**Bundesrat** **Drucksache 45/21 (Beschluss)**

**05.03.21**

# Beschluss
**des Bundesrates**

---

## Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

**COM(2020) 823 final**

Der Bundesrat hat in seiner 1001. Sitzung am 5. März 2021 gemäß §§ 3 und 5 EUZBLG die folgende Stellungnahme beschlossen:

Allgemeines

1. Der Bundesrat begrüßt die Absicht der Kommission, die Resilienz und die Kapazitäten auf dem Gebiet der Cybersicherheit innerhalb der Union zu verbessern. Die fortschreitende Digitalisierung und Vernetzung bringt neue Cybersicherheitsrisiken mit sich, die nicht an Ländergrenzen haltmachen und nicht nur die einzelnen Mitgliedstaaten, sondern Europa insgesamt vor wachsende Herausforderungen stellen. Der Bundesrat teilt die Auffassung der Kommission, dass ein hohes gemeinsames Cybersicherheitsniveau eine wichtige Voraussetzung ist, um Europa für das digitale Zeitalter zu rüsten und eine zukunftsfähige Wirtschaft zu schaffen.

   Er begrüßt die grundsätzlich mit der vorgeschlagenen Richtlinie verfolgte Verbesserung der Sicherheit von Netz- und Informationssystemen durch eine noch bessere Zusammenarbeit der privaten und staatlichen Stellen.

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

2. Es ist allerdings fraglich, ob der Richtlinienvorschlag vollumfänglich von der allgemeinen Binnenmarktkompetenz des Artikels 114 AEUV gedeckt ist. So werden über Artikel 4 Absatz 23 des Richtlinienvorschlags nunmehr auch Teile der öffentlichen Verwaltung mit in den Anwendungsbereich der Richtlinie einbezogen. Aus dem Anhang I ergibt sich ferner, dass diese unter die Definition der „wesentlichen Einrichtungen“ im Sinne des Artikels 4 Absatz 25 des Richtlinienvorschlags fallen. Außerdem erstreckt sich der Geltungsbereich der vorgeschlagenen Richtlinie auf die Verwaltungsebenen des Bundes, der Landesverwaltungen (NUTS Level 1) sowie die Ebene der statistischen Regionen (NUTS Level 2).

3. Die Einbeziehung der „öffentlichen Verwaltung“ in den Anwendungsbereich der vorgeschlagenen Richtlinie wurde bereits im Verfahren zur Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (Richtlinie (EU) 2016/1148, vergleiche BR-Drucksache 92/13 (Beschluss)) kritisch betrachtet. Der Richtlinienvorschlag bezieht über Artikel 4 Absatz 23 und 25 sowie den Anhang I erhebliche Teile der öffentlichen Verwaltung in den Anwendungsbereich der vorgeschlagenen Richtlinie ein, ohne dass der Richtlinienvorschlag den hierzu erforderlichen Binnenmarktbezug begründen würde. Auf die Binnenmarktkompetenz aus Artikel 114 Absatz 1 AEUV kann eine Maßnahme nur gestützt werden, wenn sie objektiv der Verbesserung des Funktionierens des Binnenmarktes dient, indem Handelshemmnisse abgebaut oder Wettbewerbsverzerrungen beseitigt werden.

4. Die föderalen Strukturen einiger Mitgliedstaaten sind im weiteren Verfahren umfassend zu berücksichtigen. Sofern eine Einbeziehung der Verwaltungsebenen auf den NUTS Level 1 und 2 erfolgen soll, müssen das beabsichtigte Zusammenspiel aus Pflichten gegenüber Einrichtungen sowie Aufsicht und Durchsetzung der Vorgaben diese auch angemessen beachten. So sieht der Richtlinienvorschlag in Artikel 31 Absatz 6 zwar die Möglichkeit einer mitgliedstaatlichen Ausnahme dazu vor, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung im Sinne von Artikel 4 Absatz 23 des Richtlinienvorschlags, die den in der Richtlinie festgelegten Verpflichtungen unterliegen, Geldbußen verhängt werden können. Im Rahmen der Aufsicht und Durchsetzung fehlt es jedoch an einer solchen Klarstellung. Es muss sichergestellt werden, dass die föderale Kompetenzverteilung berücksichtigt wird und die Auf-

sichtsfunktionen im Kontext der föderalen Prinzipien auf den jeweiligen zuständigen Verwaltungsebenen verbleiben. Andernfalls stellt sich unweigerlich die Frage, wer diese Aufsicht in einem föderalen Staat durchführen soll, da eine Aufsicht auf Bundesebene im föderalen System verfassungsrechtlichen Bedenken begegnet.

5. Durch die signifikante Ausdehnung des Anwendungsbereichs der vorgeschlagenen Richtlinie werden für viele Unternehmen zusätzliche Belastungen entstehen. Dies kann die Wettbewerbsfähigkeit dieser Unternehmen nachhaltig negativ beeinträchtigen, insbesondere im Vergleich mit Unternehmen aus Drittstaaten. Aufwand und Nutzen von gesetzlich vorgeschriebenen Mindestanforderungen bei Cybersicherheitsmaßnahmen müssen daher gründlich abgewogen werden.

6. Der Bundesrat spricht sich dafür aus, dass gesetzlich vorgeschriebene, einheitliche Mindeststandards bei der Cybersicherheit für Unternehmen gelten sollten, die eine wesentliche Bedeutung für das staatliche Gemeinwesen oder für die Wirtschaft haben.

7. Die sektorale Ausdehnung auf „wichtige Einrichtungen“ und die Abschaffung sektorspezifischer Schwellenwerte werden aller Voraussicht nach dazu führen, dass zukünftig auch zahlreiche Unternehmen in den Anwendungsbereich der vorgeschlagenen Richtlinie fallen, die weder eine große Bedeutung für das staatliche Gemeinwesen oder die Versorgungssicherheit noch für die Wirtschaft oder einzelne Wirtschaftssektoren haben.

8. Der Bundesrat ist der Auffassung, dass gesetzlich auferlegte Cybersicherheitsanforderungen in einem angemessenen Verhältnis zu den möglichen Schäden und Beeinträchtigungen stehen sollten, die aufgrund eines Cybersicherheitsvorfalls in einem Unternehmen bei Dritten entstehen.

9. Er bezweifelt, dass die im Hinblick auf Risikomanagementanforderungen und Meldepflichten vorgesehene Gleichbehandlung von Unternehmen aus so unterschiedlichen (Teil-)Sektoren wie beispielsweise Energie und Trinkwasser („wesentliche Einrichtungen“) auf der einen sowie Maschinenbau und Herstellung elektrischer Ausrüstungen („wichtige Einrichtungen“) auf der anderen Seite dem Grundsatz der Verhältnismäßigkeit ausreichend Rechnung trägt.

10. Der Bundesrat bittet die Bundesregierung deshalb darum, im weiteren Verfahren darauf hinzuwirken, dass unverhältnismäßige Belastungen für einzelne Unternehmen oder bestimmte Branchen vermieden werden.

    Er bittet die Bundesregierung, hierbei insbesondere zu berücksichtigen, welche Vor- und Nachteile mit der Ausdehnung des Anwendungsbereichs auf weitere (Teil-)Sektoren, mit der Abschaffung sektorspezifischer Schwellenwerte und mit einer möglichen Differenzierung bei Risikomanagementanforderungen und Meldepflichten für „wesentliche“ und „wichtige Einrichtungen“ einhergehen könnten.

11. Der Bundesrat weist zudem darauf hin, dass neben der Verschärfung regulatorischer Vorgaben auch eine stärkere Unterstützung der Unternehmen maßgeblich dazu beitragen kann, das gemeinsame Cybersicherheitsniveau zu verbessern. Er bittet die Bundesregierung, sich für den weiteren Ausbau von Unterstützungsangeboten an die Wirtschaft sowie insbesondere an Kleine und Mittlere Unternehmen einzusetzen, wie etwa die Bereitstellung von aktuellen und wertvollen Informationen zur Cybersicherheitslage.

Zu einzelnen Vorschriften

Zu Artikel 4 Nummer 23

12. Der Bundesrat stellt zustimmend fest, dass durch die Begriffsbestimmung in Artikel 4 Nummer 23 des Richtlinienvorschlags „Einrichtungen der öffentlichen Verwaltung“, die Tätigkeiten in den Bereichen öffentliche Sicherheit, Strafverfolgung, Verteidigung oder nationale Sicherheit ausüben, vom Anwendungsbereich der vorgeschlagenen Richtlinie ausgenommen werden. Es handelt sich um den Kernbereich hoheitlichen Handelns, der auch auf anderen Gebieten des Unionsrechts den Mitgliedstaaten überlassen bleibt. Für die Gerichte ergibt sich ebenfalls kein Anwendungsbereich der vorgeschlagenen Richtlinie, da sie aufgrund ihrer institutionellen Unabhängigkeit eigenen Anforderungen an die Informationssicherheit unterliegen.

13. Der Bundesrat bittet, in Artikel 4 Nummer 23 des Richtlinienvorschlags ergänzend klarzustellen, dass im Kernbereich hoheitlichen Handelns nicht nur die Strafverfolgung, sondern auch die Strafvollstreckung (einschließlich des Justiz-

vollzugs) aus dem Anwendungsbereich der vorgeschlagenen Richtlinie ausgenommen sind.

Zu Artikel 29 Absatz 6 Satz 2 und Absatz 9 Satz 2

14. Der Bundesrat äußert Bedenken hinsichtlich der in Artikel 29 Absatz 6 Satz 2 des Richtlinienvorschlags enthaltenen Verpflichtung der Mitgliedstaaten, in den nationalen Rechtsordnungen sicherzustellen, dass „eine natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt," für Pflichtverstöße haftbar gemacht werden kann. Die Haftung natürlicher Personen steht im Widerspruch zu den Grundsätzen der nationalen Rechtsordnungen, die bei Pflichtverletzungen in Ausübung dienstlich oder betrieblich veranlasster Tätigkeiten Haftungseinschränkungen zugunsten von Beamtinnen und Beamten, Arbeitnehmerinnen und Arbeitnehmern sowie Beschäftigen vorsehen. So enthält das deutsche Recht etwa für den öffentlichen Dienst in § 839 BGB in Verbindung mit Artikel 34 Grundgesetz eine vorrangige Sonderregelung, die in ihrem Anwendungsbereich andere Haftungsnormen verdrängt und stattdessen eine Staatshaftung begründet. Arbeitnehmerinnen und Arbeitnehmern kann gegenüber ihrem Dienstherrn ein Freistellungsanspruch zustehen. Diese aus dem Gedanken der Fürsorgepflicht erwachsenen Grundsätze müssen unangetastet bleiben, so dass Artikel 29 Absatz 6 Satz 2 des Richtlinienvorschlags in dieser Form keinen Eingang in die vorgeschlagene Richtlinie finden sollte.

15. Die Regelung des Artikels 29 Absatz 6 Satz 2 des Richtlinienvorschlags begegnet in ihrer Weite rechtlichen Bedenken, da eine Verpflichtung der Mitgliedstaaten, eine Haftung der natürlichen Personen vorzusehen, als Verpflichtung zur Einführung einer Durchgriffshaftung gegen die Geschäftsleitung und andere Beschäftige von Einrichtungen und Unternehmen (Haftung im Außenverhältnis zu Dritten) zu verstehen sein könnte. Eine solche Außenhaftung für Pflichtverletzungen nach der Richtlinie würde den gesellschaftsrechtlichen und zivilrechtlichen Trennungsgrundsätzen der deutschen Rechtsordnung widersprechen und auch mit den Grundgedanken des europäischen Gesellschaftsrechts nicht in Einklang stehen.

16. Der Bundesrat weist darauf hin, dass die Voraussetzungen einer Haftung der Geschäftsleitung oder anderer natürlicher Personen in Artikel 26 Absatz 9 Satz 2 des Richtlinienvorschlags bislang konturenlos sind. Eine persönliche Haftung an jede Pflichtverletzung zu knüpfen, die der betroffenen Einrichtung obliegt, wäre unverhältnismäßig. Außerdem wäre auf allgemeine Grundsätze, unter denen die Geschäftsleitung gegenüber einer Einrichtung im Innenverhältnis haftet, Rücksicht zu nehmen (vergleiche etwa § 93 Absatz 1 und Absatz 2 Satz 1 AktG).