Falls Ihnen der Newsletter weitergeleitet wurde und Sie ihn regelmäßig beziehen möchten, besuchen Sie: www.compliance-plattform.de

Compliance

Die Zeitschrift für Compliance-Verantwortliche

November 2026

SCHWERPUNKT FINANCE

Inhalt



© IMAGO / Ikon Images

Aufmacher

Erweiterte Strafbarkeit durch UK Financial Crime Compliance

Europäische und deutsche Finanzinstitute und Unternehmen mit Bezug zu Großbritannien können die Einhaltung der neuen und erweiterten britischen Finanzstrafrechtsregelungen nicht mehr als lokale Zusatzverschärfungen behandeln. Mit Einführung des Crime und Policing Act 2026 zum 29. Juni 2026 ist in strafrechtlicher Hinsicht eine neue Verschärfung eingetreten, die auch deutsche Unternehmen und Finanzinstitute zu beachten haben.

Recht



© KI-generiert / Christina Kahlen-Pappas / Flux 2 Pro

Der „DORO" im Gefüge des Beauftragtenwesens
Mit der Verordnung (DORA) 2022/2554 hat der europäische Gesetzgeber eine neue Governance-Rolle eingeführt: den Digital Operational Resilience Officer (DORO). Diese Funktion stellt Finanzunternehmen vor erhebliche organisatorische und rechtliche Herausforderungen.

Praxis

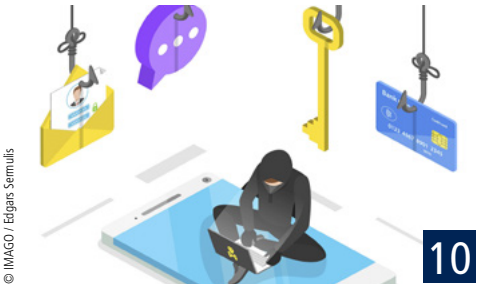


© KI-generiert / Christina Kahlen-Pappas / Flux 2 Pro

Arbeitszeiterfassung: Rechtslage, Bußgelder und behördliche Befugnisse
Schreiben von Aufsichtsbehörden mit Forderungen nach umfangreichen Arbeitszeitnachweisen und Hinweisen auf mögliche Bußgelder verunsichern derzeit viele Unternehmen. Die aktuellen Anforderungen zur Arbeitszeiterfassung bedürfen daher einer rechtlichen Einordnung.

8 Interne Ermittlungen wirksam steuern

News



© IMAGO / Edgars Semuls

EuGH: Verbraucherschutz steht nach Zahlungsbetrug im Vordergrund
Ein aktuelles Urteil des Europäischen Gerichtshofs (15. Oktober 2026 – C-70/25) stellt klar: Grobe Fahrlässigkeit des Kunden entbindet die Bank nicht von ihrer Pflicht zur unverzüglichen Rückerstattung nicht autorisierter Zahlungen.

Umfrage zur Umsetzung des HinSchG in deutschen Unternehmen



Veranstaltungen

CYBER//RESILIENT |
10.11.2026 | Online

Update Unternehmensstrafrecht |
18.11.2026 | Online

Compliance & KI 2.0 |
03.-04.12.2026 | Online

4. Praxisseminar Geldwäscheprävention |
25.02.2027 | Frankfurt am Main

Deutsche Compliance Konferenz 2027 |
27.-28.04.2027 | Frankfurt am Main

Erweiterte Strafbarkeit durch UK Financial Crime Compliance

Europäische und deutsche Finanzinstitute und Unternehmen mit Bezug zu Großbritannien können die Einhaltung der neuen und erweiterten britischen Finanzstrafrechtsregelungen nicht mehr als lokale Zusatzverschärfungen behandeln. Mit Einführung des Crime und Policing Act 2026 zum 29. Juni 2026 ist in strafrechtlicher Hinsicht eine neue Verschärfung eingetreten, die auch deutsche Unternehmen und Finanzinstitute zu beachten haben.



© IMAGO / Ikon Images

Auf Senior-Manager richten sich nun schneller alle Finger.

Großbritannien hat die strafrechtliche Verantwortung der Unternehmen und deren maßgeblicher Senior-Manager in den Bereich einer Prüfung vorverlagert, ob überhaupt Präventionsmaßnahmen im Unternehmen vorliegen, um strafbare Handlungen zu verhindern. Das Vorliegen einer Compliance-Organisation für die Exculpation von etwaigen strafbaren Handlungen ist nicht mehr maßgeblich.

Der Auslöser dafür war der expandierende „Failure to Prevent"-Normenrahmen. Drei britische Unternehmensdelikte – alle mit faktischer extraterritorialer Auswirkung – teilen nun dieselbe Rechtsarchitektur: eine verschärfte Unternehmensstraftat, verknüpft mit einer verfahrensbasierten Verteidigung.

UK-Bribery Act 2010 führte eine strikte Strafbarkeit und Haftung für das Versagen von Mechanismen im Unternehmen ein, wenn Korruption und Bestechung nicht ausgeschlossen werden. Diese strafrechtliche Verschärfung wurde durch die Möglichkeit ausgeglichen, eine angemessene Verfahrensverteidigung durchzuführen.

Criminal Finances Act 2017 erweiterte die Strafbarkeit mit Bezug auf Steuerhinterziehung, ergänzt mit einer ähnlichen angemessenen Präventionsverteidigungsmöglichkeit.

Economic Crime and Corporate Transparency Act (ECCTA) 2023, der auf Betrug ausgeweitet wurde, erweiterte die Strafbarkeit. Von diesem Gesetz erfasste größere Unternehmen können strafrechtlich verantwortlich sein, wenn eine verbundene Person eine bestimmte Betrugsstraftat zum Vorteil des Unternehmens oder ihrer Kunden begeht, es sei denn, das Unternehmen kann angemessene Präventionsmaßnahmen nachweisen. Unter anderem für deutsche Unternehmen ist dies nicht lediglich eine weitere Compliance-Verpflichtung. Sie verlagert den Schwerpunkt von der Einhaltung regulatorischer Vorschriften hin zur operativen Prävention, damit strafbare Handlungen nicht begangen werden können. Es ist jeweils zu prüfen, ob Kontrollen, die beispielsweise Anreize, Produkte, Drittbeziehungen und Managementinformationen schützen, in der Lage sind, Fehlverhalten zu verhindern, bevor ein solches eintritt.

Crime and Policing Act 2026 verschärft diese Gesetzeslage nunmehr zusätzlich. Insbesondere hebt Section 250, das vorherige ECCTA-Senior-Manager-Haftungsregime, das zuvor auf Wirtschaftsstraftaten beschränkt war, auf und ersetzt es. Es erweitert die Strafbarkeit von reinen Wirtschaftsstraftaten nunmehr auf alle britischen Straftaten. Begeht ein Senior-Manager eine Straftat im tatsächlichen oder scheinbaren Umfang seiner Befugnis, begeht das Unternehmen diese Straftat ebenfalls.

Entscheidend ist hierbei, dass Section 250 keine Verteidigung mit dem Argument zulässt, eine Compliance-Organisation bestehe im Unternehmen. Ein Unternehmen kann auch dann strafrechtlich verantwortlich bleiben, wenn Compliance-Rahmenbedingungen bestehen. Entscheidend für einen Ausschluss der Strafbarkeit ist es, ob geeignete Präventionsmaßnahmen um Unternehmen eingeführt wurden, die diese strafbaren Handlungen hätten ausschließen können und müssen. Damit liegt eine substantielle Erweiterung einer strafrechtlichen Gefährdungslage vor. Großbritannien führt damit ein Unternehmensstrafrecht ein, bei dem von den erfassten größeren Unternehmen mit UK-Bezug gesetzlich gefordert wird, ihre eigenen internen Compliance- und Kontrollsysteme zu überwachen und um die erforderlichen Präventionsmaßnahmen zu erweitern.

Für die erfassten deutschen Unternehmen ist es damit nicht entscheidend, ob eine Compliance-Organisation im Unternehmen besteht. Maßgeblich ist nunmehr der Präventionsaspekt mit den gebotenen Präventionsmaßnahmen im Unternehmen.

Die im Gesetz geregelte Anwendungsausnahme von Section 250 ist enger gefasst, als sie zunächst scheint: Ein Unternehmen entgeht der Strafbarkeit nur, wenn das gesamte relevante Handeln des betreffenden Unternehmens vollständig außerhalb von Großbritannien sattgefunden hat. Andernfalls ist dem Unternehmen die Strafbarkeit der Senior-Manager zuzurechnen. Für deutsche Unternehmen, mit Bezug zu Großbritannien, sind damit auch die Rechtsnormen des neuen Crime and Policing Act 2026 zu beachten.

Großbritannien fügt damit nicht nur weitere Strafnormen hinzu. Vielmehr wird eine erweiterte Compliance-Philosophie „exportiert". Prävention zuerst, immer Evidenz und Verantwortlichkeit des Senior-Managements und mit direkter Auswirkung auf eine eigene Strafbarkeit des Unternehmens.

Nabeel Osman und Dr. José A. Campos Nave



© SPENCER WEST

Nabeel Osman, Barrister (England and Wales) ist Partner von SPENCER WEST und verantwortet die Bereiche Risk, Investigations & Disputes.



© SPENCER WEST

Dr. José A. Campos Nave, EMBA (Accounting & Controlling), Rechtsanwalt, Fachanwalt für Steuer-, Gesellschafts- und Handelsrecht, ist Managing Partner von SPENCER WEST Middle East.

Compliance & KI 2.0 – Das Update

Bereit für den rechtssicheren Einsatz künstlicher Intelligenz nach der KI-VO

Basis- & Aufbau-Webinar

Eine Veranstaltung der Kommunikation & Recht

03. & 04. Dezember 2026, 09.00 bis 12.00 Uhr | Zoom

Jetzt anmelden!

BASIS-WEBINAR Donnerstag, 03. Dezember
KI-Compliance verstehen

- **Einführung und Rahmen der KI-Regulierung**
- **Technische Basics & Anwendungsmöglichkeiten von KI**
- **Grundlagen der Risikoklassifizierung und Folgecompliance**
  - Überblick und Anwendungsbeispiele
  - Compliance bei Hochrisiko-KI-Systemen
  - Anforderungen für sonstige KI-Systeme und KI-Modelle
  - Praktische Herausforderungen
- **Rahmen und Umsetzungsbeispiele von KI-Kompetenz nach Art. 4 KI-VO**
- **Fragestellungen beim Einsatz von GenAI**
- **Überblick zu datenschutzrechtlichen Fragestellungen**
- **Normative Schnittstellen der KI-VO**
- **Tipps und Praxisbeispiele**

AUFBAU-WEBINAR Freitag, 04. Dezember
KI-Compliance in der Praxis

- **Das Omnibus-Paket**
  - Änderungen für Hochrisiko-KI-Systeme, Auswirkungen auf KI-Compliance, Umsetzung des AI Acts
- **Deep dive und best practices bei der Verwendung von Hochrisiko-KI-Systemen**
  - Umsetzungsbeispiele von Compliance bei Hochrisiko-KI-Systemen und Normierungsstand
- **Nationales Durchführungsgesetz der KI-VO**
- **Einordnung und Verwendung von RAG-Systemen**
  - Compliance nach der KI-VO und datenschutzrechtliche Aspekte
- **Klassifizierung und Einordnung von Agentic AI**
- **Aufbau einer eigenen KI-Governance in der Organisation**
- **Wichtige Punkte bei Third-Party KI-Systemen**
- **Tipps und Praxisbeispiele**

SEMINARLEITER & MODERATOR



Dr. Robert Müller, LL.M.

Aufbau-Webinar auch einzeln buchbar!

Jetzt anmelden & KI-Kompetenzen nach Art. 4 KI-VO sichern!

Ihre Ansprechpartnerin:

Frau Maria Belz
Projektmanagerin

Deutscher Fachverlag GmbH
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de



Teilnahmegebühren (zzgl. MwSt.):

359,– EUR Abonnent:innen K&R, CB, DSB
449,– EUR Normalpreis

Sie möchten auf das Basis-Webinar verzichten und nur am Aufbau-Webinar teilnehmen? Dann erhalten Sie **50 % Rabatt.** Weitere Informationen unter www.ruw.de/COKI.

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

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

Der „DORO“ im Gefüge des Beauftragtenwesens

Mit der Verordnung (DORA) 2022/2554 hat der europäische Gesetzgeber eine neue Governance-Rolle eingeführt: den Digital Operational Resilience Officer (DORO). Diese Funktion stellt Finanzunternehmen vor erhebliche organisatorische und rechtliche Herausforderungen.



© KI-generiert / Christina Kahlen-Pappas / Flux 2 Pro

„Exotin“ unter den Beauftragten: Digital Operational Resilience Officer – DORO.

Das europäische Beauftragtenwesen entstand als Reaktion auf die Finanzkrise 2007/2008. Heute sind Finanzunternehmen verpflichtet, mehrere spezialisierte Beauftragtenrollen zu besetzen: Compliance Officer, Risk Management Officer, Datenschutzbeauftragte, Revisionsbeauftragte, Geldwäschebeauftragte und Auslagerungsbeauftragte.

Diese Vielfalt führt besonders bei kleineren Instituten zu erheblichen Kostensteigerungen und schafft Zuständigkeitskonflikte. Der deutsche Gesetzgeber begegnet diesen Konflikten durch das Prinzip der Rollenverteilung: Überwachungspflichten müssen auf verschiedene Personen verteilt werden, wenn deren Ausübung kollidierende Interessen mit sich bringt.

Datenschutzbeauftragte unterliegen dem Prinzip der Datenminimierung. Dies führt zu fundamentalen Interessenskollisionen mit anderen Beauftragten, die umfassende Datensammlungen benötigen, wie etwa der Risk Manager oder Compliance Officer.

Revisionsbeauftragte stehen in fundamentaler Inkompatibilität mit allen anderen Rollen. Nach dem 3-Lines-of-Defense-Modell muss die Interne Revision alle anderen Funktionen unabhängig überprüfen können.

Risk Management Officer sollten je nach Institutsgröße von Rollen der „Marktfolge“, also solchen, die direkt mit dem laufenden Geschäftsbetrieb verbunden sind und Marktaktivitäten überwachen, getrennt bleiben.

Geldwäschebeauftragte können mit anderen Funktionen kombiniert werden, allerdings unter strikter Datentrennung gemäß § 7 Abs. 6 GWG.

Compliance Officer und Auslagerungsbeauftragte unterliegen weniger strikten Kombinationsbeschränkungen.

Der DORO unterscheidet sich fundamental von diesen klassischen Beauftragten. Die DORA schreibt die Funktion nicht ausdrücklich vor, sondern verlangt in Art. 6 Abs. 4 nur, dass die Verantwortung für IKT-Risikomanagement an eine unabhängige „Kontrollfunktion“ übertragen wird. Der DORO hat darum auch keine eigenständige Aufgabenkompetenz wie andere Beauftragte. Seine Aufgaben leiten sich aus den allgemeinen IKT-Managementpflichten der Geschäftsleitung ab. Der DORO nimmt somit Geschäftsleitungsaufgaben wahr, anstatt eigene Kompetenzen auszuüben. Dies erklärt, warum Konkurrenzen mit anderen Beauftragten de jure nicht entstehen.

Dennoch muss unter Berücksichtigung der hohen Anforderungen an die Unabhängigkeit unterschieden werden:

Der DORO ist vereinbar mit: Compliance Officer, Risk Management Officer (mit Einschränkungen), Geldwäschebeauftragtem (unter strikter Datentrennung) und Auslagerungsbeauftragtem.

Nicht vereinbar ist er hingegen mit: Datenschutzbeauftragtem und Revisionsbeauftragtem.

Die Geschäftsleitung trägt die volle Verantwortung für die Einhaltung der Rollentrennung. Bei Rollenkombinationen muss die Geschäftsleitung die Vereinbarkeit nachvollziehbar begründen können. Geschäftsleitungsmitglieder, die die DORO-Funktion übernehmen, müssen selbst die Unabhängigkeit ihrer Position beurteilen und gewährleisten.

Den ausführlichen Beitrag von Prof. em. Dr. Dieter Krimphove und Sebastian Vogel unter anderem mit einer tiefgreifenden Analyse der Interessenskollisionen zwischen Datenschutzbeauftragten und anderen Rollen unter Bezug auf Art. 25 DSGVO; einer systematische Erörterung des 3-Lines-of-Defense-Modells und dessen Implikationen für die Revisionsbeauftragtenfunktion sowie eine ausführliche Diskussion der Besonderheiten des Geldwäschebeauftragten unter Berücksichtigung von § 7 Abs. 6 GWG und konkrete Handlungsempfehlungen für die Geschäftsleitung bei der Implementierung der DORO-Funktion lesen Sie im Compliance-Berater 2026, 449.



© privat

Prof. em. Dr. jur. Dieter Krimphove ist emeritierter Inhaber des Lehrstuhls „Europäisches und deutsches Wirtschaftsrecht“, sowie Jean-Monet Professor „ad personam“ und Professor der Donau-Universität Krems.



© privat

Sebastian Vogel ist Prüfer für Informationssicherheit und digitale operationale Resilienz im Bereich Banking und Finance bei der Wirtschaftsprüfungsgesellschaft Grant Thornton AG in Frankfurt.

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
UStIdNr. 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
Jede Verwertung innerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeisung in eine Datenbank.

SAVE THE DATE
Heute schon Termin vormerken

Eine Veranstaltung des
Compliance Berater

27. bis 28. April 2027 | Frankfurt am Main

Deutsche Compliance Konferenz

JETZT ANMELDEN UNTER
www.deutsche-compliance-konferenz.de
oder QR-Code scannen

Frühbucherpreis sichern!

Veranstaltungsort:
dfv Mediengruppe
Mainzer Landstraße 251
60326 Frankfurt am Main

Anmeldeschluss: 26. April 2027
Eine frühzeitige Anmeldung wird empfohlen.
Anmeldung unter www.deutsche-compliance-konferenz.de

Fortbildungsveranstaltung nach § 15 FAO!

Ihre Ansprechpartnerin:
Frau Maria Belz
Projektmanagerin
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de



Sie möchten Partner werden?
Ihr guter Name steht im Mittelpunkt!
Sprechen Sie uns an:
Tel.: +49 69 7595-2779
E-Mail: Mikhail.Tsyganov@dfv.de



Teilnahmegebühren (zzgl. MwSt.):

849,–	EUR	Unternehmensvertreter:innen
1.029,–	EUR	Abonnent:innen CB, GWuR
1.199,–	EUR	Normalpreis

Rabatte – so sparen Sie intelligent:

5 % Frühbucherrabatt
bei Anmeldung bis 22. Januar 2027.

5 % Mehrbucherrabatt
bei Anmeldung von mehr als 2 Teilnehmer:innen einer Kanzlei / eines Unternehmens ab der 3. Anmeldung (mit anderen Rabatten kombinierbar).

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

Arbeitszeiterfassung: Rechtslage, Bußgelder und behördliche Befugnisse

Schreiben von Aufsichtsbehörden mit Forderungen nach umfangreichen Arbeitszeitnachweisen und Hinweisen auf mögliche Bußgelder verunsichern derzeit viele Unternehmen. Die aktuellen Anforderungen zur Arbeitszeiterfassung bedürfen daher einer rechtlichen Einordnung.



© KI-generiert / Christina Kahlen-Pappas / Flux 2 Pro

Arbeitszeitnachweise: Unternehmen sollten sich durch Aufsichtsbehörden nicht verunsichern lassen.

Nach § 16 Abs. 2 ArbZG i.V.m. § 3 Satz 1 ArbZG waren Arbeitgeber bislang nur verpflichtet, die über acht Stunden hinausgehende werktägliche Arbeitszeit der Arbeitnehmer aufzuzeichnen und diese Aufzeichnungen mindestens zwei Jahre aufzubewahren. Eine Pflicht zur vollständigen Erfassung der täglichen Arbeitszeit ergibt sich aus dem Arbeitszeitgesetz in seiner geltenden Fassung nicht.

Durch den Beschluss des BAG vom 13. September 2022 – den sogenannten „Stechuhr-Beschluss" – hat sich diese Rechtslage grundlegend geändert. Das Gericht entschied, dass Arbeitgeber verpflichtet sind, Beginn, Ende und Dauer der gesamten täglichen Arbeitszeit ihrer Beschäftigten zu erfassen. Diese Verpflichtung leitete das Gericht aus § 3 Abs. 2 Nr. 1 Arbeitsschutzgesetz in unionsrechtskonformer Auslegung dieser Vorschrift her.

Das BAG machte dabei bewusst keine Vorgaben zur Art der Zeiterfassung. Die Erfassung kann daher in Papierform oder elektronisch erfolgen. Die Zeiterfassung kann auch auf Arbeitnehmer delegiert werden. Ausgenommen von der Erfassungspflicht bleiben leitende Angestellte (§ 18 Abs. 1 Nr. 1 ArbZG i.V.m. § 5 Abs. 3 BetrVG).

Wird keine Arbeitszeit erfasst, hängen die bußgeldrechtlichen Folgen davon ab, welche Arbeitszeit nicht erfasst wurde:

Verstoß gegen die ArbZG-Aufzeichnungspflicht: Ein Verstoß gegen die Pflicht zur Aufzeichnung der werktäglichen Arbeitszeit, die acht Stunden überschreitet, ist gemäß § 22 Abs. 1 Nr. 9 ArbZG bußgeldbewehrt und kann mit einer Geldbuße von bis zu 30.000 EUR geahndet werden. Adressaten eines Bußgeldbescheids können das Unternehmen, die Geschäftsführung oder sonstige verantwortliche Personen sein.

Verstoß gegen die Arbeitsschutzgesetz-Aufzeichnungspflicht: Ein Verstoß gegen die aus dem Arbeitsschutzgesetz folgende Pflicht zur Aufzeichnung der werktäglichen Arbeitszeit, die acht Stunden nicht überschreitet, ist nach überwiegender Auffassung bislang nicht ohne Weiteres bußgeldbewehrt, da eine entsprechende gesetzliche Bußgeldvorschrift fehlt.

Im Koalitionsvertrag von CDU, CSU und SPD wurde die „unbürokratische" Einführung einer Pflicht zur elektronischen Arbeitszeiterfassung vereinbart. Für kleine und mittlere Unternehmen sollen Übergangsregelungen geschaffen werden. Vertrauensarbeitszeit soll ohne Zeiterfassung „im Einklang mit der EU-Arbeitszeitrichtlinie" möglich bleiben.

Mitte Juni 2026 wurde ein Referentenentwurf aus dem Bundesarbeitsministerium bekannt, der eine Pflicht zur elektronischen Arbeitszeiterfassung vorsah. Ausnahmen sollten nur für Arbeitgeber mit bis zu zehn Arbeitnehmern gelten. Dieser Entwurf wurde allseits kritisiert – insbesondere auch deshalb, weil die Vereinbarung einer wöchentlichen (statt werktäglichen) Arbeitszeit den Tarifvertragsparteien vorbehalten bleiben sollte. Das Bundesarbeitsministerium erklärte daraufhin, es habe sich nur um ein internes Arbeitspapier gehandelt.

Nach § 17 Abs. 2 ArbZG kann die Aufsichtsbehörde die erforderlichen Maßnahmen anordnen, um die Einhaltung des Arbeitszeitgesetzes sicherzustellen. Nach § 17 Abs. 4 ArbZG kann sie vom Arbeitgeber Auskünfte verlangen und Unterlagen wie Arbeitszeitnachweise, Geschäftsunterlagen und Tarifverträge anfordern.

Allerdings: Eine allgemeine, ungezielte Ausforschung eines Arbeitgebers ist unzulässig. § 17 Abs. 4 ArbZG verlangt für ein Tätigwerden der Aufsichtsbehörde aber auch nicht, dass konkrete Verstöße bereits feststehen. Ausreichend, aber auch erforderlich, ist ein berechtigter Anlass zu prüfen, ob ein Arbeitgeber die Arbeitszeitvorschriften einhält.

Ein solcher berechtigter Anlass kann vorliegen, wenn eine Betriebsprüfung Anhaltspunkte für Verstöße ergeben hat oder bei der Behörde (anonyme) Hinweise eingegangen sind.

Erteilt ein Arbeitgeber angeforderte Auskünfte nicht, nicht richtig oder nicht vollständig oder legt angeforderte Unterlagen nicht oder nicht vollständig vor, stellt dies eine Ordnungswidrigkeit dar, die mit einer Geldbuße von bis zu 30.000 EUR geahndet werden kann (§ 22 Abs. 1 Nr. 10 ArbZG).

Voraussetzung ist jedoch, dass das Auskunftsverlangen der Aufsichtsbehörde zulässig ist und der Arbeitgeber angehört wurde. Ist bereits das Auskunftsersuchen unzulässig, weil es anlasslos erfolgt, kann die Nichtübermittlung von Arbeitszeitnachweisen auch keine Ordnungswidrigkeit darstellen.

Fazit: Arbeitgeber sind zur Erfassung von Beginn, Ende und Dauer der täglichen Arbeitszeit verpflichtet. Die Erfassung kann manuell oder elektronisch erfolgen. Leitende Angestellte sind von der Zeiterfassungspflicht ausgenommen. Ein Verstoß gegen diese Pflicht kann derzeit nicht ohne Weiteres als Ordnungswidrigkeit geahndet werden – es fehlt an einer gesetzlichen Grundlage. Bußgeldbewehrt sind bislang nur Verstöße gegen die Aufzeichnungspflicht für diejenige Arbeitszeit, die acht Stunden werktäglich überschreitet.

Arbeitgeber sollten Schreiben von Aufsichtsbehörden darum sorgfältig prüfen und beachten, dass anlasslose Anforderungen von Arbeitszeitnachweisen unzulässig sind.



© Pusch Wahlig Workplace Law

Kristina Schilder, Rechtsanwältin und Fachanwältin für Arbeitsrecht, Associated Partnerin bei Pusch Wahlig Workplace Law.

3. Fachtagung „Cyber-Angriff“

Akute Bewältigung von Cyber-Angriffen durch Technik, Recht und Kommunikation

Eine Veranstaltung von Kommunikation & Recht

in Kooperation mit DUNKELBLAU, DigiFors, SPIRIT LEGAL

25. Februar 2027 | Gondwanaland, Zoo Leipzig

Jetzt anmelden!

Den Überblick im Cyber-Dschungel behalten – leichter gesagt als getan, wenn ein Angriff von Online-Kriminellen das eigene Unternehmen trifft. Welche technischen Maßnahmen müssen ergriffen werden, um die Systeme wieder zum Laufen zu bringen? Was gibt es bei der Zusammenarbeit mit Behörden und was im Bereich Datenschutz/-sicherheit zu beachten? Wie führt man Lösegeldverhandlungen – und was ist die rechtliche Grundlage dafür? Und nicht zuletzt: Wie kommuniziert man an Mitarbeitende, Kunden und Zulieferer, wenn wenig sicher ist und nichts funktioniert?

Unsere hochkarätigen Gäste bringen Licht ins Dunkel und beantworten Ihnen einen Tag lang alle Fragen, die Sie sich rund um die Vorbereitung auf ein solches Szenario stellen sollten – übrigens unabhängig davon, wie groß Ihr Unternehmen ist und in welcher Branche Sie tätig sind.

FREUEN SIE SICH UNTER ANDEREM AUF:

- Cyberwar trifft Wirtschaft: Wie Staaten Unternehmen angreifen – und was wir von ihren Angreifern lernen können
- Vom Cyber-Angriff zur Unternehmenskrise: Wer steuert eigentlich, wenn die Krise das Business erreicht?
- Breach, Beweis, Lösegeld – Cybersecurity trifft IT-Forensik trifft Verhandlung
- Von der Reaktion zur Resilienz: Krisenmanagement im Konzern etablieren
- Schlüsseldienst für Kriminelle: Passwortknacken erklärt
- Streitgespräch zum Datenschutz

Get-together im Auerbachs Keller & Eintritt ins Gondwanaland inklusive!

MIT DIESEN UND WEITEREN SPEAKERN:



Marcus Ewald
DUNKELBLAU



Dirk Kunze
Cyber Resilience Lab



Jörg Schauff
SimSpace



Olga Stepanova
ByteLaw Rechtsanwälte



Peter Hense
Spirit Legal



Christian Klaus-Birkner
DigiFors



Janine Rauch
Schnellecke Group



Johann Rabbow
Oneconsult Deutschland



Martin Wölfel
Wavestone Germany

Fortbildungsveranstaltung nach § 15 FAO!

Ihre Ansprechpartnerin: Frau Maria Belz

Projektmanagerin
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de



Sie möchten Partner werden?
Ihr guter Name steht im Mittelpunkt!

Sprechen Sie uns an:

Tel.: +49 69 7595-2779
E-Mail: Mikhail.Tsyganov@dfv.de



Teilnahmegebühren (zzgl. MwSt.):

599,– EUR Abonnent:innen KuR, CB, DSB
779,– EUR Normalpreis

Rabatte – so sparen Sie intelligent:

5 % Frühbucherrabatt
bei Anmeldung bis zum 30. Oktober 2026.

5 % Mehrbucherrabatt
bei Anmeldung von mehr als 2 Teilnehmer:innen einer Kanzlei / eines Unternehmens ab der 3. Anmeldung (mit anderen Rabatten kombinierbar).

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

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

Interne Ermittlungen wirksam steuern

Kaum ein Instrument der Compliance-Arbeit wird ebenso häufig angewendet und unterschätzt wie die interne Ermittlung. Stehen Regelverstöße im Raum, muss ein Unternehmen unverzüglich handeln, darf aber nichts überstürzen. Wer vorbereitet ist, kann Ermittlungen zielgerichteter und mit echtem Mehrwert für die Compliance-Organisation durchführen.



KI-generiert / Christina Kahlen-Pappas / Flux 2 Pro

Interne Ermittlungen: Sie müssen von Beginn an gut organisiert sein.

Fehler passieren schon vor dem eigentlichen Start einer internen Ermittlung, indem diese hinausgezögert wird. Häufige Ursache ist die Sorge, mit dem Beginn bereits rechtliche Fristen auszulösen, etwa für eine außerordentliche Kündigung. Diese Sorge ist in aller Regel unbegründet, denn Fristen werden gehemmt, solange der Sachverhalt mit der gebotenen Eile, aber auch Tiefe aufgeklärt wird. Zeitverlust vor Beginn schafft also keine Sicherheit, sondern schadet der Ermittlung selbst, weil Erinnerungen und Spuren verblassen und das Risiko der Vernichtung von Beweismitteln, zufällig oder absichtlich, steigt.

Auch die personelle Aufstellung entscheidet über Erfolg oder Misserfolg einer internen Untersuchung. Einem zu kleinen oder fachlich zu eng gefasstem Team mangelt es an Durchsetzungskraft und Tiefe. Ein zu großes Team krankt an Zuständigkeitsrangeleien, aufwändigen internen Abstimmungsprozessen und steigendem Risiko, dass Informationen durchsickern. Generell gilt: Art und Umfang des Vorwurfs definieren die Größe des Ermittlerteams, dessen Zusammensetzung während des Prozesses laufend validiert und gegebenenfalls verändert werden sollte. Vor allem bedarf es eines Steuerungsgremiums mit Entscheidungskompetenz, bei dem alle Fäden zusammenlaufen und das regelmäßig den Lauf und Fortgang der Ermittlungen evaluiert.

Ein besonders gravierender Fehler liegt darin, technische Fakten zu schaffen, bevor hierfür eine rechtliche Grundlage steht. Zu Beginn der Ermittlungen überkommt alle Beteiligten häufig eine Art „Übereifrigkeit". Postfächer werden umfassend gesichert und teilweise schon ausgewertet, obwohl der erforderliche Anfangsverdacht (§ 26 Abs. 1 S. 2 BDSG) und die beabsichtigten Ermittlungsschritte noch nicht dokumentiert sind. Folge kann ein Verwertungsverbot im späteren arbeitsgerichtlichen Verfahren sein (siehe LAG Hessen). Klassiker sind auch die vermeintlich nur dienstlichen E-Mail-Accounts betroffener Arbeitnehmer, deren private Nutzung der Arbeitgeber duldet. Hier darf nicht „mit Schleppnetz gefahndet", sondern nur anlassbezogen und auf der Grundlage ordnungsgemäßer vorheriger Dokumentation geprüft werden. Ähnlich verhält es sich mit dem Adressatenkreis einer Ermittlung: Ist dieser zu groß, steigen Rechtsrisiken, vor allem aber ist die Vertraulichkeit nicht gewahrt.

Wer nicht weiß, wonach er sucht, übersieht Relevantes oder verliert sich in Nebensächlichkeiten. Fehlt zu Beginn eine klare Zielsetzung, laufen Ermittlungsteams Gefahr, jeden zufällig entdeckten Nebenaspekt mit derselben Intensität zu verfolgen wie den ursprünglichen Verdacht. Das treibt Kosten und Dauer der Ermittlungen in die Höhe. Das umgekehrte Extrem ist ebenso fatal: Wird von Beginn an nur mit Tunnelblick nach Bestätigung des schon vorweg vermeintlich feststehenden Ergebnisses gesucht, gehen entlastende Hinweise unter.

Wird ohne konkreten Anlass gegen eine bereits im Fokus stehende Person „in alle Richtungen" ermittelt, ist dies unverhältnismäßig, mit der Folge, dass die Erkenntnisse nicht oder jedenfalls nur eingeschränkt verwertet werden dürfen (siehe BAG-Urteil). Wird hingegen nur in eine Richtung ermittelt, um einen ursprünglichen Verdacht zu erhärten, ohne dabei entlastende Hinweise zu berücksichtigen, wird das von den Arbeitsgerichten ebenso negativ aufgefasst (siehe BAG, Urt. v. 13. März 2008 – 2 AZR 961/06).

Häufig atmen Unternehmen auf, sobald die Ermittlungen abgeschlossen sind, Schlüsse werden aber jenseits des konkreten Falls nicht gezogen. Bleiben die strukturellen Ursachen unangetastet, ist es nur eine Frage der Zeit, bis sich Ähnliches wiederholt. Wer stattdessen aus wenigen zentralen Erkenntnissen konkrete, mit klarer Verantwortung versehene Maßnahmen für Prozesse und Kontrollen ableitet, gewinnt mehr als nur die Aufklärung eines Einzelfalls. Auch nach Abschluss behördlicher oder gerichtlicher Verfahren lohnt sich ein zweiter Blick, denn oft liefern die endgültigen Ergebnisse weitere Erkenntnisse für die Compliance-Struktur.

Die beschriebenen Schwachstellen haben eines gemeinsam: Sie sind selten Ausdruck fehlender rechtlicher oder forensischer Kompetenz, sondern organisatorischer Natur. Unternehmen, die interne Ermittlungen von Beginn an klar strukturieren, konsequent am eingangs definierten Ermittlungsziel ausrichten und ihre Ergebnisse systematisch in verbesserte Prozesse und Kontrollen überführen, machen aus jedem Verdachtsfall einen Baustein für eine belastbarere und sich stetig verbessernde Compliance-Organisation.

Dr. Hans-Hermann Aldenhoff, LL.M. (Sydney), und Mag. iur. Max Lange



© Simmons & Simmons

Dr. Hans-Hermann Aldenhoff, LL.M. ist Rechtsanwalt und Partner bei Simmons & Simmons. Er leitet die Globale Investigations-Gruppe der Sozietät.



© Simmons & Simmons

Max Lange ist wissenschaftlicher Mitarbeiter am Düsseldorfer Standort von Simmons & Simmons in der Praxisgruppe Dispute Resolution.

Rüstung & Reputation

Heikle Themen, hoch reguliert und Spannungen innen und außen:

Best Practice Kommunikation in der Zeitenwende

Eine Veranstaltung von
Rüstung, Sicherheit & Recht
Zeitschrift für Verteidigung, Heimatschutz, Cyber & Space
Kommunikation & Recht

in Kooperation mit
DUNKELBLAU

11. Februar 2027 | München

Verteidigungsunternehmen stehen nicht mehr gelegentlich im Fokus, sondern dauerhaft. Bürgerinitiativen klagen gegen neue Standorte. Cyberangriffe legen Zulieferdaten offen. Exportkontrollverfahren bedrohen die Existenz mittelständischer Hersteller, Desinformation richtet sich gezielt auf die Branche. Und Belegschaften tragen die neue Rolle ihres Arbeitgebers nicht automatisch mit. Kommunikation bewegt sich hier im Spannungsfeld von Haftungsrecht, Exportkontrolle, Politik und Öffentlichkeit.

Konzerne haben dafür eigene Stäbe. Mittelständler, Zulieferer, Dual-Use-Unternehmen und Start-ups in der Regel nicht.

Für sie ist „Rüstung & Reputation" konzipiert.

FREUEN SIE SICH UNTER ANDEREM AUF DIESE SPANNENDEN WIE HEIKLEN THEMEN:

- Communication Governance: Regeln mit Partnern, Kunden und Aufsicht, um die Informationshoheit zu sichern
- Medien und Rüstungsimage: Wie Redaktionen die Aufrüstung sehen und was sie von Unternehmen erwarten
- Recht als Angriffswerkzeug: Wie Dritte juristisch gegen Defence-Unternehmen vorgehen
- Krisenkommunikation und Akzeptanz: Cybervorfälle, Standortprojekte, sensible Exporte
- Informationskrieg: Was Unternehmen aus der Ukraine lernen können
- inklusive Get-together am Vorabend

Frühbucherpreis sichern!

Veranstaltungsort:
PresseClub München e. V.
Marienplatz 22
80331 München

Anmeldeschluss: 10. Februar 2027
Eine frühzeitige Anmeldung wird empfohlen.
Anmeldung unter **www.ruw.de/ruestung**

Fortbildungsveranstaltung nach § 15 FAO!

Ihre Ansprechpartnerin:
Frau Maria Belz
Projektmanagerin
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de



Sie möchten Partner werden?
Ihr guter Name steht im Mittelpunkt!
Sprechen Sie uns an:
Tel.: +49 69 7595-2779
E-Mail: Mikhail.Tsyganov@dfv.de



Teilnahmegebühren (zzgl. MwSt.):
499,– EUR Abonnent:innen RüSiR, KuR, CB, DSB
699,– EUR Normalpreis

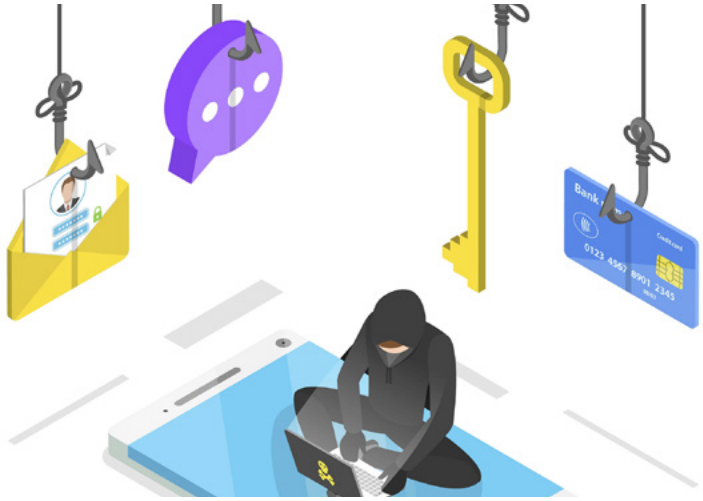
Rabatte – so sparen Sie intelligent:
5 % Frühbucherrabatt
bei Anmeldung bis zum 20. November 2026.
5 % Mehrbucherrabatt
bei Anmeldung von mehr als 2 Teilnehmer:innen einer Kanzlei / eines Unternehmens ab der 3. Anmeldung (mit anderen Rabatten kombinierbar).

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

// WIR FEIERN **80 JAHRE** /
R&W Fachkonferenzen
Eine Medienmarke der dfv Mediengruppe

EuGH: Verbraucherschutz steht nach Zahlungsbetrug im Vordergrund

Ein aktuelles Urteil des Europäischen Gerichtshofs (15. Oktober 2026 – C-70/25) stellt klar: Grobe Fahrlässigkeit des Kunden entbindet die Bank nicht von ihrer Pflicht zur unverzüglichen Rückerstattung nicht autorisierter Zahlungen. Der EuGH etabliert eine Vorgehensweise in zwei Schritten, die den Verbraucherschutz priorisiert.



IMAGO / imagebroker

Phishing betrifft auch personalisierte Sicherheitsmerkmale im Online-Banking.

Eine polnische Bankkundin fiel auf einen Phishing-Anschlag herein: Ein Betrüger täuschte mit einem gefälschten Link die Transaktion auf einer Online-Verkaufsplattform vor. Die Bankkundin gab ihre Banking-Zugangsdaten ein, der Täter nutzte die Daten, um ca. 700 Euro auf sein Konto zu überweisen. Die Kundin meldete ihrer Bank den Betrug am Folgetag, die Bank weigerte sich jedoch, der Kundin die Summe zu erstatten und berief sich auf grobe Fahrlässigkeit der Kundin: Sie habe ihre personalisierten Sicherheitsmerkmale nicht angemessen geschützt.

In der Folge kam es zu einem Rechtsstreit vor einem polnischen Gericht, das den EuGH fragt, ob die Bank in ihrer Eigenschaft als Zahlungsdienstleister gemäß dem Unionsrecht verpflichtet ist, den Betrag eines nicht autorisierten Zahlungsvorgangs unverzüglich zu erstatten, selbst wenn sie der Ansicht ist, dass der Kunde grob fahrlässig gehandelt habe.

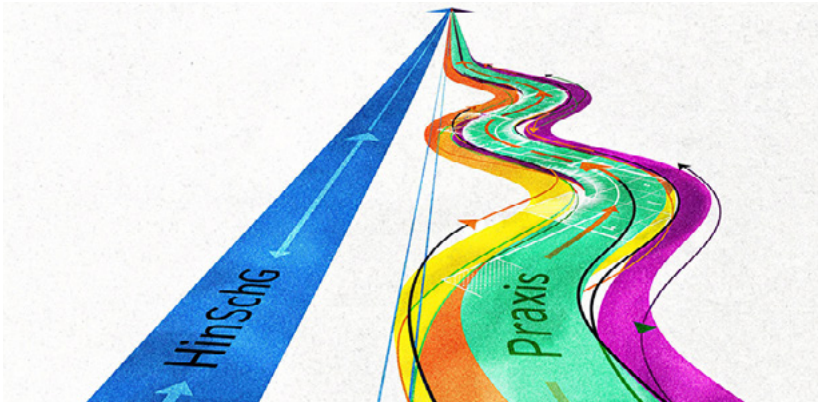
Der EuGH bejaht die Frage und stellt folgende Regel in zwei Schritten auf:

1. Schritt – Unverzügliche Erstattung: Zahlungsdienstleister müssen den Betrag spätestens bis Ende des nächsten Geschäftstags erstatten, sobald sie von dem Betrug erfahren – unabhängig davon, ob sie eine Fahrlässigkeit des Kunden vermuten. Von der Pflicht zur unverzüglichen Erstattung ist eine einzige Ausnahme vorgesehen, für den Fall, dass der Zahlungsdienstleister berechtigte Gründe für den Verdacht hat, dass ein vom Kunden begangener Betrug vorliegt, und die Bank diese Gründe der zuständigen nationalen Behörde schriftlich mitteilt.

2. Schritt – Regress-Anspruch: Erst nach der Erstattung darf die Bank vom Kunden Schadensersatz fordern – aber nur, wenn sie nachweist, dass die Verluste auf vorsätzliches oder grob fahrlässiges Verhalten des Kunden zurück zu führen sind. Die Beweislast trägt der Zahlungsdienstleister.

Der Verbraucherschutz geht also ausdrücklich vor. Der EuGH begründet seine Entscheidung damit, dass Kunden sonst gezwungen würden, kostspielige Verfahren anzustrengen, um legitime Ansprüche durchzusetzen. *chk*

Umfrage zur Umsetzung des HinSchG in deutschen Unternehmen



© KI-generiert / Christina Kahlen-Pappas / Flux 2 Pro

In der Praxis oft kein gerader Weg: Die Umsetzung des HinSchG.

Im Rahmen einer Dissertation an der Hochschule Heilbronn wird die Umsetzung des Hinweisgeberschutzgesetzes (HinSchG) in Unternehmen unterschiedlicher Größe in Deutschland untersucht. Hierzu wird derzeit eine anonyme Online-Umfrage durchgeführt, die sich an Compliance-Officer und Meldestellenbeauftragte in Deutschland richtet. Mit der Umfrage werden praktische Erfahrungen und Einschätzungen gesammelt und erforscht, um einen Vergleich zwischen dem gesetzlichen Anspruch des HinSchG und der betrieblichen Praxis zu ermöglichen sowie Unterschiede in Bezug auf die Unternehmensgröße zu erfassen.

Die Umfrage beginnt mit allgemeinen Angaben zu den teilnehmenden Unternehmen, bevor Fragen zur internen Meldestelle, den dort eingehenden Meldungen und dem internen Meldeverfahren folgen. Anschließend werden kurz die Themen Personal und die sich rasant weiterentwickelnde KI beleuchtet. Die Umfrage schließt ab mit einer individuellen Beurteilung sowohl zur eigenen Unternehmenspraxis als auch zum HinSchG selbst sowie der Möglichkeit zur Nennung von Verbesserungsvorschlägen für das Gesetz. *chk*

Bitte um Unterstützung

Ihre Teilnahme trägt wesentlich zu einem besseren Verständnis der praktischen HinSchG-Umsetzung bei. Die Umfrage ist vollkommen anonym und dauert etwa 5-7 Minuten. Sie kann über den folgenden Link erreicht werden: https://forms.cloud.microsoft/e/ccKKpkSMyU

Neuerscheinung

AMLR wird wirksam. Sind Sie bereit?



Die Geldwäsche-Compliance steht vor einem tiefgreifenden Umbruch: Mit dem EU-Geldwäschepaket und der ab dem 10. Juli 2027 unmittelbar geltenden AMLR werden die geldwäscherechtlichen Anforderungen neu geordnet und erweitert. Das Handbuch unterstützt Geldwäschebeauftragte und ihre Teams bei der praxisgerechten Umsetzung der geldwäscherechtlichen Vorgaben und gibt Orientierung für die aktuellen und künftigen Anforderungen.

Themenschwerpunkte im Überblick:

- Geldwäscherechtliche Anforderungen und deren praktische Umsetzung im Unternehmen
- Aufgaben, Pflichten und Verantwortlichkeiten von Geldwäschebeauftragten und ihren Teams
- Best Practices und Anforderungen der Aufsichtsbehörden, insbesondere der Bafin
- AMLR und künftige Anforderungen: Auswirkungen auf Prozesse, Compliance und Aufsicht

Der Autor

Dr. **Paul Schultess** ist Rechtsanwalt, externer Geldwäschebeauftragter und Lehrbeauftragter. Er berät Institute und Unternehmen insbesondere zu aufsichtsrechtlichen Fragen der Corporate Governance, Geldwäscheprävention und Compliance und begleitet Prüfungen durch Aufsichtsbehörden und Wirtschaftsprüfer. Als langjähriger externer Geldwäschebeauftragter verschiedener BaFin-beaufsichtigter Institute kennt er die Praxis der Geldwäscheprävention aus erster Hand. An der Goethe-Universität Frankfurt am Main lehrt er am Institut für Versicherungsrecht insbesondere zu Unternehmenshaftung und -versicherung.

Paul Schultess
Geldwäschebeauftragte
Ein Praxishandbuch zur operativen Umsetzung regulatorischer Vorgaben

1. Auflage 2026 | Compliance-Berater Schriftenreihe
486 Seiten | Broschur | € 89,00
ISBN: 978-3-8005-1863-0

Weitere Informationen
shop.ruw.de

Keine Buch-Neuerscheinung mehr verpassen? Abonnieren Sie doch gerne unseren Newsletter: **shop.ruw.de/newsletter**

dfv Mediengruppe
www.shop.ruw.de | Deutscher Fachverlag GmbH | Frankfurt am Main
Tel 08581 9605-0 | Fax 08581 754 | E-Mail info@suedost-service.de
R&W Fachmedien Recht und Wirtschaft