

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Lisa Schubert, Luke Hoß, Janine Wissler, weiterer Abgeordneter und der Fraktion Die Linke
– Drucksache 21/4184 –**

Kündigung von Konten politischer Organisationen („Debanking“) sowie Zahlungssouveränität in der Europäischen Union

Vorbemerkung der Fragesteller

In den letzten Wochen kam es zu mehreren Fällen von mutmaßlich politisch motivierten Kontokündigungen in Deutschland, die nach Ansicht der Fragestellenden zeigen, wie stark private und öffentliche Banken heute faktisch US-Sanktions- und Terrorlisten folgen: So haben die Sparkasse Göttingen und die GLS Bank den Kontovertrag mit dem linken Solidaritätsverein Rote Hilfe e. V., der eine über 100 Jahre alte Geschichte aufweist und rund 19 000 Mitglieder organisiert, ohne nachvollziehbare rechtliche Begründung gekündigt; zeitlich eng verknüpft mit der Eintragung der sogenannten Antifa Ost auf einer US-Terrorliste (<https://taz.de/Etappensieg-vor-Gericht/!6146219/>). Die Rote Hilfe hat daraufhin rechtliche Schritte eingeleitet, und das Landgericht Göttingen hat die Sparkasse kurzfristig verpflichtet, das Konto zumindest fortzuführen (www.ndr.de/nachrichten/niedersachsen/braunschweig_harz_goettingen/goettingen-konto-der-roten-hilfe-gekuendigt-sparkasse-scheitert-vor-gericht,rotehilfe-114.html) – ein Fall, der auch in großen Medien aufgegriffen wurde. Zudem hat die US-Regierung unter Donald Trump Teile der Führung des Internationalen Strafgerichtshofs (ICC) mit Sanktionsmaßnahmen belegt, inklusive Einfrierung von Konten und Zahlungsverboten, was dazu führte, dass betroffene Richter und Mitarbeitende selbst von Zahlungsdiensten abgeschnitten wurden und öffentliche Debatten über die Rechtsstaatlichkeit solcher extraterritorialen Maßnahmen ausgelöst hat (<https://verfassungsblog.de/u-s-sanctions-on-the-international-criminal-court>).

Diese Entwicklungen verweisen auch auf den Umstand, dass die EU-Zahlungsinfrastruktur maßgeblich von US-basierten Zahlungsdienstleistern wie Visa, Mastercard, Google Pay, Apple Pay und PayPal abhängt. So haben etwa die beiden erstgenannten einen Anteil von 90 Prozent an den innereuropäischen Kartenzahlungen (www.europarl.europa.eu/RegData/etudes/IDAN/2025/779852/ECTI_IDA%282025_Prozent29779852_EN.pdf). Aus Sicht der Fragestellenden ist dies Ausweis für eine zunehmend gefährliche Abhängigkeit und strukturelle Schwäche der europäischen Finanz- und Zahlungssouveränität. Institutionelle Studien zeigen, dass dieses Abhängigkeitsverhältnis eine geopolitische Anfälligkeit darstellt und die Notwendigkeit eigener Zahlungsverfahren, etwa durch einen sicheren, souveränen und öffentlich bereit-

gestellten Digitalen Euro, unterstreicht. Vor diesem Hintergrund wird in politischen und zivilgesellschaftlichen Kreisen die Frage diskutiert, wie die EU-Blocking-Verordnung (Verordnung (EU) Nummer 2271/96) und andere Mechanismen so umgesetzt werden können (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01996R2271-20180807>), dass private Banken zur Priorisierung von EU-Recht gegenüber ausländischen Sanktionen verpflichtet werden bzw. dass eine sanktionssichere, öffentliche Zahlungsinfrastruktur geschaffen wird, die EU-Bürgerinnen und EU-Bürger sowie Organisationen wirklich vor extraterritorialen Drittstaatseingriffen schützt.

1. Welche Kenntnisse hat die Bundesregierung von den in der Vorbemerkung der Fragesteller dargestellten Vorgängen?

Die Bundesregierung hat die Medienberichterstattung zu Kündigungen von Konten bei den beiden in der Vorbemerkung der Fragestellerinnen und Fragesteller genannten Kreditinstituten zur Kenntnis genommen.

Soweit sich die Frage auf die Aufsicht der beiden Kreditinstitute durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bezieht, ist diese als „VS-VERTRAULICH“ eingestuft. Eine eingestufte Beantwortung ist im Rahmen einer Güterabwägung geboten, sofern gleich- oder höherwertige Güter von Verfassungsrang betroffen sind, die mit dem parlamentarischen Informationsanspruch kollidieren. Einer offenen Beantwortung parlamentarischer Fragen kann das Wohl des Bundes oder eines Landes (Staatswohl) entgegenstehen, das durch das Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden kann (vgl. BVerfGE 124, 78 [123]).

Die Funktionsfähigkeit staatlicher Aufsicht über Banken und andere Finanzinstitute und die Stabilität des Finanzmarktes sind Belange des Staatswohls, die die Antwortpflicht der Bundesregierung auf parlamentarische Fragen beschränken können (vgl. BVerfGE 147, 50, LS 6b). Die Kontroll- und Aufsichtstätigkeit der BaFin dient der Stabilität des Finanzmarkts und der Prävention von Geldwäsche und Terrorismusfinanzierung. Sie unterliegt strengen Sicherheits- und Datenschutzstandards, sodass diese Informationen grundsätzlich bereits geheimhaltungsbedürftig sind. Ein Bekanntwerden der Kenntnisse und konkreten Vorgehensweise der BaFin in Einzelfällen im Bereich der Aufsicht von Kreditinstituten sowie der Bekämpfung von Geldwäsche und Terrorismusfinanzierung wäre für die erfolgreiche Durchführung entsprechender Aufsichtsmaßnahmen und somit für die Sicherheit und die Interessen der Bundesrepublik Deutschland mindestens nachteilig. Es könnte dadurch die Effektivität und generell die Ausübung der Kontroll- und Aufsichtsaufgaben der BaFin in anderen Fällen nachteilig beeinflusst werden. Das Staatswohl könnte daher gefährdet werden.

Im Falle von Auskünften, die sich auf die Bewertung der Geschäftstätigkeit von einzelnen Instituten durch die BaFin beziehen, sind zudem regelmäßig Betriebs- und Geschäftsgeheimnisse (Artikel 12 Absatz 1 des Grundgesetzes (GG)) sowie das Grundrecht auf informationelle Selbstbestimmung des jeweiligen Instituts (Artikel 2 Absatz 1 GG i. V. m. Artikel 1 Absatz 1 GG) betroffen.

Die BaFin unterliegt daher gemäß § 9 des Kreditwesengesetzes (KWG) und § 54 des Geldwäschegesetzes (GwG) strengen Verschwiegenheitsregelungen. Einfachgesetzliche Verschwiegenheitsregelungen sind für sich genommen zwar nicht geeignet, den parlamentarischen Informationsanspruch zu beschränken (vgl. BVerfGE 147, 50 [133]). Sie können aber insoweit von Relevanz sein, als sie einen Ausgleich konfligierender (Verfassungs-)Rechte darstellen (vgl. BVerfGE 147, 50).

Es ist deshalb eine sorgfältige Güterabwägung erforderlich, die hier im Ergebnis dazu führt, dass Teile der Antwort auf die Frage 1 nach Abwägung des Informationsinteresses der Fragestellerinnen und Fragesteller mit den oben genannten Interessen, insbesondere mit der Funktionsfähigkeit staatlicher Aufsicht über Kreditinstitute und den Betriebs- und Geschäftsgeheimnissen von Unternehmen nach Artikel 12 Absatz 1 GG, mit dem Grad „VS-VERTRAULICH“ einzustufen und in der Geheimschutzstelle des Deutschen Bundestages zu hinterlegen sind.*

Es wird zudem darauf hingewiesen, dass Kreditinstitute im Rahmen der Vertragsfreiheit grundsätzlich frei entscheiden, mit wem sie Geschäftsbeziehungen unterhalten. Diese grundsätzliche Vertragsfreiheit ist bei Sparkassen im Verhältnis zu natürlichen Personen und gegenüber politischen Parteien eingeschränkt.

Allgemein richten sich die Kündigungsmöglichkeiten eines Kreditinstituts nach den Regelungen des Bürgerlichen Gesetzbuches (§ 675h BGB) sowie ergänzend nach den Vereinbarungen in den Allgemeinen Geschäftsbedingungen des jeweiligen Instituts.

Ein Kreditinstitut ist zur Kündigung einer Kontoverbindung verpflichtet, wenn im Einzelfall eine Beendigungspflicht nach dem Geldwäschegesetz besteht, weil die geldwäscherechtlichen Sorgfaltspflichten in Bezug auf die jeweilige Kundin oder den jeweiligen Kunden nicht erfüllt werden können.

Die Bundesregierung ist mit den in der Vorbemerkung dargestellten Vorgängen hinsichtlich des IStGH vertraut

Zur EU-Zahlungsinfrastruktur ist zu bemerken, dass der digitale Euro ein strategisches Projekt zur Stärkung der europäischen Souveränität und Resilienz im Zahlungsverkehr ist. Die Bundesregierung unterstützt seine Einführung und setzt sich für einen schnellen Abschluss des europäischen Gesetzgebungsverfahrens ein. Deutschland verfügt mit der Girocard über ein wichtiges nationales Kartennetzwerk, das in Deutschland sehr weit verbreitet ist; in 14 Ländern des Euroraums erfolgen Kartentransaktionen jedoch ausschließlich über internationale Kartenzahlverfahren (69 Prozent der Transaktionsmenge im gesamten Euroraum entfallen auf außereuropäische Kartenanbieter und etwa ein Drittel auf nationale Kartenzahlverfahren, vgl. <https://publikationen.bundesbank.de/publikationen-de/berichte-studien/monatsberichte/monatsbericht-dezember-2025-972182?article=zahlungsverkehr-im-wandel-aktuelle-entwicklung-des-kartenmarkts-in-deutschland-972188>). Der digitale Euro hat das Potenzial, Abhängigkeit zu reduzieren und die europäische Zahlungsverkehrslandschaft wettbewerbsfähiger und innovativer zu machen.

2. Hat nach Kenntnis der Bundesregierung die Aufnahme einer dort als „Antifa Ost“ bezeichneten Gruppierung auf eine Liste von Gruppierungen, gegen die die US-Regierung Sanktionen betreffend u. a. den Finanzverkehr verhängt hat, Auswirkungen auf das Führen von Konten durch Organisationen wie die Rote Hilfe e. V. und ggf. weitere, und wenn ja, welche?

Die US-Sanktionsregelungen entfalten Rechtswirkung ausschließlich innerhalb der US-Jurisdiktion. Dies betrifft sowohl Primär- als auch Sekundärsanktionen.

* Das Bundesministerium der Finanzen hat die Antwort als „VS-VERTRAULICH“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

3. Gibt es darüber hinaus nach Kenntnis der Bundesregierung Auswirkungen des Verbots „der Antifa“ in den USA vermittels eines Sanktionsregimes gegen Gruppierungen weltweit und insbesondere in Deutschland, die „der Antifa“ zugerechnet werden?

Am 22. September 2025 hat US-Präsident Donald Trump die „Antifa“ im Wege einer Executive Order in den USA als inländische terroristische Vereinigung eingestuft.

Darüber hinaus wurden die Gruppierung „Antifa-Ost aka Hammerbande“ am 20. November 2025 als „Specially Designated Global Terrorists“ (SDGT) sowie als „Foreign Terrorist Organization“ (FTO) eingestuft.

Aus der medialen Berichterstattung ist der Bundesregierung bekannt, dass Konten der Rote Hilfe e. V. seitens der „Sparkasse Göttingen“ und der „GLS Gemeinschaftsbank eG“ gekündigt wurden. Auswirkungen des US-Sanktionsregimes auf Gruppierungen in Deutschland, die sich selbst dem Aktionsfeld des „Antifaschismus“ zurechnen, sind dem Bundesamt für Verfassungsschutz (BfV) lediglich mittelbar über die o. g. Auswirkungen auf die Rote Hilfe e. V. bekannt.

Eine darüber hinausgehende Auskunft zum Erkenntnisstand des BfV kann aufgrund entgegenstehender überwiegender Belange des Staatswohls nicht erfolgen, auch nicht in eingestufte Form. Eine weitere Ausführung oder Veröffentlichung der in Rede stehenden Informationen würde hier Rückschlüsse auf den Aufklärungsbedarf, den Erkenntnisstand sowie die generelle Arbeitsweise des BfV ermöglichen bzw. zu einer Offenlegung führen. Dies würde die Funktionsfähigkeit des BfV nachhaltig beeinträchtigen und damit einen schweren Nachteil für die Interessen der Bundesrepublik Deutschland bedeuten.

Nach sorgfältiger Abwägung der Informationsrechte des Deutschen Bundestags und seiner Abgeordneten mit den negativen Folgen für die künftige Arbeitsfähigkeit und Aufgabenerfüllung des BfV sowie den daraus resultierenden Beeinträchtigungen der Sicherheit der Bundesrepublik Deutschland folgt, dass auch eine Auskunft nach Maßgabe der Geheimschutzordnung und damit einhergehende Einsichtnahme über die Geheimschutzstelle des Deutschen Bundestages ausscheidet. Eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängerinnen und Empfängern wird dem Schutzbedarf nicht gerecht. Dies gilt umso mehr, als bei einem Bekanntwerden die betroffenen nachrichtendienstlichen Methoden und Werkzeuge nur noch eingeschränkt oder gar nicht mehr eingesetzt werden können. Hieraus ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsinteresse hier überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Bundesregierung zurückstehen.

4. Bestehen Befugnisse des Bundesamtes für Verfassungsschutz im Rahmen seiner Tätigkeit Geldinstituten und anderen privaten Stellen nahezulegen, durch Kündigung privatrechtlicher Verträge einen Beitrag zur Bekämpfung „extremistischer“ oder verfassungsfeindlicher Bestrebungen zu leisten, und wenn ja, welche, und ist ein solches Vorgehen erfolgt (Anwendungsfälle bitte nennen)?

Nein, derartige Befugnisse des BfV bestehen nicht.

5. Gibt es nach Kenntnis der Bundesregierung Verdachtsmeldungen zu Terrorismusfinanzierung bei der Financial Intelligence Unit (FIU), die im Zusammenhang mit Sanktions- und Terrorlisten aus Drittstaaten stehen, und wenn ja, wie viele davon beziehen sich auf Sanktionsmaßnahmen, welche sich weder die EU noch Deutschland zu eigen machen?

Für die Arbeit der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) sind die unmittelbar geltenden Sanktionslisten der Europäischen Union maßgeblich. Daneben sind auch die Sanktionsbeschlüsse des Sicherheitsrats der Vereinten Nationen relevant, die in der Regel über EU-Verordnungen in unmittelbar geltendes Recht umgesetzt werden. Ergänzend können nationale Maßnahmen nach dem Außenwirtschaftsrecht von Bedeutung sein.

Reine Drittstaatenlisten sind für die FIU rechtlich nicht verbindlich, solange sie nicht durch eine EU-Verordnung in das europäische Sanktionsregime überführt werden. Eine systematische Überprüfung solcher Drittstaatenlisten gehört nicht zum gesetzlichen Kernauftrag der FIU; dementsprechend werden hierzu auch keine gesonderten statistischen Erhebungen geführt.

- a) Existieren Empfehlungen, insbesondere Typologien zur Erkennung von Terrorismusfinanzierung seitens der FIU, die Banken nahelegen, es als Anhaltspunkt für erhöhte Aufmerksamkeit zu betrachten, wenn Kundinnen und Kunden „Kritik an der Regierung“ äußern, und wenn ja, welche?
- b) Existieren Empfehlungen, insbesondere Typologien zur Erkennung von Terrorismusfinanzierung seitens der FIU, die „Extremismus“ oder „Radikalismus“ als Anhaltspunkt für erhöhte Aufmerksamkeit nennen, vor dem Hintergrund, dass der Bundesregierung laut BMI (Bundesministerium des Innern)-Bericht im Jahr 2020 (vgl. www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI21003-sektorale-risikoanalyse.pdf?__blob=publicationFile&v=14) keine Erkenntnisse über eine systematische Finanzierung linksextremistisch motivierten Terrors in Deutschland vorlagen, und wenn ja, welche?

Die Fragen 5 a und 5 b werden zusammen beantwortet.

Die FIU stellt derzeit in Bezug auf die konkreten Fragegegenstände keine unmittelbar einschlägigen Empfehlungen bzw. Typologien zur Verfügung.

- c) Werden Verdachtsmeldungen zu Terrorismusfinanzierung zur Erstellung von Typologien zur automatisierten risikobasierten Filterung herangezogen, und wenn ja, welche, und welchen Einfluss nehmen das Bundesamt für Verfassungsschutz und weitere Partnerbehörden der FIU auf die Kriterien der automatisierten Auswertung, die auf Sanktionsmaßnahmen von Drittstaaten zurückgehen?

Sowohl im Bereich der Terrorismusfinanzierung wie ebenso im Geldwäschebereich wird über die von der FIU angewandten Kriterien zur teilautomatisierten Identifizierung entsprechender Verdachtsmeldungen laufend mit den benannten Behörden das erforderliche Benehmen hergestellt und eine fortlaufende Evaluierung vorgenommen; die Auswertung der aus der Analyse von Verdachtsmeldungen gewonnenen Erkenntnissen ist hierbei ein fester Bestandteil. Hierzu besteht mit der Regelung des § 30 Absatz 2 GwG auch eine zugehörige Verpflichtung, der laufend entsprochen wird.

Soweit der Verstoß gegen Sanktionsmaßnahmen betroffen ist, wird dies bei der Bearbeitung von Verdachtsmeldungen ausschließlich nach Maßgabe der jeweils gültigen EU-Verordnungen bewertet. Hierzu ist darauf hinzuweisen, dass die FIU in diesem Bereich keine unmittelbare Zuständigkeit besitzt, sondern sie ‚nur‘ an der Feststellung von Geldern und wirtschaftlichen Ressourcen be-

stimmter Personen oder Personengesellschaften mitwirkt, die aufgrund eines im Amtsblatt der Europäischen Gemeinschaften oder der Europäischen Union veröffentlichten unmittelbar geltenden Rechtsaktes der Europäischen Gemeinschaften oder der Europäischen Union, die der Durchführung einer vom Rat der Europäischen Union im Bereich der Gemeinsamen Außen- und Sicherheitspolitik beschlossenen wirtschaftlichen Sanktionsmaßnahme dient, einer Verfügungsbeschränkung unterliegen, § 28 Absatz 1a GwG. Das BfV nimmt keinen Einfluss auf die Kriterien der automatisierten Auswertung, die auf Sanktionsmaßnahmen von Drittstaaten zurückgehen.

6. Welche Meldegründe für Verdachtsfälle stellt die FIU gemäß § 3 Absatz 1 Satz 1 Nummer 3 GwG (Geldwäschegesetz)-Meldeverordnung zur Auswahl?

Um die Verdachtsmeldung bei Abgabe mit einer ersten inhaltlich zusammenfassenden Angabe zu versehen, steht den Verpflichteten ein umfangreicher sog. Indikatorenkatalog zur Verfügung, aus welchem die einschlägigen Meldegründe aus Sicht des Meldenden individuell ausgewählt werden können. Im Einzelnen handelt es sich um derzeit 124 Auswahlmöglichkeiten.

Indikator	Bezeichnung
A1000	Geldwäsche
A1001	Transaktion i. Z. m. Geldwäsche (FIU-Zustimmung erforderlich, § 46 Absatz 1)
A1002	Transaktion i. Z. m. Geldwäsche (Aufschub nicht möglich, § 46 Absatz 2)
A1003	Transaktion i. Z. m. Geldwäsche (nachträgliche Feststellung)
A1004	Geschäftsbeziehung i. Z. m. Geldwäsche
A1005	Maklergeschäft i. Z. m. Geldwäsche
A2000	Terrorismusfinanzierung
A2001	Transaktion i. Z. m. Terrorismusfinanzierung (FIU-Zustimmung erforderlich, § 46 Absatz 1)
A2002	Transaktion i. Z. m. Terrorismusfinanzierung (Aufschub nicht möglich, § 46 Absatz 2)
A2003	Transaktion i. Z. m. Terrorismusfinanzierung (nachträgliche Feststellung)
A2004	Geschäftsvorfall i. Z. m. Terrorismusfinanzierung
A2005	Vermögensgegenstand i. Z. m. Terrorismusfinanzierung
A3000	Sonstiger Grund
A3001	Verstoß gegen die Offenlegungspflicht
A3002	Nachmeldung
A3003	Anderer Grund
A4000	Eiliger Sachverhalt
B1000	Kundenbezogene Besonderheiten
B1101	Politisch exponierte Person (PEP)
B1102	Listentreffer in Sanktionslisten Terrorismus VO (EG) Nr. 2580/2001 oder Nr. 881/2002
B1103	Listentreffer in sonstigen Sanktionslisten
B1104	Kenntnis von strafrechtlichen Ermittlungen gegen den Kunden
B1105	Kunde oder wirtschaftlich Berechtigter aus Staat, ohne gleichwertige Standards in Bezug auf Geldwäscheprävention
B1201	Vorlage gefälschter/auffälliger Personaldokumente (Verschleierung der Identität)
B1202	Unregelmäßigkeiten im Rahmen des Postident-Verfahrens

Indikator	Bezeichnung
B1203	Verweigerung erforderlicher Angaben zur Identifizierung des Kunden
B1204	Auffälliges Verhalten der Kundin oder des Kunden
B1205	Verwendung falscher oder auffälliger Dokumente/Geschäftsunterlagen
B1206	Nutzung auffälliger Adressen (Postfächer, Briefkastenfirmen, Sammeladressen)
B1207	Verweigerung/Verschleierung der Offenlegung des/der wirtschaftlich Berechtigten
B1208	Verschleierung der Offenlegung des/der wirtschaftlich Berechtigten durch komplexe/internationale Unternehmensstruktur
B1301	Kundenprofil ist unpassend zum Geschäftsgegenstand
B1302	Auffälliger/nicht nachvollziehbarer wirtschaftlicher Hintergrund des Kunden
B1303	Kundin oder Kunde verfügt über keine geschäftsspezifischen Kenntnisse oder eigene gewerbliche Hintergründe, die der Transaktion/Geschäftsbeziehung angemessen sind
B1304	Kundin oder Kunde bindet ohne nachvollziehbaren Grund Vermittler oder Dritte ein
B1305	Kundin oder Kunde handelt offensichtlich für Dritte (Strohmannfunktion)
B1306	Örtlich nicht plausible Geschäftsbeziehung zwischen Kunden und Verpflichteten
B1307	Beteiligung von/an Scheinunternehmen
B1308	Kunde, der oder die sich als nicht anerkannte NGO oder NPO darstellt
B2000	Transaktionen/Geschäftsbeziehungen bezogene Besonderheiten
B2101	Wirtschaftlich nicht plausible Transaktion
B2102	Transaktion widerspricht wirtschaftlichem Hintergrund der Kundin oder des Kunden
B2103	Transaktion widerspricht Geschäftszweck der Kundin oder des Kunden
B2104	Unbekannte Mittelherkunft
B2105	Auffälliger Verwendungszweck
B2106	Nicht plausible Nutzung verschiedener Konten/Durchlaufkonten/Sammelkonten
B2107	Nutzung von anonymen Zahlungsverfahren
B2108	Transaktion soll aus nicht nachvollziehbaren Gründen unter großem Zeitdruck durchgeführt werden
B2109	Kurz vor Abschluss der Transaktion werden neue Beteiligte oder Vereinbarungen eingeführt
B2110	Unerwartete Änderungen hinsichtlich der Finanzierung
B2111	Unerklärlicher Wechsel der Kontoverbindung
B2112	Transaktion liegt über oder unter dem angekündigten Wert
B2113	Abwicklung von Bezahlservices außerhalb des üblichen Bankensektors
B2114	Transaktion dient offensichtlich keinem wirtschaftlich nachvollziehbaren Zweck
B2115	Smurfing (Splitten und Zusammenführen von Geldbeträgen unterhalb von Schwellenwerten)
B2201	Umtausch von Bargeld in/von 500 Euro-Banknoten
B2202	Hoher oder ungewöhnlicher Umtausch von Bargeld in andere Stückelungen der gleichen Währung
B2203	Sonstiger ungewöhnlicher/hoher Bargeldtausch

Indikator	Bezeichnung
B2204	Ungewöhnlich hohe Barzahlungen/Bargeldabhebungen
B2205	Vielzahl von Bargeldein-/Auszahlungen ohne nachvollziehbare Erklärung
B2206	Unübliche Barzahlung im Geschäftsverkehr
B2301	Transaktionen erfolgen aus ungewöhnlichen Quellen oder unsicheren Ländern
B2302	Transaktion in/aus Offshore-Finanzplatz
B2303	Transaktion in/aus Drittstaaten, die nicht über hinreichende Systeme zur Verhinderung, Aufdeckung und Bekämpfung von Geldwäsche und Terrorismusfinanzierung verfügen
B2304	Transaktionen in/aus Drittstaaten, in denen Korruption und andere kriminelle Tätigkeiten signifikant stark ausgeprägt sind
B2305	Transaktion in/aus Staaten, gegen die beispielsweise die EU oder die UN-Sanktionen, Embargos oder ähnliche Maßnahmen verhängt hat/haben
B2306	Transaktionen in/aus Staaten, die terroristische Aktivitäten finanziell oder anderweitig unterstützen oder in denen bekannte terroristische Organisationen aktiv sind
B2401	Sonstige Tatsachen
C1001	Auffälligkeiten i. Z. m. Kreditgeschäften/Treuhandgeschäften
C1002	Auffälligkeiten i. Z. m. Wertpapiergeschäften
C1003	Auffälligkeiten i. Z. m. Akkreditivgeschäften
C1004	Auffälligkeiten i. Z. m. Versicherungsgeschäften
C1005	Auffälligkeiten i. Z. m. Leasinggeschäften
C1006	Auffälligkeiten i. Z. m. dem Außenhandel (internationaler Warenverkehr)
C1007	Auffälligkeiten i. Z. m. Währungsumtausch
C1008	Auffälligkeiten i. Z. m. Prepaidkarten
C1009	Auffälligkeiten i. Z. m. der Nutzung von Kreditkarten
C1010	Auffälligkeiten i. Z. m. E-Geld
C1011	Auffälligkeiten i. Z. m. Kryptowährungen (z. B. Bitcoin)
C1012	Auffälligkeiten i. Z. m. Schecks
C1013	Auffälligkeiten i. Z. m. Schließfächern
C1014	Auffälligkeiten i. Z. m. Glücksspiel/Wetten
C1015	Auffälligkeiten i. Z. m. Kauf/Verkauf von Immobilien
C1016	Auffälligkeiten i. Z. m. Kauf/Verkauf von Kraftfahrzeugen
C1017	Auffälligkeiten i. Z. m. Kauf/Verkauf von Schiffen und Motorbooten
C1018	Auffälligkeiten i. Z. m. Kauf/Verkauf von Luftfahrzeugen
C1019	Auffälligkeiten i. Z. m. Kauf/Verkauf von Edelmetallen
C1020	Auffälligkeiten i. Z. m. Kauf/Verkauf von Edelsteinen
C1021	Auffälligkeiten i. Z. m. Kauf/Verkauf von Schmuck und Uhren
C1022	Auffälligkeiten i. Z. m. Kauf/Verkauf von Kunstgegenständen und Antiquitäten
C1023	Auffälligkeiten i. Z. m. Kauf/Verkauf von sonstigen hochwertigen Gütern
C1024	Auffälligkeiten i. Z. m. sonstigen Geschäftsbereichen
D1001	Korruption, Straftaten im Amt (z. B. Bestechung und Bestechlichkeit)
D1002	Betrug und Untreue
D1003	Rauschgiftdelikte
D1004	Steuerdelikte
D100401	Sozialleistungsbetrug
D1005	Waffendelikte

Indikator	Bezeichnung
D1006	Terrorismusfinanzierung, Staatsschutz, Embargoverstöße
D1007	Straftaten gegen die öffentliche Ordnung (Bildung/Mitgliedschaft in krimineller/terroristischer Vereinigung)
D1008	Geld- und Wertzeichenfälschung
D1009	Straftaten gegen die sexuelle Selbstbestimmung (z. B. Zuhälterei)
D1010	Straftaten gegen die persönliche Freiheit (z. B. Menschenhandel, Zwangsprostitution, Ausbeutung der Arbeitskraft, Menschenraub, Geiselnahme)
D1011	Diebstahl und Unterschlagung
D1012	Raub und Erpressung
D1013	Begünstigung und Hehlerei
D1014	Geldwäsche (§ 261 StGB)
D1015	Strafbarer Eigennutz (Verbotenes Glücksspiel)
D1016	Straftaten gegen den Wettbewerb
D1017	Straftaten gegen die Umwelt
D1018	Nebengesetze
D101801	Verstöße gegen das Außenwirtschaftsgesetz (§§ 17, 18 AWG)
D101802	Verstöße gegen das Aufenthaltsgesetz (Einschleusen von Ausländern)
D101803	Verstöße gegen das Asylgesetz (Verleitung zur missbräuchlichen Asylantragstellung)
D101804	Verstöße i. S. d. § 38 des Wertpapierhandelsgesetzes
D101805	Verstöße gegen das Markengesetz
D101806	Verstöße gegen das Urhebergesetz
D101807	Verstoß gegen § 25 Gebrauchsmustergesetz
D101808	Ungenehmigte Nutzung eines eingetragenen Designs / Gemeinschaftsgeschmacksmusters (§§ 51, 65 Designgesetz)
D101809	Verstöße im Sinne des § 142 des Patentgesetzes
D101810	Verstöße im Sinne des § 10 des Halbleitergesetzes
D101811	Verstöße im Sinne des § 39 des Sortenschutzgesetzes
D1019	Andere Straftat
D1020	Straftat nicht erkennbar

7. Wer ist derzeit Mitglied in der Public Private Partnership – Anti Financial Crime Alliance (AFCA) (bitte nach öffentlichen Institutionen und Unternehmen auflisten)?

Unternehmen/Institutionen Finanzsektor

- Aareal Bank AG
- Barclays Bank Ireland PLC, Frankfurt Branch
- Bayerische Landesbank Anstalt des öffentlichen Rechts
- BBBank eG
- Berliner Volksbank eG
- BMW Bank GmbH
- Coinbase Germany GmbH
- Commerzbank AG
- DekaBank Deutsche Girozentrale
- Deutsche Bank AG

- Deutsche Börse AG für Clearstream
- DZ BANK AG Deutsche Zentral-Genossenschaftsbank
- Finoa GmbH
- flatexDEGIRO Bank AG
- HSBC Deutschland
- ING-DiBa AG
- Joh. Berenberg, Gossler & Co. KG (Berenberg)
- KfW Kreditanstalt für Wiederaufbau
- Kreissparkasse Diepholz
- Landesbank Baden-Württemberg
- Landesbank Hessen-Thüringen Girozentrale Anstalt des öffentlichen Rechts
- ODDO BHF AG
- Rabobank Frankfurt
- S-Kreditpartner GmbH
- Société Générale S.A., Zweigniederlassung Frankfurt
- Sparkasse KölnBonn
- Standard Chartered Bank AG
- Sumitomo Mitsui Banking Corp.
- TARGOBANK AG
- The Bank of New York Mellon – Filiale Frankfurt
- UBS Europe SE
- Unicredit Bank AG
- Western Union Payment Services Ireland Ltd.

Unternehmen/Institutionen Nichtfinanzsektor

- Engel & Völkers AG
- Jones Lang LaSalle SE
- ODDSET Sportwetten GmbH
- Spielbank Berlin GmbH & Co. KG
- Tipico Co. Ltd.
- von Poll Immobilien GmbH
- Merkur Spielbanken NRW GmbH (ehem. Westdeutsche Spielbanken GmbH & Co.KG)

Weitere Unternehmen/Institutionen

- Kerberos Compliance-Managementsysteme GmbH

Behörden

- Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin
- Bundeskriminalamt, BKA
- Bundeszentralamt für Steuern, BZSt
- Freie und Hansestadt Hamburg Behörde für Inneres und Sport

- Gemeinsame Glücksspielbehörde der Länder (Anstalt des öffentlichen Rechts)
- Hessisches Ministerium des Innern und für Sport
- Landgericht Berlin
- Ministerium des Innern des Landes Nordrhein-Westfalen
- Ministerium des Innern und für Sport Rheinland-Pfalz
- Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg
- MWAE Ministerium für Wirtschaft, Arbeit und Energie (Brandenburg)
- Senatsverwaltung für Wirtschaft, Energie und Betriebe (Berlin)
- Zollkriminalamt, ZKA
- Ministerium für Wirtschaft, Infrastruktur, Tourismus und Arbeit Mecklenburg-Vorpommern
- Bundesnotarkammer, BNotK
- Bundesrechtsanwaltskammer, BRAK
- Bundessteuerberaterkammer, BStBk
- Wirtschaftsprüferkammer, WPK
- Zentralstelle für Finanztransaktionsuntersuchungen (FIU).

8. Betrachtet die Bundesregierung Organisationen, die in Gänze einem „extremistischen“ Phänomenbereich zugeordnet werden können, weiterhin als besonders risikobehaftet in Bezug auf Terrorismusfinanzierung, so wie es aus der Risikoanalyse Terrorismusfinanzierung des BMI (vgl. www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI21003-sektorale-risikoanalyse.pdf?__blob=publicationFile&v=14) hervorgeht, und was qualifiziert eine Organisation als „extremistisch“?
- a) Hat die Bundesregierung wie in der Risikoanalyse Terrorismusfinanzierung des BMI (vgl. S. 55) angekündigt einen Austausch zwischen Non-Profit-Organisationen (NPO) und dem Bankensektor herbeigeführt, um die negativen Konsequenzen von De-Risking-Maßnahmen, welche zu Debanking führen können, zu reduzieren, und wenn ja, mit welchen Teilnehmenden (bitte auflisten), und mit welchem Ergebnis?
 - b) Hat die Bundesregierung, wie in der Risikoanalyse Terrorismusfinanzierung des BMI (vgl. Seite 55) angekündigt, eine Prüfung von möglichen Maßnahmen im Bankensektor durchgeführt, welche den negativen Konsequenzen von De-Risking-Praktiken (vgl. S. 39) entgegenwirken sollen, wenn nein, warum nicht, und wenn ja, mit welchem Ergebnis?
 - c) Hat die Bundesregierung, wie in der Risikoanalyse Terrorismusfinanzierung des BMI (vgl. S. 55) angekündigt, Informationsangebote für NPOs (Non-Profit-Organizations) geschaffen bezüglich des Umgangs mit Sanktions- und Listungsregimes von Nicht-EU-Staaten, und wenn ja, welche?
 - d) Wurde die statistische Erfassung von Terrorismusfinanzierungsfällen mit NPO-Bezug verbessert, seit eine solche Verbesserung in der Risikoanalyse angekündigt wurde, und wenn ja, welche neuen Erkenntnisse und Statistiken liegen dazu vor?

Die Fragen 8 bis 8d werden gemeinsam beantwortet.

Die Bundesregierung hat den in der Sektoralen Risikoanalyse – Terrorismusfinanzierung durch (den Missbrauch von) Non-Profit-Organisationen in Deutschland des Bundesministeriums des Innern angekündigten Austausch umgesetzt. Am 21. März 2024 fand auf Einladung des Bundesministeriums der Finanzen ein strukturierter Drei-Parteien-Dialog zwischen Non-Profit-Organisationen (NPOs), Kreditwirtschaft, und Verwaltung statt. Teilgenommen haben Vertreterinnen und Vertreter der zuständigen Bundesressorts und nachgeordneter Behörden (inklusive der Sicherheitsbehörden) sowie der BaFin und der Bundesbank. Darüber hinaus waren Vertreterinnen und Vertreter großer Bankenverbände und Kreditinstitute sowie Vertreterinnen und Vertreter von NPO-Dachverbänden und ausgewählter Organisationen beteiligt. Eine Veröffentlichung der Klarnamen der Teilnehmerinnen und Teilnehmer erfolgt aus datenschutzrechtlichen Gründen nicht. Im Ergebnis konnte ein gemeinsames Verständnis der regulatorischen Anforderungen und praktischen Herausforderungen, insbesondere im Zusammenhang mit De-Risking-Maßnahmen, erreicht werden. Eine Fortsetzung des Dialogformats ist vorgesehen.

In der zitierten NPO-Risikoanalyse geht es um Informationsangebote für den Umgang mit Sanktions- und Listungsregimen für NPO, nicht speziell um Regime von nicht-EU-Staaten (s. S. 55). Diese wurden ebenfalls im Rahmen des Drei-Parteien-Dialog adressiert. Aktuell arbeitet das Bundeskriminalamt (BKA) an einer generellen Verbesserung der polizeilichen Statistik zu Terrorismusfinanzierungssachverhalten.

9. Sind der Bundesregierung Fälle bekannt, in denen privatrechtliche Verträge bei Banken und Zahlungsdienstleistern gekündigt wurden, weil das Bundesamt für Verfassungsschutz (BfV) zu den Vertragspartnern im Rahmen der Bestandsdatenauskunftsverlangen oder aufgrund anderer Rechtsgrundlagen Informationen herausverlangt hat, und wenn ja, wie viele Fälle betraf dies seit 2021 (bitte nach privaten Kreditinstituten, Anstalten des öffentlichen Rechts und privaten Zahlungsdienstleistern differenzieren)?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

10. Wie informiert das BfV im Rahmen von besonderen Auskunftsverlangen nach § 8a des Bundesverfassungsschutzgesetzes (BVerfSchG) die Auskunftspflichtigen vom Verbot einseitiger Handlungen zulasten ihrer Vertragspartner allein aufgrund eines Auskunftsverlangens (§ 8b Absatz 5 BVerfSchG)?

Das BfV informiert im Rahmen von besonderen Auskunftsverlangen nach § 8a Bundesverfassungsschutzgesetz (BVerfSchG) die Auskunftspflichtigen vom Verbot einseitiger Handlungen zulasten ihrer Vertragspartnerinnen und Vertragspartner aufgrund eines Auskunftsverlangens (§ 8b Absatz 5 BVerfSchG) jedes Mal im Anschreiben über das genannte Verbot. Dort wird auf dieses Verbot explizit hingewiesen und zudem auf die Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (AuA) der BaFin verwiesen. Die AuA enthalten in der aktuellen Fassung auf Seite 92 a. E. ebenfalls einen Hinweis auf das hier genannte Verbot.

- a) Hat die Bundesregierung Kenntnis von solchen Vorgängen, in denen der Verdacht einer solchen pflichtwidrigen Kündigung bestand?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

- b) Welche Schwierigkeiten bestehen aus Sicht der Bundesregierung gerade im Bereich der Finanzdienstleistungen für Finanzinstitute, eine solche Kündigung nach einem Auskunftsverlangen nicht auszusprechen, da hiermit immer ein Risiko der Verletzung von Compliance-Regelungen der Finanzinstitute einhergeht?
- c) Welche Maßnahmen hat die Bundesregierung ergriffen, um das Fernwirkungsverbot von Auskunftsverlangen in § 8b Absatz 5 BVerfSchG abzusichern und ggf. durchzusetzen?

Die Fragen 10 b und 10 c werden zusammen beantwortet.

Im Rahmen des Anwendungsbereichs von § 8a BVerfSchG besteht für die Verpflichteten eine gesetzliche Pflicht, nicht allein aufgrund eines Auskunftsverlangens einseitige Handlungen zulasten ihrer Vertragspartnerinnen und Vertragspartner vorzunehmen. Kommen die Verpflichteten dieser gesetzlichen Pflicht nach, stellt dies keine Verletzung von Compliance-Regelungen dar (siehe § 8b Absatz 5 BVerfSchG).

- d) Gibt es in Zusammenhang mit diesen Fragen Vorgänge oder Beschwerden bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die sich gegen Kontokündigungen im Zusammenhang mit politischer Betätigung vermeintlich extremistischer Gruppierungen richten?

Die BaFin hat weniger als zehn Eingaben zum Thema Kündigungen von Konten des Vereins Rote Hilfe e. V. erhalten. Diese erfolgten jedoch nicht durch den Verein selbst, sondern durch Dritte. Es handelt sich daher nicht um Beschwerden, sondern um Hinweise auf die Kündigungen.

Die BaFin ist in der Vergangenheit bereits vergleichbaren Fallkonstellationen nachgegangen. Aus aufsichtlicher Sicht hat es dabei keine systematischen Verstöße gegeben. Auch aus Verbraucherschutzperspektive gab es in diesen Fällen keine systematische Verbraucherbenachteiligung.

- 11. Welche Kenntnis hat die Bundesregierung über Over-Compliance-Strategien privater Banken bei der faktischen Durchsetzung extraterritorialer US-Sanktions- und Terrorlisten innerhalb der EU?
- 12. Haben, nach Kenntnis der Bundesregierung, private Banken in Deutschland in den letzten zwei Jahren eine Over-Compliance-Strategie verfolgt, und wenn ja, welche Banken?
- 13. Versucht die Bundesregierung, Over-Compliance-Strategien privater Banken zu verhindern, und wenn ja, durch welche Mittel?
- 14. Welche konkreten Maßnahmen hat die Bundesregierung bislang ergriffen, um die EU-Blocking-Verordnung im Bereich des Finanz- und Zahlungsverkehrs faktisch durchzusetzen?
- 15. Wie ist nach Kenntnis der Bundesregierung sichergestellt, dass private Banken und Zahlungsdienstleister in Deutschland US-amerikanische Sanktions- und Terrorlisten nicht anwenden, sofern diese nicht Bestandteil des EU-Sanktionsrechts sind?

Die Fragen 11 bis 15 werden zusammen beantwortet.

Die US-Sanktionsregelungen entfalten Rechtswirkung ausschließlich innerhalb der US-Jurisdiktion. Dies betrifft sowohl Primär- als auch Sekundärsanktionen.

Sofern Verbindungen europäischer Kreditinstitute oder Zahlungsdienstleister zur US-Jurisdiktion bestehen, kann es für diese Unternehmen geschäftspolitische Gründe geben, US-Sanktionsmaßnahmen zu beachten. Es liegt zunächst grundsätzlich in der Verantwortung der jeweiligen Kreditinstitute, unter Abwägung von Kosten-/Nutzenaspekten sowie unter Risikogesichtspunkten über die Aufrechterhaltung von Geschäftsbeziehungen bzw. Vertragsverhältnissen zu entscheiden. Kreditinstitute dürften in der Regel aus ihren Allgemeinen Geschäftsbedingungen (AGB) grundsätzlich berechtigt sein, Vertragsverhältnisse aus geschäftspolitischen Gründen zu kündigen.

Die Bundesregierung lehnt die extraterritoriale Anwendung von Sanktionen grundsätzlich ab. Auf EU-Ebene wurde bereits 1996 die Verordnung 2271/96 (sog. „Blockingverordnung“) geschaffen, um europäischen Rechtsteilnehmerinnen und Rechtsteilnehmern die Einhaltung von Drittstaatsanktionen in bestimmten Länderkontexten zu untersagen.

Bei der Blocking-Verordnung handelt es sich um direkt anwendbares europäisches Recht, das keiner nationalen Umsetzung bedarf. Gemäß Artikel 9 der Verordnung erlassen die Mitgliedstaaten Vorschriften zur Ahndung von Zuwiderhandlungen gegen diese Verordnung. Der deutsche Gesetzgeber hat mit § 82 Absatz 2 der Außenwirtschaftsverordnung in Verbindung mit § 19 Absatz 4 Satz 1 Nummer 1 des Außenwirtschaftsgesetzes eine entsprechende Ahndungsvorschrift geschaffen. Verstöße stellen danach eine Ordnungswidrigkeit dar. Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 6, 8 und 9 auf die Kleine Anfrage „Durchsetzung der US-Blockade gegen Kuba im Rechtsraum der Europäischen Union und ihre Auswirkungen auf die deutsch-kubanischen Wirtschaftsbeziehungen“ auf Bundestagsdrucksache 21/3723 vom 19. Januar 2026 hingewiesen.

16. Wie stellt die Bundesregierung sicher, dass die Kreditanstalt für Wiederaufbau (KfW) US-amerikanische Sanktions- und Terrorlisten nicht anwenden, sofern diese nicht Bestandteil des EU-Sanktionsrechts sind?

Die Bundesregierung überwacht im Rahmen ihrer Rechtaufsicht nach § 12 des Gesetzes über die Kreditanstalt für Wiederaufbau (KfWG) die Beachtung der geltenden Gesetze durch die Kreditanstalt für Wiederaufbau (KfW).

17. In wie vielen Fällen wurden Banken oder Zahlungsdienstleister in Deutschland nach Kenntnis der Bundesregierung a) überprüft, b) beanstandet, c) sanktioniert, weil sie unzulässigerweise Drittstaatsanktionen befolgt haben?

Fälle im Sinne der Frage sind der Bundesregierung nicht bekannt.

18. Teilt die Bundesregierung die Einschätzung der Fragestellenden, dass die EU-Blocking-Verordnung derzeit unter einem strukturellen Vollzugsdefizit leidet, insbesondere im Bankensektor, und wenn nein, wie schätzt die Bundesregierung die Wirksamkeit der EU-Blocking-Verordnung ein?

Die Bundesregierung teilt diese Einschätzung nicht. Im Übrigen wird auf die Antwort zu den Fragen 11 bis 15 hingewiesen.

Die Tatsache, dass die Blocking-Verordnung geschäftspolitischen Erfordernissen der Marktakteure Rechnung trägt, indem sie in Artikel 5 Marktakteuren die Möglichkeit einräumt, soweit andernfalls ihre Interessen oder die der Gemein-

schaft schwer geschädigt würden, Ausnahmegenehmigungen zu beantragen, stellt kein strukturelles Vollzugsdefizit dar.

19. Welche Weisungen, Auslegungshinweise oder Leitlinien existieren seitens des Bundesministeriums der Finanzen (BMF), der BaFin oder der Deutschen Bundesbank, die Banken verpflichten, EU-Recht gegenüber Drittstaatsanktionen ausdrücklich zu priorisieren?

Die Blocking-Verordnung findet in Deutschland direkte Anwendung, ohne dass es behördlicher Umsetzungsakte wie Weisungen oder dergleichen bedürfte. Weisungsbefugnisse mit Blick auf geschäftspolitische Entscheidungen gegenüber Finanzinstituten haben das Bundesministerium der Finanzen, die BaFin oder die Deutsche Bundesbank nicht.

20. Hält die Bundesregierung eine Verschärfung der aufsichtsrechtlichen Praxis oder der gesetzlichen Vorgaben für erforderlich, um die faktische Anwendung extraterritorialen US-Rechts im deutschen Finanzsystem zu unterbinden?

Auf die Antwort zu den Fragen 11 bis 15 und 18 wird verwiesen.

21. Teilt die Bundesregierung die Einschätzung der Fragestellenden, dass die geplante EZB (Europäische Zentralbank)-basierte Zahlungsinfrastruktur wie der digitale Euro, die auf externe private Compliance-Dienstleister angewiesen ist, nicht sanktionssicher gegenüber Drittstaaten ist?
 - a) Gibt es nach Kenntnis der Bundesregierung diesbezüglich Unterschiede zwischen den geplanten Online- und Offlinefunktionen des digitalen Euro, und wenn ja, welche?
 - b) Sieht die Bundesregierung in einer solchen öffentlichen Wallet- oder Konteninfrastruktur eine Möglichkeit, existenzielle Zahlungsfunktionen auch bei Drittstaatsanktionen zuverlässig zu sichern?
 - c) Welche Möglichkeiten gibt es nach Kenntnis der Bundesregierung, den Zugang zur sogenannten White-Label-Solution des digitalen Euro so auszugestalten, dass Sanktionssicherheit gegenüber Drittstaaten sichergestellt werden kann?
 - d) Wurde geprüft, inwiefern bestehende oder geplante Zahlungsverkehrssysteme der EZB technisch, organisatorisch oder vertraglich von US-Recht, US-Cloud-Infrastruktur oder US-Compliance-Anbietern abhängig sind, und welche Schlussfolgerungen zieht die Bundesregierung daraus für das erklärte Ziel der europäischen Finanz- und Zahlungssouveränität?

Die Fragen 21 bis 21d werden gemeinsam beantwortet.

Die Europäische Kommission hat am 28. Juni 2023 einen Legislativvorschlag für eine Verordnung zur Einführung des digitalen Euro vorgelegt. Das europäische Gesetzgebungsverfahren zum Legislativvorschlag dauert an. Der EZB-Rat wird erst nach Verabschiedung der Verordnung zur Einführung des digitalen Euro über die Ausgabe eines digitalen Euro entscheiden.

Der Legislativvorschlag der Europäischen Kommission für eine Verordnung zur Einführung des digitalen Euro sieht unter anderem vor, dass Zahlungsdienstleister die Einhaltung der gemäß Artikel 215 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) erlassenen Sanktionen der Union überwachen müssen. Ferner werden für den digitalen Euro sämtliche an-

wendbare EU-Verordnungen gelten. Diese zielen darauf ab, ein Gleichgewicht zwischen Privatsphäre und Sicherheit herzustellen.

Die technische Zahlungsinfrastruktur für den digitalen Euro wird das Eurosystem, bestehend aus Europäischer Zentralbank (EZB) und den nationalen Zentralbanken der Mitgliedstaaten, deren Währung der Euro ist, entwickeln und bereitstellen. Nach Darstellung der EZB wird sie dafür sowohl mit einem Zusammenschluss nationaler Zentralbanken des Euroraums (darunter auch die Deutsche Bundesbank) als auch mit privaten Dienstleistern kooperieren. Funktionen wie die Zahlungsabwicklung und die eigentliche Ausgabe („Issuance“) des digitalen Euro werden vom Eurosystem selbst übernommen.

Zur Stärkung der europäischen Souveränität soll beispielsweise auch die notwendige Cloud-Infrastruktur von drei europäischen Notenbanken aufgebaut und betrieben werden (u. a. der Deutschen Bundesbank). Andere Dienste werden von privaten Unternehmen bereitgestellt. Die Vergabe an private Unternehmen erfolgte an EU-ansässige Unternehmen unter europäischer Kontrolle (vgl. Übersicht der ausgewählten Dienstleister: www.ecb.europa.eu/press/intro/news/html/ecb.mipnews251002.en.html). Die Arbeiten an der technischen Infrastruktur dauern an.

Um sicherzustellen, dass das System für den digitalen Euro überall im Euroraum einheitlich umgesetzt wird, arbeitet das Eurosystem derzeit in Kooperation mit Marktteilnehmern zudem ein Regelwerk für den digitalen Euro aus. Das Regelwerk soll einheitliche Regeln, technische Standards und Verfahren festlegen und damit in allen Euro-Ländern ein gleichwertiges Angebot von grundlegenden Diensten rund um den digitalen Euro gewährleisten. Auch diese technischen Arbeiten dauern an.

Weitergehende Bewertungen der konkreten rechtlichen und technischen Ausgestaltung des digitalen Euro durch die Bundesregierung bleiben dem laufenden europäischen Gesetzgebungs- und technischen Entwicklungsprozess im Eurosystem vorbehalten.

- e) Welche Haltung nimmt die Bundesregierung zur Option eines Single-Tier-digitalen Euro ein, bei dem Bürgerinnen und Bürger direkte Konten oder Wallets bei der EZB oder ersatzweise bei den nationalen Zentralbanken (z. B. der Deutschen Bundesbank) führen könnten?

Der Vorschlag der Europäischen Kommission vom 28. Juni 2023 für eine Verordnung zur Einführung des digitalen Euro sieht vor, dass die Nutzerinnen und Nutzer des digitalen Euro nur mit Zahlungsdienstleistern eine vertragliche Beziehung zur Nutzung des digitalen Euro eingehen. Es wird ausdrücklich festgehalten, dass die Nutzerinnen und Nutzer des digitalen Euro in keiner vertraglichen Beziehung zur Europäischen Zentralbank oder zu den nationalen Zentralbanken stehen. Demnach sollen Zahlungsdienstleister die Konten für den digitalen Euro im Namen der Nutzerinnen und Nutzer verwalten und Zahlungsdienste im Zusammenhang mit dem digitalen Euro anbieten. Auch das Verhandlungsmandat des Rates vom 19. Dezember 2025 verfolgt diesen Ansatz zur Ausgabe des digitalen Euro.

- 22. Hat die Bundesregierung die Möglichkeit evaluiert, den GNU Taler als technische Basis für Zentralbankengeld vorzuschlagen, oder plant, sie dies zu tun, und wenn nein, warum nicht?

Die Entwicklung der technischen Infrastruktur für den digitalen Euro obliegt dem Eurosystem.

- a) Welche Bedeutung misst die Bundesregierung Open-Source-Software generell hinsichtlich digitaler Zahlungssysteme bei, insbesondere hinsichtlich größtmöglicher digitaler Unabhängigkeit?

Der Vorschlag der Europäischen Kommission vom 28. Juni 2023 für eine Verordnung zur Einführung des digitalen Euro sieht vor, dass die Europäische Zentralbank, soweit möglich, die Interoperabilität von Standards für Zahlungsdienste gewährleistet. Der Legislativvorschlag sieht ferner vor, dass die Interoperabilität unter anderem durch die Verwendung offener Standards unterstützt werden kann. Die Bundesregierung erkennt die Bedeutung von offenen technischen Standards und Interoperabilität im Kontext europäischer Souveränität. Gleichzeitig verfolgt der Legislativvorschlag einen technologieneutralen Ansatz, und die konkrete Entwicklung der technischen Infrastruktur obliegt dem Eurosystem.

Die Bundesregierung begrüßt es, dass das Verhandlungsmandat des Rates vom 19. Dezember 2025 die Verpflichtung der EZB vorsieht, technologische Entwicklungen laufend zu beobachten und zu bewerten. Wo sachgerecht, etwa zur Erhöhung der Privatsphäre oder Resilienz der Infrastruktur, wären neue Technologien fortlaufend zu implementieren.

- b) Welche Zahlungssysteme sind der Bundesregierung bekannt, die einerseits eine mit Bargeld vergleichbare Anonymität für Käuferinnen und Käufer sicherstellen, gleichzeitig aber Geldwäsche und Steuerhinterziehung durch Identifizierung der Zahlungsempfänger ermöglichen, und wäre der GNU Taler nach Ansicht der Bundesregierung ein geeignetes Zahlungssystem nach dieser Maßgabe?

Die Bundesregierung verweist hier insbesondere auf die Möglichkeit von sog. Offline-Zahlungen beim digitalen Euro. Hierbei soll die Privatsphäre besonders geschützt werden. Sowohl bei Überweisungen an andere Personen als auch beim Bezahlen in Geschäften sollen persönliche Transaktionsdaten nur der zahlenden Person und der Person, die das Geld erhält, bekannt sein – so hätte selbst die Bank des Zahlenden keinen Zugang zu Zahlungsinformationen. Bei Ein- und Auszahlungen von Guthaben würde der Zahlungsdienstleister, der den digitalen Euro bereitstellt, Kontrollen zur Bekämpfung von Geldwäsche durchführen – so, wie das heute bei Barabhebungen und -einzahlungen der Fall ist.

Zudem trägt die Möglichkeit von Offline-Zahlungen zur Stärkung der Resilienz bei, denn Offline-Zahlungen wären selbst bei einem Strom- oder Internetausfall zwischen Endgeräten in räumlicher Nähe möglich. Die genaue technische Ausgestaltung der Offline-Lösung obliegt dem Eurosystem, das gegenwärtig unterschiedliche Architekturmodelle erwägt und derzeit mögliche Vorschläge sondiert.

Zur Minimierung geldwäscherechtlicher Risiken sieht der Verordnungsvorschlag der Europäischen Kommission zum digitalen Euro zudem entsprechende Transaktions- und Haltelimits für Offline-Zahlungen vor, die von der Europäischen Kommission auf Basis einer Einschätzung der europäischen Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AMLA) einzuführen wären.

Die Abwicklung von Transaktionen in digitalen Euro (online und offline) soll so gestaltet sein, dass weder die Europäische Zentralbank noch die nationalen Zentralbanken die Daten identifizierten oder identifizierbaren Nutzerinnen und Nutzern des digitalen Euro zuordnen können.

23. Wurde geprüft, ob nationale Zentralbanken (analog zu früheren Regelungen etwa für Beschäftigte der Deutschen Bundesbank) Zahlungskonten mit ausschließlich EU-rechtlicher Compliance für bestimmte Personengruppen oder generell bereitstellen könnten?
24. Welche konkreten regulatorischen oder infrastrukturellen Optionen sieht die Bundesregierung insgesamt, um Bürgerinnen und Bürger sowie Organisationen in Deutschland wirksam vor der Anwendung extraterritorialer US-Sanktions- und Terrorlisten zu schützen, und welche dieser Optionen verfolgt die Bundesregierung aktiv, welche werden derzeit nicht verfolgt, und aus welchen Gründen?

Die Fragen 23 und 24 werden zusammen beantwortet.

Grundsätzlich prüft die Bundesregierung laufend Ansätze wie auf die extraterritoriale Anwendung von Drittstaaten-Sanktionen reagiert werden kann.

25. Hat die BaFin im Zusammenhang mit Listungen deutscher Organisationen auf US-amerikanischen Sanktionslisten wie der FDTO (Foreign Terrorist Organizations)-Liste bei deutschen Banken Erkundigungen ange stellt oder Nachfragen an diese gerichtet, und wenn ja, in wie vielen Fällen, und bei welchen Banken (bitte nach Jahren und Monaten ab 2016 aufschlüsseln)?

Auf die Antwort zur Frage 19 wird verwiesen.

