HEUKING KÜHN LÜER WOJTEK

Rechtlicher Rahmen: Edge wie Einfach?

Cloud-to-Edge: Schwappt der Cloud-Hype auf die Edge hinüber?

23.11.2023

Dr. Lutz M. Keppeler

Fachanwalt für IT-Recht

RECHTSANWÄLTE UND STEUERBERATER

Agenda

I. Einleitung

II. Allgemeine Rechtsfragen zu Edge

III. Schrems II...immer noch ein Thema?

IV. Digitalstrategie der EU

1. Cyber Resilience Act

2. Data Act

3. NIS-2-Richtlinie und das NIS2-Umsetzungsgesetz

IV. Fazit

Allgemeine Rechtsfragen zu Edge

Allgemeine Rechtsfragen zu Edge

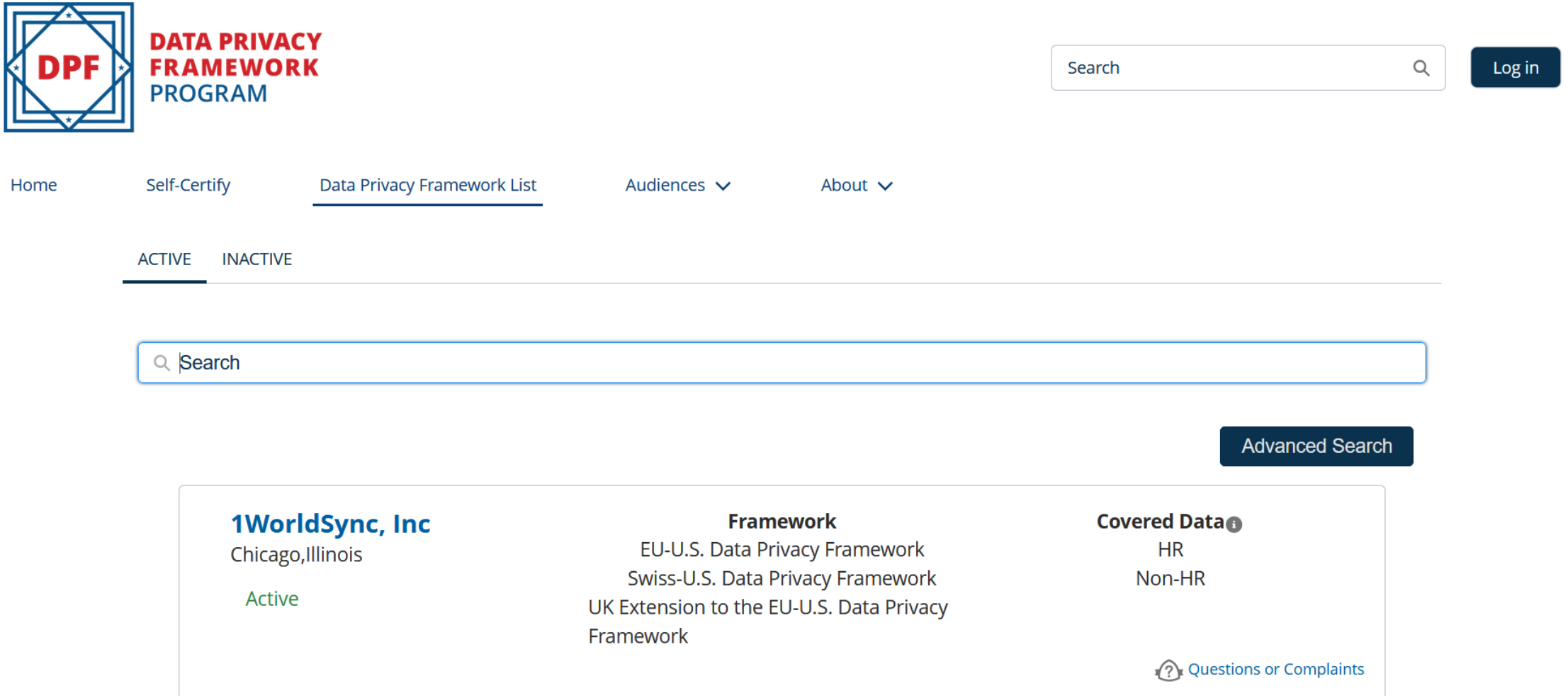
- Keine Spezialgesetze zu Edge
  - Folge: Alle individuell wichtigen Punkte müssen auf vertraglicher Ebene gelöst werden
    - Bsp: Latenz/Antwortzeiten
    - Bsp: Service Level
    - Bsp: IT-Sicherheit
- Datenschutz und Edge
  - Größere Kontrolle über den Speicherort von sensiblen Daten
  - Eingrenzung der Möglichkeit eines internationalen Datentransfer
  - Themen haben bei Datenschutzbeauftragten eine gewisse Überzeugungskraft
  - Aber Grenze der „Erforderlichkeit“ beachten

Schrems II.....immer noch ein Thema?

Schrems II und das EU-US Privacy Framework

- Am 10.07.2023 hat die EU-Kommission einen neuen Angemessenheitsbeschluss nach Art. 45 Abs. 3 DGVO angenommen „EU-US Privacy Framework“
- Standardvertragsklauseln, welche die Datenschutzbehörden teilweise als nicht ausreichenden Schutz für betroffene Personen angesehen haben, sind damit auch als zulässig anzusehen.
- Unterschiedliche Ansichten von Datenschutzaufsichtsbehörden: https://www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/unterschiedliche-ansichten-der-deutschen-aufsichtsbehoerden-zur-wirksamkeit-des-data-privacy-framework-nutzung-von-us-cloud-services.html
- Zunächst Rechtssicherheit, so dass sich das Thema des Datentransfers in die USA mit dem Privacy Framework für die Praxis nahezu erledigt hat

Schrems II und das EU-US Privacy Framework



Schrems II und das EU-US Privacy Framework

Other Covered Entities

Amazon Advertising LLC

Amazon Web Services, Inc.

Amazon.com Services LLC

Amazon.com, Inc.

Audible, Inc.

Participation

UK Extension to the EU-U.S. Data Privacy Framework: Active
Original Certification Date: 08/10/2023
Next Certification Due Date: 01/10/2024
Data Collected: NON-HR

Swiss-U.S. Data Privacy Framework: Active
Original Certification Date: 08/16/2017
Next Certification Due Date: 01/10/2024
Data Collected: NON-HR

EU-U.S. Data Privacy Framework: Active

Schrems II und das EU-US Privacy Framework

PURPOSE OF DATA COLLECTION

In general, the personal information we collect enables us to provide goods and services to customers, users, vendors, and sellers and helps us to personalize and improve the experience at our web sites. We use the information for different purposes depending upon the goods or services being provided. Among other things, these purposes may include the following: handling orders; delivering products and services; processing payments; processing for other purposes as required by our services; communicating with customers, users, vendors, and sellers about orders, products, services and promotional offers; updating our records and generally maintaining customer, user, vendor, and seller accounts; displaying content; and recommending merchandise and services that might be of interest to our customers, users, vendors, or sellers. We also use this information to prevent or detect fraud or abuses of our web sites, and enable third parties to carry out technical, logistical or other functions on our behalf.

Privacy Policy

Non-HR Data
Document1: Amazon Web Services Privacy Notice
Description:
For Amazon Web Services, Inc., this privacy statement describes what personal data we collect and how we use it.
Effective Date: 01/10/2023

Non-HR Data
Document1: Amazon Privacy Notice
Description:
For all covered entities other than Amazon Web Services, Inc., this privacy statement describes what personal data we collect and how we use it.
Effective Date: 01/01/2023

VERIFICATION METHOD

Self-Assessment

Schrems II und das EU-US Privacy Framework

Dispute Resolution

QUESTIONS OR COMPLAINTS?

If you have a question or complaint regarding the covered data, please contact Amazon.com, Inc. at:

Greg Luloff
Associate General Counsel, Privacy
Amazon.com, Inc.
2021 7TH Ave
Seattle, Washington 98121-2601

dataprivacyframework@amazon.com
Phone: (206) 266-1000

Data Privacy Framework organizations must respond within 45 days of receiving a complaint.

If you have not received a timely or satisfactory response from Amazon.com, Inc. to your question or complaint, please contact the independent recourse mechanism listed below

NON-HR RECOURSE MECHANISM
VeraSafe DPF Dispute Resolution Program

Appropriate statutory body with jurisdiction to investigate any claims against Amazon.com, Inc. regarding possible unfair or deceptive practices and violations of laws or regulations covering privacy Federal Trade Commission

Die Digitalstrategie der EU

II. Einordnung der Rechtsakte der EU

Gestaltung der digitalen Zukunft Europas: Die EU Digitalstrategie bis 2030

Schlussfolgerungen zur Cybersicherheitsstrategie der EU

- Resilienz, technologische Souveränität und Führungsrolle
- Aufbau operativer Kapazitäten zur Verhinderung, Abschreckung und Reaktion
- Förderung eines globalen und offenen Cyberspace durch verstärkte Zusammenarbeit

Umsetzung in Rechtsakten:

Organisationen	Produkte und Dienstleistungen
NIS-2-Richtlinie	Cyber Resilience Act
CER-Richtlinie	Data Act
Digital Operational Resilience Act	Data Governance Act
Cyber Solidarity Act	Artificial Intelligence Act

II. Gesetzgebungen im Rahmen der EU Digitalstrategie (Auszug)

	Aktueller Stand	Sanktionen
Digital Services Act	In Kraft getreten am 16. November 2022, gilt ab **17. Februar 2024**	bis zu 6 % des Jahresumsatzes für Verstöße sehr großer Online-Plattformen; im Übrigen sollen Mitgliedstaaten Sanktionen festlegen
Digital Markets Act	In Kraft getreten am 1. November 2022, gilt ab **02. Mai 2023**	bis zu 10 % des Jahresumsatzes
Data Act	Politische Einigung zwischen dem Europäischen Parlament und dem Rat der EU am 28. Juni 2023; Annahme des Datengesetzes durch das Europäische Parlament	Mitgliedstaaten sollen Sanktionen festlegen.
Data Governance Act	In Kraft getreten, ab dem **24. September 2023** anwendbar	"Abschreckende Geldstrafen"
Cyber Resiliance Act	Entwurf vom 15. September 2022; Kompromisstext des Rates der EU liegt seit dem 15. Juni 2023 vor; Beginn des Trilogs voraussichtlich September 2023 und in Kraft treten in 2024 angestrebt	15 Mio. Euro oder 2,5 % des weltweiten Jahresumsatzes
NIS-2-Richtlinie	In Kraft getreten; Umsetzungsfrist **07. Oktober 2024**	Für wesentliche Einrichtungen 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes
AI Regulation	Annahme des Gesetzesentwurfes am 14. Juni 2023; Beginn des Trilogs	maximal 30 Mio. Euro oder 6 % des weltweiten Jahresumsatzes
Richtlinie über KI-Haftung	Entwurf **28.09.2022**	Keine
Digital Operational Resilience Act (DORA)	In Kraft getreten am 16. Januar 2023; Anwendbar ab **17. Januar 2025**	Sanktionen sollen von Mitgliedsstaaten festgelegt werden
European Health Data Space (Regulation)	Entwurf vom **03.05.2022**	Sanktionen sollen von Mitgliedsstaaten festgelegt werden

Cyber Resilience Act

II. CRA (in a nutshell)

- Der Entwurf des Cyber Resilience Act („**CRA-E**“) richtet sich an
  - Hersteller,
  - Einführer und
  - Händler
  - von „Produkten mit digitalen Elementen“

- Unter „Produkte mit digitalen Elementen“ fallen sowohl Hard- und Software als solche, als auch deren einzelne Komponenten. Voraussetzung ist jedoch, dass das Produkt über „Ferndatenverarbeitungslösungen“ verfügt, also internetfähig ist.
  - SaaS ist nach aktuellen Entwürfen erfasst.
  - Also sind alle Edge „Produkte“ miterfasst.
- Ausnahmen für einzelne Sektoren: z.B. Medizinprodukte, Automotive

II. CRA (in a nutshell)

- Produkte mit digitalen Elementen müssen ohne bekannte ausnutzbare Schwachstellen geliefert werden.
- Auf der Grundlage einer verpflichtenden Risikobewertung müssen Produkte mit digitalen Elementen:
  - die Verfügbarkeit wesentlicher Funktionen schützen, einschließlich der Widerstandsfähigkeit gegen und der Abschwächung von Denial-of-Service-Angriffen
  - sicherheitsrelevante Informationen durch Aufzeichnung und/oder Überwachung relevanter interner Aktivitäten speichern („Logfiles“)
- Hersteller sind zur „Marktüberwachung“ bzgl. IT-Sicherheit verpflichtet
- Informationspflichten zur Cybersicherheit gegenüber dem Nutzer („Beipackzettel“)
- Zurverfügungstellung von „Software Bill of Materials“ (umstritten!)
  - Details über alle Komponenten und „Lieferkette“ => Inkl. Edge “Infrastruktur“

II. Bußgelder

- Art. 53 Penalties :

3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

4. The non-compliance with ~~any other~~ **the** obligations **set out in Articles [Articles12; 13; 14; 15; 16; 17; 20; 22 (1)-(4); 23 (1)-(4); 24(1)-(3); 29; 31; 37; 38; 42]** under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Data Act

II. Verpflichtungen DA (Auszug)

- „Vernetzte Produkte werden so konzipiert und hergestellt und verbundene Dienste werden so konzipiert und erbracht, dass die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.“ (Art. 3 Abs. 1)
- Art. 3 Abs. 2: Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein vernetztes Produkt werden dem Nutzer vom Verkäufer, Vermieter oder Leasinggeber – wobei es sich auch um den Hersteller handeln kann – mindestens folgende Informationen in klarer und verständlicher Art und Weise bereitgestellt:
  - Art, das Format und der geschätzte Umfang der Produktdaten, die das vernetzte Produkt generieren kann
  - (…)

II. Bußgeld, Rechtstreitigkeiten

- Wettbewerber können nach UWG vorgehen
  - Gegen Vermarktung eines Smart Devices, das gegen DA verstößt
  - Gegen AGB, die gegen DA verstoßen

- DA gewährt direkte zivilrechtlich einklagbare Ansprüche

- Zuständige Behörde kann Daten herausverlangen (noch unklar, wer in Deutschland die zuständige Behörde wird)

- Art. 40: „Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diese Verordnung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.“

NIS-2-Richtlinie und NIS2UmsuCG

II. NIS-2-Richtlinie und NIS2UmsuCG – Wesentliche Inhalte

NIS-2-Richtlinie

- Adressaten sind „**wesentliche“ und „wichtige Einrichtungen“**, die ihre Dienste in der EU erbringen oder Tätigkeit dort ausüben.
- Ziel ist die Sicherstellung eines hohen gemeinsamen Cybersicherheitsniveaus in der EU.
- Einordnung als wesentliche oder wichtige Einrichtung richtet sich nach mehreren Faktoren
- Wesentliche Pflichten betreffen Governance-Vorgaben an die Geschäftsleitung, Umsetzung von Risikomanagementmaßnahmen, Melde- und Berichtspflichten
- Umsetzung in Deutschland: NIS2UmsuCG bzw. IT-Sicherheitsgesetz 2024

NIS2UmsuCG (Entwurf)

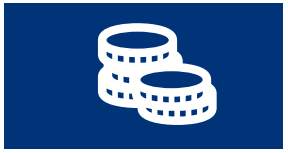
- Adressaten sind „**wichtige**“ und „**besonders wichtige Einrichtungen**“ sowie „**Betreiber kritischer Anlagen“.**
- Betreiber kritischer Anlagen sind automatisch wesentliche Einrichtungen im Sinne der NIS-2-Richtlinie.
- Umsetzung der Governance-Vorgaben an die Geschäftsleitung, Umsetzung von Risikomanagementmaßnahmen, Melde- und Berichtspflichten
- Hohe Bußgelder bei Pflichtverletzungen

II. NIS-2-Richtlinie und NIS2UmsuCG – Übersicht der Sektoren

Anhang I: Sektoren mit hoher Kritikalität


Energie


Verkehr

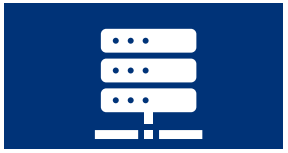

Bankwesen


Finanzmarktinfrastruktur


Gesundheitswesen


Trinkwasser


Abwasser


Digitale Infrastruktur


Verwaltung von IKT-Diensten


Öffentliche Verwaltung


Weltraum

Anhang II: Sonstige Kritische Einrichtungen


Post- und Kurierdienste


Abfallwirtschaft


Produktion, Herstellung und Handel mit chemischen Stoffen


Produktion, Verarbeitung und Vertrieb von Lebensmitteln


Verarbeitendes Gewerbe/Herstellung von Waren


Anbieter digitaler Dienste


Forschung

II. NIS-2-Richtlinie und NIS2UmsuCG – Übersicht der Sektoren

Größenunabhängige wesentliche Einrichtungen

- Qualifizierte Vertrauensdienste-anbieter
- TLD-Anbieter der obersten Stufe
- DNS-Diensteanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder -dienste
- Einrichtungen öffentlicher Verwaltung der Zentralregierung
- Kritische Einrichtungen gemäß CER-RL
- Betreiber wesentliche Dienste gemäß RL 2016/1148 (vor 16.01.2023)
- Sonstige nach nationale Recht eingestufte Einrichtungen (Anhang I oder II)

Größenunabhängige wichtige Einrichtungen

- Nach nationalem Recht eingestufte Einrichtungen (Anhang I oder II + Kriterien zur Kritikalität in Art. 2 Abs. 2 lit. b bis e)

II. NIS-2-Richtlinie und NIS2UmsuCG – Governance-Pflichten

Pflichten der Geschäftsleitung

- Pflicht zur Einführung, Billigung und Überwachung der Umsetzung der Risikomanagementmaßnahmen
- Pflicht zur Teilnahme an Schulungen im Bereich Cybersicherheit.

Sanktionen gegenüber Geschäftsleitung

- Persönliche Haftung: Leitungspersonal soll für Verstöße gegen Governance-Pflichten verantwortlich sein
- Befugnis der Behörden zur vorübergehenden Untersagung der Wahrnehmung von Leitungsaufgaben, falls Durchsetzungsmaßnahmen nicht oder nicht wirksam umgesetzt werden (nur bei wesentlichen Einrichtungen!)

Geplante Umsetzung in Deutschland

- Persönliche Haftung für Schäden gegenüber der Einrichtung (ohne Möglichkeit auf Verzicht oder Vergleich)
- Schadensbegriff soll Regressansprüche und **Bußgeldforderungen** erfassen

Konsequenz: Cyber-Security ist Aufgabe der Geschäftsleitung!

II. NIS-2-Richtlinie und NIS2UmsuCG – Risikomanagement

Risikomanagementpflichten

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme (**Sicherheitskonzepte**)
- Maßnahmen zur **Bewältigung von Sicherheitsvorfällen**
- Maßnahmen zur **Aufrechterhaltung des Betriebs** (Backup-Management und die Notfall-Wiederherstellung von Daten, Krisenmanagement)
- **Sicherheit der Lieferkette** und Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen (einschließlich Management und Offenlegung von Schwachstellen)
- Konzepte und Verfahren zur **Bewertung der Wirksamkeit der Risikomanagementmaßnahmen** im Bereich Cybersicherheit
- Grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich Cybersicherheit
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und ggfs. **Verschlüsselung**
- **Sicherheit des Personals**, Konzepte für die **Zugriffskontrolle** und Management von Anlagen
- **Verwendung von Lösungen zur Multi-Faktor-Authentifizierung** oder kontinuierlichen **Authentifizierung**, **gesicherte Sprach-, Video- und Text-Kommunikation** sowie ggfs. gesicherte **Notfallkommunikationssysteme**

HEUKING KÜHN LÜER WOJTEK

Vielen Dank
für Ihre Aufmerksamkeit

www.heuking.de

Berlin
Kurfürstendamm 32
10719 Berlin
T +49 30 88 00 97-0
F +49 30 88 00 97-99

Düsseldorf
Georg-Glock-Straße 4
40474 Düsseldorf
T +49 211 600 55-00
F +49 211 600 55-050

Hamburg
Neuer Wall 63
20354 Hamburg
T +49 40 35 52 80-0
F +49 40 35 52 80-80

München
Prinzregentenstraße 48
80538 München
T +49 89 540 31-0
F +49 89 540 31-540

Chemnitz
Weststraße 16
09112 Chemnitz
T +49 371 38 203-0
F +49 371 38 203-100

Frankfurt
Goetheplatz 5-7
60313 Frankfurt am Main
T +49 69 975 61- 0
F +49 69 975 61-200

Köln
Magnusstraße 13
50672 Köln
T +49 221 20 52-0
F +49 221 20 52-1

Stuttgart
Augustenstraße 1
70178 Stuttgart
T +49 711 22 04 579-0
F +49 711 22 04 579-44

Zürich
Bahnhofstrasse 69
8001 Zürich/Schweiz
T +41 44 200 71-00
F +41 44 200 71-01

Ansprechpartner

Dr. Lutz M. Keppeler

Partner

Fachanwalt für IT-Recht

Magnusstraße 13

50672 Köln

T +49 221 2052-426

F +49 221 2052-1

l.keppeler@heuking.de

Kompetenzen

- IT-Recht mit Spezialisierung auf IT-Sicherheitsrecht und Open Source Lizenzen
- Datenschutzrecht
- Telekommunikationsrecht

Mitgliedschaften

- Fellow der European Free Software Foundation (FSFE)
- International Bar Association (IBA)

Veröffentlichungen (Auszug)

- Die Open-Source-Bereichsausnahme im Entwurf des Cyber-Resilience-Act Zeitschrift für Product Compliance (ZfPC) 2023, S. 117-123
- Kapitel „Cyberversicherungen“ in: Wollinger / Schulze (Hrsg.) Handbuch Cybersecurity für die öffentliche Verwaltung, 2020
- § 2, 4a,4b,5b,7a-c,9b BSIG, § 11 EnWG, § 109 TKG in Ritter, Kommentar zum IT-Sig. 2.0 (2021)
- „Datenschutz und SSL-Decryption“ K&R 2017, 453 ff.
- Technische und rechtliche Probleme bei der Umsetzung der DSGVO Löschpflichten ZD 2017, 314 ff.