EU Cybersecurity Act, NIS-Richtlinie und DSGVO: Rechtliche Anforderungen an die Sicherheit von IKT-Produkten und -Diensten

Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E
Senior Researcher | Senior Consultant
markus.kastelitz@researchinstitute.at

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher | Senior Consultant
walter.hoetzendorfer@researchinstitute.at

Ing. Dr. iur. Christof Tschohl
Wissenschaftlicher Leiter | Gesellschafter | Prokurist
christof.tschohl@researchinstitute.at

Dr. iur. Heidi Scheichenbauer
Senior Researcher | Senior Consultant
heidi.scheichenbauer@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart Rights Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center

Das **Research Institute (RI)** ist ein Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.

Portfolio:

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **Smart.Rights.Consulting:** Beratung zu rechtlichen, technischen und organisatorischen Fragen des Datenschutzes
- **Schulungen**, auf Wunsch zugeschnitten auf Ihre Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit renommierten Partnern auf nationaler und internationaler Ebene.

research institute

Warum Cybersecurity?
"The S in IoT stands for Security"

11.02.2019 17:35 Uhr | Security

Kühlsysteme mit schwachem Standardpasswort übers Internet manipulierbar

Um nicht eiskalt von Angreifern erwischt zu werden, sollten Betreiber von Kühlsystemen der Firma Resource Data Management umgehend das Standardpasswort ändern.

Kinder-Smartwatch mit Tracking-Funktion: Hersteller Enox sieht kein Problem mit Spionage-Uhr

Die Kinder-Smartwatch Safe-KID-One kann von Fremden aus dem Netz abgehört und verfolgt werden. Der Hersteller sieht keinen Hinderungsgrund für den Verkauf.

12.02.2019 11:16 Uhr 66

29.01.2019 18:40 Uhr

Smart-Home-Hack: Tuya veröffentlicht Sicherheits-Update

Der Smart-Home-Hardware-Hersteller Tuya veröffentlicht ein Update, das die auf dem 35C3 veröffentlichten Sicherheitslücken schließen soll.

SMART HOME

Alexa sent private audio to a random contact, Portland family says

A family in Oregon says their Alexa device recorded audio of a private conversation and sent it out to a random contact without warning.

BY RY CRIST | MAY 24, 2018 2:15 PM PDT

California Governor Approves Bills Tightening Security, Privacy of IoT Devices

Senate Bill 327 and Assembly Bill 1906, signed Sept. 28 by Gov. Jerry Brown, would require makers of Internet-connected devices to improve their security.

BY THEO DOUGLAS / SEPTEMBER 28, 2018

EU Cybersecurity Act I

- VO-Vorschlag über die „EU-Cybersicherheitsagentur“ (ENISA) […] sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik **(„Rechtsakt zur Cybersicherheit“ - CSA**), COM(2017) 477 final
  - **Status**: Trilog erfolgreich beendet (Einigung 10.12.2018), Parlamentsausschuss ITRE stimmt zu (14.01.2019)
  - Frei verfügbare Letztfassung Ratsdokument v. 20.12.2018: ST 15786 2018 INIT
  - → EP stimmt darüber voraussichtlich am 12.03.2019 ab
  - **Ziele**:
    - **Sensibilisierung** der Unternehmen u. Bürger für Cybersicherheit
    - **Vermeidung eines Nebeneinanders** unterschiedlicher Zertifizierungssysteme in der EU (Kosten, Marktfragmentierung, Interoperabilität, …) → Harmonisierung
    - **Stärkung des Vertrauens** in den digitalen Binnenmarkt und in digitale Innovationen durch **Transparenz** bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit von IKT-Produkten und **„security by design“** (bereits bei ihrer technischen Konzeption und Entwicklung)
      Ausdrückliche Bezugnahme durch Kommission auf „Internet of Things“ (IoT)

EU Cybersecurity Act II

- **Rahmenregelwerk** für die Schaffung europäischer Systeme für die Zertifizierung der Cybersicherheit von IKT-Produkten und -Diensten
- **Allgemeine Anforderungen** an die Cybersicherheit für die Zwecke der Zertifizierung, ergänzt durch besondere **Cybersicherheitsziele** (im Wesentlichen: Verfügbarkeit, Authentizität, Integrität, Vertraulichkeit; s. Art 45)
- **Keine** Schaffung unmittelbar operativer Zertifizierungssysteme, sondern:
  - **System (Rahmen, „scheme“) für die Ausarbeitung spezifischer Zertifizierungssysteme** für bestimmte IKT-Produkte/-Dienste

    = Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung von Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden
  - Cybersicherheitszertifizierung soll bestimmte Anforderungen (je nach Vertrauenswürdigkeitsstufe) an zertifizierte IKT-Produkte und -Dienste gewährleisten (siehe Art 45)

EU Cybersecurity Act III

- **3 Vertrauenswürdigkeitsstufen** nach beabsichtigter Verwendung:
  - „**niedrig**“: **Selbstbewertung** der Konformität ist möglich
    (Art 46a; ursprüngl. im KOM-Vorschlag nicht vorgesehen)
    *„evaluated to a level which aims to minimise the **known basic risks** […] evaluation activities shall include at least a review of a technical **documentation**, or where not applicable they shall include substitute activities with equivalent effect”*
  - „**mittel**“: Zertifizierung durch **Konformitätsbewertungsstelle** erforderlich
    *„evaluated to a level which aims to minimise **known cyber risks** […] carried out by actors with **limited skills and resources**. The evaluation activities shall include at least: reviewing the **non-applicability of publicly known vulnerabilities and** testing that the ICT products, processes or services correctly” implement the necessary security functionality”*
  - „**hoch**“: Zertifizierung durch nationale **Cybersicherheitszertifizierungsbehörde** erforderlich
    *„evaluated to a level which aims to minimise the **risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources**. The evaluation activities shall include at least: reviewing the non-applicability of publicly known vulnerabilities, testing that the ICT products, processes or services correctly implement the necessary security functionality, at the **state-of-the-art**, and assessing their **resistance to skilled attackers via penetration testing**; or where not applicable they shall include substitute activities”*

EU Cybersecurity Act IV

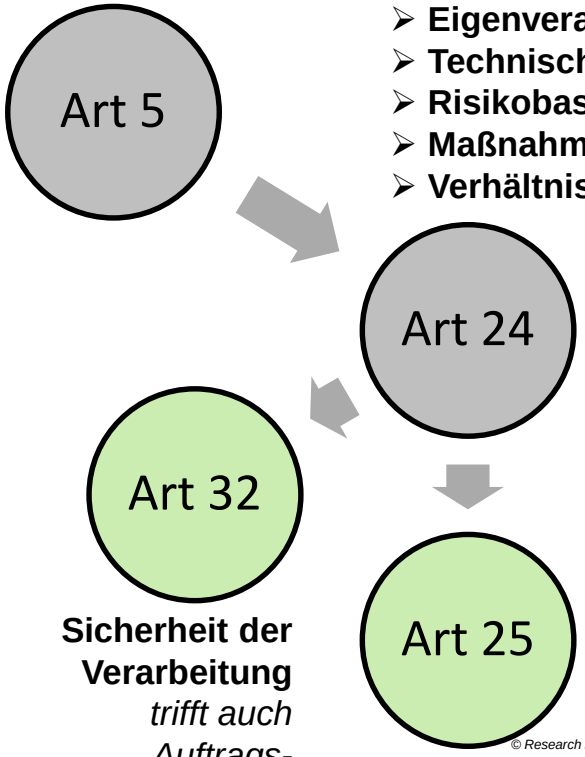
- Zertifikate werden für eine Höchstdauer von **drei Jahren** erteilt; verlängerbar
- Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen gem. DSGVO (auch wenn solche Vorgänge in Produkte und Dienste eingebettet sind) bleiben vom Cybersecurity Act unberührt (ErwGr 54)
- Recht auf Beschwerde natürlicher und jurist. Personen beim Zertifikatsaussteller bzw. Cybersicherheitszertifizierungsbehörde (Art 53a)

EU Cybersecurity Act: Kritik

- Zertifizierung ist **freiwillig**, sofern nicht anderweitig im Unionsrecht oder nationalen Recht festgelegt
- Aussagekraft eines Zertifikats?
- Zertifizierung als „**Momentaufnahme**“
- Tlw. **Selbstbewertung der Konformität** durch Hersteller zulässig
  - effiziente Marktüberwachung?
  - Sanktionen den MS überlassen
- Anstelle bestehender Normungsorganisationen eigene, neue Gremien geschaffen → Effizienz? Wann einsatzbereit?
- Hersteller von Endverbraucher-Produkten hat **kaum ökonomische Anreize** für nachhaltige Sicherheit über den Produktlebenszyklus ➔ Werden die Kunden zu zertifizierten Produkten greifen?
- Welche Ansätze könnten Sicherheit über den Produktlebenszyklus bringen?
  - Verpflichtendes ein Ablaufdatum für Sicherheitsupdates, das beim Verkauf von IoT-Produkten angegeben werden muss
  - Nach Erreichen des Ablaufdatums muss die Firmware Open Source werden

Pflichten des Verantwortlichen: Überblick und Zusammenhänge

Datenschutzgrundsätze
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht



- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

Sicherheit der Verarbeitung
trifft auch Auftrags-verarbeiter

Privacy by Design und by Default
(vor und während der Verarbeitung)

ART 42 DSGVO: ZERTIFIZIERUNG

Datenschutzgrundsätze
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht

Art 5

- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

Art 24

ART 24 ABS 3 DSGVO: *Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.*

Art 32

ART 32 ABS 3 DSGVO: *Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

Sicherheit der Verarbeitung
trifft auch Auftrags-verarbeiter

Art 25

Privacy by Design und by Default
(vor und während der Verarbeitung)

ART 25 ABS 3 DSGVO: *Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

DATENSICHERHEIT IN DER DSGVO

- Sicherheit neu unter den Datenschutz-Grundsätzen in Art 5 Abs 1 lit f: „Sicherheit der personenbezogenen Daten“, „Integrität und Vertraulichkeit“
- Art 32 nennt ausdrücklich folgende Schutzmaßnahmen:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
    - Verpflichtung zur Pseudonymisierung, wenn der konkrete Verarbeitungszweck auch mit pseudonymisierten Daten zu erreichen ist (sofern kein unverhältnismäßig hoher Aufwand)
    - Verpflichtung zur Verschlüsselung der Daten bei Speicherung und Übertragung, außer in begründeten Ausnahmefällen
  - Fähigkeit, folgende Schutzziele auf Dauer sicherzustellen:
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - Belastbarkeit
  - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Recovery)
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

DSGVO:
Faktische Wirkung Für Hersteller

ErwGr 78 DSGVO:

In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, ***sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden****, das* ***Recht auf Datenschutz bei der Entwicklung und Gestaltung*** *der Produkte, Dienste und Anwendungen* ***zu berücksichtigen*** *und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen,* ***dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen****. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.*

➔ Faktische Wirkung auf Hersteller von Produkten, denn Verantwortliche sind dazu verpflichtet, solche Produkte zu erwerben, die die Vorgaben des Art 25 erfüllen

research institute

ZUSAMMENSCHAU
CSA, NIS & DSGVO

- **Cybersecurity Act**
  - Grds. freiwillige Zertifizierung (Ausnahme: unionsrechtlich oder im Recht des MS zwingend)
  - **Weiter** Anwendungsbereich
  - Neue Zertifizierungs-Schemes, aber Anknüpfung an bestehende Standards (Art 47, in erster Linie sollen internationale Standards herangezogen werden)
- **NIS-RL/NISG**
  - Verpflichtend für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste
  - **Enger** Anwendungsbereich
  - Anknüpfung an bestehende Standards
- **DSGVO**
  - Grds. verpflichtend für alle Verantwortlichen und Auftragsverarbeiter, jedoch nur mittelbar für Hersteller
  - **Weiter** Anwendungsbereich: Verarbeitung personenbezogener Daten (darauf jedoch beschränkt)
  - Problem der Durchsetzung

Weitere Rechtsvorschriften mit IT-Sicherheitsbezug

- Vielfältig über unterschiedliche Rechtsmaterien „verstreut“:
  - Telekommunikationsgesetz, Gesundheitstelematikgesetz, Informationssicherheitsgesetz, Zahlungsdienstegesetz etc.
  - Deutschland: technische Richtlinie für Routersicherheit

- **Zivilrechtliche Aspekte:**
  - Dzt. Entwurf einer RL über bestimmte vertragsrechtliche Aspekte des Warenhandels enthält Regeln zu sog. „Smart Goods“ (Updatepflicht etc.)
  - PHG: Produktbegriff (bewegl. körperl. Sache) erfasst IoT → in Österreich dazu (soweit überblickbar) keine belastbare höchstgerichtl. Rsp.; bei Sachschäden limitierter SchE
  - § 82 AktG und § 22 GmbHG: Persönliche Haftung der Geschäftsleitung für die Errichtung eines internen Kontrollsystems
  - Vgl. auch OGH 20.08.1998, 10 Ob 212/98v: ÖNORMen bilden grds. den Haftungsmaßstab, weil sie festhalten, was branchenüblich ist

Abschließende Hinweise

- Paneldiskussion „Mensch und IoT“ zur Regulierung des IoT, im Anschluss um 16 Uhr, Hörsaal 212, es diskutieren:
  - Hanna Maria Kreuzbauer, Uni Salzburg
  - Rigo Wenning, W3C
  - Christopher Frauenberger, TU Wien, Forschungsprojekt COMPASS
  - Christof Tschohl, Research Institute, Forschungsprojekt COMPASS
  - Chair: Walter Hötzendorfer, Research Institute, Forschungsprojekt COMPASS
- Vortrag von *Alexander Novotny*: „Stand der Technik von NIS-Maßnahmen - Auslegungshilfen zwischen IT, OT und IoT“, im Anschluss um 16 Uhr, Hörsaal 211

Die Inhalte dieses Vortrags basieren zum Teil auf Arbeiten im Forschungsprojekt COMPASS, finanziert im Programm IKT der Zukunft von FFG und BMVIT.

WEITERFÜHRENDES

- EP (Legislative Observatory), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0225(COD)
- ENISA, IoT Security Standards Gap Analysis (2019), https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis
- NIS Cooperation Group, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
- NIST, Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT), NISTIR 8200
- NIST, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, Draft NISTIR 8228
- IoT Security Guidance (u.a. mit Manufacturer IoT Security Guidance) https://www.owasp.org/index.php/IoT_Security_Guidance
- *Kleinhans*, Improving IoT security in the EU (2018), https://www.stiftung-nv.de/sites/default/files/european_iot_product-database.pdf
- *Ross*, https://www.heise.de/newsticker/meldung/Kommentar-zur-IoT-Sicherheit-Europas-Verordnung-ist-zahnlos-4208938.html
- *Kipker/Scholz*, EU Cybersecurity-Verordnung, DuD 2018, 701

EU Cybersecurity Act, NIS-Richtlinie und DSGVO: Rechtliche Anforderungen an die Sicherheit von IKT-Produkten und -Diensten

Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E
Senior Researcher | Senior Consultant
markus.kastelitz@researchinstitute.at

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher | Senior Consultant
walter.hoetzendorfer@researchinstitute.at

Ing. Dr. iur. Christof Tschohl
Wissenschaftlicher Leiter | Gesellschafter | Prokurist
christof.tschohl@researchinstitute.at

Dr. iur. Heidi Scheichenbauer
Senior Researcher | Senior Consultant
heidi.scheichenbauer@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart Rights Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

Ing. Mag. Dr. iur. Christof Tschohl

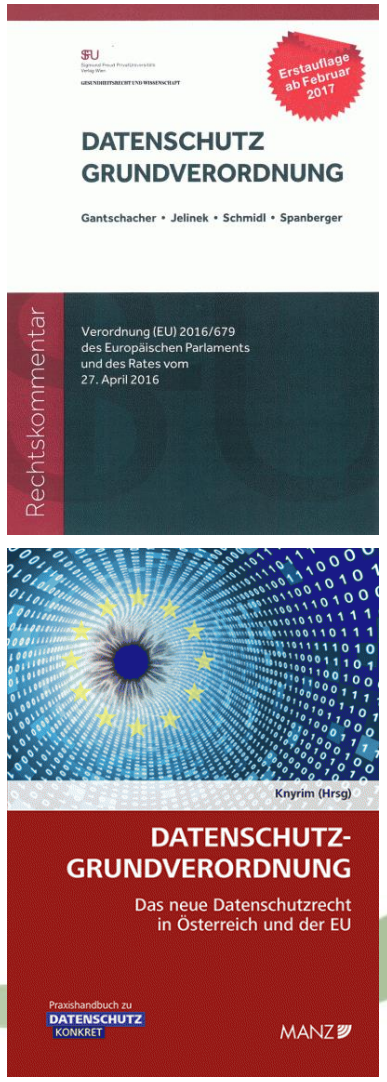
- Nachrichtentechniker (HTL Rankweil, Ericsson, Kapsch) und Jurist
- Bis 2012 Ludwig Boltzmann Institut für Menschenrechte und Uni Wien
- Seit Ende 2012: Wissenschaftlicher Leiter und Gesellschafter der Research Institute AG & Co KG
- Forschung und Beratung – Schnittstelle von Technik und Recht
- Lehre (aktuell: Uni Wien, Lehrgang für Informations- und Medienrecht; Vienna Human Rights Master; Universität Hannover, Masterprogramme IT Law; Donau Uni Krems, Big Data und Datenschutz; FH St. Pölten: Ethik in der Technologieentwicklung; Anwaltsakademie Österreich)
- Mitgliedschaften:
  - epicenter.works – Plattform für digitale Grundrechte (vormals AKVorrat), Obmann
  - Österreichische Computer Gesellschaft (OCG), Co-Leiter „OCG Forum Privacy“
  - Österreichische RichterInnenvereinigung, Fachgruppe Grundrechte, a.o. Mitglied, regelmäßig Vortragender in Aus- und Fortbildung seit 2008
  - Mitglied des CERT-Beirats im österreichischen Bundeskanzleramt
  - Akkreditiert bei ASI zur Datenschutz und ISO27000 Normung (CEN+ISO)

Dipl.-Ing. Dr. iur. Walter Hötzendorfer

- Wirtschaftsinformatiker und Jurist
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- Autor des Buches „**Datenschutz und Privacy by Design im Identitätsmanagement**“ und Mitautor zweier aktueller Bücher zur Datenschutz-Grundverordnung
- Vorstandsmitglied der Österreichischen Computer Gesellschaft (**OCG**) und Co-Leiter **OCG Forum Privacy**
- Mitglied in der ASI-AG 001 18, die derzeit einen Datenschutz-Management-Standard ausarbeitet
- Vortragender im In- und Ausland
- **Erfahrungen** in:
  - Wissenschaft (RI, Uni Wien, Arbeitsgruppe Rechtsinformatik)
  - Rechtsberatung
  - Software Engineering
  - Prozessmanagement
- **Forschungsschwerpunkte**:
  - Technische und organisatorische Aspekte des Datenschutzrechts
  - Privacy Engineering, Privacy by Design
  - Datensicherheit/Netzwerk- und Informationssicherheit (NIS)
  - Identity Management
  - Telekommunikationsrecht
  - Öffentliche Sicherheit

Mag. Markus Kastelitz, LL.M., CIPP/E

- Jurist mit IT-Rechts-Ausbildung
- Zertifizierter Information Privacy Professional (IAPP)
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- Mitautor von Büchern zur Datenschutz-Grundverordnung
- Co-Gründer und Vorstandsmitglied **Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at**
- Lehrgangsbeiratsmitglied und Vortragender am Lehrgang **Datenschutz und Privacy** (Donau-Universität Krems)
- **Erfahrungen** in:
  - Wissenschaft (Uni Hannover, Lehrstuhl Prof. Dr. Forgó)
  - Rechtsberatung (u.a. MedUni Wien, Industriekonzern, Parlamentsdirektion, RTR)
  - Datenschutzbeauftragter (MedUni Wien, Research Institute)
- **Forschungsschwerpunkte**:
  - Umsetzung der DSGVO
  - Datenschutz in der Forschung mit Schwerpunkt medizinische Forschung
  - Moderne Technologien und Datenschutz



Dr. iur. Heidi Scheichenbauer

- Juristin
- **Senior Researcher** und **Senior Consultant**, Research Institute
- Autorin von Fachbeiträgen in datenschutzrechtlichen Fachzeitschriften (Jus-IT, Datenschutz-konkret)
- Mitautorin mehrerer aktueller Bücher zur Datenschutz-Grundverordnung (jusIT Spezial: DS-GVO, Handbuch Datenschutz Verlag WEKA) Vortragstätigkeiten
- Datenschutz für Vereine (Verlag Linde)
- **Erfahrungen** in:
  - Wissenschaft (RI, KMU Forschung Austria)
  - Öffentlichkeitsarbeit (Fundraising Verband Austria)
  - Rechtsberatung
- **Forschungsschwerpunkte**:
  - Datenschutzrecht für gem. Organisationen
  - Bilddaten
  - Geodaten

RECHTLICHE HINWEISE

Zweck: Dieses Dokument dient als Präsentationsunterlage.

Erstellt von den auf der Titelseite genannten AutorInnen

Disclaimer:

Dieses Dokument wurde auf Basis jener Informationen erstellt, die den AutorInnen als für den Zweck des Dokuments relevant erschien. Der Autor(en) übernimmt jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Dokument enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.