IT-Sicherheit als Mangel: Neue Pflichten für Softwarehersteller

Die EU-Kommission hat kürzlich den Entwurf eines Cyber Resilience Act (CRA) veröffentlicht. Sie verspricht sich eine höhere Cybersicherheit insbesondere durch besseres Produktdesign. Diese Anforderungen bergen jedoch etliche Schwierigkeiten für Softwarehersteller und -anbieter. Sie müssen zudem bei Missachtung der Anforderungen ein strenges Sanktionsregime fürchten, wenn der CRA so umgesetzt wird.

Der CRA ist Teil der Digitalstrategie der EU. Er soll in Ergänzung des Cybersecurity Act digitale Produkte auf dem europäischen Markt sicherer und damit die Wirtschaft insgesamt weniger anfällig für Cyberattacken machen. Dabei sollen Hersteller von Software („materieller und immaterieller digitaler Produkte“) einheitlichen Cybersicherheitsregeln für ihre Produkte unterworfen werden.

Konkret soll Cyberkriminalität entgegengewirkt werden, die allein 2021 weltweit Schäden von etwa 5 Billionen Euro angerichtet hat. Die EU sieht zwei zentrale Problemfelder: Fehlendes Wissen und Informationen über die sichere Verwendung von digitalen Produkten durch die Nutzer, aber auch unzureichende Cybersicherheit, die bereits von dem Design der Produkte selbst ausgeht.

Letzteres soll durch den CRA in Angriff genommen werden. Für Hersteller steigen die regulatorischen Anforderungen damit erheblich – von der DSGVO sind sie regelmäßig nicht direkt adressiert. Mit dem CRA wird auch insofern ein weitreichendes Sanktionsregime Einzug halten.

Erhöhte Cybersicherheit durch Produktdesign

Die Hersteller, Importeure und Händler von Software sollen nach dem Entwurf des CRA für die Lebensdauer des Produkts dessen Cybersicherheit gewährleisten und für etwaige Sicherheitslücken haften („Security by Design“). Diskutiert wird eine Begrenzung

dieser sog. „Nachmarktpflicht“ auf einen Zeitraum von fünf Jahren nach dem Inverkehrbringen des Produkts.

Aus der DSGVO bekanntes Sanktionsregime

Der CRA-Entwurf bestimmt, dass Sanktionen „wirksam, verhältnismäßig und abschreckend“ sein sollen (Art. 53). Bei entsprechenden Verstößen sind denn auch Bußgelder in Höhe von bis zu 15 Millionen Euro oder 2,5% des gesamten weltweiten Umsatzes des sanktionierten Unternehmens vorgesehen (die höhere Grenze gilt).

Einbindung des CRA-Entwurfs in das New Legislative Framework

Der CRA-Entwurf fügt sich in das sog. New Legislative Framework (NLF) der EU ein. NLF bezeichnet ein EU-Harmonisierungskonzept mit einheitlichen Rahmenregelungen für den freien Warenverkehr unter besonderer Berücksichtigung der Produktsicherheit. Über das NLF werden Begriffe und rechtliche Rahmenbedingungen vereinheitlicht. Dies zeigt sich auch im CRA-Entwurf. Dies erleichtert den Normverpflichteten Verständnis und Umsetzung der Regelungen.

Gute Ansätze weiterentwickeln

Im aktuell vorliegenden Entwurf des CRA sind denn bereits überzeugende Ansätze enthalten, die indes noch weiterzuentwickeln sind: So bleibt z.B. die Einteilung in „critical“ und „highly critical products“ denkbar pauschal und holzschnittartig, ohne ausreichend den Verwendungszweck einzubeziehen. Auch ist die zu begrüßende EU-Konformitätserklärung für „sichere Produkte“ nicht ausgereift: Es fehlt noch an Regelungen zu den dafür notwendigen harmonisierten Normen, wann ein Produkt entsprechend sicher ist.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de