TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Konferenz

Berlin, 26.06.2026

Update
IT-Sicherheitsrecht

Karsten U. Bartels LL.M.
Stv. Vorstandsvorsitzender TeleTrusT, Leiter AG IT-Sicherheitsrecht
Rechtsanwalt HK2

HK2

Gesetz zur Stärkung der Cybersicherheit

HK2

Bearbeitungsstand: 24.02.2026 15:54

Referentenentwurf

des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

A. Problem und Ziel

Cyberangriffe in Deutschland nehmen in Qualität und Quantität zu. Deutschland a
rende Wirtschaftsnation in Europa ist verstärkt im Fokus auch hochprofessioneller C
griffe mit großem Wirkpotential. Angesichts der geopolitischen Lage gewinnen auch
Bedrohungen zunehmend an Bedeutung.

Der Krieg in der Ukraine verdeutlicht, wie essentiell Cybersicherheit für einen r
Staat wie Deutschland ist. Die Gewährleistung einer verlässlichen und sichere
der Informationstechnologie und der zugrundeliegenden Kommunikationsinfra
essentielle Voraussetzung für das Funktionieren des Gemeinwesens. Deutsch
schaftlicher Erfolg, gesellschaftlicher Zusammenhalt und die nationale Sicherh
der Gewährleistung von Cybersicherheit untrennbar verbunden. Angriffe im
überwinden mühelos Landes- oder Zuständigkeitsgrenzen und können sich
sämtliche Lebensbereiche sowie Sektoren einschließlich der Kommunikation
insgesamt auswirken. Gezielte Angriffe auf kritische Infrastrukturen und wicht
men, Aktionen von Cyberkriminellen oder Angriffe auf bzw. Sabotage von sta
turen sind geeignet, die Funktionsfähigkeit des Gemeinwesens, der Wirts
Staats- und Verwaltungswesens massiv und anhaltend zu beeinträchtigen.

Dieser sicherheitspolitischen Herausforderung kann nur begegnet werde
kennung und Abwehr von Cyberangriffen ausgebaut und hierzu wirksam

Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Berlin, 16.03.2026

Stellungnahme

zum

BMI-Referentenentwurf eines Gesetzes zur Stärkung der Cyber-Sicherheit

Kontakt:
RA Karsten U. Bartels, LL.M.
HK2 Rechtsanwälte
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Stellvertretender Vorstandsvorsitzender
Leiter TeleTrusT-AG "IT-Sicherheitsrecht"
bartels@hk2.eu

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breitgefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

HK2

BSI-Gesetz-E (Referentenentwurf)

§ 31 Absatz 2 wird wie folgt gefasst:

„(2) Betreiber kritischer Anlagen sind verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter, Merkmale aus dem laufenden Betrieb sowie regelmäßige Verfügbarkeitsindikatoren der kritischen Anlage kontinuierlich und automatisch erfassen, auswerten und angebunden an das Bundesamt ausleiten, soweit das Bundesamt nicht auf die Anbindung verzichtet. Das Bundesamt legt die Anforderungen an die Anbindung und Ausleitung fest und veröffentlicht diese auf seiner Internetseite. Die Systeme zur Angriffserkennung sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

HK2

BKA-Gesetz-E

§ 62e

Erheben, Löschen und Verändern von Daten in informationstechnischen Systemen

(1) Das Bundeskriminalamt darf zur Abwehr einer Gefahr nach § 62b Absatz 1 Daten eines informationstechnischen Systems, auch durch Eingriff mit technischen Mitteln in das informationstechnische System ohne Wissen des Betroffenen, erheben, löschen oder verändern.

(2) Dabei ist sicherzustellen, dass vorgenommene Veränderungen bei Beendigung der Maßnahme rückgängig gemacht werden, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht, und vom Bundeskriminalamt eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung geschützt werden.

(3) Die Maßnahmen dürfen auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

Deutscher Bundestag
21. Wahlperiode

Drucksache 21/6585
22.06.2026

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

A. Problem und Ziel

Cyberangriffe in Deutschland nehmen in Qualität und Quantität zu. Deutschland als führende Wirtschaftsnation in Europa ist verstärkt im Fokus auch hochprofessioneller Cyberangriffe mit großem Wirkpotential. Angesichts der geopolitischen Lage gewinnen auch hybride Bedrohungen zunehmend an Bedeutung.

Der Krieg in der Ukraine verdeutlicht, wie essentiell Cybersicherheit für einen modernen Staat wie Deutschland ist. Die Gewährleistung einer verlässlichen und sicheren Nutzung der Informationstechnologie und der zugrundeliegenden Kommunikationsinfrastruktur ist essentielle Voraussetzung für das Funktionieren des Gemeinwesens. Deutschlands wirtschaftlicher Erfolg und gesellschaftlicher Zu-

BSI-Gesetz-E (Regierungsentwurf)

(3) Betreiber kritischer Anlagen sind verpflichtet, innerhalb von zwölf Monaten, nachdem sie erstmals oder erneut als Betreiber kritischer Anlagen gelten, jedoch nicht früher als zwölf Monate nach der Veröffentlichung der Anforderungen gemäß Absatz 6, Folgendes an das Bundesamt automatisiert zu übermitteln:

1. kontinuierlich Verfügbarkeitsindikatoren der informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, und

2. Indikatoren zu tatsächlichen und potentiellen Angriffen sowie Informationen zu Schwachstellen, die in Systemen zur Angriffserkennung nach Absatz 2 zu erheblichen Bedrohungen, Störungen oder Beeinträchtigungen der Sicherheit in der Informationstechnik anfallen,

Das Bundesamt kann gegenüber dem Betreiber der kritischen Anlage auf eine Anbindung und Übermittlung der in Satz 1 genannten Informationen verzichten.

rierte Fassung

HK2

BSI-Gesetz-E (Regierungsentwurf)

§ 68d

Auslesen, Löschen und Verändern gefahrgegenständlicher Daten in informationstechnischen Systemen

(1) Das Bundeskriminalamt darf zur Abwehr einer Gefahr gefahrgegenständliche Daten in dem informationstechnischen System, von dem die Gefahr ausgeht, auch durch Eingriff mit technischen Mitteln und ohne Wissen des Betroffenen, auslesen, löschen oder verändern.

(2) Gefahrgegenständliche Daten sind die Daten von Schadprogrammen oder sonstigen informationstechnischen Angriffswerkzeugen, einschließlich Steuerungs- oder Protokolldateien, und Spuren, die technisch mit dem Angriff verbunden sind, sowie Daten, die selbst Gegenstand eines Angriffs auf die Sicherheit in der Informationstechnik sind, insbesondere Daten, die durch diesen Angriff an ein informationstechnisches System weitergeleitet werden oder wurden

(3) Bei Maßnahmen nach Absatz 1 ist sicherzustellen, dass, soweit möglich, technische Vorkehrungen getroffen werden, damit das Auslesen, Löschen oder Verändern auf gefahrgegenständliche Daten beschränkt wird. In den informationstechnischen Systemen vorgenommene Veränderungen sind bei Beendigung der Maßnahme rückgängig zu machen, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht. Vom Bundeskriminalamt eingesetzte Mittel sind nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(4) Die Maßnahmen nach Absatz 1 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. § 68c Absatz 2 Satz 2 und 3 gilt entsprechend.

(5) Für die Löschung nach Absatz 1 erlangter personenbezogener Daten gilt § 79.

HK2

25. Juni 2026 (86. Sitzung)

Uhrzeit	TOP	Thema	Status / Abstimmung	
09:00		Sitzungseröffnung	folgt	
09:00	24	Stärkung der Cybersicherheit a) Erste Beratung des von der Bundesregierung eingebrachten Entwurfs eines Gesetzes zur Stärkung der Cybersicherheit Drucksache 21/6585 b) Beratung des Antrags der Fraktion Die Linke Gegen die Einführung von Hackbacks und offensive Cyberabwehr Drucksache 21/...	folgt	Details ausblenden ✕

HK2

NIS-2

Bundesgesetzblatt

Teil I

2025 Ausgegeben zu Bonn a

Ges
zur Umsetzung der NIS-2-Richtlinie und
des Informationssicherheitsmanage

Vom 2. Dezember 2025

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

Artikel 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)

Bundesgesetzblatt

Teil I

2026 Ausgegeben zu Bonn am 16. März 2026 Nr. 66

Gesetz
zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen*

Vom 11. März 2026

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Artikel 1

Dachgesetz
zur Stärkung der physischen Resilienz kritischer Anlagen
(KRITIS-Dachgesetz – KRITISDachG)

§ 1

Nationale KRITIS-Resilienzstrategie

Bearbeitungsstand: 26.05.2026 09:28

Referentenentwurf

des Bundesministeriums des Innern

Verordnung zur Bestimmung kritischer Anlagen nach dem KRITIS-Dachgesetz*

(Kritisverordnung – KritisV)

A. Problem und Ziel

Das Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen vom 11. März 2026 (BGBl. 2026 I Nr. 66) ist am 17. März 2026 in Kraft getreten. Artikel 1 dieses Gesetzes enthält das KRITIS-Dachgesetz (KRITISDachG). Mit dem KRITISDachG werden im Hinblick auf physische Maßnahmen zur Stärkung der Resilienz kritischer Anlagen erstmals einheitliche bundesgesetzliche sektorenübergreifende Mindestanforderungen normiert. Das KRITISDachG enthält unter anderem Verpflichtungen zur Erstellung nationaler und betreiberseitiger Risikoanalysen und Risikobewertungen sowie zum Ergreifen von Resilienzmaßnahmen und zur Meldung von erheblichen Vorfällen durch die Betreiber kritischer Anlagen.

Mit dem KRITISDachG wurde zudem die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164) (sogenannte CER-Richtlinie) umgesetzt. In Artikel 6 dieser Richtlinie werden Kriterien für die Identifizierung kritischer Einrichtungen vorgegeben. Der Anwendungsbereich wurde europarechtlich durch die Delegierte Verordnung (EU) 2023/2450 der Kommission vom 25. Juli 2023 zur Ergänzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates durch eine Liste wesentlicher Dienste (ABl. L, 2023/2450, 30.10.2023) weiter konkretisiert.

Der Schutz der IT-Sicherheit kritischer Infrastrukturen ist im BSI-Gesetz (BSIG) niedergelegt. Der Anwendungsbereich des BSIG wird seit 2016 mittels der auf dem BSIG beruhenden BSI-Kritisverordnung (BSI-KritisV) bestimmt.

Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Berlin, 15.06.2026

Stellungnahme

zum

Referentenentwurf
Verordnung zur Bestimmung kritischer Anlagen nach dem KRITIS-Dachgesetz
(Kritisverordnung - KritisV)

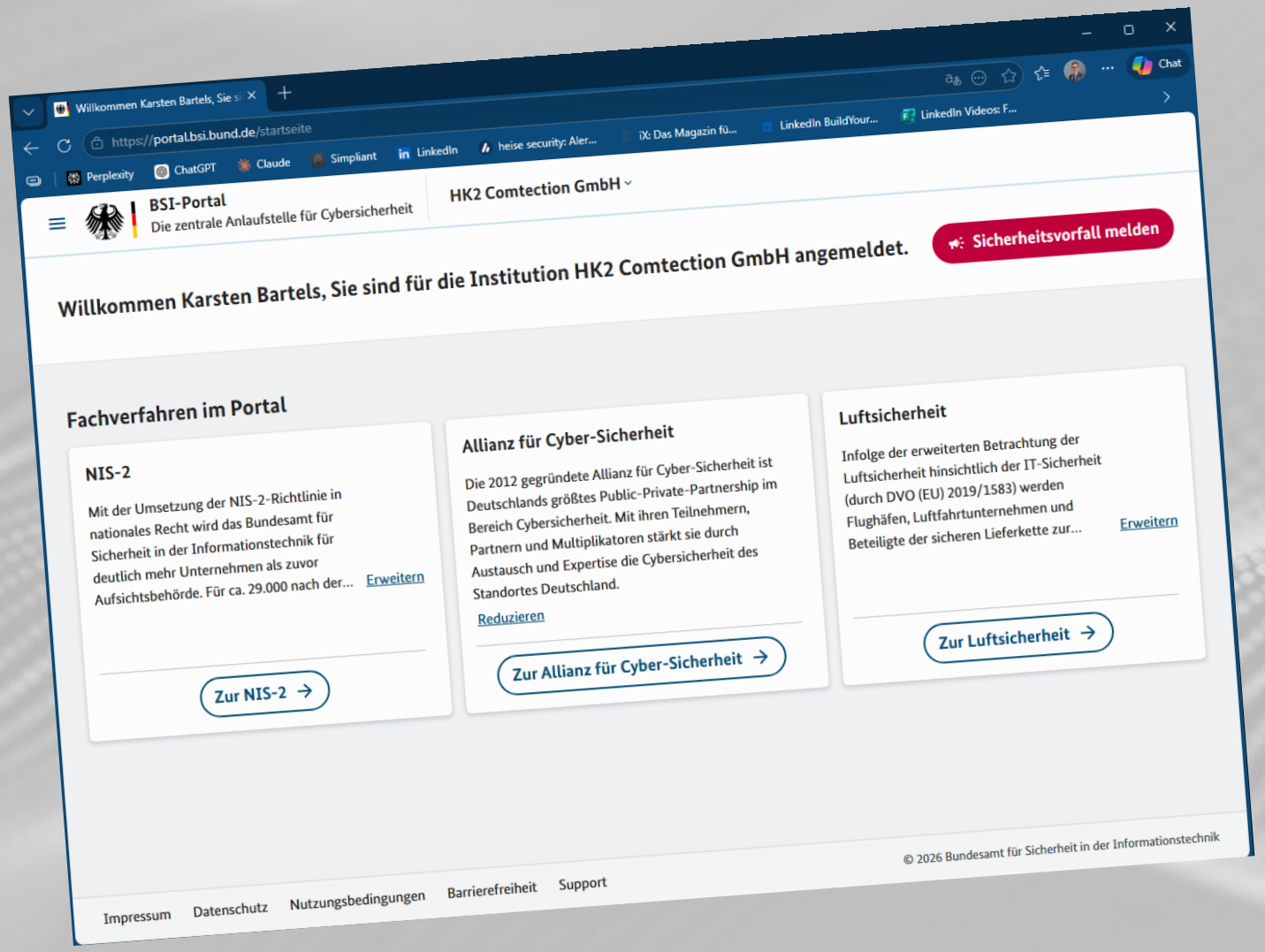
Kontakt:
RA Karsten U. Bartels, LL.M.
HK2 Rechtsanwälte
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Stellvertretender Vorstandsvorsitzender
Leiter TeleTrusT-AG "IT-Sicherheitsrecht"
bartels@hk2.eu

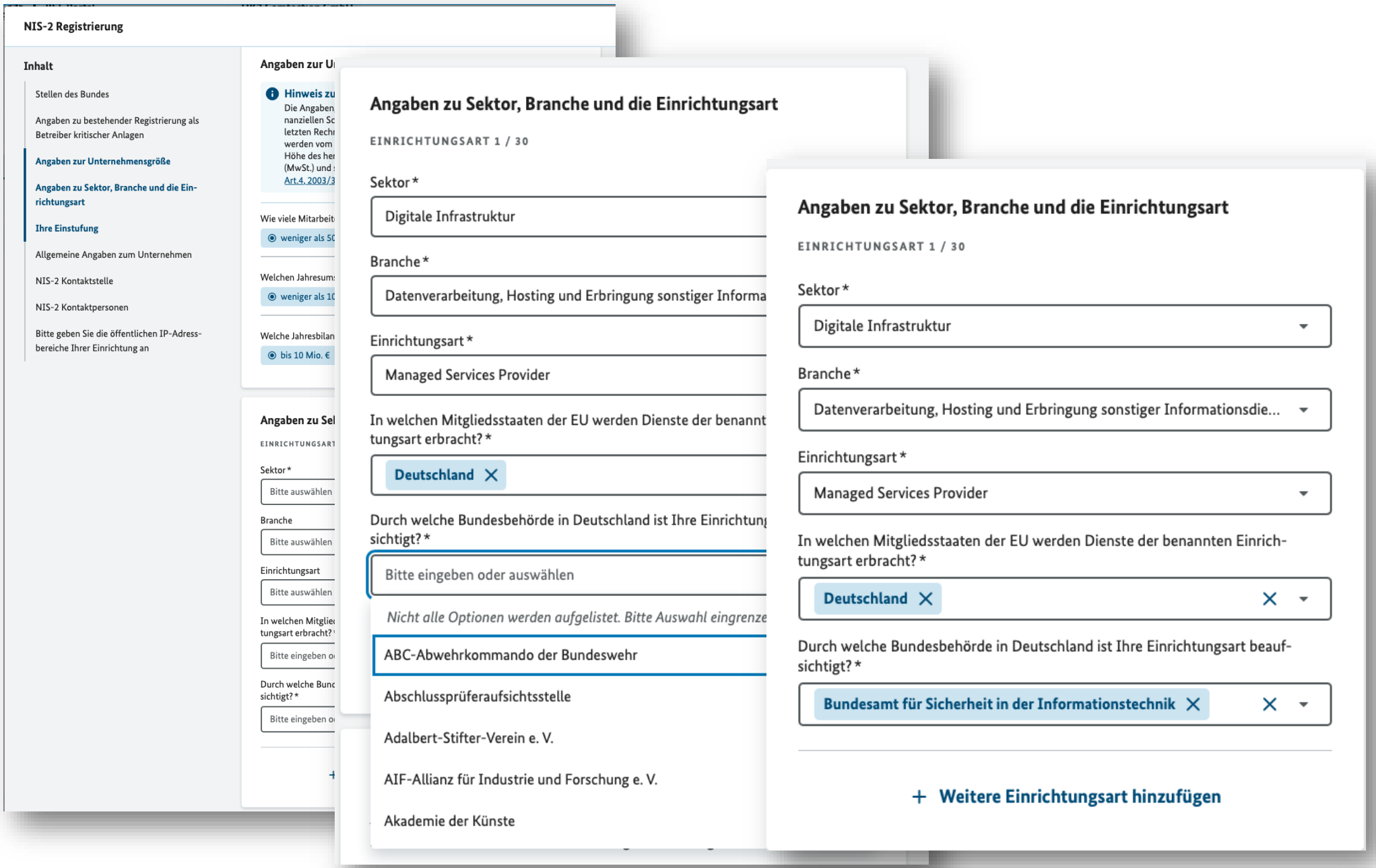
Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen verkörpert TeleTrusT nen umfasst. Durch die breitgefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310

HK2


Willkommen Karsten Bartels, Sie s
https://portal.bsi.bund.de/startseite
Perplexity
ChatGPT
Claude
Simpliant
LinkedIn
heise security: Aler...
iX: Das Magazin fü...
LinkedIn BuildYour...
LinkedIn Videos: F...
Chat
BSI-Portal
Die zentrale Anlaufstelle für Cybersicherheit
HK2 Comtection GmbH
Sicherheitsvorfall melden
Willkommen Karsten Bartels, Sie sind für die Institution HK2 Comtection GmbH angemeldet.
Fachverfahren im Portal
NIS-2
Mit der Umsetzung der NIS-2-Richtlinie in nationales Recht wird das Bundesamt für Sicherheit in der Informationstechnik für deutlich mehr Unternehmen als zuvor Aufsichtsbehörde. Für ca. 29.000 nach der...
Erweitern
Zur NIS-2
Allianz für Cyber-Sicherheit
Die 2012 gegründete Allianz für Cyber-Sicherheit ist Deutschlands größtes Public-Private-Partnership im Bereich Cybersicherheit. Mit ihren Teilnehmern, Partnern und Multiplikatoren stärkt sie durch Austausch und Expertise die Cybersicherheit des Standortes Deutschland.
Reduzieren
Zur Allianz für Cyber-Sicherheit
Luftsicherheit
Infolge der erweiterten Betrachtung der Luftsicherheit hinsichtlich der IT-Sicherheit (durch DVO (EU) 2019/1583) werden Flughäfen, Luftfahrtunternehmen und Beteiligte der sicheren Lieferkette zur...
Erweitern
Zur Luftsicherheit
Impressum
Datenschutz
Nutzungsbedingungen
Barrierefreiheit
Support
© 2026 Bundesamt für Sicherheit in der Informationstechnik



HK2
Rechtsanwälte

HK2

Ihre Einstufung

Auf Grundlage der gemachten Angaben ist Ihre Institution von der NIS-2 Richtlinie betroffen und ist als “**besonders wichtige Einrichtung**” einzustufen.

☐ Ich bin mit der Einstufung nicht einverstanden und möchte diese auf eigen Verantwortung hin anpassen.

Ihre NIS-2-Einstufung *

Besonders wichtige Einrichtung

Ihre Einstufung

Bitte füllen Sie alle obigen Formularfelder aus um eine Einstufung nach NIS-2 zu erhalten.

☑ Ich bin mit der Einstufung nicht einverstanden und möchte diese auf eigene Verantwortung hin anpassen.

Ihre NIS-2-Einstufung *

Freiwillig

- **Freiwillig** ✓
- Wichtige Einrichtung
- Besonders wichtige Einrichtung

HK2
Rechtsanwälte

Wie war das mit den Kommunen
und
Bildungseinrichtungen?

IT-PLANUNGSRAT

Won

Der IT-Planungsrat | **Beschlüsse & Informationen** | Föderale Zusammenarbeit | Produkte

IT-PLANUNGSRAT › BESCHLÜSSE & INFORMATIONEN › BESCHLUSS 2023/39 | UMSETZUNG NIS-2-RICHTLINIE

Umsetzung NIS-2-Richtlinie

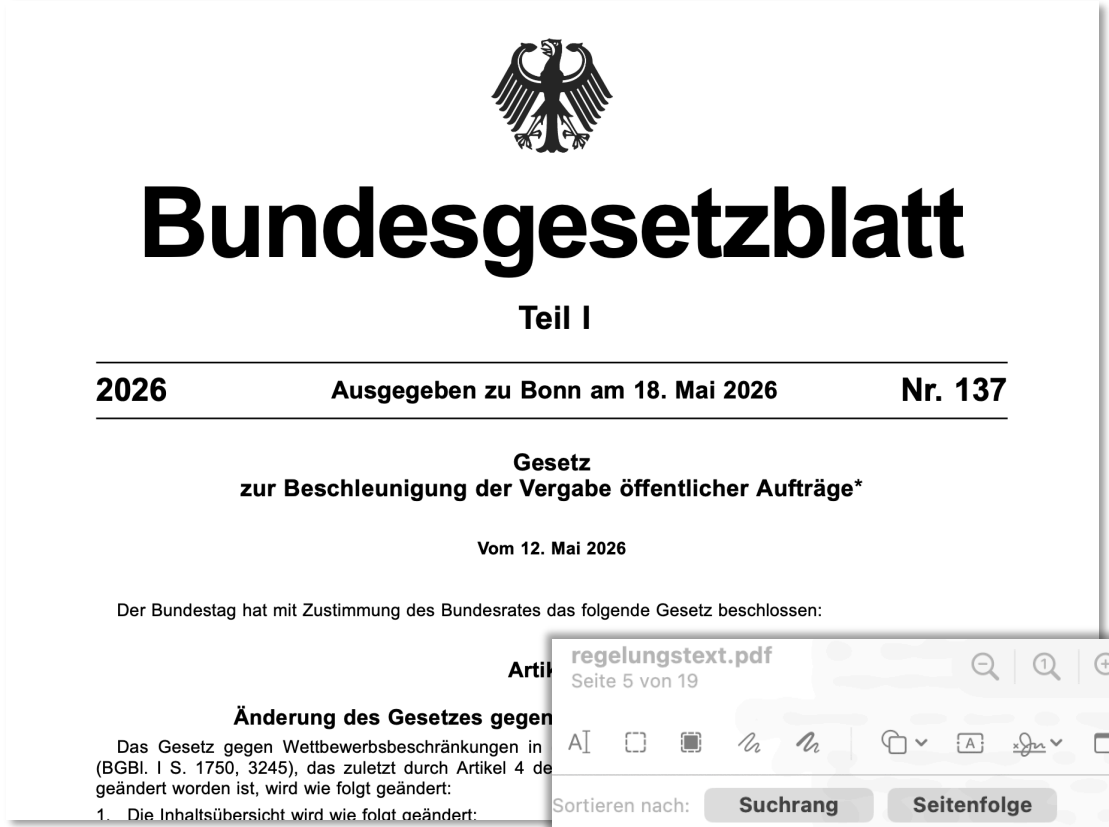
IT-Planungsrat | 03.11.2023 | 42. Sitzung | Beschluss 2023/39

1. Der IT-Planungsrat beschließt das von der AG Informationssicherheit vorgelegte Identifizierungskonzept der Länder zur Umsetzung der NIS-2-Richtlinie auf regionaler Ebene und bittet die Länder bei der landesrechtlichen Umsetzung der Richtlinie das Identifizierungskonzept einheitlich anzuwenden.
2. Er nimmt den Sachstandsbericht der AG Informationssicherheit zur Kenntnis und bittet die Länder und den Bund, von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen.
3. Ferner bittet der IT-Planungsrat die AG Informationssicherheit darum, die Abstimmungen zwischen Bund und Ländern insbesondere zu der Frage einer Adressierung von Landeseinrichtungen durch Bundesrecht fortzuführen.
4. Die AG Informationssicherheit wird gebeten, zur 43. Sitzung erneut zu berichten.

HK2

Vergabebeschleunigungsgesetz

HK2
Rechtsanwälte



Bundesgesetzblatt

Teil I

2026 **Ausgegeben zu Bonn am 18. Mai 2026** **Nr. 137**

Gesetz
zur Beschleunigung der Vergabe öffentlicher Aufträge*

Vom 12. Mai 2026

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

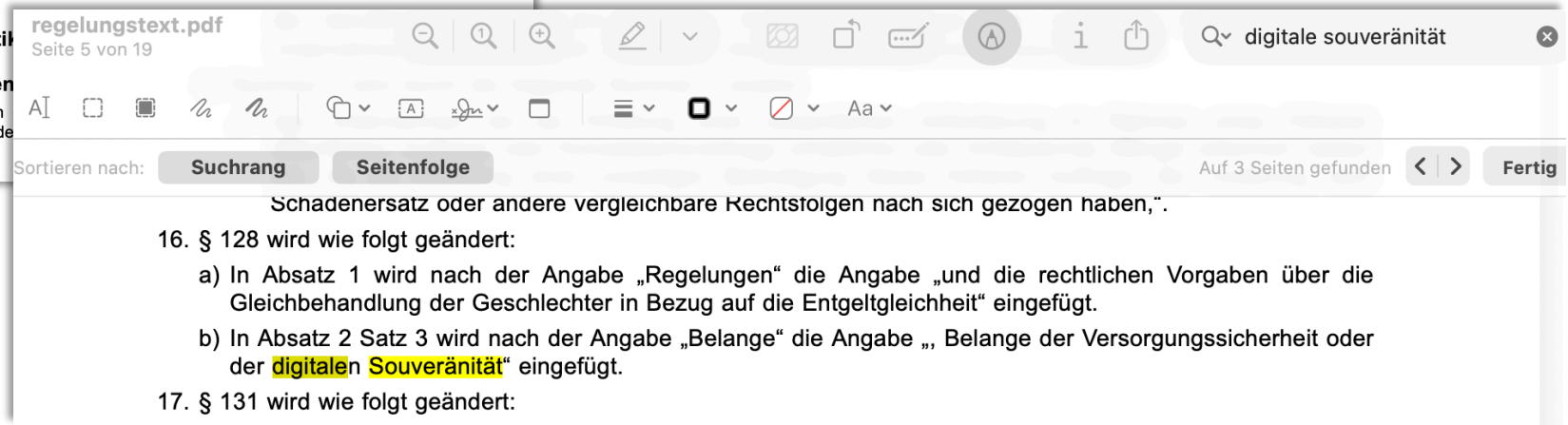
Artik

Änderung des Gesetzes gegen

Das Gesetz gegen Wettbewerbsbeschränkungen in
(BGBl. I S. 1750, 3245), das zuletzt durch Artikel 4 de
geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

Ab 01.07.2026 in Kraft!



regelungstext.pdf
Seite 5 von 19

digitale souveränität

Sortieren nach: Suchrang Seitenfolge Auf 3 Seiten gefunden Fertig

Schadenersatz oder andere vergleichbare Rechtsfolgen nach sich gezogen haben,“.

16. § 128 wird wie folgt geändert:
    a) In Absatz 1 wird nach der Angabe „Regelungen“ die Angabe „und die rechtlichen Vorgaben über die Gleichbehandlung der Geschlechter in Bezug auf die Entgeltgleichheit“ eingefügt.
    b) In Absatz 2 Satz 3 wird nach der Angabe „Belange“ die Angabe „, Belange der Versorgungssicherheit oder der digitalen Souveränität“ eingefügt.
17. § 131 wird wie folgt geändert:

HK2

TKG

HK2

Allgemeinverfügung
zur Festlegung der Umsetzungsfristen für den Einsatz kritischer Komponenten

Gem. §§ 165 Abs. 4, 167 Abs. 1 S. 1 Nr. 1 und Abs. 2 Telekommunikationsgesetz (TKG) i.V.m. § 35 S. 2 Verwaltungsverfahrensgesetz (VwVfG) legt die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Folgendes fest:

1. Die Ausführungen in Kapitel „2.4 Zertifizierung von kritischen Komponenten" der Anlage 2 des Kataloges von Sicherheitsanforderungen (Verfügung Nr. 63/2021 vom 25.08.2021 (ABl. BNetzA Nr. 16/2021)) werden durch nachfolgenden Text ersetzt:

2.4 Zertifizierung von kritischen Komponenten

I. Grundlagen und Reichweite der Zertifizierung
Kritische Komponenten im Sinne von § 2 Abs. 13 BSIG dürfen nach § 165 Abs. 4 TKG[1] von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden. Die Zertifizierung der kritischen Komponenten hat auf der Grundlage der TR-03163 des Bundesamtes für Sicherheit in der Informationstechnik zu erfolgen. Sollte zum Zeitpunkt des erstmaligen Einsatzes einer kritischen Komponente keine Möglichkeiten zur Zertifizierung verfügbar sein oder der Einsatz vor der Stichtagsregelung (s.u. II.) erfolgen, so müssen pflichtige Netzbetreiber und Diensteerbringer beim Einsatz kritischer Komponenten geeignete und angemessene technische Vorkehrungen und sonstige Maßnahmen zur Gefahrenabwehr treffen. Die Produktzertifizierung wird Anforderungen an die Einsatzumgebung bzw. an den sicheren Betrieb von Produkten vorgeben. Nur durch die Einhaltung der im Zertifikat oder der durch den Hersteller beschriebenen Auflagen kann ein sicherer Betrieb der Komponente innerhalb des Zertifizierungs-Fokus gewährleistet werden.

II. Übergangsregelung
Hinsichtlich der Anforderungen zum Einsatz zertifizierter kritischer Komponenten gilt die folgende Übergangsregelung bis zum unten bestimmten Stichtag.

Stichtag
Als Stichtag für die jeweilige kritische Komponente gilt spätestens der letzte Tag des 24. Monats, nachdem die Zertifizierung des Produktes, zu dem die jeweilige kritische Komponente gehört, nach TR-03163 des BSI erstmals möglich ist, frühestens aber der 01.01.2026. Für die Möglichkeit der Zertifizierung bedarf es sowohl der Veröffentlichung der TR-03163, wie auch der Verfügbarkeit produktbezogener Anforderungsdokumente. Die Veröffentlichung der TR-03163 und der Verweis auf die entsprechenden Anforderungsdokumente mit Benennung des für den Produkttyp geltenden Stichtages erfolgt auf der Webseite des BSI (www.bsi.bund.de). Für die Berechnung und Einhaltung des Stichtages ist es unerheblich, wenn die Dokumente für die Zertifizierung (TR-03163 oder die

Katalog von Sicherheitsanforderungen

(ENTWURFSFASSUNG)

für das Betreiben von

Telekommunikations- und

Datenverarbeitungssystemen

sowie für die Verarbeitung

personenbezogener Daten nach

§ 167 Telekommunikationsgesetz (TKG)

Stand: Oktober 2025

HK2

Digital Operational Resilience Act (DORA)

HK2

IKT-Drittdienstleister, Art. 30 DORA

- KPI‘s (Abs. 3)

a) vollständige Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen, mit präzisen quantitativen und qualitativen Leistungszielen innerhalb der vereinbarten Dienstleistungsgüte, um dem

- Kündigungsrechte nach Vorstellung der BaFin (Abs. 2)

h) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden;

HK2

European Digital Identity Wallet

HK2

Digitale Identitätengesetz (DIdG)

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften

(Digitale Identitätengesetz – DIdG)

A. Problem und Ziel

Ziel der Verordnung (EU) Nr. 910/2014 ist es, sichere, vertrauenswürdige und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgerinnen und Bürgern und öffentlichen Verwaltungen grenzüberschreitend in der gesamten Europäischen Union zu ermöglichen.

Die im April 2024 bekannt gegebene unionsrechtliche Verordnung (EU) 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 führt einen auch in der Bundesrepublik Deutschland unmittelbar geltenden Rechtsrahmen für die Europäische Brieftasche für die Digitale Identität ein. Diese sogenannte EUDI-Wallet schafft mit wesentlichen Vereinfachungen für Bürgerinnen und Bürger in vielfältigen Lebens- und Wirtschaftsbereichen echten Mehrwert und einen hohen Nutzen für den Wirtschaftsstandort Deutschland sowie für den Binnenmarkt in der Europäischen Union: Die EUDI-Wallet ist ein elektronisches Identifizierungsmittel, das es ihren Nutzern ermöglicht, Personenidentifizierungsdaten sowie Bescheinigungen zur Authentifizierung von Merkmalen, Rechten oder Erlaubnissen, die in elektronischer Form vorliegen (elektronische Attributsbescheinigungen), sicher zu speichern, zu verwalten und zu validieren, um sie vertrauenden Beteiligten und anderen Nutzern Europäischer Brieftaschen für die Digitale Identität zu präsentieren oder mittels qualifizierter elekt-

1. Referentenentwurf
2. Stellungnahmen der Länder und Verbände zum Referentenentwurf
3. Kabinettbeschluss (Regierungsentwurf)

3. Kabinettbeschluss (Regierungsentwurf)

Digitale Identitätengesetz Kabinettfassung (Regierungsentwurf) [PDF, 1 MB]

4. Stellungnahme im Bundesrat
5. Lesungen im Bundestag
6. Abschluss des Gesetzes (Inkrafttreten)

HK2

Council of the European Union

Brussels, 22 May 2026
(OR. en)

7659/26

Interinstitutional File:
2025/0358 (COD)

TELECOM 142
COMPET 562
MI 464
DATAPROTECT 154
JAI 570
CODEC 896

NOTE

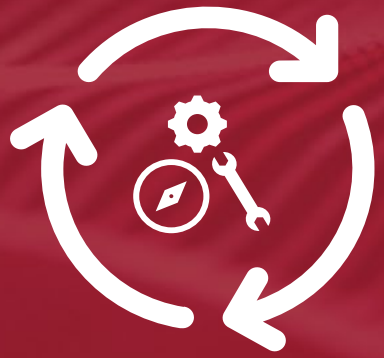
From:	Presidency
To:	Permanent Representatives Committee
No. Cion doc.:	15701/25 + ADD 1
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of European Business Wallets - General approach

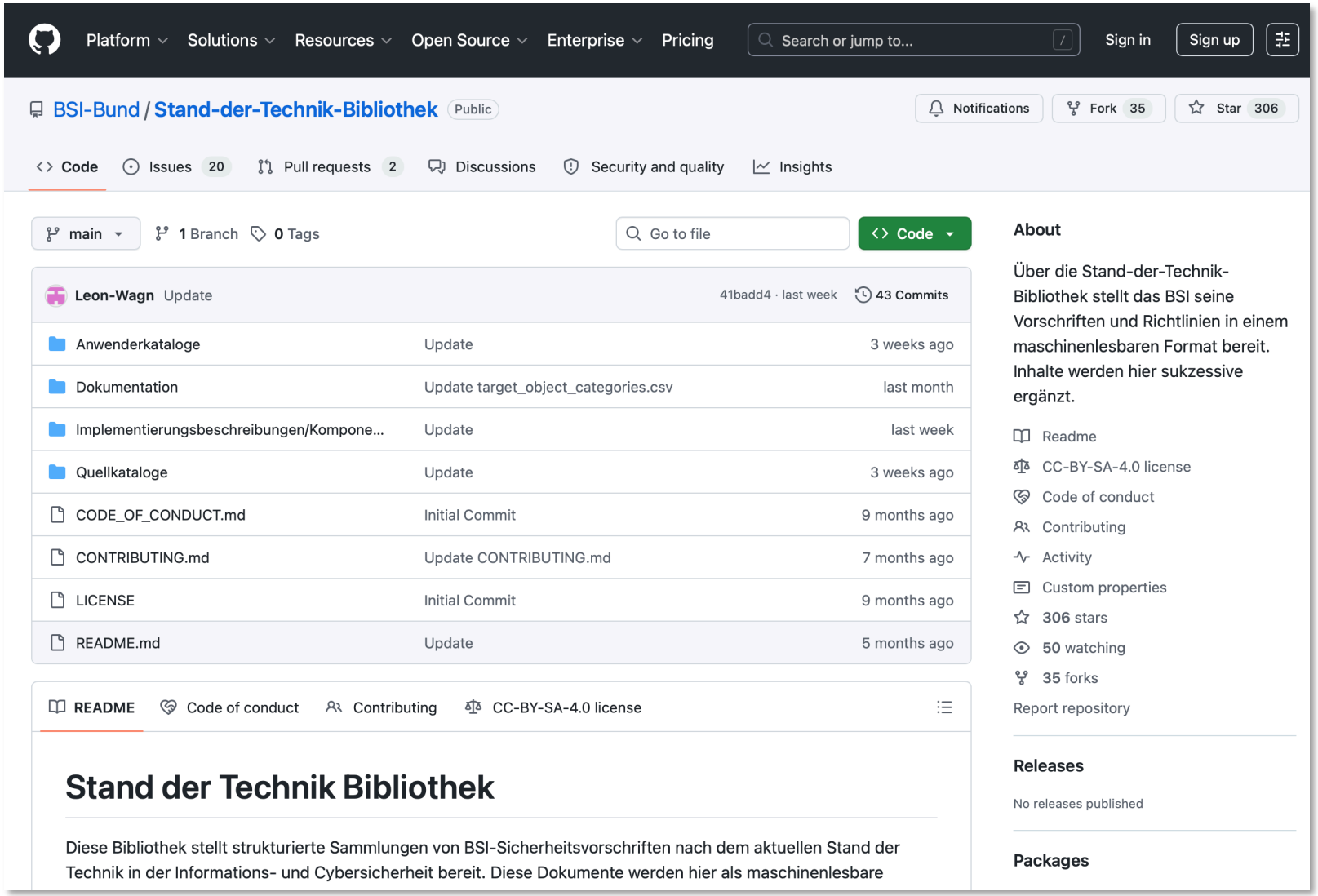
I. BACKGROUND

1. The Commission adopted the proposal for a Regulation on the establishment of European Business Wallets (EBW) on 19 November 2025. The proposal builds on the

HK2

Stand der Technik





https://github.com/BSI-Bund/Stand-der-Technik-Bibliothek, 22.06.2026

HK2 Rechtsanwälte

HK2

Künstliche Intelligenz

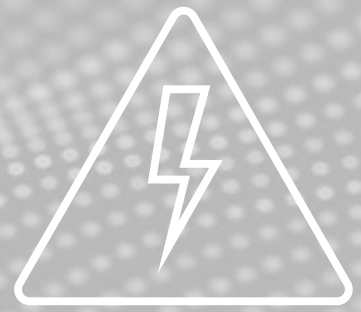
HK2

KI-Omnibus

Anforderungen an Hochrisiko-KI gelten
ab dem 02.08.2028, statt ab dem 02.08.2027.
Achtung: noch nicht in Kraft.

HK2

Umsetzung von IT-Sicherheit in Hochrisiko-KI-Systemen



HK2

Beschaffenheit und Mängel von Software in Zeiten KI-geprüfter IT-Sicherheit

Kontakt

linkedin.com/in/karstenbartels

www.hk2.eu

www.comtection.de

HK2
Rechtsanwälte

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Lehrbeauftragter für IT-Sicherheitsrecht, Ludwig-Maximilians-Universität München
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Leiter Arbeitsgruppe IT-Sicherheitsrecht Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik