahlungen Zugang zu seinem PM-Konto gewähren, sofern die OeNB darüber informiert wurde.<br><br>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 gelegen – Zugang zum PM-Konto jener Zweigstelle, sofern die OeNB darüber informiert wurde. | ein PM-Konto bei der OeNB 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.<br><br>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.<br><br>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 OeNB oder als erreichbare Partei über einen TIPS-Geldkontoinhaber.<br><br>4. Multi-Adressaten-Zugang durch Zweigstellen kann wie folgt gewährt werden:<br><br>a) Ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 lit a oder b, 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 OeNB darüber informiert wurde.<br><br>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 OeNB darüber informiert wurde. |
| Art 12 Abs 3 | 3. 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 genutzt werden. Im letztgenannten Fall werden die Berechnung und Zahlung der für die Mindestreserven anfallenden Zinsen durch die Verordnung (EG) Nr. 2531/98 des Rates vom 23. November 1998 über die Auferlegung einer Mindestreservepflicht durch die Europäische Zentralbank und die Verordnung (EG) Nr. 1745/2003 der Europäischen Zentralbank vom 12. September 2003 über die Auferlegung einer Mindestreservepflicht (EZB/2003/9) geregelt.<br><br>(Fußnoten nicht übernommen) | 3. 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 (EU) Nr. 2531/98 des Rates und die Verordnung (EU) Nr. 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.<br><br>(Fußnoten nicht übernommen) |
| Art 28 | Artikel 28 – Sicherheitsanforderungen<br><br>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.<br><br>2. Die Teilnehmer informieren die OeNB über alle sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern. Die OeNB kann weitere Informationen über den Vorfall anfordern und erforderlichenfalls verlangen, dass der Teilnehmer angemessene Maßnahmen ergreift, um solche Ereignisse zukünftig zu vermeiden.<br><br>3. Die OeNB kann für alle Teilnehmer und/oder Teilnehmer, die von der OeNB als systemkritisch angesehen werden, zusätzliche Sicherheitsanforderungen verlangen, insbesondere im Hinblick auf Cybersicherheit oder Betrugsbekämpfung.<br><br>4. Teilnehmer übermitteln der OeNB ihre TARGET2-Selbstzertifizierung und die Bescheinigung über ihre Einhaltung der Endpunktsicherheitsanforderungen des TARGET2-Netzwerkdienstleisters. Sofern Teilnehmer die | Artikel 28 – Sicherheitsanforderungen und Kontrollverfahren<br><br>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.<br><br>2. Die Teilnehmer informieren die OeNB über alle sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern. Die OeNB kann weitere Informationen über den Vorfall anfordern und erforderlichenfalls verlangen, dass der Teilnehmer angemessene Maßnahmen ergreift, um solche Ereignisse zukünftig zu vermeiden.<br><br>3. Die OeNB kann für alle Teilnehmer und/oder Teilnehmer, die von der OeNB als systemkritisch angesehen werden, zusätzliche Sicherheitsanforderungen verlangen, insbesondere im Hinblick auf Cybersicherheit oder Betrugsbekämpfung.<br><br>4. Teilnehmer i) gewähren der OeNB dauerhaften Zugang zu ihrer Bescheinigung über die Einhaltung der Endpunktsicherheitsanforderungen des von ihnen gewählten |

| | | |
|---|---|---|
| | Endpunktsicherheitsanforderungen nicht einhalten, übermitteln sie ein Dokument, in dem alternative Risikominderungsmaßnahmen zur Zufriedenheit der OeNB beschrieben sind.<br><br>5. Teilnehmer, die Dritten Zugang zu ihrem PM-Konto gemäß Artikel 5 Abs 2, 3 und 4 gewähren, tragen dem mit der Erlaubnis eines solchen Zugangs verbundenen Risiko im Einklang mit den in den Abs 1 bis 4 genannten Sicherheitsanforderungen Rechnung. In der in Abs 4 genannten Selbstzertifizierung ist festgelegt, dass der Teilnehmer Dritte, die Zugang zu seinem PM-Konto haben, zur Einhaltung der Endpunktsicherheitsanforderungen des TARGET2-Netzwerkdienstleisters verpflichtet. | TARGET2-Netzwerkdienstleisters und ii) übermitteln der OeNB jährlich die auf der Website der OeNB und der Website der EZB in englischer Sprache veröffentlichte TARGET2-Selbstzertifizierungserklärung.<br><br>4a) Die OeNB 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 IX aufgeführt, die neben den in Artikel 2 Absatz 1 genannten Anlagen Bestandteil dieser Bedingungen sind.<br><br>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 OeNB unterrichtet die betreffenden Aufsichtsbehörden über den Stand der Einhaltung durch den jeweiligen Teilnehmer.<br><br>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 OeNB beurteilt jährlich erneut die Einhaltung der Anforderungen durch die Teilnehmer.<br><br>4e) Die OeNB kann Teilnehmern, deren Grad der Einhaltung der Anforderungen als geringfügige oder gravierende Nichteinhaltung eingestuft wurde, mit zunehmendem Schweregrad folgende Abhilfemaßnahmen auferlegen:<br><br>i) verstärkte Überwachung: Der Teilnehmer legt der OeNB 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;<br><br>ii) Suspendierung: Die Teilnahme an TARGET2-OeNB kann bei Vorliegen der in Artikel 34 Absatz 2 Buchstaben b und c dieser Geschäftsbestimmungen beschriebenen Umstände suspendiert werden. Abweichend von Artikel 34 dieser Geschäftsbestimmungen 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;<br><br>iii) Beendigung: Die Teilnahme an TARGET2-OeNB kann bei Vorliegen der in Artikel 34 Absatz 2 Buchstaben b und c dieser Geschäftsbestimmungen beschriebenen Umstände beendet werden. Abweichend von Artikel 34 dieser Geschäftsbestimmungen 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 OeNB behoben hat.<br><br>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. |
| Art 39 Abs 1 | 1. Die Teilnehmer sind sich ihrer gesetzlichen Pflichten zum Datenschutz sowie zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst und treffen insbesondere angemessene Vorkehrungen bei den Zahlungen, die auf ihren PM-Konten verbucht werden. Ferner machen sich die Teilnehmer vor Abschluss des Vertrags mit dem TARGET2-Netzwerkdienstleister mit den Regelungen des TARGET2-Netzwerkdienstleisters zur Wiederherstellung verloren gegangener Daten vertraut. | 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. |
| Art 46 Abs 3 und 4<br><br>Eingefügt | --- | 3. 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.<br><br>4. 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. |
| Anlage I Nummer 8 Abs 4b) | b) der User-to-Application-Modus (U2A)<br><br>Der U2A 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 und JavaScript unterstützen. Weitere Einzelheiten sind im ICM-Benutzerhandbuch aufgeführt. | b) der User-to-Application-Modus (U2A)<br><br>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. |
| Anlage IV Number 6 lit g) | g) Für die Abwicklung von Zahlungsaufträgen in der Notfallabwicklung stellen die Teilnehmer zusätzliche Sicherheiten bereit. Während der Notfallabwicklung können eingehende Notfallzahlungen zur Finanzierung von ausgehenden Notfallzahlungen verwendet werden.<br><br>Die OeNB wird die verfügbare Liquidität der Teilnehmer für die Zahlungsabwicklung im Rahmen der Notfallabwicklung nicht berücksichtigen. | 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.<br><br>Die OeNB wird die verfügbare Liquidität der Teilnehmer für die Zahlungsabwicklung im Rahmen der Notfallabwicklung nicht berücksichtigen. |
| Anlage IX | --- | Anlage IX<br><br>Anforderungen an das Informationssicherheitsmanagement und das Business-Continuity-Management<br><br>Informationssicherheitsmanagement<br><br>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).<br><br>Anforderung 1.1: Informationssicherheitsstrategie<br><br>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, das 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.<br><br>Anforderung 1.2: Interne Organisation<br><br>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.<br><br>Anforderung 1.3: Externe Parteien<br><br>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.<br><br>Anforderung 1.4: Verwaltung von Informationswerten<br><br>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.<br><br>Anforderung 1.5: Klassifizierung von Informationswerten<br><br>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.<br><br>Anforderung 1.6: Personelle Sicherheit<br><br>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 Dritte sind hinreichend zu überprüfen, besonders bei sensiblen Stellen bzw. Aufträgen. Mitarbeiter, Vertragspartner und Dritter, 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.<br><br>Anforderung 1.7: Physische und umgebungsbezogene Sicherheit<br><br>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.<br><br>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.<br><br>Anforderung 1.8: Betriebsmanagement<br><br>Für die Verwaltung und den Betrieb von informationsverarbeitenden Einrichtungen, die durchgängig alle zugrunde liegenden Systeme der Zahlungstransaktionskette abdecken, werden Verantwortlichkeiten und Verfahren festgelegt.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Anforderung 1.9: Zugangskontrolle<br><br>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).<br><br>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 |

[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.

| | | |
|---|---|---|
| | | von Nutzern, die keinen Zugang mehr benötigen.<br><br>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).<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Anforderung 1.11: Informationssicherheit bei Beziehungen zu Anbietern[3]<br><br>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.<br><br>Anforderung 1.12: Umgang mit Informationssicherheitsvorfällen und diesbezügliche Verbesserungen<br><br>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.<br><br>Anforderung 1.13: Überprüfung der Erfüllung technischer Anforderungen<br><br>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 |

[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.

| | | |
|---|---|---|
| | | kryptografische Kontrollen) entsprechen.<br><br>Anforderung 1.14: Virtualisierung<br><br>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.<br><br>Anforderung 1.15: Cloud Computing<br><br>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.<br><br>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.<br><br>Business-Continuity-Management (gilt nur für kritische Teilnehmer)<br><br>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:<br><br>Anforderung 2.1: Pläne zur Aufrechterhaltung des Geschäftsbetriebs sind erstellt, und Verfahren zu deren Pflege sind |

| | | |
|---|---|---|
| | | umgesetzt.<br><br>Anforderung 2.2: Es muss ein Ausweichstandort vorhanden sein.<br><br>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.<br><br>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.<br><br>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.<br><br>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.“ |
| Geschäftsbestimmungen der OeNB für die Teilnahme an TARGET2 Securities-OeNB (GB T2S-OeNB) | | **Annex II (amendments to Annex IIa to the Guideline ECB/2012/27):** |
| Art. 1<br><br>Definition „Instant Payment-Auftrag” | — „Instant-Payment-Auftrag“ („instant payment order)“: entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst) des European Payments Council (EPC) eine Zahlungsanweisung, die an jedem Kalendertag des Jahres rund um | – „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 |

| | | |
|---|---|---|
| | die Uhr am Tag ausgeführt werden kann – mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; | 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; |
| Art. 1<br>Eingefügte Definitionen | --- | – „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;<br><br>– „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;<br><br>– „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;<br><br>– „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; |

| | | |
|---|---|---|
| Art. 1<br>Definition „T2S-Netzwerdienstleister" entfernt | — „T2S-Netzwerkdienstleister" („T2S network service provider"): ein Unternehmen, das mit dem Eurosystem einen Lizenzvertrag über die Bereitstellung von Anschlüssen im Rahmen von T2S geschlossen hat; | --- |
| Art. 4 Abs 2 lit fc) | fc) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto und Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto; | fc) Aufträge zur Liquiditätsübertragung von einem TIPS- Geldkonto auf ein PM-Konto und Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto; |
| Art. 4 Abs 2 lit fd)<br>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 |
| Art. 4 Abs 3 | 3. TARGET2 ist ein Echtzeit-Brutto-Zahlungsverkehrssystem in Euro, über das Zahlungen von und auf PM-Konten, T2S-Geldkonten und TIPS-Geldkonten in Zentralbankgeld abgewickelt werden. TARGET2 wird auf der Grundlage der SSP 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 betrifft, wird TARGET2 auf der TIPS-Plattform eingerichtet und betrieben.<br><br>Die OeNB 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 OeNB, die für solche Handlungen und Unterlassungen gemäß Artikel 21 haftet. Die Teilnahme gemäß diesen Bedingungen begründet keine vertragliche Beziehung zwischen den T2S-Kontoinhabern und den SSP-Anbieter-NZBen oder der 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 der OeNB erhalten oder an diese gesendet. | 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.<br><br>Die OeNB 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 OeNB, die für solche Handlungen und Unterlassungen gemäß Artikel 21 dieser Geschäftsbestimmungen haftet. Die Teilnahme gemäß diesen Bedingungen begründet keine vertragliche Beziehung zwischen den T2S-Kontoinhabern und den SSP-Anbieter-NZBen oder der 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 der OeNB erhalten oder an diese |

| | | |
|---|---|---|
| | | gesendet. |
| Art. 8 Abs 3 | 3. Im Fall eines Antrags nach Absatz 1 wird der T2S-Geldkontoinhaber so gestellt, als habe er dem Zentralverwahrer, bei dem die verknüpften Wertpapierkonten geführt werden, die Ermächtigung zur Belastung des T2S-Geldkontos mit den Beträgen erteilt, die bei den Wertpapierumsätzen auf diesen Wertpapierkonten anfallen. | 3. Hat die OeNB 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. |
| Art. 28 Abs 1 | 1. Die T2S-Geldkontoinhaber sind sich ihrer gesetzlichen Pflichten zum Datenschutz sowie zur Bekämpfung der Geldwäsche, der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst und treffen insbesondere angemessene Vorkehrungen bei den Zahlungsaufträgen, die auf ihren T2S-Geldkonten verbucht werden. Die T2S-Geldkontoinhaber machen sich vor Abschluss des Vertrags mit dem T2S-Netzwerkdienstleister mit dessen Regelungen zur Wiederherstellung verloren gegangener Daten vertraut. | 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. |
| Art. 30 | Artikel 30 – Vertragsverhältnis mit dem T2S-Netzwerkdienstleister<br><br>1. Jeder T2S-Geldkontoinhaber schließt mit einem T2S-Netzwerkdienstleister eine besondere Vereinbarung zum Bezug der Dienste, die der T2S-Geldkontoinhaber für die Nutzung des T2S-Geldkontos benötigt. Das Rechtsverhältnis zwischen einem T2S-Geldkontoinhaber und dem T2S-Netzwerkdienstleister unterliegt ausschließlich den Bedingungen der von ihnen geschlossenen besonderen Vereinbarung.<br><br>2. Die vom T2S-Netzwerkdienstleister bereitgestellten Dienste sind nicht Bestandteil der Dienstleistungen, die die OeNB im Rahmen von TARGET2 erbringt.<br><br>3. Die OeNB haftet daher weder für Handlungen, Fehler oder Unterlassungen des T2S-Netzwerkdienstleisters (einschließlich seiner Direktoren, Mitarbeiter und Zulieferer) noch für Handlungen, | Artikel 30 – Vertragsverhältnis mit einem Netzwerkdienstleister<br><br>1. T2S-Geldkontoinhaber müssen entweder<br><br>a) einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abgeschlossen haben, um eine technische Verbindung zu TARGET2-OeNB herzustellen, oder<br><br>b) die technische Verbindung über eine andere Stelle herstellen, die einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abgeschlossen hat.<br><br>2. Das Rechtsverhältnis zwischen einem T2S-Geldkontoinhaber und dem Netzwerkdienstleister unterliegt ausschließlich den Bedingungen des mit einem |

| | | |
|---|---|---|
| | Fehler oder Unterlassungen von Dritten, die die T2S-Geldkontoinhaber ausgewählt haben, um Zugang zum Netz des T2S-Netzwerkdienstleisters zu erhalten. | Netzwerkdienstleister gemäß Absatz 1 lit a abgeschlossenen separaten Vertrags.<br><br>3. Die vom Netzwerkdienstleister erbrachten Dienste sind nicht Bestandteil der Dienstleistungen, die die OeNB im Rahmen von TARGET2 erbringt.<br><br>4. Die OeNB 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. |
| Art. 34a<br><br>Eingefügt | | Artikel 34a – Übergangsbestimmungen<br><br>Sobald das TARGET-System den Betrieb aufnimmt und der Betrieb von TARGET2 eingestellt wurde, werden T2S-Geldkontoinhaber zu T2S-Geldkontoinhabern im TARGET-System. |
| Verweise/Referenzen auf „T2S-Netzwerkdienstleister“ | | Die Bezugnahmen auf „T2S-Netzwerkdienstleister“ (Singular oder Plural) in 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 bis 3, Artikel 27 Absatz 5, Artikel 28 Absatz 1, Artikel 29 Absatz 1 und Anlage I Nummer 1 werden durch Bezugnahmen auf „Netzwerkdienstleister“ ersetzt. |
| Anlage I Nummer 7 Abs 1 lit b) | b) User-to-Application-Modus (U2A)<br><br>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 und JavaScript unterstützen. Weitere Einzelheiten sind im T2S-Benutzerhandbuch aufgeführt. | b) User-to-Application-Modus (U2A)<br><br>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. |
| Geschäftsbestimmungen der OeNB für die Teilnahme an TIPS-OeNB (GB TIPS-OeNB) | | **Annex III (amendments to Annex IIb to the Guideline ECB/2012/27):** |
| Verweise/Referenzen auf „TIPS-Netzwerkdienstleister“ | | 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. |
| Art 1<br>Definition „erreichbare Partei” | — „erreichbare Partei“ („reachable party“): eine Stelle, die a) Inhaberin eines Business Identifier Codes (BIC), b) von einem TIPS-Geldkontoinhaber als solche bestimmt wird, c) Korrespondent, Kunde oder Zweigstelle eines TIPS-Geldkontoinhabers ist und d) die entweder über den TIPS-Geldkontoinhaber Zahlungsaufträge oder, falls eine entsprechende Genehmigung des TIPS-Geldkontoinhabers erteilt wurde, direkt Zahlungsaufträge bei der TIPS-Plattform einreichen und über diese Zahlungen empfangen kann; | - erreichbare Partei“ („reachable party“): eine Stelle, die a) Inhaberin eines Business Identifier Codes (BIC), 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; |
| Art 1<br>Definition „Zahlungsauftrag” | — „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 PMKonto auf ein TIPS-Geldkonto oder von einem TIPS-Geldkonto auf ein PM-Konto; | – „Zahlungsauftrag“ („payment order“): mit Ausnahme der Verwendung in Artikel 16 bis 18 dieser Geschäftsbestimmungen 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; |
| Art 1<br>Definition „Instant Payment-Auftrag” | — „Instant-Payment-Auftrag („instant payment order“): entsprechend dem SEPA Instant Credit Transfer Scheme (SCT Inst) des European Payments Council (EPC) eine Zahlungsanweisung, die an jedem Kalendertag des Jahres rund um die Uhr am Tag ausgeführt werden kann – mit sofortiger oder nahezu sofortiger Verarbeitung und Mitteilung an den Zahler; | – „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; |
| Art 1<br>Eingefügte Definitionen | | – „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 Payment-Aufträgen in seinen eigenen Büchern unterhalten wird;<br><br>– „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;<br><br>– „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;<br><br>– „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“ oder „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;<br><br>– „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;<br><br>– „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;<br><br>– „IBAN“: die internationale Kontonummer (International Bank Account Number), die ein Einzelkonto bei einem bestimmten Finanzinstitut in einem bestimmten Land eindeutig identifiziert. |
| Art 1<br>Definition „TIPS-Netzwerkdienstleister” entfernt | — „TIPS-Netzwerkdienstleister“ („TIPS network service provider“): ein Unternehmen, das: a) im Einklang mit den in Anlage V beschriebenen und genannten Regeln und Verfahren alle für die technische Anbindung an die TIPS-Plattform erforderlichen Voraussetzungen erfüllt und eine technische Verbindung hergestellt hat und b) die TIPS connectivity hosting terms and conditions unterzeichnet hat, die auf der Website der EZB abgerufen werden können; | --- |
| Art 3 Verweis auf Anlage V entfernt | Anlage V: Technische Voraussetzungen für die TIPS-Anbindung | --- |
| Art 4 Abs 2 lit ia)<br><br>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; |
| Art 4 Abs 3 | (3) TARGET2 ist ein Echtzeit-Brutto-Zahlungsverkehrssystem in Euro, über das Zahlungen von und auf PM-Konten, T2S-Geldkonten und TIPS-Geldkonten in Zentralbankgeld abgewickelt werden. TARGET2 wird auf der Grundlage der SSP betrieben, über | (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 – |

| | | |
|---|---|---|
| | die – technisch in gleicher Weise – Zahlungsaufträge eingereicht und verarbeitet sowie schließlich Zahlungen empfangen werden. Was die technische Führung von TIPS-Geldkonten 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. | 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. |
| Art 6 Abs 1 lit a Punkt i) | i) Installation, Verwaltung, Betrieb, Überwachung und Gewährleistung der Sicherheit der für den Anschluss 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 der beantragende TIPS-Geldkontoinhaber verpflichtet, mit einem oder mehreren TIPS-Netzwerkdienstleistern eine Vereinbarung zu treffen, um die erforderliche Anbindung gemäß den technischen Spezifikationen in Anlagen I und V zu erhalten, und | 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 |
| Art 9 | Artikel 9 – TIPS-Netzwerkdienstleister<br><br>(1) Teilnehmer benutzen für den Austausch von Nachrichten mit der TIPS-Plattform einen oder mehrere TIPS-Netzwerkdienstleister und schließen hierfür mit diesen Anbietern einen separaten Vertrag ab.<br><br>(2) Eine aktuelle Fassung der Liste der TIPS-Netzwerkdienstleister kann auf der Website der EZB abgerufen werden. Die Liste dient ausschließlich Informationszwecken. Wird ein TIPS-Netzwerkdienstleister von der Liste der TIPS-Netzwerkdienstleister entfernt, benachrichtigt die OeNB die TIPS-Geldkontoinhaber, die diesen TIPS-Netzwerkdienstleister nutzen, entsprechend.<br><br>(3) Die OeNB haftet daher weder für Handlungen, Fehler oder Unterlassungen eines TIPS-Netzwerkdienstleisters (einschließlich seiner Direktoren, Mitarbeiter und Zulieferer) als Anbieter der TIPS-Netzwerkdienste noch für Handlungen, Fehler oder Unterlassungen von TIPS-Netzwerkdienstleistern, die die Teilnehmer ausgewählt haben, um Zugang zur TIPS-Plattform zu erhalten. Die OeNB haftet darüber hinaus nicht für Verluste oder Schäden, die daraus resultieren, dass der TIPS-Netzwerkdienstleister eine Anbindung | Artikel 9 – Vertragsverhältnis mit einem Netzwerkdienstleister<br><br>(1) Die Teilnehmer müssen entweder:<br><br>a) einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abschließen, um eine technische Verbindung zu TARGET2-OeNB herzustellen, oder<br><br>b) die technische Verbindung über eine andere Stelle herstellen, die einen Vertrag mit einem Netzwerkdienstleister im Rahmen des Konzessionsvertrags mit diesem Netzwerkdienstleister abgeschlossen hat.<br><br>(2) Das Rechtsverhältnis zwischen einem Teilnehmer und dem Netzwerkdienstleister unterliegt ausschließlich den Bedingungen ihres separaten Vertrags gemäß Absatz 1 Buchstabe a.<br><br>(3) Die vom Netzwerkdienstleister erbrachten Dienste sind nicht Bestandteil der Dienstleistungen, die die OeNB im Rahmen |

| | | |
|---|---|---|
| | an die TIPS-Plattform nicht mehr zur Verfügung stellt, unabhängig davon, ob der TIPS-Netzwerkdienstleister die in Anlage V beschriebenen und genannten Anschlussvoraussetzungen nicht mehr erfüllt oder die TIPS connectivity hosting terms and conditions nicht mehr gelten oder andere Gründe vorliegen. | von TARGET2 erbringt.<br>(4) Die OeNB 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. |
| Art 10<br>Entfernt | Artikel 10 – Unterstützung eines Netzwerkdienstleisters<br>(1) Möchte eine TIPS-Geldkontoinhaber die Dienste eines Netzwerkdienstleisters in Anspruch nehmen, der nicht auf der in Artikel 9 Absatz 2 genannten Liste aufgeführt ist, so kann der TIPS-Geldkontoinhaber bei der OeNB die Überprüfung, ob ein Netzwerkdienstleister als TIPS-Netzwerkdienstleister tätig sein kann, beantragen.<br>(2) Ein Netzwerkdienstleister kann als TIPS-Netzwerkdienstleister tätig werden, sofern er die Überprüfung, die gemäß den in Anlage V beschriebenen Vorschriften und Verfahren vorgenommen wird, bestanden hat und nachdem er die auf der EZB-Website veröffentlichten TIPS connectivity hosting terms and conditions in jeweils aktueller Fassung unterzeichnet hat.<br>(3) Die OeNB informiert den TIPS-Geldkontoinhaber innerhalb von 120 Kalendertagen ab dem Tag des Eingangs des Antrags über das Ergebnis der in Absätzen 1 und 2 genannten Überprüfung. Wird der Netzwerkdienstleister abgelehnt, informiert die OeNB den TIPS-Geldkontoinhaber über die Gründe für die Ablehnung.<br>(4) Die in Absatz 1 genannten Anträge können ab 1. Juni 2019 bei der OeNB eingereicht werden. | --- |
| Art 11a<br>Eingefügt | --- | Artikel 11a - MPL-Verzeichnis<br>(1) Das zentrale MPL-Verzeichnis enthält die Proxy-IBAN-Entsprechungstabelle für die Zwecke des MPL-Dienstes.<br>(2) Jeder Proxy darf nur mit einer IBAN verknüpft werden. Eine IBAN kann mit einem oder mehreren Proxys verknüpft werden.<br>(3) Artikel 29 findet Anwendung auf die im MPL-Verzeichnis |

| | | |
|---|---|---|
| | | enthaltenen Daten. |
| Art 12 point 9<br>Entfernt | (9) Es obliegt den TIPS-Geldkontoinhabern, in ihrem eigenen Interesse und gemäß ihrem separaten Vertrag mit ihrem TIPS-Netzwerkdienstleister zu überwachen, dass ihr gewählter TIPS-Netzwerkdienstleister ständig eine aktive Verbindung zur TIPS-Plattform zur Verfügung stellt und seinen Status als TIPS-Netzwerkdienstleister aufrechterhält. Diese Verbindung muss die in Anlage V beschriebenen und genannten Verbindungsvoraussetzungen erfüllen. | --- |
| Art 15 Abs 5 | (5) TIPS-Geldkonten werden entweder mit 0 % oder zum Einlagesatz, je nachdem, welcher dieser Zinssätze niedriger ist, verzinst, sofern diese Konten nicht zur Haltung einer Mindestreserve genutzt werden. Im letztgenannten Fall werden die Berechnung und Zahlung der für die Mindestreserven anfallenden Zinsen durch die Verordnung (EG) Nr. 2531/98 und die Verordnung (EG) Nr. 1745/2003 (EZB/2009/3) geregelt. | (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.<br><br>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.<br><br>Footnotes have been added accordingly. |
| Art 16 | Artikel 16 – Arten von Zahlungsaufträgen auf TIPS-Geldkonten<br><br>Im Rahmen des TIPS-Dienstes gelten als Zahlungsaufträge:<br><br>a) Instant-Payment-Aufträge;<br><br>b) Positive Rückruf-Antworten;<br><br>c) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto. | Artikel 16 – Arten von Zahlungsaufträgen auf TIPS-Geldkonten<br><br>Im Rahmen des TIPS-Dienstes gelten als Zahlungsaufträge:<br><br>a) Instant-Payment-Aufträge;<br><br>b) Positive Rückruf-Antworten;<br><br>c) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto;<br><br>d) Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein technisches TIPS-Nebensystemkonto;<br><br>e) Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto. |

| | | |
|---|---|---|
| Art 18 Abs 6 | (6) Wurde ein Auftrag zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto, wie in Artikel 17 beschrieben, angenommen, prüft TARGET2-OeNB, ob auf dem TIPS-Geldkonto des Zahlers ausreichend Mittel verfügbar sind. Sind keine ausreichenden Mittel verfügbar, wird Auftrag zur Liquiditätsübertragung zurückgewiesen. Sind ausreichenden Mittel verfügbar, wird Auftrag zur Liquiditätsübertragung sofort abgewickelt. | (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-OeNB, ob auf dem Konto des Zahlers ausreichend Mittel verfügbar sind. Sind keine ausreichenden Mittel verfügbar, wird Auftrag zur Liquiditätsübertragung zurückgewiesen. Sind ausreichende Mittel verfügbar, wird Auftrag zur Liquiditätsübertragung sofort abgewickelt. |
| Art 20 Abs 1 lit b) | b) Aufträge zur Liquiditätsübertragung vom TIPS-Geldkonto auf das PM-Konto und positive Rückruf-Antworten in TARGET2-OeNB gelten zu dem Zeitpunkt als eingebracht und sind zu dem Zeitpunkt unwiderruflich, zu dem das maßgebliche TIPS-Geldkonto belastet wird. | 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-OeNB 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-OeNB gelten zu dem Zeitpunkt als eingebracht und sind zu dem Zeitpunkt unwiderruflich, zu dem das maßgebliche technische TIPS-Nebensystemkonto belastet wird. |
| Art 30 Abs 1 | (1) Die TIPS-Geldkontoinhaber sind sich ihrer gesetzlichen Pflichten zum Datenschutz sowie zur Bekämpfung der Geldwäsche, der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst und treffen insbesondere angemessene Vorkehrungen bei den Zahlungen, die auf ihren TIPS-Geldkonten verbucht werden. Ferner machen sich die TIPS-Geldkontoinhaber vor Aufnahme vertraglicher Beziehungen mit ihrem gewählten TIPS-Netzwerkdienstleister mit den Regelungen des TIPS-Netzwerkdienstleisters zur Wiederherstellung verloren gegangener Daten vertraut. | (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. |
| Art 35a<br>Eingefügt | --- | Artikel 35a - Übergangsbestimmung<br>Sobald das TARGET-System den Betrieb aufnimmt und der Betrieb von TARGET2 eingestellt wurde, werden TIPS-Geldkontoinhaber zu TIPS-Geldkontoinhabern im TARGET-System. |
| Anlage I Number 2 | Nachrichtentyp Nachrichtenname<br>Pacs.002 FIToFIPayment Status Report<br>Pacs.004 PaymentReturn<br>Pacs.008 FIToFICustomerCreditTransfer<br>GB TIPS-OeNB 57<br>Pacs.028 FIToFIPaymentStatusRequest<br>camt.003 GetAccount<br>camt.004 ReturnAccount<br>camt.011 ModifyLimit<br>camt.019 ReturnBusinessDayInformation<br>camt.025 Receipt<br>camt.029 ResolutionOfInvestigation<br>camt.050 LiquidityCreditTransfer<br>camt.052 BankToCustomerAccountReport<br>camt.053 BankToCustomerStatement<br>camt.054 BankToCustomerDebitCreditNotification<br>camt.056 FIToFIPaymentCancellationRequest<br>acmt.010 AccountRequestAcknowledgement<br>acmt.011 AccountRequestRejection<br>acmt.015 AccountExcludedMandateMaintenanceRequest<br>reda.016 PartyStatusAdviceV01 | Nachrichtentyp Nachrichtenname<br>Pacs.002 FIToFIPayment Status Report<br>Pacs.004 PaymentReturn<br>Pacs.008 FIToFICustomerCreditTransfer<br>Pacs.028 FIToFIPaymentStatusRequest<br>camt.003 GetAccount<br>camt.004 ReturnAccount<br>camt.005 GetTransaction<br>camt.006 ReturnTransaction<br>camt.011 ModifyLimit<br>camt.019 ReturnBusinessDayInformation<br>camt.025 Receipt<br>camt.029 ResolutionOfInvestigation<br>camt.050 LiquidityCreditTransfer<br>camt.052 BankToCustomerAccountReport<br>camt.053 BankToCustomerStatement<br>camt.054 BankToCustomerDebitCreditNotification<br>camt.056 FIToFIPaymentCancellationRequest<br>acmt.010 AccountRequestAcknowledgement<br>acmt.011 AccountRequestRejection<br>acmt.015 AccountExcludedMandateMaintenanceRequest |

| | | |
|---|---|---|
| | reda.022 PartyModificationRequestV01 | reda.016 PartyStatusAdviceV01<br>reda.022 PartyModificationRequestV01 |
| Anlage I Nummer 6 Abs 1 b) | b) User-to-Application-Modus (U2A)<br>Der U2A-Modus ermöglicht die direkte Kommunikation zwischen dem TIPS-Geldkontoinhaber und der TIPSGUI. Die Informationen werden in einem Browser angezeigt, der auf einem PC-System läuft. Für den U2A-GB Zugriff muss die IT-Infrastruktur Cookies und JavaScript unterstützen. Weitere Einzelheiten sind im TIPS-Benutzerhandbuch aufgeführt. | b) User-to-Application-Modus (U2A)<br>Der U2A-Modus ermöglicht die direkte Kommunikation zwischen dem TIPS-Geldkontoinhaber und der TIPSGUI. 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. |
| Anlage IV Nummer 2 und 3 | 2. Die ersten zehn Millionen Instant Payment-Aufträge und positiven Rückruf-Antworten, die insgesamt bis Ende 2019 bei der TIPS-Plattform eingehen, sind gebührenfrei. Im darauffolgenden Jahr berechnet die OeNB den Inhabern der verknüpften PM-Konten Gebühren für sämtliche weiteren Instant Payment-Aufträge und positiven Rückruf-Antworten, die bis Ende 2019 bei der TIPS-Plattform eingehen.<br>3. Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto und Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto werden dem Inhaber des verknüpften PM-Kontos nach Anhang II Anlage IV in Rechnung gestellt. | 2. Aufträge zur Liquiditätsübertragung von einem PM-Konto auf ein TIPS-Geldkonto und Aufträge zur Liquiditätsübertragung von einem TIPS-Geldkonto auf ein PM-Konto werden dem Inhaber des verknüpften PM-Kontos nach Anhang II Anlage IV in Rechnung gestellt. |
| Anlage V<br>entfernt | Anlage V<br>TECHNISCHE VORAUSSETZUNGEN FÜR die TIPS-Anbindung<br>Dienstleistungen des TIPS-Netzwerkdienstleisters<br>Allgemeine Beschreibung der Dienstleistungen<br>1. Der TIPS-Netzwerkdienstleister verbindet den TIPS-Geldkontoinhaber und/oder seine erreichbare Partei mit der TIPS-Plattform und stellt einen sicheren Nachrichtendienst auf Basis einer geschlossenen Benutzergruppe (Closed Group of Users – CGU) und PKI sowie Unterstützung und Leistungen des Vorfallmanagements zur Verfügung. | --- |

| | | |
|---|---|---|
| | 2. Alle vom TIPS-Netzwerkdienstleister gegenüber den TIPS-Geldkontoinhabern zur Verfügung gestellten Dienstleistungen werden im Rahmen eines separaten Vertrags angeboten, den die beiden Parteien abgeschlossen haben, und stehen im Einklang mit den detaillierten Anforderungen an Netzwerkdienstleister, die in der jeweils aktuellen Fassung der Anbindungsdokumentation (nachfolgend die „Anbindungsdokumentation“) beschrieben sind. Die Anbindungsdokumentation ist auf der Website der EZB verfügbar und besteht aus: a) dem Dokument mit der Überschrift „Connectivity – technical requirements“ und den folgenden Anlagen dazu: „MEPT – Message Exchange Processing for TIPS“ und „NSP Compliance Check Procedure“, und b) den TIPS connectivity hosting terms and conditions. Die TIPS-Geldkontoinhaber werden aufgefordert, die Anbindungsdokumentation in ihren Vertrag mit dem TIPS-Netzwerkdienstleister aufzunehmen.<br><br>3. Damit ein Netzwerkdienstleister einen Vertrag mit einem TIPS-Geldkontoinhaber als TIPS-Netzwerkdienstleister abschließen kann, wird die Erfüllung der Anforderungen seitens des Netzwerkdienstleisters überprüft, um sicherzustellen, dass der Dienstleister die technischen Anforderungen erfüllt, die im Dokument „Connectivity – technical requirements“ aufgeführt sind. Hierzu gehört erstens eine Bewertung des technischen Angebots des Netzwerkdienstleisters. Fällt diese Bewertung positiv aus, erfolgt ein zweiter Schritt der Überprüfung auf Erfüllung der Anforderungen, der auch eine Reihe von Tests der technischen Lösung des Netzwerkdienstleisters umfasst. Die Überprüfung auf Erfüllung der Anforderungen wird näher beschrieben in der in Nummer 2 genannten Anlage „NSP Compliance Check Procedure“.<br><br>4. Hat der Netzwerkdienstleister die Überprüfung auf Erfüllung der Anforderungen bestanden, unterzeichnet er die TIPS connectivity hosting terms and conditions der Banca d’Italia. Danach kann dieser TIPS-Netzwerkdienstleister im Rahmen eines zwischen ihm und einem TIPS-Geldkontoinhaber geschlossenen Vertrags von jedem TIPS-Geldkontoinhaber in Anspruch genommen werden und die Namen der beiden werden rein informationshalber auf der Website der EZB veröffentlicht. Die in Nummer 3 erwähnte Überprüfung auf Erfüllung der Anforderungen ist innerhalb von 120 Kalendertagen ab dem Tag der amtlichen Bekanntgabe des | |

| | | |
|---|---|---|
| | Beginns dieses Verfahrens gegenüber dem TIPS-Geldkontoinhaber durchzuführen.<br><br>5. Besteht ein Netzwerkdienstleister einen Teil der in Nummer 3 erwähnten Überprüfung auf Erfüllung der Anforderungen nicht, so informiert die OeNB den TIPS-Geldkontoinhaber, auf dessen Verlangen die in Nummer 3 erwähnte Beurteilung vorgenommen wurde, über die Ablehnung und die Gründe dafür.<br><br>6. Es obliegt den TIPS-Geldkontoinhabern, in ihrem eigenen Interesse und gemäß ihrem separaten Vertrag mit ihrem TIPS-Netzwerkdienstleister zu überwachen, ob die von ihrem TIPS-Netzwerkanbieter bereitzustellenden Anbindungsleistungen zum Zeitpunkt des Verfahrens zur Überprüfung auf Erfüllung der Anforderungen und während des gesamten Zeitraums, während dessen die TIPS-Geldkontoinhaber mit der TIPS-Plattform verbunden sind, alle in Nummer 2 genannten technischen und operativen Anforderungen erfüllen.<br><br>7. Überwacht eine Anbieter-NZB der TIPS-Plattform die Erfüllung der technischen und operativen Anforderungen durch einen TIPS-Netzwerkdienstleister, so erfolgt dies ausschließlich zum Schutz der Integrität der TIPS-Plattform und daher unbeschadet der Überwachung durch den TIPS-Geldkontoinhaber gemäß Nummer 6.<br><br>8. Die Verbindung eines TIPS-Netzwerkdienstleisters zur TIPS-Plattform kann getrennt werden, wenn er die Bedingungen der in Nummer 2 beschriebenen Anbindungsdokumentation nicht länger erfüllt oder wenn die TIPS connectivity hosting terms and conditions aus anderen Gründen gemäß den entsprechenden Bedingungen nicht länger gelten oder gekündigt werden. Wird ein Anschluss an die TIPS-Plattform durch einen TIPS-Netzwerkdienstleister eingestellt, so wird dieser von der Liste der TIPS-Netzwerkdienstleister gestrichen. | |

| | | |
|---|---|---|
| Abschnitt B<br>Eingefügt | --- | **Abschnitt B**<br><br>**TIPS-DIENST FÜR NEBENSYSTEME, DIE INSTANT PAYMENTS ABWICKELN**<br><br>1. Begriffsbestimmungen<br><br>In diesem Abschnitt gelten folgende Begriffsbestimmungen zusätzlich zu den in Abschnitt A Artikel 1 festgelegten:<br><br>- ‚Nebensystem-Zentralbank' (‚ancillary system central bank (ASCB)'): die Zentralbank des Eurosystems, mit der das betreffende Nebensystem, das Instant Payment-Aufträge in seinen eigenen Büchern abwickelt, eine bilaterale Vereinbarung über die Abwicklung von Instant Payment-Aufträgen des Nebensystems abgeschlossen hat.<br><br>- ‚zugrunde liegendes Bruttovolumen' (‚underlying gross volume'): die Anzahl der in den eigenen Büchern des Nebensystems abgewickelten Instant Payment-Aufträge, die durch auf dem technischen TIPS-Nebensystemkonto gehaltene Mittel ermöglicht werden. Nicht inbegriffen sind Instant Payment-Aufträge an oder von TIPS-Geldkonten oder anderen technischen TIPS-Nebensystemkonten.<br><br>- ‚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.<br><br>2. Einbringung von Zahlungsaufträgen in das System und deren Unwiderruflichkeit<br><br>Die Anwendung von Abschnitt A 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 Payment-Aufträgen in den eigenen Büchern von Nebensystemen

1. Zur Unterstützung der Abwicklung von Instant Payment-Aufträgen 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<br><br>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 der Leitlinie der Europäischen Zentralbank EZB/2021/27 idgF[4] für Sicherungsguthaben gelten.<br><br>4. Abwicklungsverfahren<br><br>1. Das betreffende Nebensystem verwendet ein technisches TIPS-Nebensystemkonto, um die erforderliche, von seinen Verrechnungsmitgliedern bereitgestellte Liquidität zur Deckung ihrer Positionen zu sammeln.<br><br>2. Auf Wunsch wird das Nebensystem über Gutschriften und Belastungen auf seinem technischen TIPS-Nebensystemkonto informiert.<br><br>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.<br><br>5. Benutzerschnittstelle<br><br>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. |

[4] Leitlinie der Europäischen Zentralbank vom vom 5. Dezember 2012 über ein transeuropäisches automatisiertes Echtzeit-Brutto-Express- Zahlungsverkehrssystem (EZB/2012/27) in der Fassung Leitlinie (EU) 2019/1849 der Europäischen Zentralbank vom 4. Oktober 2019

| | | |
|---|---|---|
| | | 2. Der Zugang zur TIPS-Plattform ermöglicht den Inhabern technischer TIPS-Nebensystemkonten,<br><br>a) Informationen über ihre Konten abzurufen und CMBs zu steuern,<br><br>b) Aufträge zur Liquiditätsübertragung von einem technischen TIPS-Nebensystemkonto auf ein TIPS-Geldkonto zu erteilen und<br><br>c) bestimmte Stammdaten zu verwalten.<br><br>6. Gebührenverzeichnis und Rechnungsstellung<br><br>1. Ein Nebensystem in TIPS hat Gebühren gemäß den beiden folgenden Posten zu entrichten:<br><br>a) eine Transaktionsgebühr, die auf der Basis des für die TIPS-Geldkontoinhaber in Abschnitt A Anlage IV erstellten Gebührenverzeichnisses berechnet wird;<br><br>b) eine Gebühr auf der Basis des zugrunde liegenden Bruttovolumens der auf der eigenen Plattform des Nebensystems abgewickelten Instant Payment-Aufträgen, die durch die vorfinanzierten Positionen auf dem technischen TIPS-Nebensystemkonto ermöglicht werden. Die Gebühr beträgt 0,0005 EUR je Instant Payment-Auftrag.<br><br>2. Das zugrunde liegende Bruttovolumen der Instant Payment-Aufträge 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.<br><br>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.<br><br>4. Für die Zwecke der Gebührenverzeichnisse und der Rechnungsstellung gemäß diesem Abschnitt gilt Folgendes:<br><br>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.<br><br>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:<br><br>i) es handelt sich um eine formelle Regelung auf vertraglicher oder regulatorischer Basis;<br><br>ii) es hat mehr als einen Teilnehmer, ausgenommen den Systembetreiber dieses Systems;<br><br>iii) es wurde für die Zwecke des Clearing, der Verrechnung und/oder der Abwicklung von Zahlungen und/oder Wertpapieren zwischen den Teilnehmern eingerichtet;<br><br>iv) es wendet gemeinsame Bedingungen und standardisierte Regelungen auf das Clearing, die Verrechnung und die Abwicklung von Zahlungen und Wertpapieren zwischen den Teilnehmern an.<br><br>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.“ |
| **Gebühren und Konditionen der OeNB für den Zahlungsverkehr mit der OeNB** | | |
| Nummer 2.3. Listenüberschrift | Mio. EUR/Tag | Mio. EUR/Geschäftstag |
| Nummer 2.4. Punkt iv) Letzter Absatz gestrichen | Die ersten zehn Millionen InstantPayment-Aufträge und positiven Rückruf-Antworten, die insgesamt bis Ende 2019 bei der TIPS- | --- |

| | | |
|---|---|---|
| | Plattform eingehen, sind gebührenfrei. Im darauffolgenden Jahr berechnet die OeNB dem Nebensystem als Inhaber des verknüpften PM-Kontos Gebühren für sämtliche weiteren InstantPayment-Aufträge und positiven Rückruf-Antworten, die bis Ende 2019 bei der TIPS-Plattform eingehen. | |