DEUTSCHE BUNDESBANK
EUROSYSTEM

23. Oktober 2020

Rundschreiben Nr. 68/2020

Hinweis: Vorherige Verlautbarung der Bundesbank zu Finanzsanktionen: Rundschreiben Nr. 67/2020

An alle
Kreditinstitute

Finanzsanktionen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen
Durchführungsverordnung (EU) 2020/1536 des Rates vom 22. Oktober 2020

Sehr geehrte Damen und Herren,

Der Rat der Europäischen Union hat mit Durchführungsverordnung (EU) 2020/1536[1] (Anlage 1) zwei natürliche Personen und eine Einrichtung in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen in Anhang I der Verordnung (EU) 2019/796[2] (Sanktionsregime Cyberangriffe) aufgenommen.

Wir bitten Sie, uns auf der Grundlage von Artikel 8 Abs. 1 der Verordnung (EU) 2019/796

spätestens bis zum 30. Oktober 2020

[1] Durchführungsverordnung (EU) 2020/1536 des Rates vom 22. Oktober 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

[2] Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

Deutsche Bundesbank, Servicezentrum Finanzsanktionen
Ludwigstraße 13, 80539 München, Telefon: 089 2889-3800, Telefax: 069 709097-3801
sz.finanzsanktionen.abfrage@bundesbank.de, www.bundesbank.de, SWIFT: MARK DE FF

…

per E-Mail oder in Ausnahmefällen per Telefax mitzuteilen, ob und welche Gelder bei Ihnen von den Durchführungsverordnungen (EU) 2020/1536 betroffen sind.

Wir möchten Sie darauf hinweisen, dass Sie auch verpflichtet sind, sich nach dieser Abfrage ergebende Änderungen bezüglich der Vermögenswerte, die von Finanzsanktionen betroffen sind, unaufgefordert zu melden.

Fehlanzeigen, die auf jeden Fall erforderlich sind, oder Positivmeldungen bitten wir ausschließlich unter Beachtung der beigefügten Hinweise (Anlage 2) zu übermitteln. Mit derart aufbereiteten Meldungen unterstützen Sie uns bei der Bearbeitung Ihrer Antworten und vermeiden Rückfragen.

Wir haben die Rechtsakte zu Finanzsanktionen auf folgender Website der Deutschen Bundesbank unter dem jeweiligen Sanktionsregime eingestellt:

https://www.bundesbank.de/de/service/finanzsanktionen/sanktionsregimes

Mit freundlichen Grüßen

Deutsche Bundesbank
Hauptverwaltung in Bayern
Mayrhofer Stange

Beglaubigt:
M. Bayer
Tarifbeschäftigte

Anlagen

Deutsche Bundesbank, Servicezentrum Finanzsanktionen
Ludwigstraße 13, 80539 München, Telefon: 089 2889-3800, Telefax: 069 709097-3801
sz.finanzsanktionen.abfrage@bundesbank.de, www.bundesbank.de, SWIFT: MARK DE FF

22.10.2020 DE Amtsblatt der Europäischen Union L 351 I/1

II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2020/1536 DES RATES

vom 22. Oktober 2020

zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen ([1]), insbesondere auf Artikel 13 Absatz 1,

auf Vorschlag des Hohen Vertreters der Union für Außen- und Sicherheitspolitik,

in Erwägung nachstehender Gründe:

(1) Der Rat hat am 17. Mai 2019 die Verordnung (EU) 2019/796 angenommen.

(2) Gezielte restriktive Maßnahmen gegen Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, gehören zu den Maßnahmen des Rahmens für eine gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“) und sind ein wichtiges Instrument, um von solchen Aktivitäten abzuschrecken und darauf zu reagieren.

(3) Um fortgesetzte und zunehmende böswillige Handlungen im Cyberraum zu verhindern, von ihnen abzuschrecken und auf sie zu reagieren, sollten zwei natürliche Personen und eine Einrichtung in die im Anhang I der Verordnung (EU) 2019/796 enthaltene Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, gegen die restriktive Maßnahmen verhängt wurden, aufgenommen werden. Diese Personen und diese Einrichtung sind verantwortlich für Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, — insbesondere für den Cyberangriff gegen den Deutschen Bundestag, der im April und im Mai 2015 stattfand — oder waren daran beteiligt.

(4) Anhang I der Verordnung (EU) 2019/796 sollte daher entsprechend geändert werden —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Anhang I der Verordnung (EU) 2019/796 wird gemäß dem Anhang der vorliegenden Verordnung geändert.

([1]) ABl. L 129I vom 17.5.2019, S. 1.

Artikel 2

Diese Verordnung tritt am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 22. Oktober 2020.

Im Namen des Rates
Der Präsident
M. ROTH

ANHANG

Die folgenden Einträge werden in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen in Anhang I der Verordnung (EU) 2019/796 aufgenommen:

A. Natürliche Personen

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Geburtsdatum: 15. November 1990 Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation) Staatsangehörigkeit: russisch Geschlecht: männlich	Dmitry Badin war an einem Cyberangriff mit erheblichen Auswirkungen gegen den Deutschen Bundestag beteiligt. Als Militärgeheimdienstbeamter des 85. Hauptzentrums für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) war Dmitry Badin Teil eines Teams von Beamten des russischen Militärgeheimdienstes, die im April und Mai 2015 einen Cyberangriff gegen den Deutschen Bundestag durchführten. Dieser Cyberangriff zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Geburtsdatum: 21. Februar 1961 Staatsangehörigkeit: russisch Geschlecht: männlich	Igor Kostyukov ist derzeit Leiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), wo er zuvor als Erster Stellvertretender Leiter tätig war. Eine der seiner Befehlsgewalt unterstehenden Einheiten ist das 85. Hauptzentrum für Spezialdienste (GTsST), auch bekannt als „Militäreinheit 26165“ (in Fachkreisen bekannt unter den Beinamen „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ und „Strontium“). In dieser Eigenschaft ist Igor Kostyukov verantwortlich für vom GTsST durchgeführte Cyberangriffe, einschließlich derjenigen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag, der im April und Mai 2015 stattfand, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugt Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen. Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020“

B. Juristische Personen, Organisationen und Einrichtungen

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„4.	85. Hauptzentrum für Spezialdienste(GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)	Anschrift: Komsomol'skiy Prospekt, 20, Moskau, 119146, Russische Föderation	Das 85. Hauptzentrum für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), auch bekannt als „Militäreinheit 26165" bekannt (in Fachkreisen bekannt unter den Beinamen „APT28", „Fancy Bear", „Sofacy Group", „Pawn Storm" und „Strontium"), ist verantwortlich für Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag, der im April und Mai 2015 stattfand, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugt Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen. Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020"

Anlage 2

Deutsche Bundesbank
Servicezentrum Finanzsanktionen

Hinweise für Rückmeldungen bei Abfragen zu Finanzsanktionsrechtsakten

Bitte beachten Sie für Ihre Rückmeldung die folgenden Hinweise:

- Antworten Sie grundsätzlich per E-Mail (möglichst mit Antwortfunktion zu diesem Mail). **Ergänzen Sie beim Antwort-Mail in der von uns vorgegebenen Thema-/ Betreff-Zeile hinter der Position „Meldung“ entweder „Fehlanzeige“ oder „siehe gesonderte Meldung“.**

- **Fügen Sie Ihre Bankleitzahl in der Thema-/Betreff-Zeile am dafür vorgesehenen Platz ein.**

- **Muster für die Thema-/Betreff-Zeile Ihres Antwort-Mails:**

  Rundschreiben Nr. 68/2020, Meldung: Fehlanzeige, BLZ: xxxxxxxx

  oder

  Rundschreiben Nr. 68/2020, Meldung: Siehe gesonderte Meldung, BLZ: xxxxxxxx

- Sofern Sie nicht die Antwortfunktion nutzen, gestalten Sie die Thema-/Betreff-Zeile Ihres Mails gemäß diesen Vorgaben und senden Sie Ihre Meldung an die **ausschließlich** für Abfragen vorgesehene E-Mail-Adresse

  sz.finanzsanktionen.abfrage@bundesbank.de

- **Die Erfassung Ihrer Meldung erfolgt elektronisch und ist begrenzt auf die vorbezeichneten Angaben in der Thema-/Betreff-Zeile. Sofern Sie für mehrere Institute (BLZ) Auskünfte erteilen, ist insoweit für jedes Institut eine gesonderte Anzeige abzugeben. Ferner ist die Meldung stets für jedes Rundschreiben getrennt zu erstatten. Sonstige über die Angaben in der Thema-/Betreff-Zeile hinausgehenden weiteren Mitteilungen sind als separates Mail an die allgemeine E-Mail-Adresse: sz.finanzsanktionen@bundesbank.de zu richten.**

- Sollten Sie ausnahmsweise Ihre Rückmeldung per Telefax senden, gestalten Sie bitte die Thema-/Betreff-Zeile ebenfalls gemäß den oben angeführten Vorgaben und übermitteln Sie Ihr Dokument an die eigens hierfür eingerichtete

  Fax-Nr. 069 709097- 3801