www.betriebs-berater.de

Betriebs Berater

BB

39|2025

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

22.9.2025 | 80. Jg.
Seiten 2177–2240

BB-Rechtsprechungsreport zur Besteuerung der Kapitaleinkünfte 2025 – Teil II

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dr. Kristina Schreiber, RAin, Partnerin bei Loschelder Rechtsanwälte, Köln. Sie berät Unternehmen in allen Fragen zum IT- und Datenrecht mit einem Fokus auf den neuen EU-Digitalrechtsakten von der Cybersicherheit bis zur Künstlichen Intelligenz.

Neues IT-Sicherheitsrecht in Deutschland: Nach Slalomfahrt auf der Zielgeraden!

Mit der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) sollte spätestens bis 17.10.2024 ein neues IT-Sicherheitsrecht für rund 30 000 Unternehmen in Deutschland gelten. Die Umsetzung ins nationale Recht ist bis heute nicht geschafft. Aber: Wir sind auf die Zielgerade eingebogen. Ende Juli 2025 hat das BMI den Regierungsentwurf veröffentlicht (BMI, Meldung vom 24.7.2025), der jetzt noch das parlamentarische Verfahren durchlaufen muss. Ziel ist die Gesetzesverkündung bis Ende des Jahres. So könnte Schlimmeres in dem von der Kommission schon vor Monaten eingeleiteten Vertragsverletzungsverfahren vermieden werden.

Deutschland zieht endlich mit in der EU-rechtlich vorgegebenen Cybersicherheitswende, aber statt 1:1-Umsetzung regiert der bürokratische Sonderweg mit Unsicherheiten und Flickenteppichen.

Für Unternehmen wird es ernst: Spätestens jetzt ist es Zeit zu klären, ob die eigene Einheit vom Anwendungsbereich erfasst ist – immerhin werden gegenüber der bisherigen KRITIS-Regulierung über 25 000 weitere Unternehmen erstmalig gesetzlich zu einer angemessenen IT-Sicherheit auch außerhalb der Verarbeitung personenbezogener Daten verpflichtet. Ist ein Unternehmen von den NIS-2-Pflichten adressiert, müssen zeitnah ein angemessenes Risikomanagement einschließlich der notwendigen Dokumentation implementiert und die geforderten Geschäftsleiterpflichten und -schulungen umgesetzt werden. Denn eine Übergangsfrist wird es nach Verkündung des deutschen Umsetzungsgesetzes nicht geben.

Die NIS-2-Richtlinie verfolgt das Ziel, das Sicherheitsniveau von Netz- und Informationssystemen in der EU anzugleichen und Kaskadeneffekte aus Cyberangriffen zu vermeiden. Sie zielt bewusst auf eine klare, sektorübergreifende Systematik, gestützt auf Mindeststandards, Meldepflichten und abgestufte Aufsicht für „wesentliche" und „wichtige Einrichtungen".

Um Unternehmen auch tatsächlich zu verpflichten, muss die EU-Richtlinie zunächst ins nationale Recht umgesetzt werden. Eine unmittelbare Wirkung der Richtlinie kommt nicht in Betracht. Grundsätzlich verfolgt das BMI dabei zwar eine 1:1-Umsetzung der NIS-2-Richtlinie, die als Mindestharmonisierung auch strengere nationale Regelungen erlauben würde. Bei genauerer Betrachtung enthält der Regierungsentwurf zur NIS-2-Umsetzung aber für die Praxis höchst relevante Abweichungen von den Richtlinienvorgaben, die gut gemeint, aber nicht gut gemacht sind.

Allen voran zu nennen sind eine EU-rechtlich kritische Ausnahme vom Anwendungsbereich im Regierungsentwurf und eine unklare Erweiterung der Geschäftsleitungspflichten:

1. Der Anwendungsbereich der NIS-2-Richtlinie ist weit. Nach dem Richtlinientext können Unternehmen unter Umständen schon durch den Betrieb einer lokalen Photovoltaik-Anlage in den Anwendungsbereich gelangen, da sie dadurch zum Stromproduzenten werden. Dem will der deutsche Gesetzgeber mit § 28 Abs. 3 BSIG RegE entgegentreten. Das ist zu begrüßen, es hilft aber nur bei EU-rechtskonformer Umsetzung. Bei einem EU-Rechtsverstoß wäre die nationale Regelung unanwendbar. Über dieses Risiko hinaus ist der Vorschlag im Regierungsentwurf auch noch völlig unklar. Er wird in der Praxis auch deshalb letztlich mit unkalkulierbaren Risiken behaftet sein: „Bei der Zuordnung … können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind", heißt es in § 28 Abs. 3 BSIG RegE. Was aber ist „vernachlässigbar"? Laut Entwurfsbegründung sind das geringfügige Nebentätigkeiten, was etwa anhand der Anzahl der im Bereich tätigen Mitarbeiter, dem dadurch erzielten Umsatz oder der Nennung im Gesellschaftervertrag ermittelt werden soll. Klare Grenzen sind dem Entwurf jedoch nicht zu entnehmen, sodass das Bewertungsrisiko vollständig beim Unternehmen selbst liegt.
2. Eine weitere Herausforderung birgt der Regierungsentwurf für die Leitungsebene des Unternehmens: Diese behält die Letztverantwortung für eine angemessene IT-Sicherheit. Sie muss, so die NIS-2-Richtlinie, die Risikomanagementmaßnahmen billigen und ihre Umsetzung überwachen. Dies sind klassische Leitungsaufgaben; das Management muss die Zügel in der Hand halten. Das Umsetzungsgesetz aber verlangt in § 38 Abs. 1 BSIG RegE nun, dass die Leitungsebene die Risikomanagementmaßnahmen „umsetzt" und diese Umsetzung zugleich überwacht. Dies ist in der Kombination misslungen und wird den Managementpflichten nicht gerecht: Die Leitungsebene sollte nicht selbst operativ umsetzen, sondern die Maßnahmen aus dem Informationssicherheitsteam kontrollieren, plausibilisieren und insofern eben „billigen". Das setzt der Regierungsentwurf im Wortlaut des § 38 Abs. 1 BSIG RegE nicht um, die Entwurfsbegründung nimmt aber doch wieder Bezug auf ein „billigen". Das bringt vermeidbare Rechtsunsicherheit.

Insgesamt bleibt zu hoffen, dass die Umsetzung im parlamentarischen Verfahren (BT-Drs. 21/1501) jetzt zügig und mit einer Präzisierung für mehr Rechtssicherheit erfolgt. Zum Inkrafttreten des Gesetzes sollten dann für die nach NIS-2 verpflichtende Registrierung aller Adressaten und Meldungen von erheblichen Sicherheitsvorfällen operativ einfach und sicher handhabbare Onlineportale zur Verfügung stehen, um das neue Recht auch administrativ mit Leben zu füllen.