"T.I.S.P. Community Meeting 2022"

Berlin, 09.-10.11.2022

IT-Sicherheitsrecht - Schwerpunkte 2023

RA Karsten U. Bartels LL.M.
HK2 Rechtsanwälte
Vorstand TeleTrusT, Leiter AG Recht

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit (TeleTrusT)
- Lehrbeauftragter Hochschule Hof für Datenschutz-Compliance
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik

HK2

Technik-Recht
IT- und Datenrecht

IT-Sicherheitsrecht
Datenschutzrecht

HK2 wurde zu den besten Wirtschaftskanzleien 2022 gewählt.

brand eins/ thema, Heft 23/ 2022

HK2 TOP-Wirtschaftskanzlei 2022 für IT & TK und Datenschutzrecht

FOCUS 06/2022

IT-Sicherheitsrecht 2023

1. „Lagebild“ IT-Sicherheitsrecht
2. IT-Sicherheitsgesetze DE + EU
3. Verträge zur IT-Sicherheit
4. Tätigkeit der Aufsichtsbehörden
5. Rechtsprechung

Supushpitha Atapattu /pexels.com

Lage IT-Sicherheitsrecht

Keine relevante Rechtsprechung

Gesetze weder vertikal noch horizontal konsolidiert. Nicht in DE und nicht in EU.

Trend bis Aktionismus: neues Schuldrecht, EVB-IT-Cloud, TTDSG

Rechtliche Bedeutung untergesetzlicher Normen begrenzt

Geänderte Vergabe/ Beauftragung seit 28.05.2021 und dem 24.02.2022

Alibi-Verträge zur IT-Sicherheit. Verträge noch immer nicht *state of the art*

… zu wenig Rechtsanwälte/-anwältinnen für IT-Sicherheitsrecht

HK2
Rechtsanwälte

Erweiterte Befugnisse

BSI

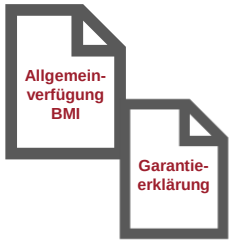
ITSiG 2.0

KRITIS - VO

Neue Pflichten

KRITIS-Betreiber

NIS-RL



Allgemein-verfügung BMI

Garantie-erklärung

HK2
Rechtsanwälte

ITSiG 3.0 / KRITIS-Dachgesetz

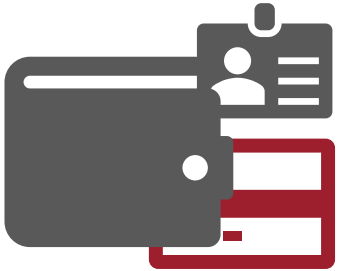
NIS-RL 2.0

HK2
Rechtsanwälte

Vertrauensdienste, z.B.

Qualifizierte elektronische Signatur + Siegel

eIDAS-VO 2.0



Trust Service Providers

Vertrauens-dienste-gesetz

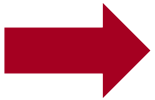
HK2
Rechtsanwälte

E-Privacy RL

§ 19
TTDSG

E-Privacy VO

Keine Bußgelder
bei mangelhafter IT-Sicherheit



https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cy 110% Suchen

Gesetz über Cyberresilienz – neue Cybersicherheitsvorschriften für digitale Produkte und Nebendienstleistungen

Ihre Meinung zählt > Veröffentlichte Initiativen > Gesetz über Cyberresilienz – neue Cybersicherheitsvorschriften für digitale Produkte und Nebendienstleistungen

- **In Vorbereitung**
- **Sondierung**
- **Öffentliche Konsultation**
  Rückmeldungs- und Konsultationszeitraum
  16 März 2022 - 25 Mai 2022
  RÜCKMELDUNGEN: GEÖFFNET BIS
- **Annahme durch die Kommission**
  19 September 2022 - 02 Januar 2023
  RÜCKMELDUNGEN: GEÖFFNET VON

Über diese Initiative

Zusammenfassung Digitale Produkte und Nebendienstleistungen eröffnen Chancen für die Volkswirtschaften und Gesellschaften der EU. Sie führen aber auch zu neuen Herausforderungen: Wenn alles miteinander vernetzt ist, kann ein Cybersicherheitsvorfall ein ganzes System beeinträchtigen und wirtschaftliche und soziale Tätigkeiten stören.

Ziel dieser Initiative ist es, den Erfordernissen des Marktes Rechnung zu tragen und die Verbraucherinnen und Verbraucher vor unsicheren Produkten zu schützen, indem gemeinsame Cybersicherheitsvorschriften für Hersteller und Anbieter materieller und immaterieller digitaler Produkte und Nebendienstleistungen eingeführt werden.

Thema	Digitale Wirtschaft und Gesellschaft
Art des Rechtsakts	Vorschlag für eine Verordnung
Kategorie	Arbeitsprogramm der Kommission

Sondierung

RÜCKMELDUNGEN: GEÖFFNET BIS

Frist für Rückmeldungen
16 März 2022 - 25 Mai 2022 (Mitternacht Brüsseler Zeit)

Eingegangene Rückmeldungen einsehen > >

Sondierung zu einer Folgenabschätzung - Ares(2022)1955751
Deutsch (467.2 KB - PDF - 5 Seiten) Herunterladen

HK2 Rechtsanwälte

Definition „Cyberresilienz“

- Keine Definition des Begriffs im ENT
- Art. 6 Abs. 5 lit. b CRA (ENT) spricht von „Widerstandsfähigkeit der gesamten Lieferkette von Produkten mit digitalen Elementen gegen Störungen“
- Bezüge zur NIS 2.0-Richtlinie (ENT) nicht weiterführend

Ziele des CRA (ENT), Art. 1

1. Vorschriften für das Inverkehrbringen von **Produkten mit digitalen Elementen**, um die **Cybersicherheit** solcher Produkte zu **gewährleisten**
2. grundlegende **Anforderungen** an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der **Wirtschaftsakteure** in Bezug auf diese Produkte hinsichtlich der Cybersicherheit

Phil Lenoir/Shutterstock.com

Ziele des CRA (ENT), Art. 1

3. grundlegende Anforderungen an die von den Herstellern festgelegten **Verfahren zur Behandlung von Schwachstellen**, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres **gesamten Lebenszyklus** zu gewährleisten, sowie Pflichten der **Wirtschaftsakteure** in Bezug auf diese Verfahren
4. Vorschriften für die **Marktüberwachung** und die **Durchsetzung** der Anforderungen.

Phil Lenoir/Shutterstock.com

Anwendungsbereich des CRA (ENT)

- **Hersteller, Importeure** und **Händler** von …
- **Produkten mit digitalen Elementen**: „Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen“
- **Kritische/ hoch kritische** Produkte mit digitalen Elementen (Art. 6. Abs. 2 und 5)
- **Bereichsausnahmen**: best. Medizinprodukte, Flugsicherheit, Fahrzeugsicherheitssysteme, nationale Sicherheit/ militärische Zwecke u. a.

Herstellerpflichten (Auszug)

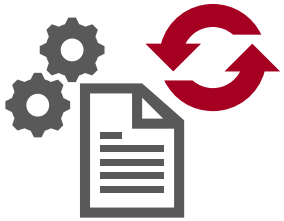
Cybersecurity by design

- Pflicht, bereits vor der Markteinführung die Cybersicherheitsanforderungen (siehe Anhang I Abschnitt 1) beim **Design, bei der Entwicklung und beim Fertigungsprozess** zu erfüllen (Art. 10 Abs. 1)

Risikobewertung

- **Bewertung** der Cybersicherheitsrisiken (Art. 10 Abs.2)
- **Berücksichtigung** des Bewertungsergebnisses in der Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase

Herstellerpflichten (Auszug)



Dokumentation

- Bewertung als **Teil der technischen Dokumentation** vor dem Inverkehrbringen (Art. 10 Abs. 3 i. V. m. Art.23 und Anhang V)
- **Aktualisierung** der technischen Dokumentation während der erwarteten Produktlebensdauer oder bis zu fünf Jahre nach Launch (Art. 23 Abs. 2)

Sichere Nutzung

- Pflicht für klare und verständliche **Informationen und Anleitungen** (Art. 10 Abs. 10)

Herstellerpflichten (Auszug)

EU-Konformitäts-Erklärung + CE-Kennzeichen

Bereitstellung der Bewertung

- **Konformitätsbewertung**: sowohl Produkte als auch Prozesse des Herstellers mittels unterschiedlicher Verfahren (Art. 10 Abs. 7 i. V. m. Art. 24 und Anhang VI)
  - internes Kontrollverfahren durch Hersteller
  - EU-Baumusterprüfverfahren durch notifizierte Stelle
  - auf Grundlage einer umfassenden Qualitätssicherung
- Pflicht zur **CE-Kennzeichnung**

- **Aufbewahrungspflicht** der Konformitätsbewertung für zehn Jahre (Art. 10 Abs. 8)

Herstellerpflichten (Auszug)

Cybersicherheitsrisiken überwachen/beheben

- **Schwachstellenmanagement / Konformitätspflicht** für erwartete Produktlebensdauer oder 5 Jahre ab Markteinführung (kürzere Frist gilt), Art. 10 Abs. 6
- Sicherheits-Updates sind kostenlos, Anhang I, Ziff. 2 Abs. 8

Meldepflichten

- **Meldepflicht** für **„aktiv ausgenutzte Schwachstellen“** und **„jeden** [IT-Sicherheits]**Vorfall“** ggü. ENISA, Art.11. Frist: unverzüglich, jedenfalls binnen 24 h.
- Achtung: Pflicht gilt nach 12 Monaten nach Inkrafttreten

Pflichten für Einführer (Auszug)

- **Sicherstellungspflicht** (Art. 13 Abs. 2), dass
  - geeignete Konformitätsbewertungsverfahren vom Hersteller durchgeführt worden sind
  - Hersteller die technische Dokumentation erstellt hat
  - CE-Kennzeichnung vorliegt und die erforderlichen Informationen und Gebrauchsanweisungen beigefügt sind

- Pflicht, den **Namen oder Kontaktinformationen** auf dem Produkt oder der Verpackung anzubringen, Art. 13 Abs. 4

Pflichten für Einführer (Auszug)

- **Konformität** bei und nach dem Inverkehrbringen des Produkts durchgängig zu wahren (Art. 13 Abs. 3, 6)
- Bei erheblichen Cybersicherheitsrisiko **Unterrichtungspflicht** ggü. Hersteller und Marktüberwachungsbehörde

- **Informationspflicht** bei Kenntnis von Schwachstellen und über ergriffene Korrekturmaßnahmen (Art. 13 Abs. 6) und über Betriebseinstellung Hersteller (Abs. 9)
- Pflicht zur **Zusammenarbeit mit der Marktüberwachungsbehörde** (Artt. 13 Abs. 8 f.)

Pflichten für Händler (Auszug)

- vor Inverkehrbringen **Prüfungspflicht** (Art. 14 Abs. 2),
  - ob eine durch den Hersteller vorgenommene CE-Kennzeichnung vorliegt
  - Hersteller und Importeure ihren Informationspflichten nachgekommen sind und
  - die Hersteller die EU-Konformitätserklärung auf dem Produkt oder in der Anleitung beigefügt hat

- **Konformitätspflicht** vor Launch und Zusammenarbeit mit der Marktüberwachungsbehörde gem. Artt. 14 Abs. 3-6 (ausgestaltet wie bei Einführer)
- Informationspflicht, wenn bekannt wird, dass Hersteller Betrieb eingestellt hat, Art. 14 Abs. 6

Pixabay/pexels.com

HK2 Rechtsanwälte

Sanktionen

- Verstoß gg. Herstellerpflicht inkl. Meldepflichten sowie Cybersicherheitsanforderungen: max. EUR **15 Mio**. oder bei Unternehmen i. H. v. bis zu **2,5 %** des weltweiten Vorjahresumsatzes
- Verstoß gg. andere Pflichten: max. EUR **10 Mio**. oder bei Unternehmen i. H. v. bis zu **2 %** des Umsatzes (wie oben)
- Verstoß gg. Auskunftspflicht: bis EUR **5 Mio.** bzw. **1%** des Umsatzes (wie oben)

HK2 Rechtsanwälte

Stand der Technik im CRA (ENT)

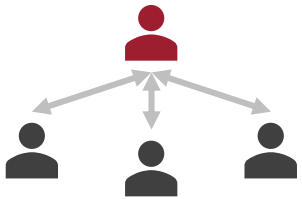
„Die notifizierte Stelle hält sich über alle Änderungen des **allgemein anerkannten Stands der Technik** auf dem Laufenden; deuten diese darauf hin, dass das zugelassene Baumuster und die Verfahren zur Behandlung von Schwachstellen nicht mehr den geltenden grundlegenden Anforderungen in Anhang I dieser Verordnung entsprechen, so entscheidet sie, ob derartige Änderungen weitere Untersuchungen nötig machen. Ist dies der Fall, so setzt die notifizierte Stelle den Hersteller davon in Kenntnis.“

Anhang VI, Konformitätsbewertungsverfahren, EU-Baumusterprüfung (auf der Grundlage von Modul B)

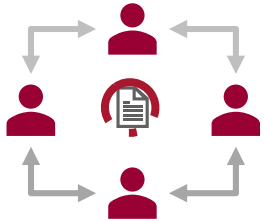
HK2
Rechtsanwälte

Verträge zur IT-Sicherheit

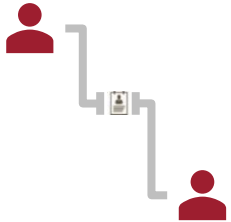
Vereinbarungen zum Datenschutz



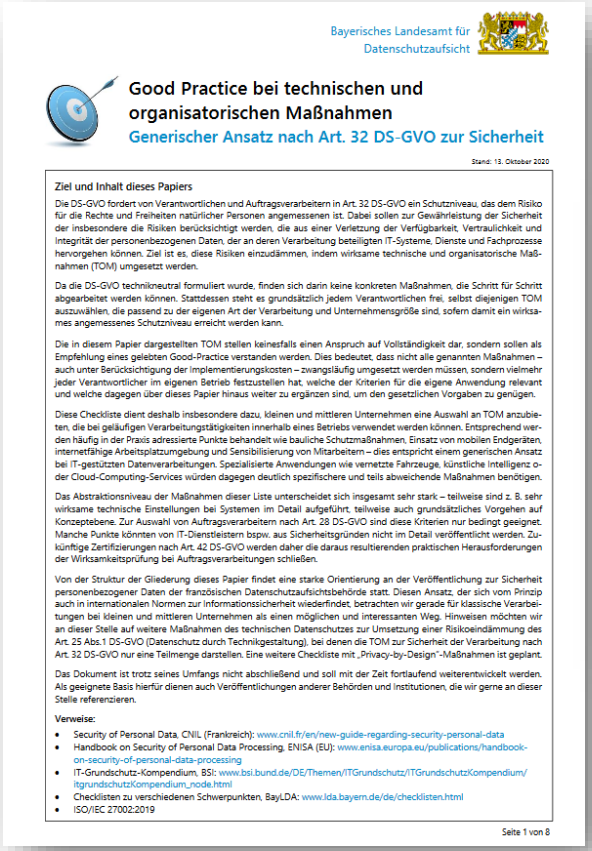
Auftragsverarbeitung



Joint controllers



getrennt Verantwortliche



Bayerisches Landesamt für Datenschutzaufsicht

Good Practice bei technischen und organisatorischen Maßnahmen

Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit

Stand: 13. Oktober 2020

Ziel und Inhalt dieses Papiers

Die DS-GVO fordert von Verantwortlichen und Auftragsverarbeitern in Art. 32 DS-GVO ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist. Dabei sollen zur Gewährleistung der Sicherheit der insbesondere die Risiken berücksichtigt werden, die aus einer Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten, der an deren Verarbeitung beteiligten IT-Systeme, Dienste und Fachprozesse hervorgehen können. Ziel ist es, diese Risiken einzudämmen, indem wirksame technische und organisatorische Maßnahmen (TOM) umgesetzt werden.

Da die DS-GVO technikneutral formuliert wurde, finden sich darin keine konkreten Maßnahmen, die Schritt für Schritt abgearbeitet werden können. Stattdessen steht es grundsätzlich jedem Verantwortlichen frei, selbst diejenigen TOM auszuwählen, die passend zu der eigenen Art der Verarbeitung und Unternehmensgröße sind, sofern damit ein wirksames angemessenes Schutzniveau erreicht werden kann.

Die in diesem Papier dargestellten TOM stellen keinesfalls einen Anspruch auf Vollständigkeit dar, sondern sollen als Empfehlung eines gelebten Good-Practice verstanden werden. Dies bedeutet, dass nicht alle genannten Maßnahmen – auch unter Berücksichtigung der Implementierungskosten – zwangsläufig umgesetzt werden müssen, sondern vielmehr jeder Verantwortlicher im eigenen Betrieb festzustellen hat, welche der Kriterien für die eigene Anwendung relevant und welche dagegen über dieses Papier hinaus weiter zu ergänzen sind, um den gesetzlichen Vorgaben zu genügen.

Diese Checkliste dient deshalb insbesondere dazu, kleinen und mittleren Unternehmen eine Auswahl an TOM anzubieten, die bei geläufigen Verarbeitungstätigkeiten innerhalb eines Betriebs verwendet werden können. Entsprechend werden häufig in der Praxis adressierte Punkte behandelt wie bauliche Schutzmaßnahmen, Einsatz von mobilen Endgeräten, internetfähige Arbeitsplatzumgebung und Sensibilisierung von Mitarbeitern – dies entspricht einem generischen Ansatz bei IT-gestützten Datenverarbeitungen. Spezialisierte Anwendungen wie vernetzte Fahrzeuge, künstliche Intelligenz oder Cloud-Computing-Services würden dagegen deutlich spezifischere und teils abweichende Maßnahmen benötigen.

Das Abstraktionsniveau der Maßnahmen dieser Liste unterscheidet sich insgesamt sehr stark – teilweise sind z. B. sehr wirksame technische Einstellungen bei Systemen im Detail aufgeführt, teilweise auch grundsätzliches Vorgehen auf Konzeptebene. Zur Auswahl von Auftragsverarbeitern nach Art. 28 DS-GVO sind diese Kriterien nur bedingt geeignet. Manche Punkte könnten von IT-Dienstleistern bspw. aus Sicherheitsgründen nicht im Detail veröffentlicht werden. Zukünftige Zertifizierungen nach Art. 42 DS-GVO werden daher die daraus resultierenden praktischen Herausforderungen der Wirksamkeitsprüfung bei Auftragsverarbeitungen schließen.

Von der Struktur der Gliederung dieses Papier findet eine starke Orientierung an der Veröffentlichung zur Sicherheit personenbezogener Daten der französischen Datenschutzaufsichtsbehörde statt. Diesen Ansatz, der sich vom Prinzip auch in internationalen Normen zur Informationssicherheit wiederfindet, betrachten wir gerade für klassische Verarbeitungen bei kleinen und mittleren Unternehmen als einen möglichen und interessanten Weg. Hinweisen möchten wir an dieser Stelle auf weitere Maßnahmen des technischen Datenschutzes zur Umsetzung einer Risikoeindämmung des Art. 25 Abs.1 DS-GVO (Datenschutz durch Technikgestaltung), bei denen die TOM zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO nur eine Teilmenge darstellen. Eine weitere Checkliste mit „Privacy-by-Design"-Maßnahmen ist geplant.

Das Dokument ist trotz seines Umfangs nicht abschließend und soll mit der Zeit fortlaufend weiterentwickelt werden. Als geeignete Basis hierfür dienen auch Veröffentlichungen anderer Behörden und Institutionen, die wir gerne an dieser Stelle referenzieren.

Verweise:

- Security of Personal Data, CNIL (Frankreich): www.cnil.fr/en/new-guide-regarding-security-personal-data
- Handbook on Security of Personal Data Processing, ENISA (EU): www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
- IT-Grundschutz-Kompendium, BSI: www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
- Checklisten zu verschiedenen Schwerpunkten, BayLDA: www.lda.bayern.de/de/checklisten.html
- ISO/IEC 27002:2019

Seite 1 von 8

- ☐ Bei Smartphones: Einsatz von biometrischen Zugangsverfahren nur bei ausschließlich lokaler Speicherung der biometrischen Templates innerhalb eines Secure-Chips auf dem Smartphone und bei personenbezogenen Daten mit keinem hohen Risiko
- ☐ Bei Smartphones: Cloud-Speicher für Datenbackup erst nach sorgfältiger Prüfung der datenschutzrechtlichen Anforderungen einsetzen (auch Beschäftigtendatenschutz bei „Find my Phone"-Funktionen)
- ☐ Bei Smartphones: Mobile Device Management Lösungen zur Konfiguration und Verwaltung der Geräte, der installierten Apps sowie dem Auffinden/Löschen im Verlustfall
- ☐ Bei Smartphones: Nur sichere Quellen werden für die Installation von Apps verwendet. Apps werden vorher getestet und freigegeben
- ☐ Regelungen prüfen, ob es ausreichend ist, bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise) auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können

sofern diese nicht als erforderlich eingeschätzt werden

9 Websites und Webanwendungen

Webseiten und Webanwendungen stellen meist leicht zugängliche Plattformen für Angriffe dar, die mit bekannten Best-Practice-Ansätzen meist gut abgesichert werden können.

- ☐ Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3)
- ☐ Absicherung von Datenbanken auf dem Webserver mittels Firewalls
- ☐ Fernzugang zu Webservern nur mit verschlüsselter Verbindung und Zwei-Faktor-Authentifizierung (z. B. SSH mit Client-Zertifikaten)
- ☐ Limitierung von Administrationsbereichen der Webanwendungen auf bestimmte IP-Adressen (z. B. Unternehmens-Gateway)

www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf

SCC-EU (2021), Anhang III

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Maßnahmen zum Schutz der Daten während der Übermittlung

Maßnahmen zum Schutz der Daten während der Speicherung

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Maßnahmen zur Gewährleistung der Datenminimierung

Maßnahmen zur Gewährleistung der Datenqualität

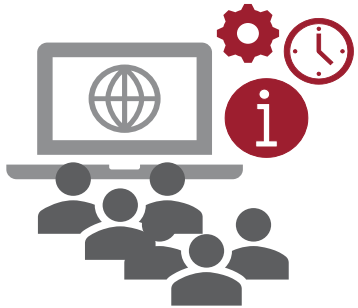
Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

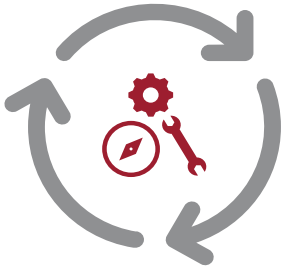
Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

IT-Sicherheitsmaßnahmen nach Art. 32 DSGVO

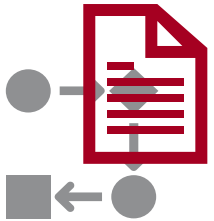
HK2 Rechtsanwälte



Risikobewertung



Stand der Technik



Dokumentation

Sicherheit der Verarbeitung
Art. 32 DSGVO

HK2 Rechtsanwälte

HK2
Rechtsanwälte

DSGVO-Zertifikate

Zertifizierung nach DSGVO

enzozo/stock.adobe.com

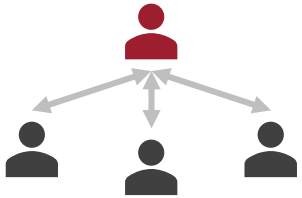
- Zertifizierungen gem. Art. 42 ff. DSGVO
  - zum Nachweis DSGVO-konformer Verarbeitung
  - für Verantwortliche und Auftragsverarbeiter
- erstes Zertifizierungsverfahren in Luxemburg in 05/2022 angenommen

Typische Probleme: Datenschutz-Vereinbarungen

HK2 Rechtsanwälte

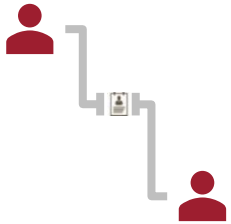
- Uneinigkeit über datenschutzrechtliche Kollaborationsform
- Unbrauchbare TOM des Anbieters. Keine Einbeziehung von Unterauftragnehmer-TOM
- Unklarheit über Leistung und nachlaufende Pflichten bei Ende des Hauptleistungsvertrags
- Mangelnde Konkretisierung von Unterstützungsleistungen des AN
- Inpraktikable Audit-Regelungen. Keine Kostentragungsregelungen. Unpassender Zertifikats-Einsatz.
- Keine Vertragsagilität.
- Vermischung mit Geheimnisschutzverpflichtung.
- Treffen „insularer“ Vereinbarungen

Vereinbarungen zu Datenschutz/ IT-Sicherheit



Auftragsverarbeitung

Joint controllers



getrennt Verantwortliche

Daten ohne Personenbezug

KRITIS

HK2
Rechtsanwälte

Verträge zur IT-Sicherheit
werden deutlich anspruchsvoller.
Nicht nur für KRITIS.

HK2 Rechtsanwälte

IT Security Agreements

- Schwachstellen-Management
  - Erkennung
  - Bewertung
  - Behebung
- Umgang mit Bedrohungen
- Beheben von
  - IT Security Incidents
  - Datenpannen (DSGVO)
- Warnungen des BSI

HK2 Rechtsanwälte

Qualitätssicherung

- Compliance-Klauseln
  - Gesetz
  - Vertrag
  - Zertifizierungen
  - Normen/ Standards/ Richtlinien
  - ggf. Branchenmindeststandard
- Stand der Technik


Panumas nikhomkhai/Pexel.com

HK2 Rechtsanwälte

Stand der Technik

- Definition
- Feststellungen zum SdT: Ist-Beschreibung, Fiktion, Vermutung
- Im Streit: ext. Bewertung
- Dokumentation
- Rechtsfolgenverknüpfung

HK2
Rechtsanwälte

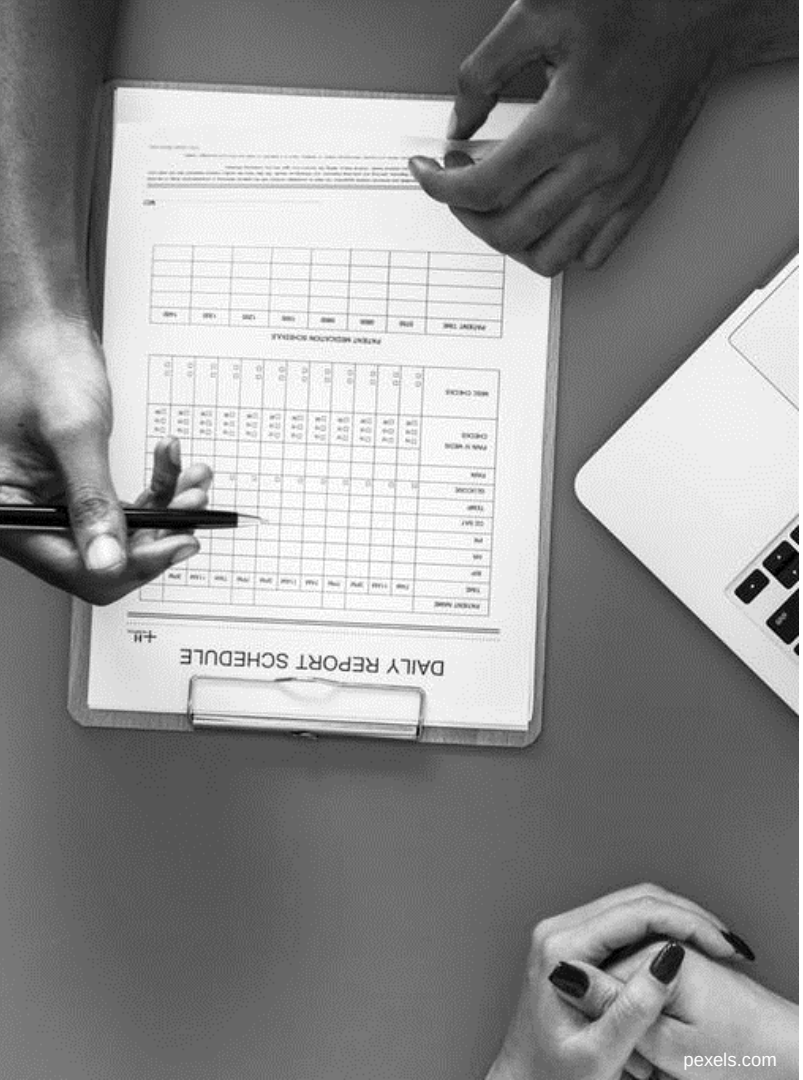
Qualitätssicherung

- Compliance-Klauseln
  - Gesetz
  - Vertrag
  - Zertifizierungen
  - Normen/ Standards/ Richtlinien
  - ggf. Branchenmindeststandard
- Stand der Technik
- Kryptoagilität

Zulieferer-Anforderungen

- IT-Sicherheits-Mindestanforderungen
- Vereinbarungen nach DSGVO
- NDA anpassen
- (Pre-)Audits
- Selbsterklärung i. S. v. § 8f BSIG unabhängig vom Status „UBI“
- Garantieerklärung i. S. v. § 9b Abs. 3 BSIG, unabhängig davon, ob „kritische Komponenten“
- Unterbeauftragungsbeschränkung
- Überprüfung Versicherungsumfang

ESB Professional/Shutterstock.com



pexels.com

HK2
Rechtsanwälte

Kontrolle und Exit

- Change Request Management
- Change of Control
- Überleitungsunterstützung
- Vertragsstrafen

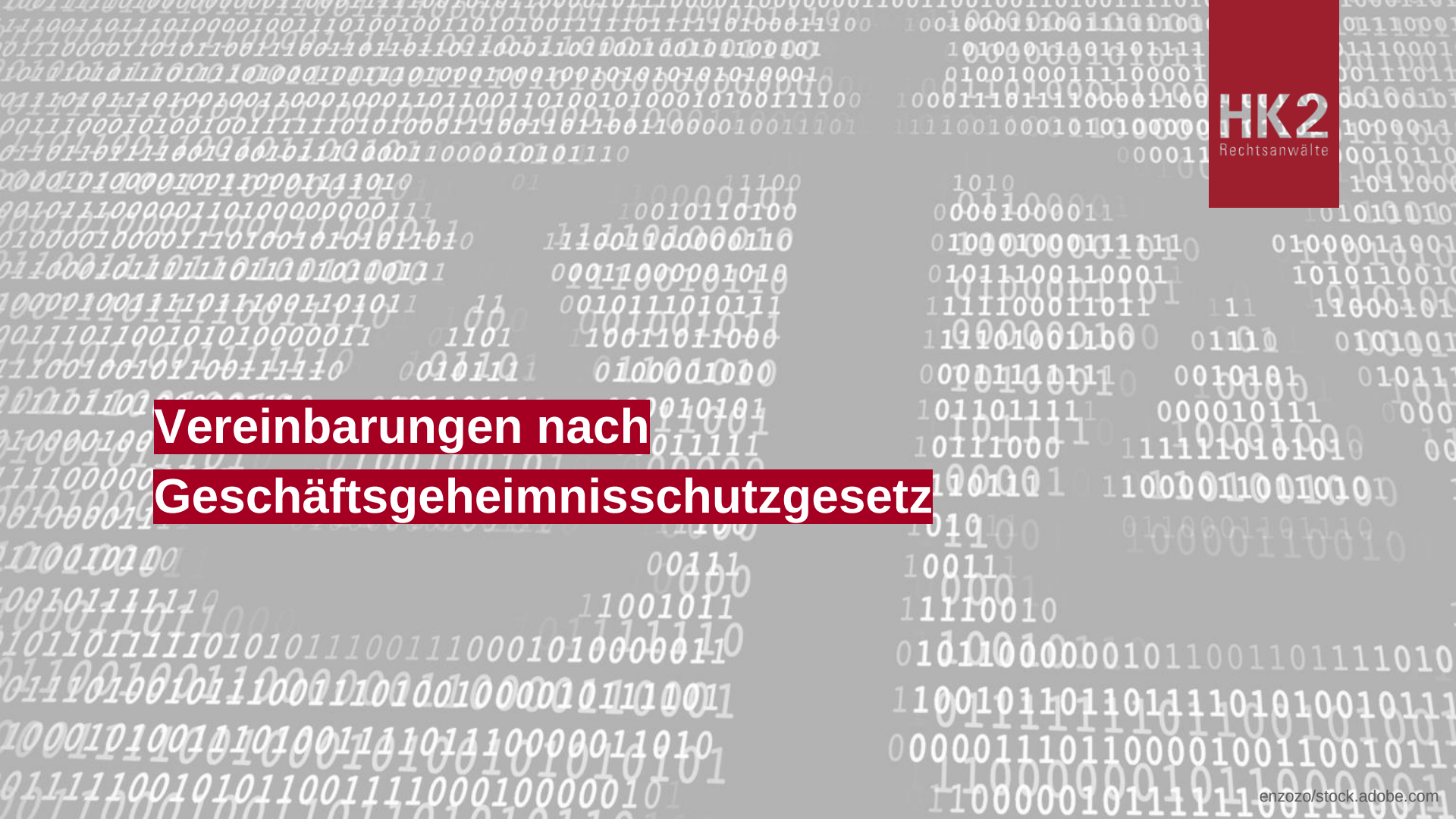
Haftung und höhere Gewalt justieren

Grahame Jenkins/Unsplash.com


HK2
Rechtsanwälte
ITSiG-Tango
Pexels.com

Vereinbarungen nach Geschäftsgeheimnisschutzgesetz

HK2 Rechtsanwälte



enzozo/stock.adobe.com

Schutz bei rechtswidrigem/r

Erwerb

Nutzung

Offenlegung

Rechtsfolgen bei Rechtsverletzungen

§ 6

Beseitigung
Unterlassung

§ 8

Auskunft
Schadensersatz

§ 7

Vernichtung
Herausgabe
Rückruf
Entfernung
Rücknahme vom Markt

Angemessene Geheimhaltungsmaßnahmen

- Objekt der Maßnahme (Informationen)
- Schutzbedarf/- niveau
- Geheimhaltungsmaßnahmen
  - technisch
  - organisatorisch
  - rechtlich
- Angemessenheit
  - Einzelfall/ individuell-konkrete Betrachtung
  - Maßstab/ Technologie-Niveau

- erforderlich: Schutzkonzept

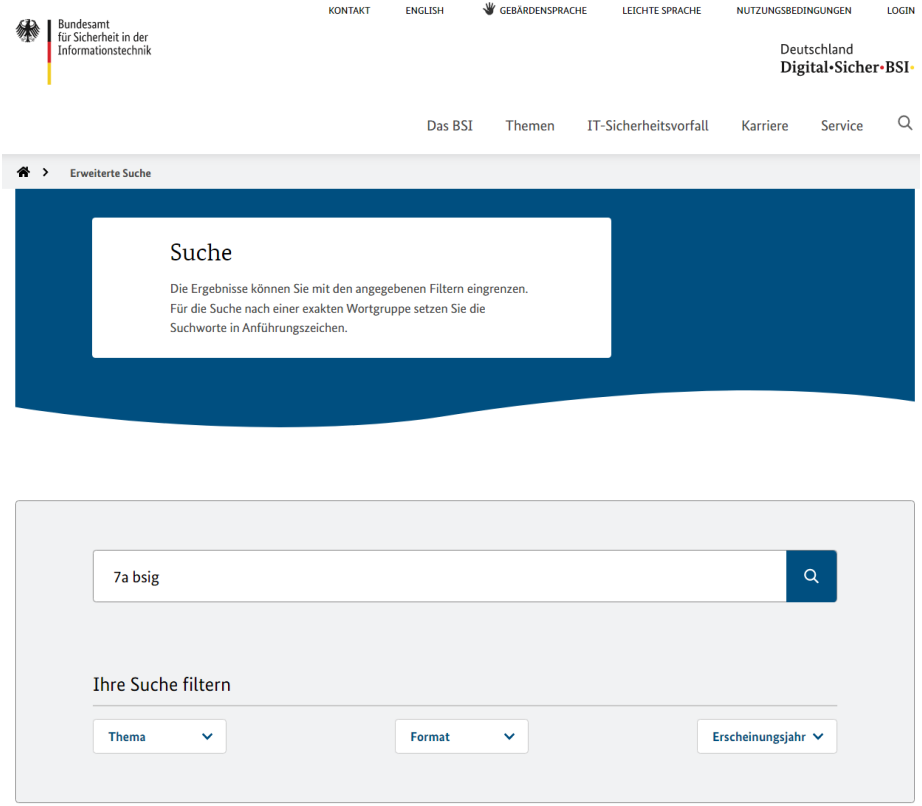
Zur persönlichen Haftung der Geschäftsleitung OLG Nürnberg vom 30.03.2022 – 12 U 1520/19

- Pflicht zur Legalität und Organisation bedingt für die Geschäftsleitung auch die **Einrichtung eines Compliance Management Systems**
- Geschäftliche Abläufe müssen daher weitgehend überwacht werden
  - Wenn nicht selber, dann durch Experten (Bsp. IT-Bereich)
- Auch die Sicherstellung der Geheimhaltung von Geschäftsgeheimnissen hiervon umfasst
- Bei Verstößen droht **Haftung mit Privatvermögen**

HK2 Rechtsanwälte

Checkliste GeschGehG

Aufgabe	Details	zuständig	erledigt
Geschäftsgeheimnisse identifizieren	Klassifizieren		
Schutzbedarfsanalyse	Risiken ermitteln		
Angemessene Geheimhaltungsmaßnahmen ermitteln	Technische, organisatorische und rechtliche Maßnahmen bestimmen anhand des Schutzbedarfs		
Dokumentation und Schutzkonzept	Umsetzung der Maßnahmen in der Unternehmenspraxis feststellen und planen		
Revision	Mindestens jährliche Überprüfung		
Organisation und Schulung im Unternehmen	Verfahren, Zuständigkeiten, Vorgaben, Ziele		
Monitoring Rechtsverletzungen	Wie wird beobachtet, dass Geheimnisse nicht unbefugt verwendet werden?		
Verträge schließen/ anpassen	✓ Arbeitsverträge ✓ Verträge mit freien Mitarbeitern ✓ Subunternehmerverträge ✓ Kooperationsverträge ✓ Lizenzverträge ✓ Forschungs- und Entwicklungsverträge ✓ NDA		



Hersteller informationstechnischer Produkte und Systeme

HK2 Rechtsanwälte

§ 7a BSIG

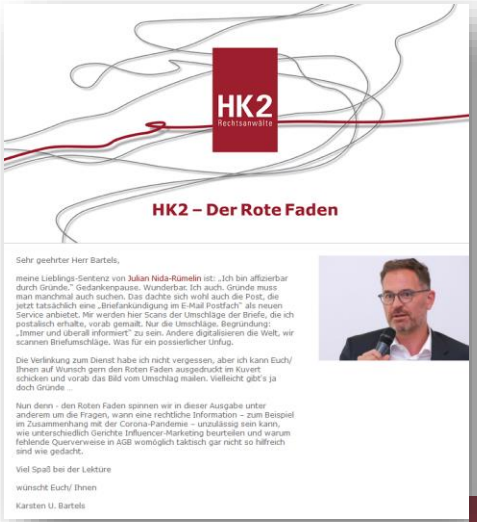
- **Untersuchungsrecht** des BSI hinsichtlich auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene IT-Produkte und –Systeme. Untersuchung durch Dritte möglich.
- **Auskunftspflicht** inkl. technischer Details („soweit erforderlich … alle notwendigen Auskünfte …“)
- **Informationsweitergabe** des BSI an Aufsichtsbehörde des Bundes oder an Ressort, wenn Behörde nicht vorhanden.
- BSI kann Erkenntnisse **weitergeben** und **veröffentlichen**, soweit erforderlich nach § 3 Abs. 1 S. 2 Nr. 1, 14, 14a, 17, 18 BSIG. Zuvor ist dem Hersteller Gelegenheit zur Stellungnahme zu geben.
- BSI kann **Öffentlichkeit** namentlich (Hersteller, Produkt) **informieren**, wenn Auskunft unterlassen wird und Gelegenheit zur Stellungnahme gegeben wurde.

Wer bewegt das jetzt …?

… Sie!

shutterstock_191690525

HK2
Rechtsanwälte



hk2.eu/newsletter

HK2
Rechtsanwälte

Slides + Kontakt

www.hk2.eu

linkedin.com/in/karstenbartels

www.comtection.de