Amtsblatt der Europäischen Union

C 328

Ausgabe in deutscher Sprache

66. Jahrgang

Mitteilungen und Bekanntmachungen 18. September 2023

Inhalt

DE

([1]) Text von Bedeutung für den EWR.

[1] Text von Bedeutung für den EWR.

II

(Mitteilungen)

MITTEILUNGEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

EUROPÄISCHE KOMMISSION

Keine Einwände gegen einen angemeldeten Zusammenschluss

(Sache M.11106 — STELLANTIS / MICHELIN / FORVIA / SYMBIO)

(Text von Bedeutung für den EWR)

(2023/C 328/01)

Am 17. Juli 2023 hat die Kommission nach Artikel 6 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 139/2004 des Rates ([1]) entschieden, keine Einwände gegen den oben genannten angemeldeten Zusammenschluss zu erheben und ihn für mit dem Binnenmarkt vereinbar zu erklären. Der vollständige Wortlaut der Entscheidung ist nur auf Englisch verfügbar und wird in einer um etwaige Geschäftsgeheimnisse bereinigten Fassung auf den folgenden EU-Websites veröffentlicht:

— der Website der GD Wettbewerb zur Fusionskontrolle (https://competition-cases.ec.europa.eu/search). Auf dieser Website können Fusionsentscheidungen anhand verschiedener Angaben wie Unternehmensname, Nummer der Sache, Datum der Entscheidung oder Wirtschaftszweig abgerufen werden,

— der Website EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=de). Hier kann diese Entscheidung anhand der Celex-Nummer 32023M11106 abgerufen werden. EUR-Lex ist das Internetportal zum Gemeinschaftsrecht.

([1]) ABl. L 24 vom 29.1.2004, S. 1.

MITTEILUNG DER KOMMISSION

Leitlinien der Kommission zur Anwendung des Artikels 4 Absätze 1 und 2 der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)

(2023/C 328/02)

I. EINLEITUNG

1. Nach Artikel 4 Absatz 3 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) ([1]) muss die Kommission bis zum 17. Juli 2023 Leitlinien zur Klarstellung der Anwendung des Artikels 4 Absätze 1 und 2 der Richtlinie bereitstellen.

2. Mit den vorliegenden Leitlinien wird die Anwendung dieser Bestimmungen präzisiert, die das Verhältnis zwischen der Richtlinie (EU) 2022/2555 und aktuellen und künftigen sektorspezifischen Rechtsakten der Union über Risikomanagementmaßnahmen oder Meldepflichten für Sicherheitsvorfälle im Bereich der Cybersicherheit betreffen. In der Anlage zu diesen Leitlinien werden die sektorspezifischen Rechtsakte der Union aufgeführt, die nach Auffassung der Kommission in den Anwendungsbereich des Artikels 4 der Richtlinie (EU) 2022/2555 fallen. Der Umstand, dass ein Rechtsakt nicht in dieser Anlage aufgeführt ist, bedeutet nicht zwangsläufig, dass er nicht in den Anwendungsbereich dieser Bestimmung fällt.

3. In Anwendung des Artikels 4 Absatz 3 Satz 3 der Richtlinie (EU) 2022/2555 hat die Kommission die Bemerkungen der NIS-Kooperationsgruppe und der Agentur der Europäischen Union für Cybersicherheit (ENISA) vor der Annahme der vorliegenden Leitlinien berücksichtigt.

4. Die vorliegenden Leitlinien lassen die Auslegung des Unionsrechts durch den Gerichtshof der Europäischen Union unberührt.

II. GLEICHWERTIGKEIT DER CYBERSICHERHEITSANFORDERUNGEN AUS SEKTORSPEZIFISCHEN RECHTSAKTEN DER UNION

5. Wenn wesentliche oder wichtige Einrichtungen gemäß sektorspezifischen Rechtsakten der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder erhebliche Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in der Richtlinie (EU) 2022/2555 festgelegten Verpflichtungen zumindest gleichwertig sind, finden laut Artikel 4 Absatz 1 der Richtlinie (EU) 2022/2555 die einschlägigen Bestimmungen dieser Richtlinie, einschließlich der Bestimmungen über Aufsicht und Durchsetzung in Kapitel VII derselben Richtlinie, keine Anwendung auf solche Einrichtungen. Weiter besagt diese Bestimmung, dass, wenn die sektorspezifischen Rechtsakte der Union nicht für alle in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallenden Einrichtungen eines bestimmten Sektors gelten, die einschlägigen Bestimmungen dieser Richtlinie weiterhin auf Einrichtungen angewandt werden, die nicht unter diese sektorspezifischen Rechtsakte der Union fallen.

II.1. Anforderungen an das Risikomanagement im Bereich der Cybersicherheit

6. Nach Artikel 4 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 gelten Maßnahmen zum Cybersicherheitsrisikomanagement, die von wesentlichen oder wichtigen Einrichtungen im Rahmen sektorspezifischer Rechtsakte der Union ergriffen werden müssen, als in ihrer Wirkung den in der Richtlinie (EU) 2022/2555 festgelegten Verpflichtungen gleichwertig, wenn diese Maßnahmen in ihrer Wirkung den in Artikel 21 Absätze 1 und 2 der Richtlinie festgelegten Maßnahmen mindestens gleichwertig sind. Bei der Beurteilung der Frage, ob die Anforderungen eines sektorspezifischen Rechtsakts der Union über Maßnahmen zum Cybersicherheitsrisikomanagement den Anforderungen des Artikels 21 Absätze 1 und 2 der Richtlinie (EU) 2022/2555 mindestens gleichwertig sind, sollten die Anforderungen des sektorspezifischen Rechtsakts der Union zumindest den Anforderungen dieser Bestimmungen entsprechen oder darüber hinausgehen, was bedeutet, dass die sektorspezifischen Bestimmungen inhaltlich detaillierter sein können als die entsprechenden Bestimmungen der Richtlinie (EU) 2022/2555.

([1]) ABl. L 333 vom 27.12.2022, S. 80.

7. Nach Artikel 21 Absatz 1 Unterabsatz 1 der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten sicherstellen, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen. Diese Maßnahmen sollten risikobasiert und geeignet sein, Sicherheitsvorfälle zu verhindern bzw. deren Auswirkungen so gering wie möglich zu halten. In Artikel 21 Absatz 1 Unterabsatz 2 der Richtlinie (EU) 2022/2555 ist festgelegt, wie die Verhältnismäßigkeit solcher Maßnahmen zu bewerten ist ([2]). Die in Artikel 21 Absatz 1 der Richtlinie (EU) 2022/2555 festgelegte Verpflichtung, wonach wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige Risikomanagementmaßnahmen im Bereich der Cybersicherheit ergreifen müssen, bezieht sich auf alle Tätigkeiten und Dienste der betreffenden Einrichtung und nicht nur auf bestimmte von der Einrichtung bereitgestellte IT-Anlagen oder bestimmte von ihr erbrachte kritische Dienste.

8. Bei der Bewertung der Gleichwertigkeit eines sektorspezifischen Rechtsakts der Union mit den einschlägigen Bestimmungen der Richtlinie (EU) 2022/2555 über das Cyberrisikomanagement sollte der Frage besondere Bedeutung beigemessen werden, ob die in dem Rechtsakt enthaltenen Sicherheitspflichten auch Maßnahmen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen umfassen. Der Begriff der „Sicherheit von Netz- und Informationssystemen" wird in Artikel 6 Nummer 2 der Richtlinie (EU) 2022/2555 definiert als die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können. Die Verwendung der Begriffe „Verfügbarkeit", „Authentizität", „Integrität" und „Vertraulichkeit" in dieser Begriffsbestimmung bezieht sich auf alle vier Schutzziele im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen. Der Begriff „Netz- und Informationssysteme" im Sinne des Artikels 6 Nummer 1 der Richtlinie (EU) 2022/2555 umfasst elektronische Kommunikationsnetze ([3]), ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, und digitale Daten, die zum Zwecke ihrer betrieblichen Nutzung, ihres Schutzes oder ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden. Folglich sollten die in einem sektorspezifischen Rechtsakt der Union vorgeschriebenen Sicherheitsmaßnahmen auch für Hardware, Firmware und Software gelten, die bei den Tätigkeiten einer Einrichtung verwendet werden.

9. Ein weiterer wichtiger Aspekt bei der Beurteilung der Gleichwertigkeit der Anforderungen eines sektorspezifischen Rechtsakts der Union mit den Anforderungen des Artikels 21 Absätze 1 und 2 der Richtlinie (EU) 2022/2555 ist, dass die in dem Rechtsakt vorgeschriebenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf einem „gefahrenübergreifenden Ansatz" beruhen müssen. Da Bedrohungen der Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, kann jede Art von Ereignis negative Auswirkungen auf die Netz- und Informationssysteme der Einrichtung haben und möglicherweise zu einem Sicherheitsvorfall führen. Deshalb sollten die von der Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit nicht nur ihre Netz- und Informationssysteme, sondern auch die physische Umgebung dieser Systeme vor Ereignissen wie Sabotage, Diebstahl, Brand, Überschwemmung, Telekommunikations- oder Stromausfällen oder unbefugtem physischen Zugang schützen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der von Netz- und Informationssystemen angebotenen oder über diese zugänglichen Dienste beeinträchtigen können. Folglich sollten sich die in einem sektorspezifischen Rechtsakt der Union vorgeschriebenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit insbesondere auch auf die physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen erstrecken, die sich aus Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder Naturereignissen ergeben ([4]).

10. Nach Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 müssen die Risikomanagementmaßnahmen im Bereich der Cybersicherheit auch die in Absatz 2 Buchstaben a bis j dieses Artikels aufgeführten spezifischen Sicherheitsanforderungen einbeziehen. Diese Anforderungen umfassen Maßnahmen wie Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme, die Bewältigung von Sicherheitsvorfällen, die Aufrechterhaltung des Betriebs, das Krisenmanagement, die Sicherheit der Lieferkette, Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung. Durch Artikel 21 Absatz 5 Unterabsatz 2 der Richtlinie (EU) 2022/2555 wird der Kommission die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung der

([2]) Siehe dazu auch die Erwägungsgründe 78, 81 und 82 der Richtlinie (EU) 2022/2555.

([3]) Artikel 2 Nummer 1 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).

([4]) Siehe Erwägungsgrund 79 der Richtlinie (EU) 2022/2555.

technischen und methodischen Anforderungen sowie erforderlichenfalls sektorspezifischer Anforderungen an die in Artikel 21 Absatz 2 der Richtlinie aufgeführten Sicherheitsmaßnahmen zu erlassen. In Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter muss die Kommission bis zum 17. Oktober 2024 Durchführungsrechtsakte zu den technischen und methodischen Anforderungen an die in Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen erlassen. In Durchführungsrechtsakten werden die wichtigsten Bedingungen und Kriterien für die Durchführung entsprechend den Vorgaben im Basisrechtsakt präzisiert, ohne den Regelungsgehalt des Basisrechtsakts zu beeinträchtigen ([5]).

II.2. **Meldepflichten**

11. Nach Artikel 4 Absatz 2 Buchstabe b der Richtlinie (EU) 2022/2555 werden Meldepflichten für erhebliche Sicherheitsvorfälle als den Verpflichtungen der Richtlinie gleichwertig betrachtet, wenn ein sektorspezifischer Rechtsakt der Union einen unmittelbaren, gegebenenfalls automatischen und direkten Zugang zu den Meldungen von Sicherheitsvorfällen durch die CSIRTs, die zuständigen Behörden oder die zentralen Anlaufstellen vorsieht und wenn die Anforderungen zur Meldung erheblicher Sicherheitsvorfälle in ihrer Wirkung mindestens den in Artikel 23 Absätze 1 bis 6 der Richtlinie (EU) 2022/2555 festgelegten Anforderungen gleichwertig sind.

12. Da die Anforderungen eines sektorspezifischen Rechtsakts der Union in Bezug auf die Meldung erheblicher Sicherheitsvorfälle in ihrer Wirkung den Anforderungen des Artikels 23 Absätze 1 bis 6 der Richtlinie (EU) 2022/2555 mindestens gleichwertig sein müssen, damit dieser Rechtsakt anstelle der Meldepflichten der genannten Richtlinie gelten kann, sind die in Artikel 23 Absätze 1 bis 6 der Richtlinie festgelegten Anforderungen für die Bewertung dieser Gleichwertigkeit von besonderer Bedeutung. In Artikel 23 Absätze 1 bis 6 der Richtlinie (EU) 2022/2555 wird ausführlicher festgelegt, welche Arten von Sicherheitsvorfällen an wen, in welchem Zeitrahmen und mit welchem Informationsinhalt zu melden sind. Dies wird in den folgenden Unterabschnitten näher erläutert:

II.2.1. *Meldung erheblicher Sicherheitsvorfälle an CSIRTs, zuständige Behörden und Empfänger*

13. Nach Artikel 23 Absatz 1 Unterabsatz 1 Satz 1 der Richtlinie (EU) 2022/2555 müssen wesentliche und wichtige Einrichtungen ihrem CSIRT oder gegebenenfalls ihrer zuständigen Behörde unverzüglich jeden erheblichen Sicherheitsvorfall melden. Nach Artikel 23 Absatz 1 Unterabsatz 1 Satz 2 der Richtlinie (EU) 2022/2555 müssen wesentliche und wichtige Einrichtungen gegebenenfalls den Empfängern ihrer Dienste unverzüglich erhebliche Sicherheitsvorfälle mitteilen, die die Erbringung dieser Dienste beeinträchtigen können.

14. Während in Artikel 6 Nummer 6 der Richtlinie (EU) 2022/2555 der Begriff „Sicherheitsvorfall" sehr weit gefasst wird als jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder Dienste, die über diese Netz- und Informationssysteme angebotenen werden bzw. zugänglich sind, beeinträchtigt, wird in Artikel 23 Absatz 1 nur für erhebliche Sicherheitsvorfälle eine Meldepflicht vorgeschrieben. Ein Sicherheitsvorfall gilt als erheblich, wenn er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann (Artikel 23 Absatz 3 Buchstabe a) oder wenn er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann (Artikel 23 Absatz 3 Buchstabe b).

([5]) Siehe Kapitel D, Zusätzliche Vorschriften zur Durchführung des Basisrechtsakts. In: Nicht bindende Kriterien für die Anwendung der Artikel 290 und 291 des Vertrags über die Arbeitsweise der Europäischen Union – 18. Juni 2019 (ABl. C 223 vom 3.7.2019, S. 1).

15. In Erwägungsgrund 101 der Richtlinie (EU) 2022/2555 wird klargestellt, dass die Meldung von Sicherheitsvorfällen auf einer von der betreffenden Einrichtung vorgenommenen Anfangsbewertung beruhen sollte. Bei einer solchen Anfangsbewertung sollten unter anderem die betroffenen Netz- und Informationssysteme und insbesondere deren Bedeutung für die Erbringung der Dienste der Einrichtung, die Schwere und die technischen Merkmale der Cyberbedrohung und alle zugrunde liegenden Schwachstellen, die ausgenutzt werden, sowie die Erfahrungen der Einrichtung mit ähnlichen Vorfällen berücksichtigt werden. Indikatoren wie das Ausmaß, in dem das Funktionieren des Dienstes beeinträchtigt wird, die Dauer eines Sicherheitsvorfalls oder die Zahl der betroffenen Nutzer von Diensten könnten eine wichtige Rolle bei der Feststellung spielen, ob die Betriebsstörung des Dienstes schwerwiegend ist.

16. Durch Artikel 23 Absatz 11 Unterabsatz 2 der Richtlinie (EU) 2022/2555 wird der Kommission die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, in denen näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich anzusehen ist. In Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke muss die Kommission solche Durchführungsrechtsakte bis zum 17. Oktober 2024 erlassen. In Durchführungsrechtsakten werden die wichtigsten Bedingungen und Kriterien für die Durchführung entsprechend den Vorgaben im Basisrechtsakt präzisiert, ohne den Regelungsgehalt des Basisrechtsakts zu beeinträchtigen ([6]).

II.2.2. *Mehrstufiger Ansatz und Zeitrahmen für die Meldung erheblicher Sicherheitsvorfälle*

17. In der Richtlinie (EU) 2022/2555 ist ein mehrstufiger Ansatz für die Meldung erheblicher Sicherheitsvorfälle festgelegt worden, der eine Frühwarnung, eine Meldung von Sicherheitsvorfällen und einen Abschlussbericht umfasst. Diese drei Elemente können möglicherweise durch Zwischenberichte und einen Fortschrittsbericht ergänzt werden.

18. Der mehrstufige Ansatz dient der Herstellung der richtigen Balance zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung erheblicher Sicherheitsvorfälle entgegenwirkt und den wesentlichen und wichtigen Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Einrichtungen und ganze Sektoren ihre Cyberresilienz im Laufe der Zeit verbessern können ([7]).

19. Nach dem mehrstufigen Ansatz müssen wesentliche und wichtige Einrichtungen zunächst unverzüglich, in jedem Fall aber innerhalb von 24 Stunden, nachdem sie von dem erheblichen Sicherheitsvorfall Kenntnis erlangt haben, dem zuständigen CSIRT oder der zuständigen Behörde eine Frühwarnung übermitteln. Anschließend müssen diese Einrichtungen unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, nachdem sie Kenntnis von dem erheblichen Sicherheitsvorfall erlangt haben, eine Meldung über den Sicherheitsvorfall übermitteln. Danach kann von einem zuständigen CSIRT oder einer zuständigen Behörde ein Zwischenbericht angefordert werden. Schließlich muss dem zuständigen CSIRT oder der zuständigen Behörde spätestens einen Monat nach der Meldung des Sicherheitsvorfalls ein Abschlussbericht vorgelegt werden, es sei denn, der Sicherheitsvorfall dauert zu diesem Zeitpunkt noch an; in diesem Fall ist zunächst ein Fortschrittsbericht und dann innerhalb eines Monats nach der Bewältigung des Sicherheitsvorfalls ein Abschlussbericht vorzulegen.

20. Für die Meldung von Sicherheitsvorfällen gemäß Artikel 23 Absatz 4 Unterabsatz 2 der Richtlinie (EU) 2022/2555 in Bezug auf Vertrauensdiensteanbieter gilt ein anderer Zeitrahmen. Diese Anbieter müssen erhebliche Sicherheitsvorfälle, die bei der Erbringung ihrer Vertrauensdienste auftreten, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden, nachdem sie Kenntnis von dem erheblichen Sicherheitsvorfall erlangt haben, melden.

([6]) Siehe Kapitel D, Zusätzliche Vorschriften zur Durchführung des Basisrechtsakts. In: Nicht bindende Kriterien für die Anwendung der Artikel 290 und 291 des Vertrags über die Arbeitsweise der Europäischen Union – 18. Juni 2019 (ABl. C 223 vom 3.7.2019, S. 1).

([7]) Siehe Erwägungsgrund 101 der Richtlinie (EU) 2022/2555.

II.2.3. *Inhalt der verpflichtenden Meldung erheblicher Sicherheitsvorfälle an CSIRTs oder zuständige Behörden*

21. Nach Artikel 23 Absatz 1 Unterabsatz 1 Satz 3 der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten in der Regel sicherstellen, dass wesentliche und wichtige Einrichtungen unter anderem alle Informationen übermitteln, die es dem zuständigen CSIRT oder gegebenenfalls der zuständigen Behörde ermöglichen zu ermitteln, ob ein Sicherheitsvorfall grenzüberschreitende Auswirkungen hat. Diese Anforderung in Bezug auf den Inhalt der verpflichtenden Meldung wird in Artikel 23 Absatz 4 der Richtlinie (EU) 2022/2555 näher ausgeführt, in dem der mehrstufige Ansatz festgelegt wird.

22. Nach Artikel 23 Absatz 4 Buchstabe a muss in der Frühwarnung gegebenenfalls angegeben werden, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall durch rechtswidrige oder böswillige Handlungen verursacht wurde, und ob er möglicherweise grenzüberschreitende Auswirkungen hat (d. h. ob dies wahrscheinlich ist). Nach Erwägungsgrund 102 der Richtlinie (EU) 2022/2555 sollte die Frühwarnung nur die Informationen enthalten, die erforderlich sind, um das zuständige CSIRT oder die zuständige Behörde über den erheblichen Sicherheitsvorfall zu unterrichten und es der betreffenden Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen.

23. Die Meldung des Vorfalls muss gegebenenfalls Aktualisierungen der im Rahmen der Frühwarnung übermittelten Informationen enthalten. Darüber hinaus muss sie eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren enthalten.

24. Falls ein Zwischenbericht verlangt wird, muss dieser auch relevante Statusaktualisierungen enthalten. Der Abschlussbericht muss eine ausführliche Beschreibung des Sicherheitsvorfalls enthalten, einschließlich seines Schweregrads und seiner Auswirkungen, der Art der Bedrohung bzw. der zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat, der getroffenen und laufenden Abhilfemaßnahmen und gegebenenfalls der grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

II.2.4. *Unmittelbarer Zugang zu Meldungen von Sicherheitsvorfällen*

25. Nach Artikel 4 Absatz 2 Buchstabe b der Richtlinie (EU) 2022/2555 muss ein sektorspezifischer Rechtsakt der Union, um bezüglich der Meldepflichten anstelle der Richtlinie anwendbar zu sein, den CSIRTs, den zuständigen Behörden oder den in der Richtlinie (EU) 2022/2555 genannten zentralen Anlaufstellen einen unmittelbaren Zugang zu den gemäß dem sektorspezifischen Rechtsakt der Union übermittelten Meldungen von Sicherheitsvorfällen ermöglichen. Nach Erwägungsgrund 24 der Richtlinie (EU) 2022/2555 kann ein solcher sofortiger Zugang insbesondere dadurch gewährt werden, dass Meldungen von Sicherheitsvorfällen unverzüglich an das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle weitergeleitet werden.

26. Der unmittelbare Zugang kann gegebenenfalls über automatische und direkte Mittel gewährt werden, die von den Mitgliedstaaten eingerichtet werden sollten. Solche automatischen und direkten Meldemechanismen stellen einen systematischen und sofortigen Informationsaustausch mit den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen zur Bearbeitung solcher Meldungen von Sicherheitsvorfällen sicher. Die Mitgliedstaaten können auch eine zentrale Anlaufstelle nutzen, die dem sektorspezifischen Rechtsakt der Union entspricht, um die Berichterstattung zu vereinfachen und den automatischen und direkten Meldemechanismus umzusetzen.

27. Bei der Beurteilung der Frage, ob die Anforderungen eines sektorspezifischen Rechtsakts der Union über die Meldung erheblicher Sicherheitsvorfälle den Anforderungen des Artikels 23 Absätze 1 bis 6 der Richtlinie (EU) 2022/2555 mindestens gleichwertig sind, sollten die Anforderungen des sektorspezifischen Rechtsakts der Union zumindest den Anforderungen des Artikels 23 Absätze 1 bis 6 entsprechen oder in ihrer Ausführlichkeit darüber hinausgehen. Die Anforderungen sollten sich auf die Art von Sicherheitsvorfällen beziehen, die gemäß der Richtlinie (EU) 2022/2555 zu melden sind, wobei insbesondere die Empfänger, der Inhalt und die geltenden Fristen zu berücksichtigen sind.

III. **FOLGEN DER GLEICHWERTIGKEIT**

III.1. **Aufsicht und Durchsetzung**

28. Wenn die Bestimmungen sektorspezifischer Rechtsakte der Union den in der Richtlinie (EU) 2022/2555 festgelegten Verpflichtungen in ihrer Wirkung zumindest gleichwertig sind, finden nicht nur die betreffenden Bestimmungen der Richtlinie über zu ergreifende Maßnahmen zum Cybersicherheitsrisikomanagement oder über die Meldung erheblicher Sicherheitsvorfälle keine Anwendung, sondern auch die in Kapitel VII der Richtlinie (EU) 2022/2555 festgelegten Bestimmungen über Aufsicht und Durchsetzung.

29. In Erwägungsgrund 25 der Richtlinie (EU) 2022/2555 wird erläutert, dass sektorspezifische Rechtsakte der Union, die in ihrer Wirkung zumindest gleichwertig sind, vorsehen könnten, dass die nach diesen Rechtsakten zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf das Cybersicherheitsrisikomanagement oder die Meldepflichten mit Unterstützung der gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden ausüben sollen. Die betreffenden zuständigen Behörden könnten zu diesem Zweck Kooperationsvereinbarungen schließen, in denen auch Verfahren für die Koordinierung der Aufsichtstätigkeiten, Verfahren für Untersuchungen und Prüfungen vor Ort nach nationalem Recht sowie ein Mechanismus für den Austausch einschlägiger Informationen über Aufsicht und Durchsetzung zwischen den zuständigen Behörden festgelegt werden. Ein solcher Mechanismus für den Austausch einschlägiger Informationen könnte auch den Zugang zu Cyberinformationen, der von den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 beantragt wird, beinhalten.

III.2. **Nationale Cybersicherheitsstrategie**

30. Jeder Mitgliedstaat muss gemäß Artikel 7 Absatz 1 der Richtlinie (EU) 2022/2555 eine nationale Cybersicherheitsstrategie aufstellen. Eine nationale Cybersicherheitsstrategie ist ein kohärenter Rahmen eines Mitgliedstaats, in dem strategische Ziele und Prioritäten im Bereich der Cybersicherheit und die zu ihrer Verwirklichung erforderliche Governance in diesem Mitgliedstaat festgelegt werden (siehe Artikel 6 Nummer 4 der Richtlinie (EU) 2022/2555). Die Cybersicherheitsstrategie muss unter anderem Ziele und Prioritäten enthalten, die insbesondere die in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Sektoren abdecken. Darüber hinaus muss diese Strategie einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten sowie die in Artikel 7 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Konzepte umfassen.

31. Außerdem sieht Artikel 7 Absatz 1 Buchstabe c der Richtlinie (EU) 2022/2555 vor, dass die nationale Cybersicherheitsstrategie einen Steuerungsrahmen umfassen muss, in dem die Aufgaben und Zuständigkeiten der jeweiligen Interessenträger auf nationaler Ebene klargestellt, die Zusammenarbeit und Koordinierung auf nationaler Ebene zwischen den nach der Richtlinie (EU) 2022/2555 zuständigen Behörden, zentralen Anlaufstellen und CSIRTs sowie die Koordinierung und Zusammenarbeit zwischen diesen Stellen und nach sektorspezifischen Rechtsakten der Union zuständigen Behörden untermauert werden.

32. Die Anforderung in Artikel 7 der Richtlinie (EU) 2022/2555, eine Cybersicherheitsstrategie aufzustellen, betrifft daher weder die Cybersicherheitsanforderungen, die wesentlichen und wichtigen Einrichtungen gemäß den Artikeln 21 und 23 der Richtlinie auferlegt werden, noch die Bestimmungen im Hinblick auf ihre Aufsicht und Durchsetzung gemäß Kapitel VII, wie in Artikel 4 Absätze 1 und 2 der Richtlinie vorgesehen. Die einschlägige Bestimmung des Artikels 7 sollte auf Sektoren, Teilsektoren und Arten von Einrichtungen Anwendung finden, für die sektorspezifische Rechtsakte der Union im Sinne des Artikels 4 der Richtlinie (EU) 2022/2555 bestehen.

III.3. **Benennung von CSIRTs**

33. Nach Artikel 10 Absatz 1 der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten ein oder mehrere CSIRTs benennen oder einrichten, die mindestens die in den Anhängen I und II der Richtlinie genannten Sektoren, Teilsektoren und Arten von Einrichtungen abdecken, d. h. auch die Sektoren, Teilsektoren und Arten von Einrichtungen, für die sektorspezifische Rechtsakte der Union bestehen. Die CSIRTs werden diesbezüglich in der Regel auch ihre Aufgaben gemäß Artikel 11 Absatz 3 der Richtlinie (EU) 2022/2555 wahrnehmen, es sei denn, in den sektorspezifischen Rechtsakten der Union sind besondere Aufgaben festgelegt.

III.4. **Nationale Rahmen für das Cyberkrisenmanagement und EU-CyCLONe**

34. Nach Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten eine oder mehrere Behörden für das Cyberkrisenmanagement benennen oder einrichten, die für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen zuständig sind. Nach Artikel 6 Nummer 7 der Richtlinie ist ein Cybersicherheitsvorfall großen Ausmaßes ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat. Nach Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 muss jeder Mitgliedstaat zudem einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen aufstellen, in dem die Ziele und Modalitäten für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen festgelegt werden. In diesem Plan sollten unter anderem die Verfahren für das Cyberkrisenmanagement, einschließlich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement und die Kanäle für den Informationsaustausch, sowie die einschlägigen öffentlichen und privaten Interessenträger und die betroffenen Infrastrukturen festgelegt werden. In diese Verfahren für das Cyberkrisenmanagement sowie die einschlägigen öffentlichen und privaten Interessenträger und Infrastrukturen könnten auch sektorspezifische Verfahren und Interessenträger einbezogen werden.

35. Durch Artikel 16 der Richtlinie (EU) 2022/2555 wird zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (*European Cyber Crises Liaison Organisation Network*, EU-CyCLONe) eingerichtet.

36. Da Artikel 9 über Rahmen für das Cyberkrisenmanagement und Artikel 16 über EU-CyCLONe weder die Cybersicherheitsanforderungen betreffen, die Einrichtungen gemäß den Artikeln 21 und 23 der Richtlinie (EU) 2022/2555 auferlegt werden, noch die Aufsicht und Durchsetzung gemäß Kapitel VII, wie in Artikel 4 Absätze 1 und 2 der Richtlinie vorgesehen, sollten die Artikel 9 und 16 in ihrer Gesamtheit für Sektoren gelten, auch wenn sektorspezifische Rechtsakte der Union im Sinne des Artikels 4 bestehen. Folglich müssen die Mitgliedstaaten eine oder mehrere Behörden für das Cyberkrisenmanagement benennen oder einrichten, die für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen in den Sektoren zuständig sind, die unter sektorspezifische Rechtsakte der Union fallen. Darüber hinaus sollten Sektoren, die unter sektorspezifische Rechtsakte der Union fallen, bei der Aufstellung des nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen nicht außer Acht gelassen werden. Schließlich sollte EU-CyCLONe seine in Artikel 16 der Richtlinie (EU) 2022/2555 festgelegten Aufgaben auch in Bezug auf Sektoren wahrnehmen, in denen für Einrichtungen sektorspezifische Rechtsakte der Union gelten.

III.5. **Ausschluss von der Anwendung des Artikels 3 Absätze 3 und 4, des Artikels 20 und des Artikels 27 Absätze 2 und 3**

37. Nach Artikel 3 Absatz 3 der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen und in den Anwendungsbereich der Richtlinie fallen, erstellen. Nach Artikel 27 Absatz 2 müssen die Mitgliedstaaten von den in Artikel 27 Absatz 1 der Richtlinie genannten Einrichtungen verlangen, dass sie den zuständigen Behörden bestimmte Angaben übermitteln. Da der Zweck dieser Bestimmungen darin besteht, einen klaren Überblick über die von der Richtlinie (EU) 2022/2555 erfassten Einrichtungen zu erlangen, um die Beaufsichtigung wesentlicher und wichtiger Einrichtungen, die in ihren Anwendungsbereich fallen, zu unterstützen, sollten diese Bestimmungen folglich nicht für Einrichtungen gelten, für die in Bezug auf das Risikomanagement und Meldepflichten im Bereich der Cybersicherheit ein sektorspezifischer Rechtsakt der Union gilt. Dies hindert die Mitgliedstaaten jedoch nicht daran, solche Einrichtungen in die Liste aufzunehmen.

Nach Artikel 20 Absatz 1 der Richtlinie (EU) 2022/2555 müssen die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung des Artikels 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können. Nach Artikel 20 Absatz 2 der Richtlinie müssen die Mitgliedstaaten dafür sorgen, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und wesentliche und wichtige Einrichtungen dazu anhalten, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben. Da die Verpflichtungen aus Artikel 20 der Richtlinie (EU) 2022/2555 untrennbar mit den Anforderungen des Artikels 21 der Richtlinie verbunden sind, sollte der Artikel 20 nicht für sektorspezifische Rechtsakte der Union im Sinne des Artikels 4 der Richtlinie gelten, die auf Anforderungen an das Cybersicherheitsrisikomanagement Anwendung finden.

ANLAGE

Sektorspezifische Rechtsakte der Union

Verordnung (EU) 2022/2554 (Verordnung über die digitale operationale Resilienz) ([1])

1. Artikel 1 Absatz 2 der Verordnung (EU) 2022/2554 (Verordnung über die digitale operationale Resilienz, DORA) sieht vor, dass in Bezug auf Finanzunternehmen, die unter die Richtlinie (EU) 2022/2555 und die entsprechenden nationalen Umsetzungsvorschriften fallen, für die Zwecke des Artikels 4 der Richtlinie (EU) 2022/2555 die Verordnung (EU) 2022/2554 als sektorspezifischer Rechtsakt der Union gilt. Diese Aussage spiegelt sich in Erwägungsgrund 28 der Richtlinie (EU) 2022/2555 wider, wonach die Verordnung über die digitale operationale Resilienz im Zusammenhang mit der Richtlinie (EU) 2022/2555 als sektorspezifischer Rechtsakt der Union in Bezug auf Finanzunternehmen betrachtet werden sollte. Folglich sollten die Bestimmungen der Verordnung (EU) 2022/2554, die sich auf das Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT) (Artikel 6 und folgende), das Management von IKT-bezogenen Vorfällen und insbesondere die Meldung von schwerwiegenden IKT-bezogenen Vorfällen (Artikel 17 und folgende) sowie die Prüfung der digitalen Betriebsstabilität (Artikel 24 und folgende), Vereinbarungen über den Informationsaustausch (Artikel 25) und Risiken durch IKT-Drittanbieter (Artikel 28 und folgende) beziehen, anstelle der Bestimmungen der Richtlinie (EU) 2022/2555 gelten. Die Mitgliedstaaten sollten daher die Bestimmungen der Richtlinie (EU) 2022/2555, die sich auf das Cybersicherheitsrisikomanagement und Meldepflichten sowie auf die Aufsicht und Durchsetzung beziehen, nicht auf Finanzunternehmen anwenden, die unter die Verordnung (EU) 2022/2554 fallen.

2. In dieser Hinsicht gelten Finanzunternehmen als Einrichtungen im Sinne des Artikels 2 Absatz 1 Buchstaben a bis t der Verordnung (EU) 2022/2554. Zu den Arten von Einrichtungen, die als Finanzunternehmen in den Anwendungsbereich der Verordnung (EU) 2022/2554 und gleichzeitig als wesentliche oder wichtige Einrichtungen in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallen, gehören Kreditinstitute, Handelsplätze und zentrale Gegenparteien. Da es wichtig ist, im Rahmen der Richtlinie (EU) 2022/2555 eine enge Beziehung zum Finanzsektor und den Informationsaustausch mit dem Finanzsektor aufrechtzuerhalten, können die Europäischen Aufsichtsbehörden und die nach der Verordnung (EU) 2022/2554 zuständigen Behörden die Beteilung an den Tätigkeiten der Kooperationsgruppe ([2]) beantragen und mit den zentralen Anlaufstellen sowie den CSIRTs und den nach der Richtlinie (EU) 2022/2555 zuständigen Behörden Informationen austauschen und zusammenarbeiten ([3]). Die nach der Verordnung (EU) 2022/2554 zuständigen Behörden sollten zudem Einzelheiten über schwerwiegende IKT-bezogene Vorfälle und gegebenenfalls über erhebliche Cyberbedrohungen auch im Rahmen der Richtlinie (EU) 2022/2555 an die CSIRTs, die zuständigen Behörden oder zentralen Anlaufstellen übermitteln. Dies kann durch den unmittelbaren Zugang zu Meldungen von Vorfällen und durch deren Weiterleitung – entweder direkt oder über eine zentrale Anlaufstelle – erfolgen. CSIRTs sollten in der Lage sein, den Finanzsektor bei ihren Tätigkeiten einzubeziehen ([4]). Die Mitgliedstaaten sollten den Finanzsektor weiterhin in ihre Cybersicherheitsstrategien einbeziehen. Die Bestimmungen über die nationalen Rahmen für das Cyberkrisenmanagement (Artikel 9 der Richtlinie (EU) 2022/2555) sowie über EU-CyCLONe (Artikel 16 der Richtlinie (EU) 2022/2555) sollten weiterhin für Einrichtungen gelten, die in den Anwendungsbereich der Verordnung (EU) 2022/2554 fallen.

([1]) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).

([2]) Artikel 14 Absatz 3 der Richtlinie (EU) 2022/2555 und Artikel 47 Absatz 1 der Verordnung (EU) 2022/2554.

([3]) Siehe Erwägungsgrund 28 der Richtlinie (EU) 2022/2555.

([4]) Ebenda.

IV

(Informationen)

INFORMATIONEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

RAT

Mitteilung an die Personen und Organisationen, die den Maßnahmen nach dem Beschluss 2011/235/GASP des Rates, durchgeführt durch den Durchführungsbeschluss (GASP) 2023/1780 des Rates, und der Verordnung (EU) Nr. 359/2011 des Rates, durchgeführt durch die Durchführungsverordnung (EU) 2023/1779 des Rates, über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in Iran unterliegen

(2023/C 328/03)

Den Personen und Organisationen, die im Anhang des Beschlusses 2011/235/GASP des Rates ([1]), durchgeführt durch den Durchführungsbeschluss (GASP) 2023/1780 des Rates ([2]), und in Anhang I der Verordnung (EU) Nr. 359/2011 des Rates ([3]), durchgeführt durch die Durchführungsverordnung (EU) 2023/1779 des Rates ([4]), über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in Iran aufgeführt sind, wird Folgendes mitgeteilt:

Der Rat der Europäischen Union hat beschlossen, dass diese Personen und Organisationen in die Liste der Personen und Organisationen aufgenommen werden sollten, die den im Beschluss 2011/235/GASP und in der Verordnung (EU) Nr. 359/2011 festgelegten restriktiven Maßnahmen unterliegen.

Die betroffenen Personen und Organisationen werden darauf hingewiesen, dass sie bei den zuständigen Behörden des bzw. der betreffenden Mitgliedstaaten (siehe Websites in Anhang II der Verordnung (EU) Nr. 359/2011) beantragen können, dass ihnen die Verwendung eingefrorener Gelder zur Deckung ihrer Grundbedürfnisse oder für bestimmte Zahlungen genehmigt wird (vgl. Artikel 4 der Verordnung).

Die betroffenen Personen und Organisationen können beim Rat vor dem 1. Januar 2024 unter Vorlage entsprechender Nachweise beantragen, dass der Beschluss, sie in die genannte Liste aufzunehmen, überprüft wird; entsprechende Anträge sind an folgende Anschrift zu richten:

Rat der Europäischen Union
Generalsekretariat
RELEX.1
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-Mail: sanctions@consilium.europa.eu

([1]) ABl. L 100 vom 14.4.2011, S. 51.
([2]) ABl. L 228 I vom 15.9.2023, S. 6.
([3]) ABl. L 100 vom 14.4.2011, S. 1.
([4]) ABl. L 228 I vom 15.9.2023, S. 1.

Die betroffenen Personen und Organisationen werden ferner darauf aufmerksam gemacht, dass sie den Beschluss des Rates unter den in Artikel 275 Absatz 2 und Artikel 263 Absätze 4 und 6 des Vertrags über die Arbeitsweise der Europäischen Union genannten Voraussetzungen vor dem Gericht der Europäischen Union anfechten können.

Mitteilung an die betroffenen Personen, die den restriktiven Maßnahmen nach dem Beschluss 2011/235/GASP des Rates und der Verordnung (EU) Nr. 359/2011 des Rates über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in Iran unterliegen

(2023/C 328/04)

Die betroffenen Personen werden gemäß Artikel 16 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([1]) auf Folgendes hingewiesen:

Rechtsgrundlagen für die Verarbeitung sind der Beschluss 2011/235/GASP des Rates ([2]), durchgeführt durch den Durchführungsbeschluss (GASP) 2023/1780 des Rates ([3]), und die Verordnung (EU) Nr. 359/2011 des Rates ([4]), durchgeführt durch die Durchführungsverordnung (EU) 2023/1779 des Rates ([5]).

Der für diese Verarbeitung Verantwortliche ist der Rat der Europäischen Union, vertreten durch den Generaldirektor der Generaldirektion Außenbeziehungen (RELEX) des Generalsekretariats des Rates, und die mit der Verarbeitung betraute Stelle ist das Referat RELEX.1, das unter folgender Anschrift kontaktiert werden kann:

Rat der Europäischen Union
Generalsekretariat
RELEX.1
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-Mail: sanctions@consilium.europa.eu

Der Datenschutzbeauftragte des Rates kann unter folgender Adresse kontaktiert werden:

Datenschutzbeauftragter

data.protection@consilium.europa.eu

Ziel der Verarbeitung ist die Erstellung und Aktualisierung der Liste der Personen, die gemäß dem Beschluss 2011/235/GASP, durchgeführt durch den Durchführungsbeschluss (GASP) 2023/1780, und der Verordnung (EU) Nr. 359/2011, durchgeführt durch die Durchführungsverordnung (EU) 2023/1779, restriktiven Maßnahmen unterliegen.

Die betroffenen Personen sind die natürlichen Personen, die die Kriterien für die Aufnahme in die Liste gemäß dem Beschluss 2011/235/GASP und der Verordnung (EU) Nr. 359/2011 erfüllen.

Die erhobenen personenbezogenen Daten umfassen die zur korrekten Identifizierung der betroffenen Person erforderlichen Daten sowie die Begründung für die Aufnahme in die Liste und andere diesbezügliche Daten.

Rechtsgrundlagen für die Verarbeitung personenbezogener Daten sind die gemäß Artikel 29 EUV erlassenen Beschlüsse des Rates und die gemäß Artikel 215 AEUV erlassenen Verordnungen des Rates, in denen natürliche Personen (betroffene Personen) benannt und das Einfrieren von Vermögenswerten und Reisebeschränkungen angeordnet werden.

Die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die gemäß Artikel 5 Absatz 1 Buchstabe a im öffentlichen Interesse liegt, und für die Erfüllung der rechtlichen Verpflichtungen aus den oben genannten Rechtsakten, denen der für die Verarbeitung Verantwortliche gemäß Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2018/1725 unterliegt.

Die Verarbeitung ist aus Gründen eines erheblichen öffentlichen Interesses gemäß Artikel 10 Absatz 2 Buchstabe g der Verordnung (EU) 2018/1725 erforderlich.

Der Rat kann personenbezogene Daten betroffener Personen von den Mitgliedstaaten und/oder dem Europäischen Auswärtigen Dienst erhalten. Empfänger der personenbezogenen Daten sind die Mitgliedstaaten, die Europäische Kommission und der Europäische Auswärtige Dienst.

([1]) ABl. L 295 vom 21.11.2018, S. 39.
([2]) ABl. L 100 vom 14.4.2011, S. 51.
([3]) ABl. L 228 I vom 15.9.2023, S. 6.
([4]) ABl. L 100 vom 14.4.2011, S. 1.
([5]) ABl. L 228 I vom 15.9.2023, S. 1.

Alle personenbezogenen Daten, die vom Rat im Rahmen autonomer restriktiver Maßnahmen der EU verarbeitet werden, werden für einen Zeitraum von fünf Jahren gespeichert, gerechnet ab dem Zeitpunkt, zu dem die betroffene Person von der Liste der Personen, deren Vermögenswerte eingefroren wurden, gestrichen wurde oder die Gültigkeit der Maßnahme abgelaufen ist, oder, wenn beim Gerichtshof Klage erhoben wird, bis ein rechtskräftiges Urteil ergangen ist. Personenbezogene Daten, die in beim Rat registrierten Dokumenten enthalten sind, werden vom Rat für im öffentlichen Interesse liegende Archivzwecke im Sinne von Artikel 4 Absatz 1 Buchstabe e der Verordnung (EU) 2018/1725 aufbewahrt.

Der Rat muss möglicherweise personenbezogene Daten über eine betroffene Person mit einem Drittland oder einer internationalen Organisation im Zusammenhang mit der Umsetzung der VN-Benennungen durch den Rat oder im Rahmen der internationalen Zusammenarbeit in Bezug auf die Politik der EU im Bereich der restriktiven Maßnahmen austauschen.

Falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, unterliegt die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation gemäß Artikel 50 der Verordnung (EU) 2018/1725 der bzw. den folgenden Bedingungen: Die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses erforderlich; die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Die Verarbeitung der personenbezogenen Daten der betroffenen Person erfolgt ohne automatisierte Entscheidungsfindung.

Die betroffenen Personen haben das Recht auf Information und das Recht auf Zugriff auf ihre personenbezogenen Daten. Sie haben außerdem das Recht, ihre Daten zu berichtigen und zu vervollständigen. Unter gewissen Umständen haben sie das Recht, eine Löschung ihrer personenbezogenen Daten zu erwirken, oder das Recht, gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen oder eine Einschränkung der Verarbeitung zu verlangen.

Betroffene Personen können diese Rechte ausüben, indem sie eine E-Mail an den für die Verarbeitung Verantwortlichen mit Kopie an den Datenschutzbeauftragten (siehe oben) senden.

Die betroffenen Personen müssen ihrem Antrag eine Kopie eines Ausweisdokuments zur Bestätigung ihrer Identität (Personalausweis oder Reisepass) beifügen. Dieses Dokument sollte eine Identifikationsnummer, das Ausstellungsland, die Gültigkeitsdauer, den Namen, die Anschrift und das Geburtsdatum enthalten. Alle anderen Angaben auf der Kopie des Ausweisdokuments, wie etwa das Foto oder andere persönliche Merkmale, können unkenntlich gemacht werden.

Betroffene Personen haben das Recht, gemäß der Verordnung (EU) 2018/1725 Beschwerde beim Europäischen Datenschutzbeauftragten (edps@edps.europa.eu) einzulegen.

Es wird empfohlen, dass die betroffenen Personen zunächst den für die Verarbeitung Verantwortlichen und/oder den Datenschutzbeauftragten des Rates kontaktieren und versuchen, auf diesem Weg Abhilfe zu schaffen.

EUROPÄISCHE KOMMISSION

Zusammenfassung von Beschlüssen der Europäischen Kommission über Zulassungen für das Inverkehrbringen zur Verwendung und/oder für eine Verwendung von Stoffen, die in Anhang XIV der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH) aufgeführt sind

(Veröffentlicht gemäß Artikel 64 Absatz 9 der Verordnung (EG) Nr. 1907/2006 ([1]))

(Text von Bedeutung für den EWR)

(2023/C 328/05)

Beschluss zum Widerruf einer Zulassung

Nummer des Beschlusses ([1])	Datum des Beschlusses	Bezeichnung des Stoffs	Adressat des Beschlusses	Widerrufene Verwendung	Aufgehobener Beschluss	Begründung des Beschlusses
C(2023) 6014	11. September 2023	Natriumdichromat, EG-Nr. 234-190-3, CAS-Nr. 10588-01-9 (wasserfrei) CAS-Nr. 7789-12-0 (Dihydrat)	Gruppo Colle S.r.l., Via G. Di Vittorio 3/5, 59025 Usella, Cantagallo, Prato, Italien	Als Beizmittel bei der Färbung von Wolle mit dunklen Farben	C(2017) 8331	Im Überprüfungsbericht wurde nicht nachgewiesen, dass es gemäß Artikel 60 Absatz 4 der Verordnung (EG) Nr. 1907/2006 für den Antragsteller keine geeigneten Alternativen gibt.

([1]) Der Beschluss kann auf der Website der Europäischen Kommission unter folgender Adresse abgerufen werden: Authorisation (europa.eu).

([1]) ABl. L 396 vom 30.12.2006, S. 1.

Euro-Wechselkurs [1]

15. September 2023

(2023/C 328/06)

1 Euro =

	Währung	Kurs		Währung	Kurs
USD	US-Dollar	1,0658	CAD	Kanadischer Dollar	1,4409
JPY	Japanischer Yen	157,50	HKD	Hongkong-Dollar	8,3416
DKK	Dänische Krone	7,4573	NZD	Neuseeländischer Dollar	1,8008
GBP	Pfund Sterling	0,85878	SGD	Singapur-Dollar	1,4524
SEK	Schwedische Krone	11,8730	KRW	Südkoreanischer Won	1 415,78
CHF	Schweizer Franken	0,9554	ZAR	Südafrikanischer Rand	20,2968
ISK	Isländische Krone	145,30	CNY	Chinesischer Renminbi Yuan	7,7561
NOK	Norwegische Krone	11,4220	IDR	Indonesische Rupiah	16 379,21
BGN	Bulgarischer Lew	1,9558	MYR	Malaysischer Ringgit	4,9922
CZK	Tschechische Krone	24,496	PHP	Philippinischer Peso	60,612
HUF	Ungarischer Forint	383,75	RUB	Russischer Rubel	
PLN	Polnischer Zloty	4,6308	THB	Thailändischer Baht	38,145
RON	Rumänischer Leu	4,9698	BRL	Brasilianischer Real	5,1860
TRY	Türkische Lira	28,7513	MXN	Mexikanischer Peso	18,2275
AUD	Australischer Dollar	1,6498	INR	Indische Rupie	88,6150

[1] *Quelle*: Von der Europäischen Zentralbank veröffentlichter Referenz-Wechselkurs.

V

(Bekanntmachungen)

VERFAHREN BEZÜGLICH DER DURCHFÜHRUNG DER WETTBEWERBSPOLITIK

EUROPÄISCHE KOMMISSION

Vorherige Anmeldung eines Zusammenschlusses

(Sache M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING)

Für das vereinfachte Verfahren infrage kommender Fall

(Text von Bedeutung für den EWR)

(2023/C 328/07)

1. Am 8. September 2023 ist die Anmeldung eines Zusammenschlusses nach Artikel 4 der Verordnung (EG) Nr. 139/2004 des Rates ([1]) bei der Kommission eingegangen.

Diese Anmeldung betrifft folgende Unternehmen:

— SAS C91 (Frankreich), kontrolliert von Électricité de France („EDF“, Frankreich),

— La Française Real Estate Managers („La Française“, Frankreich), kontrolliert von der Caisse Régionale Crédit Mutuel Nord Europe (Frankreich), die ihrerseits Mitglied der Crédit-Mutuel-Gruppe (Frankreich) ist,

— eine Immobilie in Ile-de-France („Gebäude“, Frankreich).

EDF und Crédit Mutuel werden im Sinne des Artikels 3 Absatz 1 Buchstabe b der Fusionskontrollverordnung die gemeinsame Kontrolle über das gesamte Gebäude übernehmen.

Der Zusammenschluss erfolgt durch Erwerb von Vermögenswerten.

2. Die beteiligten Unternehmen sind in folgenden Geschäftsbereichen tätig:

— EDF ist in Frankreich und im Ausland in den Bereichen Stromerzeugung und -großhandel, Stromübertragung, -verteilung und -versorgung, in der Erbringung anderer Dienstleistungen im Zusammenhang mit Strom und in geringerem Umfang in der Gasproduktion sowie im Groß- und Einzelhandel mit Gas tätig.

— Crédit Mutuel erbringt vor allem in Frankreich Bank- und Finanzdienstleistungen. Die Crédit-Mutuel-Gruppe bietet über ihre Tochtergesellschaft La Française Immobilienverwaltungsdienste an.

3. Das Gebäude ist eine Büro- und Handelsimmobilie in der Avenue de France 111 in 75013 Paris (Frankreich).

4. Die Kommission hat nach vorläufiger Prüfung festgestellt, dass das angemeldete Rechtsgeschäft unter die Fusionskontrollverordnung fallen könnte. Die endgültige Entscheidung zu diesem Punkt behält sie sich vor.

([1]) ABl. L 24 vom 29.1.2004, S. 1 („Fusionskontrollverordnung“).

Dieser Fall kommt für das vereinfachte Verfahren im Sinne der Bekanntmachung der Kommission über ein vereinfachtes Verfahren für bestimmte Zusammenschlüsse gemäß der Verordnung (EG) Nr. 139/2004 des Rates ([2]) infrage.

5. Alle betroffenen Dritten können bei der Kommission zu diesem Vorhaben Stellung nehmen.

Die Stellungnahmen müssen bei der Kommission spätestens 10 Tage nach dieser Veröffentlichung eingehen. Dabei ist stets folgendes Aktenzeichen anzugeben:

M.11239 – EDF / CREDIT MUTUEL / ILE-DE-FRANCE BUILDING

Die Stellungnahmen können der Kommission per E-Mail oder Post übermittelt werden, wobei folgende Kontaktangaben zu verwenden sind:

E-Mail: COMP-MERGER-REGISTRY@ec.europa.eu

Postanschrift:

Europäische Kommission
Generaldirektion Wettbewerb
Registratur Fusionskontrolle
Bruxelles/Brussel
BELGIQUE/BELGIË

([2]) ABl. C 366 vom 14.12.2013, S. 5.

ISSN 1977-088X (elektronische Ausgabe)
ISSN 1725-2407 (Papierausgabe)

Amt für Veröffentlichungen
der Europäischen Union
L-2985 Luxemburg
LUXEMBURG

DE