Zukunft von IT-Sicherheitsvereinbarungen – für Anbieter und Anwender

it-sa, Knowledge Forum A, Nürnberg
26.10.2022, RA Karsten U. Bartels LL.M.

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

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)

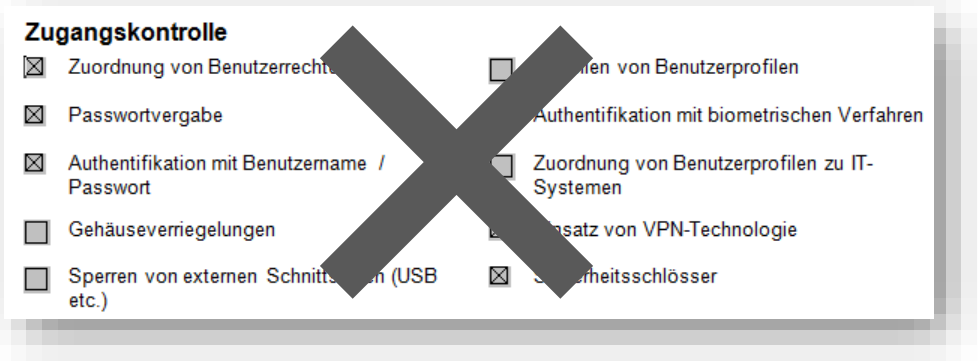
*Rechtsinformatik

Verträge zur IT-Sicherheit

- Gesetzliche Anforderungen
- Zukunft von Verträgen
  - nach DSGVO
  - zwischen KRITIS-Betreiber und Zulieferer
  - zum Geschäftsgeheimnisschutz
- Tipps

Mehr: heute, 15:00 Uhr
NCC Ost, Raum Kopenhagen

HK2
Rechtsanwälte

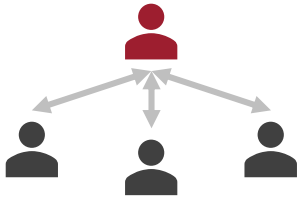


HK2
Rechtsanwälte

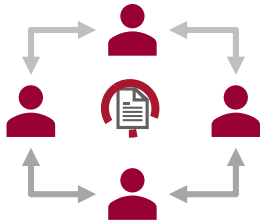
Anforderungen an Vertrag zur IT-Sicherheit?

Zweck, Gesetze, Leistungsverträge, …

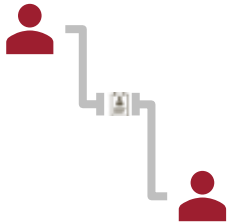
Art der Vereinbarung



Auftragsverarbeitung



Joint controllers



getrennt Verantwortliche

Daten ohne Personenbezug

KRITIS

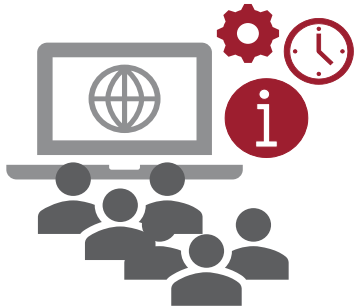
HK2
Rechtsanwälte

IT-Sicherheitsgesetz 2.0, bereichspezifische Gesetze, DSGVO, GeschGehG, …

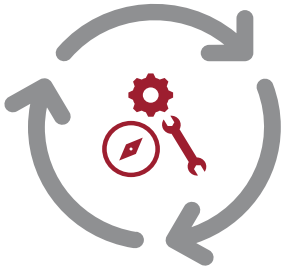
Demnächst: „KRITIS-Dachgesetz“/ ITSiG 3.0, eIDAS 2.0, NIS-RL 2.0, EU Cyber Resilience Act, …

IT-Sicherheitsmaßnahmen nach Art. 32 DSGVO

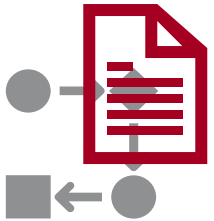
HK2 Rechtsanwälte



Risikobewertung



Stand der Technik



Dokumentation

EU-Standardvertragsklauseln (AV)
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

Typische Probleme von Datenschutz-Vereinbarungen

HK2 Rechtsanwälte

Unbrauchbare TOM des Anbieters/ Anwenders. Keine Einbeziehung von Unterauftragnehmer-TOM

Unklarheit über Leistung und nachlaufende Pflichten bei Ende des Hauptleistungsvertrags

Inpraktikable Audit-Regelungen.
Keine Kostentragungsregelungen.
Unpassender Zertifikats-Einsatz.

Mangelnde Konkretisierung von Unterstützungsleistungen des AN

Vermischung mit Geheimnisschutzverpflichtung.

Vertrag ist nicht agil.

shutterstock_191690525

HK2
Rechtsanwälte

Verträge zur IT-Sicherheit werden deutlich anspruchsvoller.

Nicht nur für KRITIS-Betreiber!

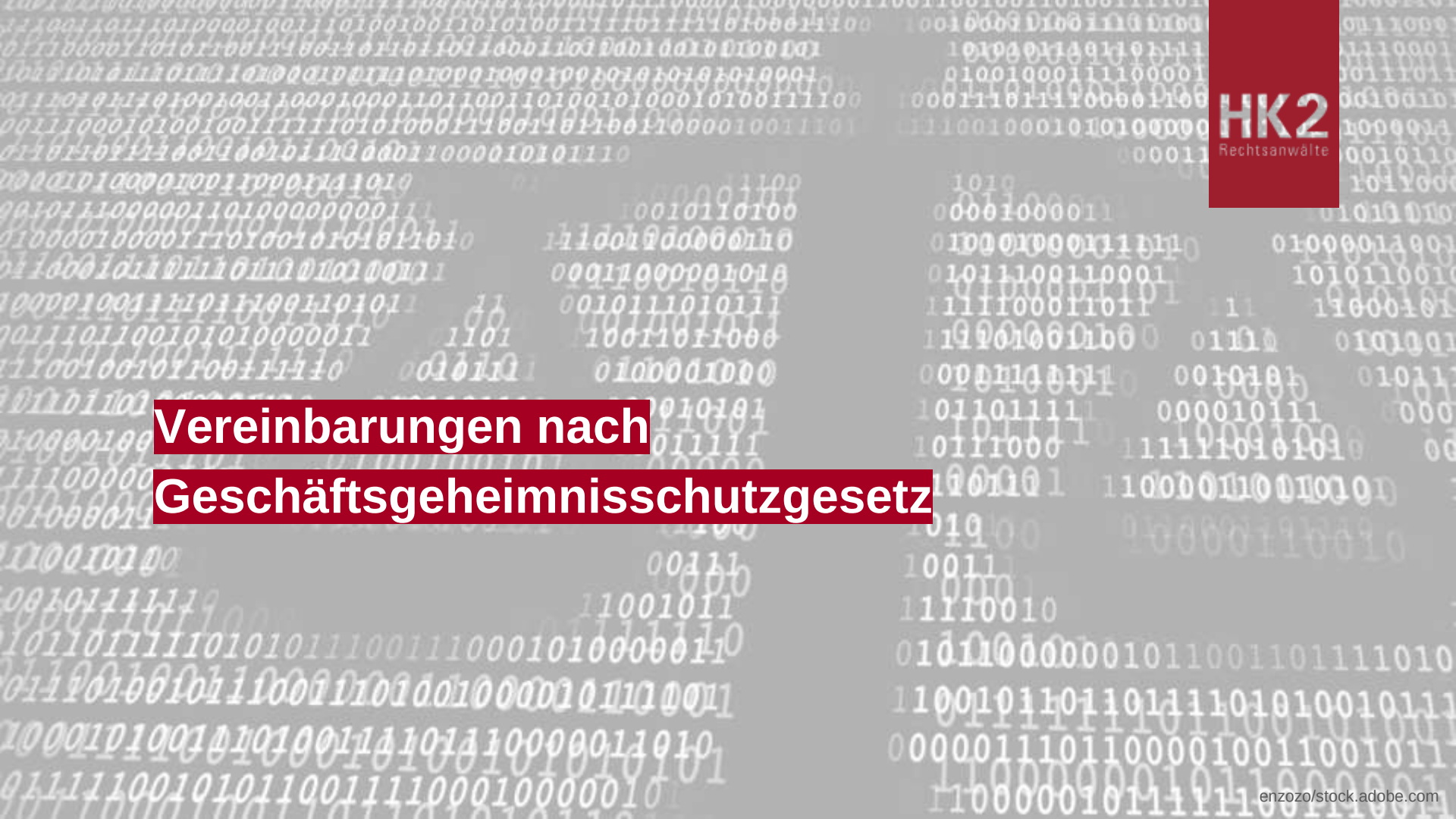
HK2 Rechtsanwälte

IT Security Agreements

- Schwachstellen-Management
- Umgang mit IT Security Incidents
- Compliance-Klauseln
- Stand der Technik
- Warnungen des BSI
- Kryptoagilität
- Anforderungen an Zulieferer

Vereinbarungen nach Geschäftsgeheimnisschutzgesetz

HK2 Rechtsanwälte



enzozo/stock.adobe.com

HK2
Rechtsanwälte

NDAs, Freelancer-/ Arbeitsverträge etc. sollten GeschGehG-Klausel haben.

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

HK2 Rechtsanwälte

- Pflicht der Geschäftsleitung zur Legalität und Organisation: **Compliance Management Systems** einzuführen!
- Geschäftliche Abläufe müssen weitgehend überwacht werden, selbst oder durch Experten
- Betrifft auch IT-Sicherheit und Schutz von Geschäftsgeheimnissen
- Pflichtverstöße können zur **Haftung mit Privatvermögen** führen

GRSI/shutterstock.com

HK2 Rechtsanwälte

Tipps (als Fragen)

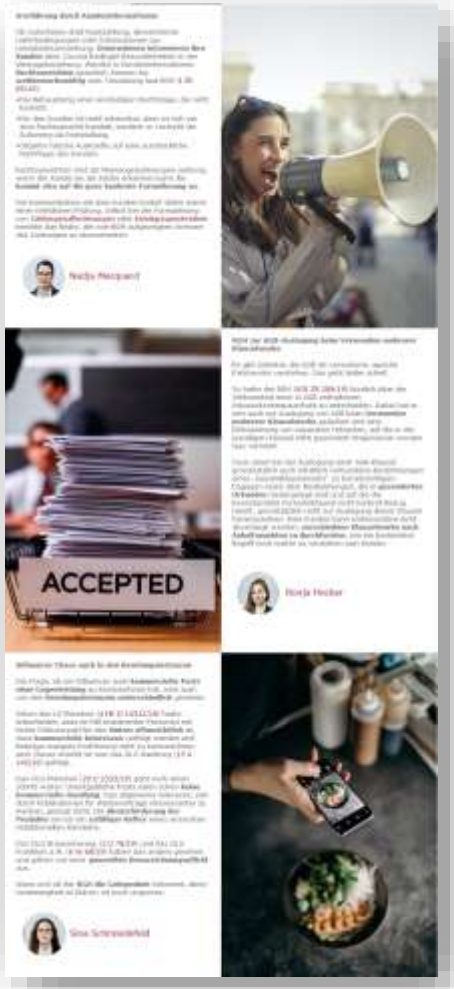
Wissen Sie, welche IT-Sicherheitsverträge mit welchen Inhalten für und gegen Ihr Unternehmen gelten?

Wurden die Verträge zur IT-Sicherheit im Team mit IT, IT-Sicherheit, IT-Recht und DSB erstellt oder geprüft?

Wie bewerten Sie, ob und wie diese Verträge die Anforderungen der DSGVO u. a. in Ihrem Interesse umsetzen?

In welchen Vertragsverhandlungen zur IT-Sicherheit befinden Sie sich derzeit?

shutterstock_191690525



HK2
Rechtsanwälte

hk2.eu/newsletter

HK2
Rechtsanwälte

Slides + Kontakt

www.hk2.eu

linkedin.com/in/karstenbartels