Aktuelle Entwicklungen im IT-Sicherheitsrecht

Die EU-Cyberstrategie kommt immer mehr zum Tragen: Am 06.03.2026 endete die Registrierungsfrist für NIS-2-Adressaten (Spoiler: rund 2/3 der adressierten Unternehmen haben sich dennoch noch nicht registriert), am 17.03.2026 ist das KRITIS-Dachgesetz in Kraft getreten und das Durchführungsgesetz zum Cyber Resilience Act ist vor Kurzem als Referentenentwurf vorgelegt worden. Anlass genug für ein aktuelles Update.

Die EU verschärft die Regulierung der Cybersicherheit, um die EU resilienter aufzustellen. Rund 30.000 Unternehmen werden von den Neuregelungen im BSIG erfasst, das in Umsetzung der NIS-2-Richtlinie novelliert wurde und seit wenigen Tagen umfassend greift. Für die knapp 5.000 KRITIS-Anlagenbetreiber in Deutschland gelten zudem ab dem 17.03.2026 die vornehmlich ergänzenden Anforderungen des KRITIS-Dachgesetzes, fokussiert auf die physische Sicherheit. Ab Herbst 2027 sind überdies digitale Produkte besonders sicher zu gestalten, im Einklang mit dem Cyber Resilience Act, zu dem aktuell das nationale Durchführungsgesetz beraten wird.

BSIG und NIS-2-Richtlinie

Zum 06.12.2025 ist das novellierte BSIG in Kraft getreten. Drei Monate später, am 06.03.2026, endete die Registrierungsfrist. Alle rund 30.000 erfassten Unternehmen müssten mithin nunmehr registriert sein – laut Presseberichterstattung waren am 09.03.2026 aber nur rund 11.000 Unternehmen tatsächlich registriert.

Wichtig ist für all jene, die adressiert sind, aber die Registrierung noch nicht vorgenommen haben, dies nunmehr aktiv anzugehen. Es ist nicht zu erwarten, dass überschaubare Fristversäumnisse in Bußgeldverfahren enden, auch wenn dies theoretisch möglich wäre. Regulatorisch kritisch – mit Bußgeldrisiken – kann es aber dann werden, wenn die Registrierung ganz unterbleibt und erst etwa im Rahmen eines Cyberincidents offenbar wird, dass trotz Adressatenstellung Pflichten aus dem BSIG nicht eingehalten wurden.

Angesichts dessen sollten Unternehmen, soweit nicht bereits geschehen, sorgfältig ihre Betroffenheit prüfen und sich dann aktiv für oder – dokumentiert – gegen eine Registrierung entscheiden. Wir führen seit geraumer Zeit unzählige Betroffenheitsanalysen durch und sehen häufig, dass Unternehmen von einem -positiven – Ergebnis überrascht sind. Grund dafür ist die enorm weite Anwendbarkeit der Pflichten, die nicht nur auf kritische Infrastrukturen begrenzt sind und meist sogar schon dann greifen, wenn in einer Unternehmensgruppe ein IT-Shared Service für andere Gruppenunternehmen erbracht wird.

Unternehmen, die vom BSIG erfasst sind, müssen sich registrieren, erhebliche Sicherheitsvorfälle melden und nach § 38 Abs. 3 BSIG die Geschäftsleiter schulen: Ein erprobtes Schulungsprogramm bietet Loschelder etwa in Kooperation mit Wessing&Partner und der Bitkom Akademie an: NIS-2 Geschäftsleiterschulung nach aktuellen BSI-Empfehlungen | Bitkom Akademie

Materiell muss ein angemessenes Cyberrisikomanagement implementiert werden. Dies ist das Herzstück des BSIG – letztlich aber auch für nicht-BSIG-Adressaten verpflichtend, aus Art. 32 DSGVO für personenbezogene Daten und aufgrund der aktuellen Bedrohungslage als allgemeine Geschäftsführungspflicht zur Abwehr von Schäden von der eigenen Gesellschaft.

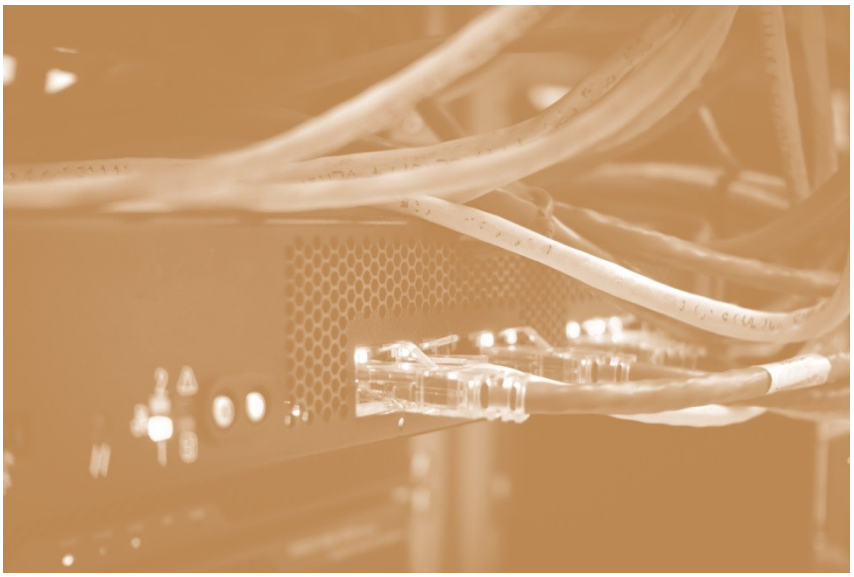
KRITIS-Dachgesetz und CER-Richtlinie

Ergänzend zur NIS-2-Richtlinie und dem BSIG ist am 17.03.2026 das KRITIS-Dachgesetz in Umsetzung der CER-Richtlinie in Kraft getreten. Das Gesetz fokussiert sich auf die physische Sicherheit kritischer Anlagen und ergänzt so das BSIG und die NIS-2-Richtlinie. KRITIS-Betreiber müssen sich auch nach diesem Gesetz registrieren, Strategien zur Resilienz erarbeiten und umsetzen und Vorfälle melden.

Cyber Resilience Act

Komplettiert wird die neue IT-Sicherheitsregulierung ab Herbst 2027 mit spezifischen Sicherheitsvorgaben für digitale Produkte. Nach dem nun vorliegenden Referentenentwurf zur Durchführung des Cyber Resilience Act wird auch insofern das BSI (Bundesamt für die Sicherheit in der Informationstechnik) die zentrale Behörde in

Deutschland werden. Angesichts der damit zu erreichenden Bündelung des Cybersachverstands in einer Behörde erscheint das folgerichtig. Der Referentenentwurf ist hier abrufbar.



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

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

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

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-465
rebecca.mossner@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