WIRTSCHAFTSPRÜFERKAMMER
Körperschaft des öffentlichen Rechts

www.wpk.de/oeffentlichkeit/stellungnahmen/

Stellungnahme zum Vorschlag der EU-Kommission für eine Verordnung zur Cyberresilienz im Finanzsektor (COM/2020/595 final) sowie zum Vorschlag für eine Richtlinie zur Änderung der Abschlussprüferrichtlinie (COM/2020/596 final)

Die WPK hat mit Schreiben vom 15. Oktober 2020 gegenüber dem Bundesministerium der Finanzen zum Vorschlag der EU-Kommission für eine Verordnung zur Cyberresilienz im Finanzsektor (COM/2020/595 final) sowie zum Vorschlag für eine Richtlinie zur Änderung der Abschlussprüferrichtlinie (COM/2020/596 final) wie nachfolgend wiedergegeben Stellung genommen.

Die Wirtschaftsprüferkammer ist eine Körperschaft des öffentlichen Rechts, deren Mitglieder alle Wirtschaftsprüfer, vereidigten Buchprüfer, Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften in Deutschland sind. Die Wirtschaftsprüferkammer hat ihren Sitz in Berlin und ist für ihre über 21.000 Mitglieder bundesweit zuständig. Ihre gesetzlich definierten Aufgaben sind unter www.wpk.de ausführlich beschrieben. Die Wirtschaftsprüferkammer ist im Transparenzregister der Europäischen Kommission unter der Nummer 025461722574-14 eingetragen.

– – –

Die WPK unterstützt grundsätzlich die in den Erwägungsgründen dargestellten Ziele des Entwurfs der Cyberresilienz-Verordnung: Ein harmonisiertes und weitgespanntes Rahmenkonzept für die Widerstandsfähigkeit von Informations- und Kommunikationssystemen für Finanzinstitute auf Unionsebene zu schaffen, sowie internationale Drittanbieter unter die direkte Aufsicht der Europäischen Aufsichtsbehörden zu stellen.

Zugleich sind wir der Auffassung, dass der vorgesehen Pflichtenkatalog und das Vorhalten eines Risikomanagementsystems für die Cyberresilienz einen enormen bürokratischen wie auch finanziellen Mehraufwand für die unter den Oberbegriff „Finanzinstitute“ gefassten Gruppen, hierin auch Abschlussprüfer und Prüfungsgesellschaften, bedeutet. Ein Übermaß an Regularien und Vorschriften kann zur einer „Überforderung“ der Verpflichteten führen und Markverwerfungen hervorrufen.

Zusammenfassend lauten unsere wesentlichen Anmerkungen zum Verordnungsvorschlag zur Cyberresilienz wie folgt:

- Abschlussprüfer (statutory auditors) und Prüfungsgesellschaften (audit firms) müssen aus dem Anwendungsbereich des Verordnungsvorschlags zur Cyberresilienz ausgenommen werden.
- Die Bestrebungen der EU-Kommission, die Cyberresilienz für Finanzinstitute auf Unionsebene zu harmonisieren, verstehen wir und können diese nachvollziehen.

Unsere Anmerkungen im Einzelnen

Unsere nachfolgenden Anmerkungen orientieren sich am Aufbau des Vorschlags der EU-Kommission vom 24. September 2020. Wir würden es begrüßen, wenn unsere Anregungen während der deutschen Ratspräsidentschaft Berücksichtigung fänden.

1. **Streichung von „statutory auditors“ und „audit firms“ (Artikel 2 Nr. 1 Buchstabe (q) des Verordnungsvorschlags)**

Der Vorschlag der EU-Kommission, eine Harmonisierung der Cyberresilienz von Finanzinstituten auf Unionsebene voranzutreiben und das verpflichtende Betreiben eines vereinheitlichten Risikomanagementsystems für Datenverarbeitungssystemen zur Stärkung der Cyberresilienz, erscheint uns nachvollziehbar.

Nicht nachvollziehbar ist, weshalb Abschlussprüfer (statutory auditors) und Prüfungsgesellschaften (audit firms) unter die in Artikel 2 des Vorschlags gewählte Definition der „Finanzinstitute“ einbezogen werden (Artikel 2 Nr. 1 Buchstabe (q) des Vorschlags) und damit dem umfassenden Pflichtenkatalog unterworfen werden müssen.

Der deutsche Berufsstand der Wirtschaftsprüfer und vereidigten Buchprüfer in seiner Rolle als gesetzliche Abschlussprüfer, wie auch insgesamt alle europäischen Abschlussprüfer und Prüfungsgesellschaften, leisten einen wichtigen Beitrag für das europäische Finanzsystem, in dem die Jahres- und Konzernabschlüsse sowie die spezifischen regulatorischen Anforderungen an diese Branche jährlich geprüft werden.

Es sollte hierbei allerdings beachtet werden, dass Abschlussprüfer und Prüfungsgesellschaften nicht Teil des europäischen Finanzsystems sind. Der Verordnungsvorschlag zielt darauf ab, die Cybersicherheit von Geld- und Zahlungsströmen sicherzustellen und zu erhöhen, was angesichts der zunehmenden Digitalisierung nachzuvollziehen ist. Denn Finanzinstitute, wie die genannten Kreditinstitute, Zahlungsabwickler, E-Geld-Institute, Investmentfirmen, Krypro-Asset-Provider usw. sind von Natur aus einem erhöhten Risiko von Cyberattacken ausgesetzt.

Abschlussprüfer und Prüfungsgesellschaften sind jedoch nicht Teil dieses Finanzsystems – sie steuern keine Zahlungs- oder Geldströme und führen keine Transaktionen aus, vergeben keine Kredite oder schließen Versicherungspolicen ab, sprich: **sind in der Finanzbranche operativ nicht tätig**. Ihre Aufgabe als Abschlussprüfer ist es, die Rechnungslegungswerke der Finanzinstitute (Konzern- und Jahresabschlüsse) auf deren Konformität mit den Rechnungslegungsregeln (in Deutschland: Handelsgesetzbuch) zu überprüfen. Insoweit ist es auch nicht gerechtfertigt, sie dem geplanten Pflichtenkanon für die Finanzbranche zu unterwerfen.

Rein vorsorglich, für den Fall, dass vorgebracht werden sollte, dass die Einbeziehung von Abschlussprüfer und Prüfungsgesellschaften wegen des Geschäftsgeheimnisschutzes gerechtfertigt sein könnte:

In Deutschland werden die Geschäftsgeheimnisse (auch) von Finanzinstituten strafrechtlich durch § 203 Abs. 1 Nr. 3 StGB gesichert. Berufsrechtlich wird dies flankiert durch die Berufspflicht, seinen Beruf verschwiegenen auszuüben (§ 43 Abs. 1 Satz 1 WPO, §§ 10, 11 Berufssatzung für WP/vBP); dies wird auch berufsaufsichtlich von der Wirtschaftsprüferkammer und im Fall eines Prüfers eines Unternehmens von öffentlichem Interesse von der Abschlussprüferaufsichtsstelle beim Bundesamt für Wirtschaft und Ausfuhrkontrolle verfolgt.

Petitum:

Abschlussprüfer (statutory auditors) und Prüfungsgesellschaften (audit firms) müssen aus dem Anwendungsbereich des Verordnungsvorschlags zur Cyberresilienz ausgenommen werden (Streichung des Artikel 2 Nr. 1 Buchstabe (q) des Vorschlags).

2. Unzumutbare Belastung auch für kleine und mittlere Praxen

Der Verordnungsvorschlag sieht vor, dass alle unter dem Oberbegriff „Finanzinstitute“ genannten Akteure dazu verpflichtet sind, entsprechend dokumentierbare Risikomanagementsysteme mit vorgegebenen Rahmenbedingungen für sämtliche verwendeten Datenverarbeitungssysteme, auch jene von Drittanbietern, vorzuhalten. Hinzu kommen umfangreiche Verpflichtungen zur Nutzung, Identifikation von Risiken, Schutz- und Vorbeugemaßnahmen, Anzeigepflichten

bei Cyberangriffen sowie die Risikobewertung von Datenverarbeitungssystemen von Drittanbietern.

Zwar werden im Verordnungsvorschlag Teile dieses Pflichtenkatalogs für sogenannte „micro-enterprise“ (Kleinstunternehmen, sowie kleine und mittlere Unternehmen nach der Richtlinie 2003/361/EU) ausgenommen.

Dennoch werden durch den entstehenden Pflichtenkatalog auch für kleine und mittlere Prüferpraxen hohe bürokratische und finanzielle Bürden aufgebaut. Dies stellt eine weitere **Markteintrittsschranke** für den Markt der gesetzlichen Abschlussprüfungen dar, nachdem der Gesetzgeber gerade erst im Jahr 2014 die Abschlussprüferrichtlinie novelliert hat (Abschlussprüfer-RL 2006/43, Änderungs-RL 2014/56/EU) und eine Verordnung über die spezifischen Anforderungen an die Abschlussprüfung bei Unternehmen von öffentlichen Interesse verabschiedet hat (Verordnung (EU) Nr. 537/2014). Die Erfahrungen mit den erhöhten regulatorischen Anforderungen im Bereich der Prüfer von Unternehmen von öffentlichen Interesse (Banken, Versicherungen und kapitalmarktorientierte Unternehmen) zeigen, dass dies zu einer **Reduzierung des Prüferpools** und damit zu einer **Marktkonzentration bei den Prüfern** führt (2015: 91, 2016: 86, 2017: 71, 2018: 71):
Der Großteil der gesetzlichen Abschlussprüfungen, also nicht die Prüfung von Unternehmen von öffentlichem Interesse, werden von Einzel-Wirtschaftsprüfern oder kleineren Prüferpraxen durchgeführt. In der Regel werden drei bis fünf Abschlussprüfungen pro Jahr durchgeführt, wobei das Hauptgeschäft in der Steuerberatung und/oder Wirtschaftsberatung liegt. Verbleibt es bei der Einbeziehung von Abschlussprüfern in den Anwendungsbereich der Verordnung, führt dies zu zusätzlichen Kosten für die Einhaltung der Pflichten. Diese können nicht an den Mandanten weitergegeben werden, da diese nicht bereit sind, für eine Pflicht-Abschlussprüfung höhere Honorare zu zahlen. Dies hat zur Folge, dass vor allem zahlreiche kleinere Prüferpraxen aus dem Markt der gesetzlichen Abschlussprüfungen gedrängt werden. Dies führt zu einer weiteren Marktkonzentration.

Petitum:

Auch der in einigen wenigen Teilen reduzierte Pflichtenkatalog für kleine und mittlere Praxen von Wirtschaftsprüfern/vereidigten Buchprüfern in ihrer Funktion als Abschlussprüfer führt im Ergebnis zu unzumutbaren Belastungen, so dass im Ergebnis alle Abschlussprüfer und Prüfungsgesellschaften von dem Verordnungsvorschlag ausgenommen werden müssen.

3. Änderung der Abschlussprüferrichtlinie fallen lassen

Die Änderung von Artikel 24a Abs. 1 Buchstabe b der Abschlussprüferrichtlinie (2006/43/EG) durch den Richtlinienvorschlag der EU-Kommission (COM/2020/596 final) sieht vor, Abschlussprüfer und Prüfungsgesellschaften zu verpflichten, die bereits bestehende interne Organisation von entsprechend verwendeten Datenverarbeitungssystemen, nunmehr den Anforderungen des Artikel 6 des Verordnungsvorschlages der EU-Kommission zur Cyberresilienz im Finanzsektor zu unterwerfen.

Artikel 24a der AP-RL setzt bereits einen hohen internen Kontroll- und Sicherheitsstandard an Abschlussprüfer und Prüfungsgesellschaften für die Verwendung von Datenverarbeitungssystemen. Eine weitere Vergrößerung des Anforderungskatalogs ist aus unserer Sicht nicht notwendig, sondern führt nur zu einer Mehrbelastung, bürokratischer und finanzieller Natur und würde die bereits oben beschriebenen Folgen mit sich bringen. Artikel 6 des Verordnungsvorschlages der EU-Kommission zur Cyberresilienz ist mit seinem Pflichtenkatalog ersichtlich auf Datenverarbeitungssysteme von Finanzinstituten ausgerichtet, möchte deren Funktionsfähigkeit sowie die Geld- und Zahlungsströme sowie durchgeführte Transaktionen sichern. Wie bereits ausgeführt, sind Abschlussprüfer und Prüfungsgesellschafen hierin nicht involviert.

Petitum:

Fallenlassen des Änderungsvorschlags der Abschlussprüferrichtlinie.

– – –

Wir würden uns freuen, wenn unsere Anregungen im weiteren Verfahren berücksichtigt werden. Inhaltlich haben wir unsere Ausführungen auf Fragestellungen beschränkt, die die berufliche Stellung und Funktion unserer Mitglieder betreffen.

– – –