Compliance
Die Zeitschrift für Compliance-Verantwortliche

Juli/August 2025

Inhalt

© IMAGO / Dreamstime

Aufmacher

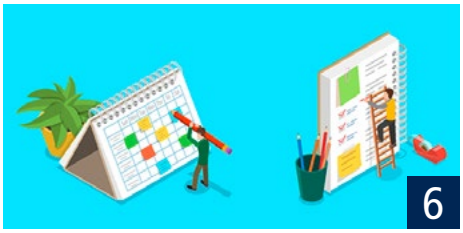
NIS2-Umsetzung à la Deutschland: Ein Lehrstück in verpassten Chancen
Zwischen regulatorischer Eile, behördlicher Bequemlichkeit und einer Unternehmenslandschaft im Dornröschenschlaf, so mutet die Umsetzung der NIS2-Richtlinie aus Sicht von Dr. Frank Schemmel an. In unserem Aufmacher beschreibt er den aktuellen Stand zu NIS2 in Deutschland.

Praxis

© IMAGO / Zoonar II

Effektive Compliance-Schulungen – Strategische Aspekte
Effektives Compliance-Management hat sich zu einer zentralen Grundlage regelkonformer und verantwortungsvoller Unternehmensführung entwickelt. Für die langfristig erfolgreiche Etablierung der notwendigen Strukturen und Maßnahmen spielen Compliance-Schulungen eine Schlüsselrolle.

Recht



© IMAGO / Zoonar

Cybersicherheit kritischer Infrastrukturen – Die NIS2-Richtlinie – Neue Pflichten
Kernstück der NIS2-Richtlinie (EU 2022/2555) sind umfangreiche Pflichten zur IT-Sicherheit, die von den erfassten Unternehmen umgesetzt und nachgewiesen werden müssen.

Research

© IMAGO / Zoonar II

Umfrage: NIS2 kennt nur jeder zweite Befragte
Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hat der TÜV-Verband im Juni eine neue repräsentative Umfrage zur Cybersicherheit in Unternehmen vorgestellt. Die Ergebnisse seien in zweifacher Hinsicht besorgniserregend, fasst das BSI in einer Mitteilung zusammen.

Veranstaltungen

17.09.2025 | Frankfurt am Main | **1. Praxistag des Deutschen Glücksspielrechtstags**

18.09.2025 | Frankfurt am Main und Online | **11. Deutscher Glücksspielrechtstag**

24. - 26.09.2025 | Düsseldorf und Online | **Datenschutzkonferenz 2025**

30.09.2025 | Frankfurt am Main | **5. Praxisseminar Geldwäschegesetz 2025**

07.10.2025 | Frankfurt am Main und Online | **4. Deutscher Futtermittelrechtstag**

16.10.2025 | Berlin | **KI im Unternehmen**

NIS2-Umsetzung à la Deutschland: Ein Lehrstück in verpassten Chancen

Zwischen regulatorischer Eile, behördlicher Bequemlichkeit und einer Unternehmenslandschaft im Dornröschenschlaf, so mutet die Umsetzung der NIS2-Richtlinie aus Sicht von Dr. Frank Schemmel an. In unserem Aufmacher beschreibt er den aktuellen Stand zu NIS2 in Deutschland.

Wurde auch Zeit: Licht am Ende des Tunnels der NIS2-Umsetzung.

„In einer idealen Welt haben wir NIS2 im Herbst im Parlament und vor Ende des Jahres im Amtsblatt", so Dr. Daniel Meltzian, Leiter des BMI-Grundsatzreferats für Cybersicherheit, jüngst im Tagesspiegel. Leider leben wir nicht in einer idealen Welt – sondern in Deutschland. Die Umsetzung der NIS2-Richtlinie nimmt hierzulande zwar wieder Fahrt auf – allerdings mit dem Charme eines Berliner Flughafens in Bauphase vier. Innenminister Dobrindt plant das Gesetz noch 2025 durch den Bundestag zu bringen. Ein finaler Referentenentwurf wurde bis Mitte Juni zwischen BMI und Digitalministerium abgestimmt – mit anschließender Verbändeanhörung. Ziel ist, einen politisch tragbaren Kabinettsentwurf noch vor der Sommerpause in den Bundestag einzubringen. Ambitioniert? Durchaus. Realistisch? Fraglich.

Die EU-Kommission hat bereits genug bzw. eher zu wenig gesehen. Gemeinsam mit 18 anderen Staaten steht Deutschland im zweiten Stadium eines entsprechenden Vertragsverletzungsverfahrens. Es droht ein ähnliches Trauerspiel wie seinerzeit bei der Umsetzung der Whistleblower-Richtlinie.

Der Anfang Juni veröffentlichte Referentenentwurf? Licht und Schatten. Viele aus der Praxis wichtige Punkte, die bereits bei der Abstimmung der Vorgängerregierung heftig diskutiert wurden, werden mithin in einem Anflug von Zeitmanagement großzügig ausgespart. „Es wird aber wichtig sein, dass die kommenden Abstimmungen so kurz wie möglich gehalten werden, um die zügige Umsetzung sicherzustellen", so eine offizielle Stimme aus dem BMI im Tagesspiegel zu möglichen Abstrichen. Es geht dabei zunächst um die abgespeckte Regulierung der Verwaltung. Dies verwundert, sind doch gerade Behörden und Verwaltungen oft am wenigsten vorbereit in Sachen Cybersecurity. Offenbar vertraut man auf eine wundersame Selbstheilung der IT-Landschaft von Behörden.

Bedauerlich aus Praxissicht ist auch, dass der bisher vorliegende Entwurf weder ausreichende Ergänzung bislang fehlender Definitionen noch dringend benötigte Klarstellung bei der Berechnung der Schwellenwerte enthält. So könnte man durch eine einfache Ergänzung im Umsetzungsgesetz tausende Shared-Service Center von Unternehmensgruppen entlasten. Denn die Erbringung von Rechenzentrums- und Clouddienstleistungen für andere Konzernunternehmen würde derzeit aufgrund einer Regelungslücke in ErwG 35 der Richtlinie wohl NIS2 unterfallen.

Und das BSI? Möchte laut eigener Aussage „mehr Helfer als Verhinderer" sein. Nett. Konkret äußert sich das darin, dass man nur dort Orientierungshilfen zu NIS2 bereitstellen möchte, wo noch keine anderweitigen existieren – was in der Praxis bedeutet: eher selten bis gar nicht. Die Begründung? „Stand der Technik" sei ein juristischer Begriff, also zu heikel für technische Hinweise. Aha.

Andere Länder – wie etwa Italien – liefern währenddessen brauchbare Leitlinien und Praxisbeispiele für Unternehmen. Deutschland hingegen hält es lieber mit der Devise: Keine Hilfe ist auch eine Hilfe. Immerhin: In einem Webinar der Allianz für Cybersicherheit hat das BSI eingeräumt, dass Aufklärung wichtiger sei als Bußgelder. Letzteres scheint auch dringend geboten, zeigt doch eine aktuelle repräsentative Cybersecurity-Studie des TÜV in Kooperation mit dem BSI, dass nur etwa die Hälfte der befragten Unternehmen überhaupt schon etwas von NIS2 gehört hat.

Was also tun in dieser regulatorischen Sedisvakanz? Auch hier gab es im vorgenannten Webinar die beste und gleichzeitig pragmatischste Empfehlung: „Macht mal die offensichtlichen Dinge und kümmert euch um die Details später." Sprich: NIS2-Betroffenheit prüfen, Gap-Analyse durchführen, Risiken neu bewerten, priorisieren und dann die größten Risiken erstmal adressieren. Hat man bereits ein nach ISO 27001, TISAX® oder anderweitig zertifiziertes ISMS, ist das Delta zu NIS2 nicht mehr allzu groß.

Klar ist zumindest: NIS2 wird künftig zum generellen Sorgfalts- und Haftungsmaßstab im Bereich Cybersicherheit – und damit zwingender Bestandteil jedes guten CMS. Das Umsetzungsgesetz wird wie sein gescheiterter Vorgänger wohl keine Übergangsfristen enthalten – also sollten Organisationen, die das Thema bisher eher stiefmütterlich betrachtet haben, spätestens die nächsten sechs Monate nutzen, um hier aufzuholen. Dann gibt es hoffentlich mehr Licht als Schatten für die Cybersicherheit in Deutschland.

Dr. Frank Schemmel, Compliance Officer (Univ.), ist Senior Director Privacy, Compliance & Public Affairs bei DataGuard in München. Schwerpunkt seiner Arbeit sind Datenschutz- und Datenwirtschaftsrecht, Informationssicherheit, Whistleblowing und die rechtlichen Herausforderungen der Digitalisierung.

Effektive Compliance-Schulungen – Strategische Aspekte

Effektives Compliance-Management hat sich zu einer zentralen Grundlage regelkonformer und verantwortungsvoller Unternehmensführung entwickelt. Für die langfristig erfolgreiche Etablierung der notwendigen Strukturen und Maßnahmen spielen Compliance-Schulungen eine Schlüsselrolle. Das gilt vor allem in Zeiten der Transformation, in denen sich Unternehmen und ihre Leitungsorgane mit vielen neuen rechtlichen Anforderungen konfrontiert sehen. Prof. Dr. Martin R. Schulz gibt hier einen Überblick zur Funktion von Schulungen als Element eines effektiven Compliance-Managements. Sein ausführlicher Beitrag mit weiteren Aspekten zum Thema erscheint in CB 9/2025.

© IMAGO / Zoonar II

Compliance-Schulungen: Sie zählen zu den Grundanforderungen an wirksame Compliance-Management-Systeme.

Unternehmen und ihre Stakeholder sind mit einer Vielzahl komplexer Regelungen konfrontiert. Informationsdefizite und Verständnislücken sind dabei oft kaum zu vermeiden. Denn die Normenflut und die damit verbundenen Rechtspflichten schwellen weiter an – trotz anhaltender Forderungen nach Deregulierung. Lücken, Unklarheiten und Interpretationsspielräume sorgen bei vielen Normen für Zweifelsfragen und „Graubereiche" – fahrlässige Regelverletzungen der Normadressaten sind nicht selten die Folge. Dieses Problem lässt sich mit Compliance-Schulungen adressieren. Sie bieten eine große Chance, Informationsdefizite zu beseitigen, den Anwendungsbezug der Regelungen im Unternehmenskontext zu vermitteln und gleichzeitig ein Verständnis für Sinn und Zweck von Compliance-Maßnahmen zu fördern. Compliance-Schulungen zählen daher zu den wichtigsten Maßnahmen, welche die Leitungsorgane in Erfüllung ihrer Compliance-Pflicht organisieren und kontrollieren müssen.

Die Compliance-Pflicht stellt eine rechtsformunabhängige Pflichtaufgabe eines jeden Geschäftsleiters und einer jeden Geschäftsleiterin dar, die in allen Unternehmen zu erfüllen ist. Die Geschäftsleitung muss alle erforderlichen und zumutbaren Vorkehrungen treffen, um Regelverstöße möglichst zu verhindern, die eingeleiteten Compliance-Maßnahmen zu kontrollieren sowie Fälle von „Non-Compliance" konsequent aufzuklären und zu sanktionieren.

Die konkrete Ausgestaltung der unternehmensspezifischen Compliance-Maßnahmen liegt dabei grundsätzlich im Gestaltungsermessen der Geschäftsleitung. Mit Blick auf die Wirksamkeit von Compliance-Maßnahmen im Sinne tatsächlicher Regelbefolgung empfiehlt sich allerdings die Beachtung derjenigen Grundanforderungen und Leitsätze, die Rechtsprechung und Rechtswissenschaft zur Beurteilung von Compliance-Fällen entwickelt haben. Hierzu zählen insbesondere die klare Festlegung von Zuständigkeiten auf Ebene der Geschäftsleitung für das Thema Compliance, die systematische Erfassung und Steuerung relevanter Compliance-Risiken, die Beachtung rechtlicher Delegationserfordernisse bei Übertragung von Compliance-Aufgaben, die Organisation von Informations- und Berichtsstrukturen, die Etablierung von Compliance-Regelwerken und Schulungen sowie die Organisation von Kontroll- und Sanktionsmechanismen in Bezug auf Regelverstöße. Zudem müssen die Compliance-Maßnahmen regelmäßig angepasst und aktualisiert werden. Diese Grundanforderungen sind auch bei Compliance-Schulungen zu beachten. Eine Organisationspflicht für Compliance-Schulungen kann bereits aus besonderen gesetzlichen Vorgaben folgen, ist aber auch Bestandteil der Compliance-Pflicht. Ferner muss die Geschäftsleitung Compliance-Schulungen auch deshalb organisieren, um den durch die Gerichte entwickelten Instruktionspflichten zu genügen und eine persönliche Haftung nach §§ 130, 9 OWiG zu vermeiden. In der Rechtsprechung finden sich diverse Fälle, bei denen bereits die unzureichende Anleitung der Mitarbeitenden als Pflichtverletzung der Geschäftsleitung gewertet wurde.

Daher muss die Geschäftsleitung adäquate Vorkehrungen für die Durchführung, die Kontrolle und die Aktualisierung von Compliance-Schulungen treffen. Sofern sie die Durchführung von Compliance-Schulungen (z. B. an Compliance Officer) delegiert, bleibt sie für die sachgerechte Auswahl, Instruktion und Kontrolle der Trainer verantwortlich. Da sich der rechtliche Rahmen für Unternehmen häufig ändert, ist eine kontinuierliche Anpassung und Aktualisierung der Compliance-Schulungen erforderlich. Auch diesen Prozess sollte die Geschäftsleitung organisieren, um Qualität und Wirksamkeit der Schulungen nachhaltig zu gewährleisten. Die ebenso notwendige Dokumentation der Schulungsmaßnahmen sollte Lernkontrollen einschließen, damit bei Compliance-Schulungen (ebenso wie bei anderen Compliance-Maßnahmen) der Nachweis eines „lebenden Compliance-Systems" gelingt.

Last but not least hängt der Erfolg von Compliance-Schulungen eng mit der gelebten Compliance-Kultur zusammen. Auch hier spielen Geschäftsleitung und Führungskräfte die entscheidende Rolle, denn sie prägen „Tone and Conduct at and from the Top". Indem sie sicherstellen, dass Schulungen adressatengerecht und praxisorientiert erfolgen und zugleich zugrunde liegende Werte vermittelt werden (Beispiel: Unbestechlichkeit als Grundlage für Anti-Korruptionsregeln) erhöhen sie die Akzeptanz bei den Schulungsteilnehmenden. Untersuchungen haben gezeigt, dass die Bejahung der Richtigkeit von Regeln durch die Normadressaten eine zentrale Rolle für die Regelbefolgung spielt.

Prof. Dr. Martin R. Schulz, LL.M. (Yale)

© privat

Prof. Dr. Martin R. Schulz, LL.M (Yale), ist Rechtsanwalt und Counsel bei CMS in Frankfurt am Main. Ferner ist er Professor für Wirtschaftsrecht an der IU Internationale Hochschule, Erfurt. Er ist Herausgeber und Co-Autor des Handbuchs „Compliance-Management im Unternehmen – Erfolgsfaktoren und praktische Umsetzung" (3. Aufl. 2025).

Mehr zu Schulungen als Element eines effektiven Compliance-Managements, zur Organisation von Schulungen als Bestandteil der Compliance-Pflicht und zur Verankerung von Compliance-Schulungen in der Unternehmensorganisation lesen Sie im ausführlichen Beitrag von Prof. Dr. Martin R. Schulz in Ausgabe 9/2025 des Compliance-Beraters, der am 21. August 2025 erscheint.

MACIM

Viadrina Compliance Center

Europa Universität Viadrina

Master of Compliance & Integrity Management

Online-Infoabend
Donnerstag, 4. September 2025 | 17.00 Uhr

Berufsbegleitend, interdisziplinär und praxisnah studieren
Profitieren Sie von umfassenden Compliance-Netzwerken, einer einmaligen Fachbibliothek sowie über 50 Lehrenden aus Wissenschaft und Praxis – nur an der Europa-Universität Viadrina.

Jetzt kostenlos anmelden:
www.europa-uni.de/macim

Cybersicherheit kritischer Infrastrukturen – Die NIS2-Richtlinie – Neue Pflichten

Kernstück der NIS2-Richtlinie (EU 2022/2555) sind umfangreiche Pflichten zur IT-Sicherheit, die von den erfassten Unternehmen umgesetzt und nachgewiesen werden müssen. In der Juni-Ausgabe von Compliance hat Dr. Dr. Fabian Teichmann einen Überblick über Inhalt und Umsetzung der NIS2-Richtlinie gegeben. Im vorliegenden Beitrag beleuchtet er nun neue Pflichten – etwa zum Risikomanagement und zur 24-Stunden-Meldung von Sicherheitsvorfällen.

Pflichten und Fristen: NIS2 stellt Unternehmen vor einige organisatorische Herausforderungen.

Im Zentrum der Pflichten zur IT-Sicherheit steht ein ganzheitliches Risikomanagement im Cybersecurity-Bereich (Art. 21 NIS2-RL). Unternehmen haben geeignete und verhältnismäßige technische, organisatorische und operative Sicherheitsmaßnahmen zu ergreifen, um Risiken für die Netz- und Informationssysteme, die sie für ihre Dienste nutzen, zu beherrschen. Die Richtlinie nennt zehn Elemente, die mindestens abgedeckt werden müssen, darunter insbesondere: regelmäßige Risikoanalysen, Konzepte zur Bewältigung von Sicherheitsvorfällen (Incident Response), Notfall- und Business-Continuity-Pläne (Aufrechterhaltung des Betriebs, Backups, Wiederanlauf), Maßnahmen zur Sicherheit in der Lieferkette (Supply-Chain-Security) sowie Verfahren für Verschlüsselung/Kryptografie und Zugangskontrollen. Diese Anforderungen gehen über die bisherigen Pflichten nach dem BSIG (etwa § 8a BSIG a.F.) deutlich hinaus. Unternehmen müssen die Umsetzung ihres Informationssicherheits-Risikomanagements zudem dokumentieren und regelmäßig einen Nachweis gegenüber der Behörde führen.

Neben präventiven Maßnahmen etabliert NIS2 ein strenges Meldewesen für IT-Sicherheitsvorfälle. Bei einem erheblichen IT-Sicherheitsvorfall (Definition in Art. 6 Nr. 40 NIS2-RL) gilt ein gestuftes Meldesystem: Innerhalb von 24 Stunden nach Kenntnis des Vorfalls ist eine erste Frühwarnmeldung an die zuständige Behörde (in Deutschland: BSI) abzusetzen. Spätestens nach 72 Stunden muss ein ausführlicherer Incident-Bericht mit einer ersten Einschätzung von Ursache und Schwere des Vorfalls folgen. Spätestens einen Monat nach der 72h-Meldung ist ein Abschlussbericht mit detaillierter Analyse und Angabe ergriffener Gegenmaßnahmen zu erstatten. Die Behörde ihrerseits muss den Eingang der Frühwarnung binnen 24 Stunden bestätigen und im Bedarfsfall operative Hilfestellung anbieten. Dieses eng getaktete Meldesystem soll Transparenz und eine rasche Reaktion auf Cybervorfälle gewährleisten, stellt Unternehmen aber vor organisatorische Herausforderungen.

Schließlich begründet NIS2 weitere Verpflichtungen: So müssen relevante Unternehmen sich bzw. ihre Betriebsstätten registrieren und einen zuständigen Ansprechpartner benennen. Für wesentliche und wichtige Einrichtungen werden zudem Mitwirkungspflichten bei Aufsichtsmaßnahmen statuiert (Duldung von Prüfungen, Herausgabe von Informationen etc., vgl. Art. 32, 33 NIS2-RL). In bestimmten Fällen können Unternehmen verpflichtet werden, die Nutzer bzw. Kunden ihrer Dienste über erhebliche Cyberbedrohungen oder Vorfälle zu informieren.

RA Dr. Dr. Fabian Teichmann, LL.M.

RA Dr. Dr. Fabian Teichmann, LL.M., ist Managing Partner der Teichmann International (Schweiz) AG sowie Verwaltungsrat der Teichmann International (IT Solutions) AG. Seine Schwerpunkte liegen im Strafrecht, der Cybersecurity und der Unternehmenscompliance. Er ist zudem als Dozent an mehreren europäischen Hochschulen tätig.

Übersicht zentraler Pflichten und Fristen

Pflichtbereich	Inhalt der Vorgabe	Wichtige Fristen
Risikomanagement (Art. 21 NIS2)	Implementierung angemessener *technischer und organisatorischer* Maßnahmen der IT-Sicherheit in zehn definierten Bereichen (u.a. Risikoanalyse, Incident Response, Business Continuity, Lieferkettensicherheit, Zugriffs- und Zugriffskontrollkonzepte, Kryptografie) und regelmäßiger Nachweis gegenüber der Behörde.	*kontinuierlich*
Meldung von Vorfällen (Art. 23 NIS2)	*Stufenmodell* bei erheblichen Sicherheitsvorfällen: Frühwarnung binnen 24 h; Folgemeldung binnen 72 h; Abschlussbericht binnen eines Monats. Behördliche Bestätigung/Rückmeldung innerhalb 24 h.	24 Stunden (Erstmeldung); 72 Stunden; ein Monat
Registrierung & Kontaktstelle	Meldung an die Behörde als (neu) betroffene Einrichtung; Benennung verantwortlicher Kontaktpersonen (z.B. IT-Sicherheitsbeauftragter).	*unverzüglich* nach Einstufung
Information Betroffener		*situationsabhängig* (bei erheblichem Vorfall auf Anordnung / bei überwiegendem Schutzinteresse der Empfänger)
Kooperation mit Behörden	Mitwirkungs- und Duldungspflichten bei Prüfungen: Ermöglichung von Vor-Ort-Kontrollen, Herausgabe angeforderter Unterlagen, Umsetzung behördlicher Anordnungen (z.B. Abstellen von Sicherheitsmängeln) – bei Zuwiderhandlung ggf. Zwangsgelder.	*anlassbezogen* (auf Anordnung der Behörde; laufend einzuhalten)

Hybrid-Veranstaltung: Teilnahme vor Ort sowie Online möglich!

Datenschutzkonferenz 2025

Praxis | Recht | Innovation

24. - 26. September 2025 | Hotel Kö59 Düsseldorf

ES ERWARTEN SIE UNTER ANDEREM DIESE THEMEN

- Datenerwerb im Unternehmenskauf – so geht's!
- Update Beschäftigtendatenschutz
- Vom Chaos zur Perlenkette: Ein bereichsübergreifender Compliance-Prozess für mehr Awareness und Effizienz
- Verhandlungen, Verständigungen und Deals mit den Datenschutzbehörden
- Grenzenlose Unsicherheit? Drittlandtransfers zwischen Risiko und Regulierung
- Fotoaufnahmen im Unternehmensalltag: Zwischen Recht am eigenen Bild und Datenschutz
- KI und Datenschutz aus aufsichtsbehördlicher Perspektive
- Training von Datenschutzkoordinatoren im Unternehmen – Wertschätzung und Wissensvermittlung als Schlüssel für ein funktionierendes DSMS
- AI (Act) aus der Sicht des DSB
- The more the merrier? Herausforderungen bei der Datenschutzumsetzung in Netzwerken und ähnlichen Strukturen
- Aktuelles aus dem EDSA
- „Allein auf weiter Flur?" – Der DSB zwischen Loyalitätsdruck und Behördenschutz
- Good Cop, Bad Cop? Datenschutzfälle aus Sicht der Aufsicht und der Beratung

FREUEN SIE SICH AUF NEUE IMPULSE DURCH DIESE UND VIELE WEITERE REFERENT:INNEN


Dr. Jens Ambrock
HmbBfDI


Dr. Jens Eckhardt
BvD e.V.


Anna Eickmeier
YPOG Rechtsanwälte


Dr. Diana Ettig
Spirit Legal


Daniel Gabel


Inna Gendelman
Scout24


Dr. Jan-Michael Grages
KNPZ Rechtsanwälte


Stephan Hansen-Oest
Rechtsanwalt


Dr. Nina Elisabeth Herbort
Short Law


Prof. Dr. Tobias Keber
LfDi BaWü


Carolin Loy
BayLDA


Dr. Carolin Monsees
Taylor Wessing


Dr. Flemming Moos
Osborne Clarke


Dr. Aileen Pasquariello
L'Oréal Austria Germany


Dr. Ruben Schneider
BfDI


Dr. Dominik Sorber
POELLATH


Dr. Lea Stegemann
Noerr


Laura L. Stoll
intersoft consulting services AG


Henrike Teitge
BlnBDI


Mona Wrobel
TeamViewer Germany GmbH


Tim Wybitul
Latham & Watkins

Ihr Ansprechpartner: Herr Jasha Baniashraf
Senior Projektmanager
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-2773
E-Mail: Jasha.Baniashraf@dfv.de

Veranstaltungsort:
Hotel Kö59 Düsseldorf
Königsallee 59
40215 Düsseldorf

Eine Fortbildungsbescheinigung nach § 15 FAO für Ihre berufliche Weiterbildung wird erteilt.

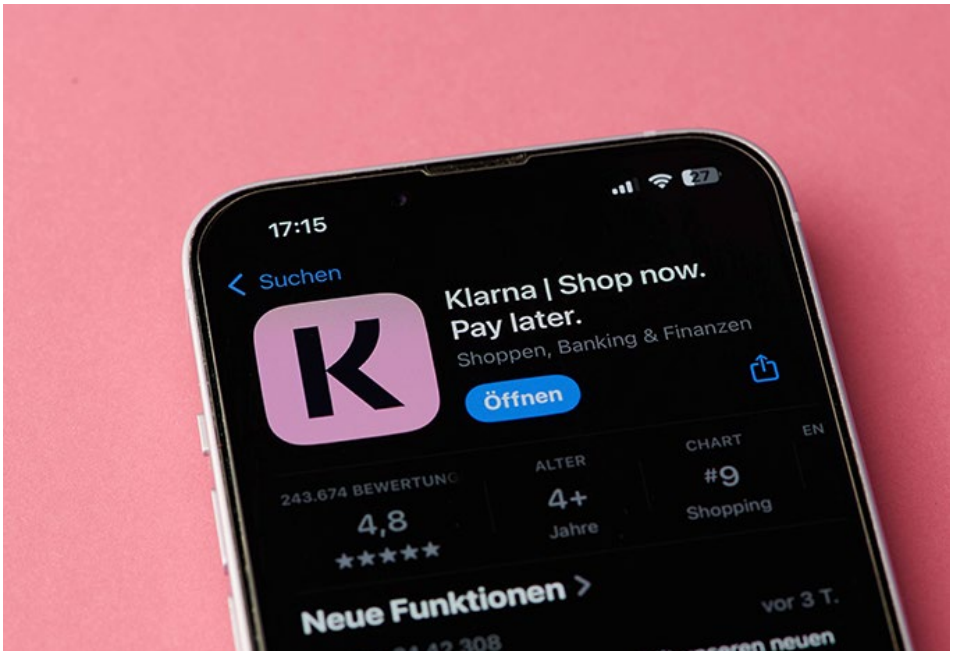
JETZT ANMELDEN UNTER
www.datenschutzkonferenz.de
oder QR-Code scannen

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

Gesetzentwurf zur Umsetzung der Verbraucherkreditrichtlinie

Verbraucherinnen und Verbraucher sollen besseren rechtlichen Schutz erhalten, wenn sie Kreditgeschäfte tätigen. Auch sogenannte Buy-now-pay-later-Modelle sollen erstmals in die verbraucherschützenden Regelungen für Kreditverträge einbezogen werden. Das sieht ein Gesetzentwurf vor, den das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) am 23. Juni 2025 veröffentlicht hat. Der Gesetzentwurf soll zugleich den europäischen Binnenmarkt für Kredite zwischen Unternehmern und Verbraucherinnen und Verbrauchern fördern. Er geht zurück auf die Verbraucherkreditrichtlinie der Europäischen Union, die damit ins deutsche Recht umgesetzt werden soll.



© IMAGO / CHROMORANGE

Jetzt einkaufen und erst später bezahlen – auch das ist ein (Kurzzeit-)Kredit.

Die EU-Verbraucherkreditrichtlinie ist bis zum 20. November 2025 in nationales Recht umzusetzen und ab dem 20. November 2026 von den Mitgliedstaaten anzuwenden. Die darin vorgeschlagenen Neuerungen sollen den Verbraucherschutz erheblich ausweiten. So werden bislang unregulierte Kreditformen erstmals in die Regelungen zu Verbraucherkrediten einbezogen. Fortan fallen beispielsweise Buy-now-pay-later-Modelle und unentgeltliche Kredite unter die Regelungen. „Buy now, pay later" bedeutet, dass bei einem Kauf das Geld erst zu einem späteren Zeitpunkt (beispielsweise 14 oder 30 Tage nach dem Kauf) vom Konto abgebucht wird. Es handelt sich dabei um einen Zahlungsaufschub und damit um einen Kurzzeitkredit.

Außerdem sollen die Vorgaben für die Kreditwürdigkeitsprüfung verschärft werden, die verpflichtend vor dem Vertragsabschluss durchzuführen ist. Insbesondere erfolgt eine Angleichung an die Maßstäbe, die bei Darlehensverträgen für Immobilien gelten.

Die Verbraucherkreditrichtlinie verfolgt einen Vollharmonisierungsansatz, der es den EU-Mitgliedstaaten grundsätzlich nicht erlaubt, strengere oder weniger strenge Verbraucherschutzvorschriften vorzusehen. Soweit Umsetzungsspielraum vorhanden ist, hat das BMJV diesen nach eigenen Angaben grundsätzlich für eine möglichst bürokratiearme Regulierung genutzt, etwa beim Umfang vorvertraglicher Informationspflichten. Auch bei der Form des Vertragsschlusses sei der Spielraum der Richtlinie genutzt worden, sodass Allgemein-Verbraucherdarlehen künftig in Textform statt bislang in Schriftform abgeschlossen werden können. Der Gesetzentwurf sehe grundsätzlich keine nationalen Verschärfungen oder Erweiterungen über die zwingenden europäischen Vorgaben vor (kein sogenanntes Goldplating), heißt es in einer Mitteilung des BMJV. *chk*

Besserer Schutz vor Einschüchterungsklagen

Gerichte sollen bessere Möglichkeiten erhalten, mit sogenannten Einschüchterungsklagen umzugehen. Das sieht ein Gesetzentwurf vor, den das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) am 20. Juni 2025 veröffentlicht hat.

Unter Einschüchterungsklagen werden unbegründete Klagen verstanden, die darauf abzielen, missliebige Beiträge zur öffentlichen Meinungsbildung zu unterdrücken. Sie richten sich zum Beispiel gegen Journalistinnen und Journalisten, Wissenschaftlerinnen und Wissenschaftler oder Nichtregierungsorganisationen. Auf Englisch werden sie auch als SLAPP bezeichnet („Strategic Lawsuits Against Public Participation"). Der veröffentlichte Gesetzentwurf geht zurück auf die Anti-SLAPP-Richtlinie der EU, die damit ins deutsche Recht umgesetzt werden soll.

Wie das BMJV mitteilt, setzte der Gesetzentwurf die Vorgaben der EU-Richtlinie im Wesentlichen 1:1 um. Beim Anwendungsbereich geht er jedoch in einem Punkt darüber hinaus: Die neuen Regelungen gelten nicht nur für Sachverhalte mit grenzüberschreitendem Bezug, sondern auch für rein nationale Sachverhalte. Die Regelungen für den Umgang mit Einschüchterungsklagen sollen dann zur Anwendung kommen, wenn mit dem Rechtsstreit unbegründete Ansprüche verfolgt werden und der Hauptzweck des Rechtsstreits darin besteht, öffentliche Beteiligung zu verhindern, einzuschränken oder zu sanktionieren. Eine öffentliche Beteiligung ist zum Beispiel die Teilnahme an einer Demonstration, die Veröffentlichung eines Artikels in einer Zeitung, ein Post in den sozialen Netzwerken oder die Veröffentlichung einer wissenschaftlichen Studie. *chk*

Umfrage: NIS2 kennt nur jeder zweite Befragte

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hat der TÜV-Verband im Juni eine neue repräsentative Umfrage zur Cybersicherheit in Unternehmen vorgestellt. Die Ergebnisse seien in zweifacher Hinsicht besorgniserregend, fasst das BSI in einer Mitteilung zusammen: „Zum einen konnte ein Anstieg der Bedrohungslage verzeichnet werden, zum anderen zeigen die Umfrageergebnisse, dass viele Firmen die Lage unterschätzen und die eigene Resilienz überbewerten." Das BSI warnt vor trügerischer Sicherheit.

NIS2? Nie gehört! Nur jeder zweite kennt die EU-Richtlinie.

Nur etwa die Hälfte der Befragten habe angegeben, die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) zu kennen. Mit der Umsetzung der NIS2-Richtlinie in nationales Recht, die aufgrund der vorgezogenen Neuwahlen in Deutschland bisher nicht erfolgt ist, werde das BSI für deutlich mehr Unternehmen als zuvor Aufsichtsbehörde. Für die bestehenden Kritischen Infrastrukturen (KRITIS) ändere sich hierdurch voraussichtlich wenig, aber für ca. 29.000 nach der NIS2-Richtlinie „wesentliche" (essential entities) und „wichtige" Einrichtungen (important entities) ergäben sich erstmals gesetzliche Pflichten, gibt das BSI zu Bedenken.

Der TÜV-Verband ergänzt: „Neun von zehn (91 Prozent) Unternehmen bewerten ihre Cybersicherheit als gut oder sehr gut. Und jedes vierte Unternehmen (27 Prozent) gibt an, dass IT-Sicherheit für sie nur eine kleine oder gar keine Rolle spielt." Eine Mehrheit spreche sich für gesetzliche Vorgaben aus, um das Schutzniveau in der Wirtschaft zu erhöhen: 56 Prozent seien der Meinung, dass alle Unternehmen verpflichtet sein sollten, angemessene Maßnahmen für ihre Cybersecurity zu ergreifen. Die Bundesregierung solle die überfällige nationale Umsetzung der NIS2-Richtlinie zügig verabschieden.

Einen Entwurf hierfür hat die neue Regierungskoalition inzwischen auf den Weg gebracht (siehe hierzu unseren Aufmacher in dieser Ausgabe auf Seite 2 „NIS2-Umsetzung à la Deutschland: Ein Lehrstück in verpassten Chancen".

Die Studie des TÜV-Verbandes zeige, dass auf dem Weg zur Cybernation Deutschland noch eine Menge Arbeit vor uns liegt, so das Resümee beim BSI. Für Besorgnis sorgt dort vor allem die geringe Bekanntheit der NIS2-Richtlinie. Umso wichtiger sei ihre zügige Umsetzung in nationales Recht. Die damit einhergehende Bürokratie und der Mehraufwand für Unternehmen, könne trotz aller Kritik an zusätzlichem Aufwand dabei helfen, die Resilienz der deutschen Wirtschaft umfassend zu erhöhen. Das BSI lege seinen Schwerpunkt dabei auf Hilfestellung und Kooperation und unterstütze Unternehmen auch heute schon mit umfangreichen Informations- und Beratungsangeboten. Das Credo laute „Cybersicherheit vor Bürokratie".

Auch der TÜV-Verband will in Sachen Cybersicherheit unterstützen und spricht unter anderem folgende Empfehlungen für Unternehmen aus:

1. Cyberrisiken ernst nehmen
   Unternehmen sollten eine qualifizierte Risikoanalyse durchführen und diese angesichts des dynamischen technologischen und geopolitischen Umfelds regelmäßig aktualisieren. Was ist besonders zu schützen? Welche Bedrohungen gibt es? Was sind potenzielle Schwachstellen im Unternehmen? Diese und weitere Fragen gelte es zu beantworten. Je nach Größe, Branche und Tätigkeitsgebiet könnten Cyberrisiken sehr unterschiedlich bewertet werden.
2. Cybersecurity-Strategie entwickeln
   Übergeordnetes Ziel der Strategie sei es, ein angemessenes Sicherheitslevel für das jeweilige Unternehmen zu definieren. Bestandteil dessen sollte eine IT-Sicherheitsrichtlinie sein. In dieser werden messbare Ziele definiert, konkrete Sicherheitsanforderungen festgelegt und klare Verantwortlichkeiten geschaffen. Sie sei die Basis für die Maßnahmenplanung.
3. Maßnahmenplan ausarbeiten
   Auf Grundlage der Risikoanalyse und strategischer Überlegungen sollten konkrete Maßnahmen festgelegt werden.

Nicht zu unterschätzen seien Lieferketten als Einfallstor: 10 Prozent der Unternehmen wurden über Zulieferer oder Kunden attackiert. Zwar stellen 32 Prozent der Unternehmen Sicherheitsanforderungen an Partner – eine echte Auditierung sei allerdings selten, stellt der TÜV-Verband fest.

chk

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Thomas Berner, Markus Gotta
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 0151 27 24 56 63, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke,
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Mikhail Tsyganov,
Telefon: 069 7595-2779, E-Mail: Mikhail.Tsyganov@dfv.de
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, dievini patch Beteiligungs GmbH; Joern-Ulrich Fink, Regulatory Adherence & Compliance Policy Governance, Deutsche Bank AG; Otto Geiß, Deutsches Netzwerk Wirtschaftsethik; Mirko Haase, Hilti Corporation; Prof. Dr. Katharina Hastenrath, ZHAW Zürcher Hochschule für Angewandte Wissenschaften; Corina Käsler, Senior Advisor, State Street Bank International GmbH; Dr. Karsten Leffrang, General Counsel Germany, Valeo; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, Global Compliance, Miele Group; Hartmut T. Renz, Partner STRATECO GmbH; Dr. Barbara Roth, State Street Bank International; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de

5. Praxisseminar Geldwäschegesetz 2025

Das brachenübergreifende Jahresupdate

Eine Veranstaltung von

GELDWÄSCHE & RECHT und GwG

30. September 2025 | Frankfurt am Main

Jetzt anmelden!

PROGRAMM

8.30 Uhr	**Registrierung und Kaffee**
9.00 Uhr	**Begrüßung** Dr. Uta Zentes, Rechtsanwältin und Syndikusrechtsanwältin, Frankfurt a. M. Sebastian Glaab, Partner, Annerton Rechtsanwälte, Frankfurt a. M.
9.10 Uhr	**Aktuelle Praxis- und Rechtsfragen zur Anwendung von KI bei KYC und AML-Risikomanagement** Dr. Joachim Kaetzler, Partner, CMS Hasche Sigle, Frankfurt a. M.
9.55 Uhr	**Erfahrungsbericht zu einer Sonderprüfung** Carsten Lang, Head Financial Crime Prevention Germany, UBS Europe SE, Frankfurt a. M.
10.40 Uhr	**Kaffeepause**
11.10 Uhr	**Aktuelle Entwicklungen aus dem Verhältnis zu den Finanzbehörden** Dr. Ocka Stumm, Partnerin, Gleiss Lutz, Frankfurt a. M.
11.55 Uhr	**Neue Vorgaben der EU-AML-VO für das KYC-Verfahren – Was muss zukünftig geändert werden?** Dr. Jacob Wende, CEO & Gründer, Regpit GmbH, Schriftleitung Geldwäsche & Recht, Berlin
12.40 Uhr	**Mittagessen**
13.40 Uhr	**Auf dem Hinterhof der Geldwäscheaufsicht. Wie das Land Berlin im Nichtfinanzektor arbeitet** Jörg Lehnert, Leiter der Geldwäscheaufsicht des Landes Berlin
14.25 Uhr	**Ermittlung des wirtschaftlichen Eigentums nach Kap. 4 EU-VO 2024/1624** Dr. Andreas Burger, Partner, Deloitte GmbH, Frankfurt a. M. Christian Paap, Rechtsanwalt und Syndikusrechtsanwalt,, Deloitte GmbH, Hamburg
15.10 Uhr	**Kaffeepause**
15.40 Uhr	**tba** Dr. Felix Wrocklage, Rechtsanwalt, Gleiss Lutz, Frankfurt a. M.
16.25 Uhr	**Fazit**


Dr. Uta Zentes


Sebastian Glaab


Dr. Joachim Kaetzler


Carsten Lang


Dr. Ocka Stumm


Dr. Jacob Wende


Dr. Andreas Burger


Christian Paap


Dr. Felix Wrocklage

Ihre Ansprechpartnerin: Frau Lena Wehrmann

Projektmanagerin
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-2784
E-Mail: Lena.Wehrmann@dfv.de

Inklusive Fortbildungsbescheinigung über 5 Stunden und 15 Minuten nach § 15 FAO.

Teilnahmegebühren (zzgl. MwSt.):

599,–	EUR	Unternehmensvertreter:innen
799,–	EUR	Abonnent:innen GWuR / CB / RdZ / BB, Käufer:innen des Kommentars Zentes/Glaab (Kopie Kaufbeleg) sowie Behördenvertreter:innen
899,–	EUR	Normalpreis

JETZT ANMELDEN UNTER
www.ruw.de/gwg
oder QR-Code scannen

R&W Fachkonferenzen
Eine Medienmarke der dfv Mediengruppe