Deutsche Stiftung für Recht und Informatik

Internationaler Datentransfer von HR / Non-HR Daten unter dem EU-U.S. Data Privacy Framework

Tilmann Fleck / Johannes Nehlsen
Julius-Maximilians-Universität Würzburg

Herbstakademie 2024

Agenda

- Beispiele aus der Praxis
- Auslegung des Begriffes HR-Data
- SCCs und TIAs
- Implikationen
- Fazit

Wer hostet Ihre HR-Systeme?

Microsoft Corporation
Redmond, WA

FRAMEWORK	STATUS	COVERED DATA	
EU-U.S. Data Privacy Framework	Active	HR Data	Non-HR Data
Swiss-U.S. Data Privacy Framework	Active	HR Data	Non-HR Data
UK Extension to the EU-U.S. Data Privacy Framework	Active	HR Data	Non-HR Data

+18 Covered Entities

FULL PROFILE

Questions or Complaints

Amazon.com, Inc.
Seattle, WA

FRAMEWORK	STATUS	COVERED DATA	
EU-U.S. Data Privacy Framework	Active		Non-HR Data
Swiss-U.S. Data Privacy Framework	Active		Non-HR Data
UK Extension to the EU-U.S. Data Privacy Framework	Active		Non-HR Data

+5 Covered Entities

FULL PROFILE

Questions or Complaints

Beispiel Esri

Non-HR Data

Name

Esri Privacy Statement

Description

The Esri Privacy Statement ("Privacy Statement") covers our use, storage, sharing, and disclosure of personal information we collect through our websites, including www.esri.com, https://my.esri.com, https://esricommunity.force.com. It also describes your choices regarding use, access and correction of your personal information.

Effective Date

11/30/2023

Policy Link

https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement

HR Data

Name

Esri Employee Privacy Notice

Description

Privacy Notice for Esri employees.

Effective Date

01/01/2023

Non-HR Data

Name

Esri Products & Services Privacy Statement Supplement

Description

This Products & Services Privacy Statement Supplement applies to products, services and related offerings.

Effective Date

11/30/2023

Policy Link

https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement

Beispiel Salesforce

Dispute Resolution

QUESTIONS OR COMPLAINTS?

If you have a question or complaint regarding the covered data, please contact Salesforce at:

Ben Casady

Email: privacy@salesforce.com

Phone:

Salesforce
415 Mission St FL 3
San Francisco, CA 94105

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

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

HR Recourse Mechanism

EU Data Protection Authorities (DPAs)
UK Information Commissioner's Office (ICO)
Swiss Federal Data Protection and Information Commissioner (FDPIC)

Non-HR Recourse Mechanism

TRUSTe Dispute Resolution

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

CLOSE

Update: EDSA FAQ v. 16.07.2024

Q3. WHAT TO DO BEFORE TRANSFERRING PERSONAL DATA TO A COMPANY IN THE U.S. WHICH IS, OR CLAIMS TO BE CERTIFIED UNDER THE EU-U.S. DATA PRIVACY FRAMEWORK?

Before transferring personal data to a company in the U.S. which claims to be self-certified under the DPF, a data exporter in the EEA must ascertain that the company in the U.S. holds an active self-certification (certifications must be renewed annually) and that this certification covers the data in question (in particular if it covers HR Data, respectively, non-HR Data).[9]

Link: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf

- Es bedarf einer expliziten (!) Zertifizierung der Datenkategorie
- Die Meinung vom LfDI BaWü ist damit nicht haltbar
- Fatal ist diese Meinung auch für Anbieter wie AWS

Aufsichtsbehörden: BayLfD / LfDI Ba-Wü

- BayLfD, Erste Hilfe zum Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework:

  „[...] Übermittlung von Personaldaten ("HR Data"), die im Rahmen eines Beschäftigungsverhältnisses erhoben werden, ist **nicht automatisch** vom EU - U.S. Data Privacy Framework **erfasst** [...].“

  „US-Unternehmen muss bei seiner Zertifizierung **explizit angeben**“

- LfDI Ba-Wü Tätigkeitsbericht 2023:

  „[...] Einerseits [wurde] eine gesonderte **(Zusatz-)Zertifizierung** für Beschäftigtendaten (HR-Daten)“ ermöglicht“

  „Anderseits [...] **kein einheitliches Verständnis** der [beiden] Seite[n] über die Reichweite dieser Zusatzzertifizierung [...].“

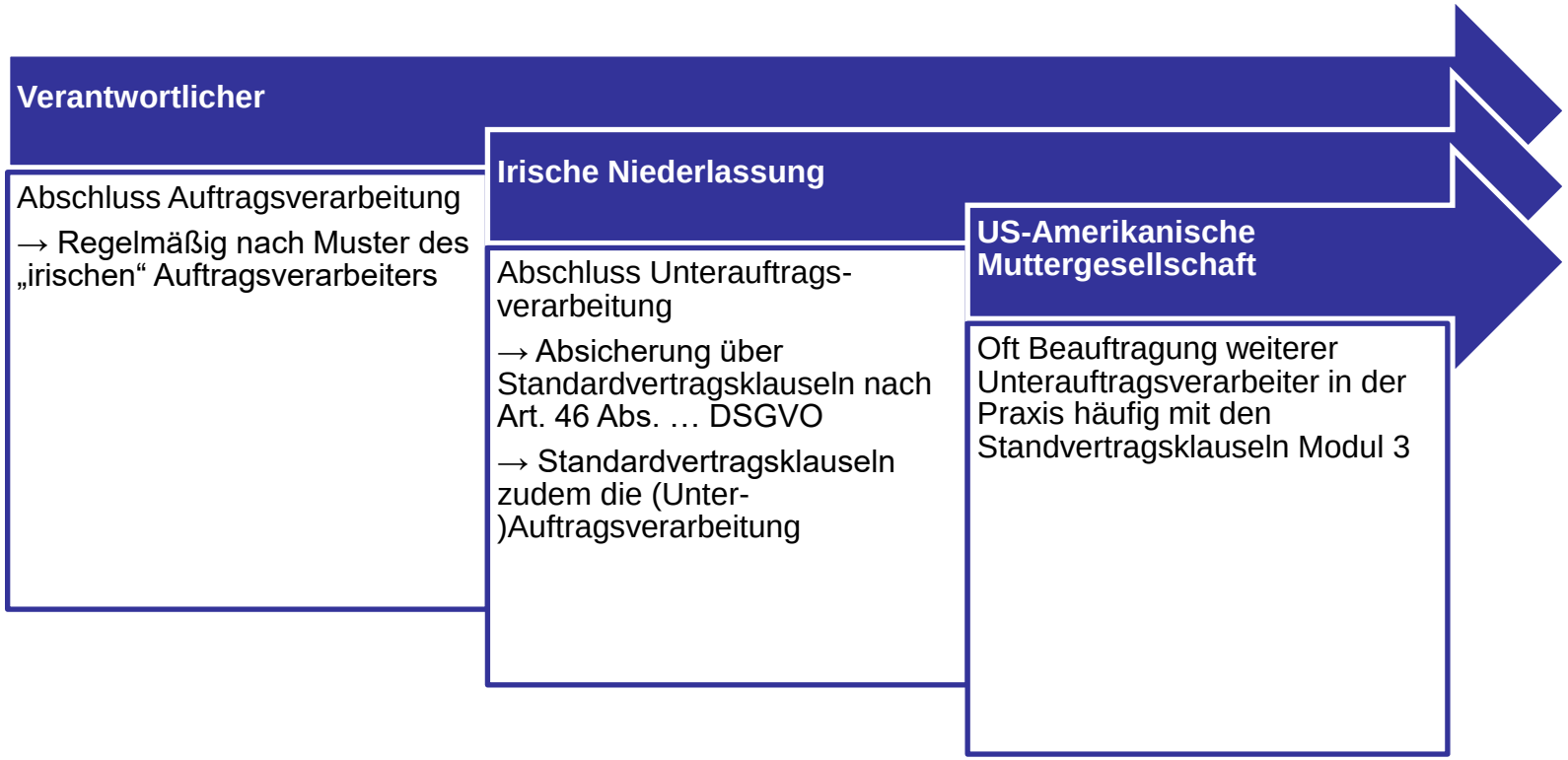
  US-Verständnis: Nur Daten der Beschäftigten des US-Importeurs!

  „Es ist somit **denkbar**, dass [EU-]Exporteure [...] einen Transfer [...] auch an solche Stellen in den USA vornehmen, die **nicht** über die **Zusatzzertifizierung für Beschäftigtendaten** verfügen.“

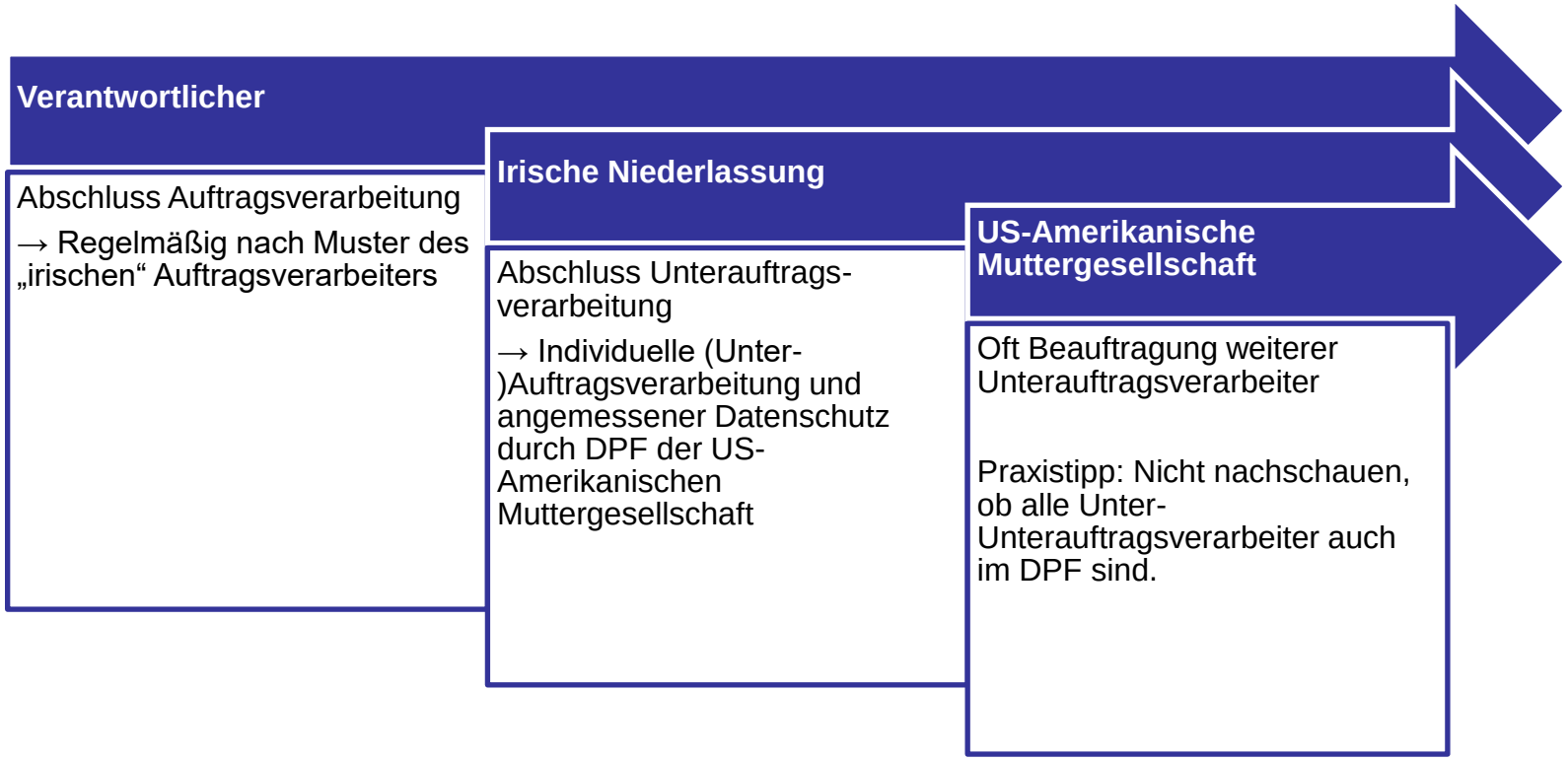
Definition von HR-Data

- Was sagt das DPF?
  „in the context of the employement relationship“ ≠ Art. 88 DSGVO
  - Systematik und Aufbau vom DPF
    - Eigener Abschnitt
    - Zusätzliche Datenschutzgewährleistungen
- Helfen die Vorgänger-Abkommen beim Verständnis?
  - Nein, Unklarheiten sind „rechtshistorisch“ bedingt
  - Kann die UK-U.S. Data Bridge beim Verständnis helfen? (-)
- Zudem EDSA-Meinung vom 28.02.2023, wonach das Konzept der HR-Daten noch mit den Behörden abzustimmen ist

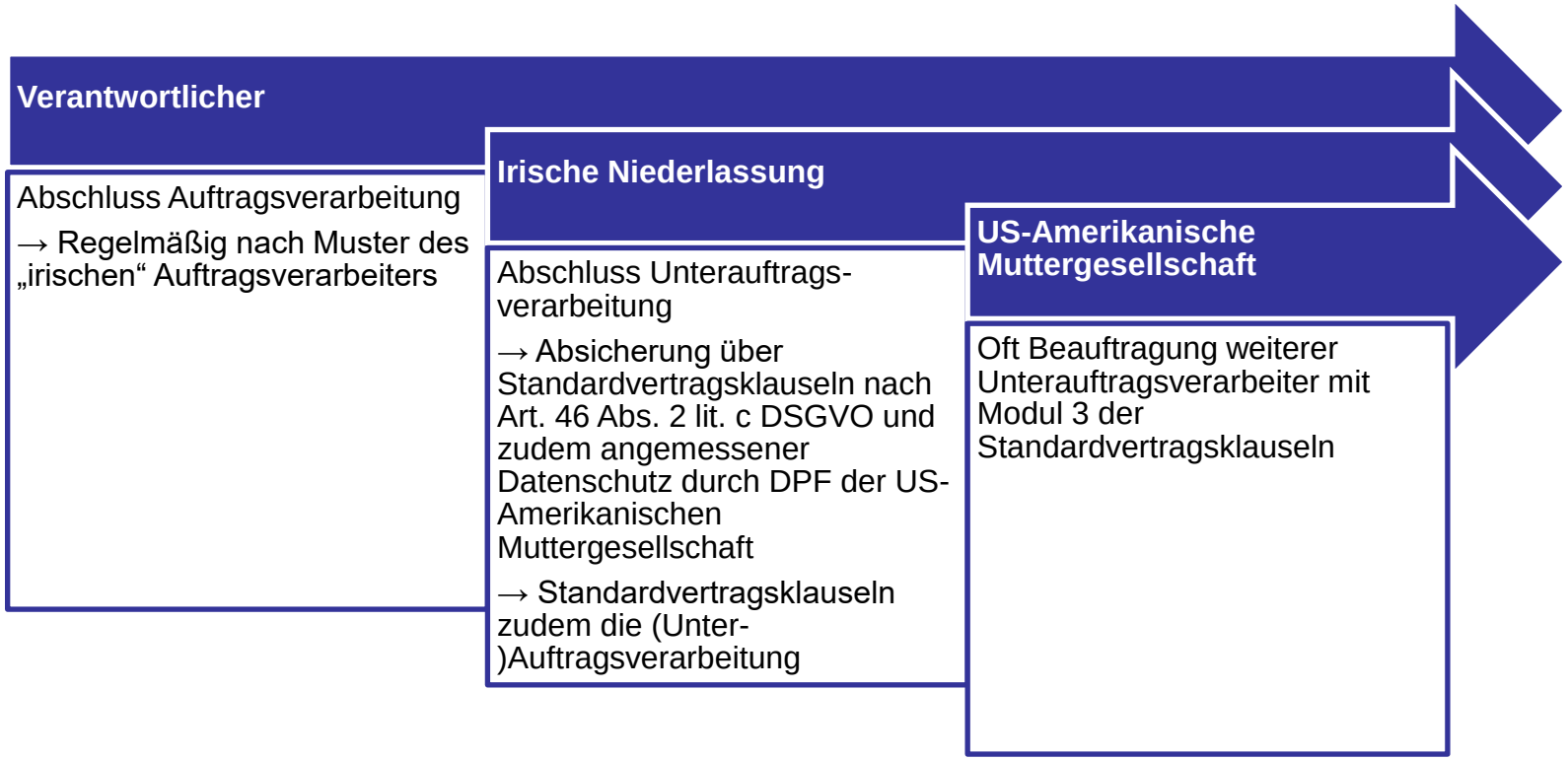
Absicherung Datenfluss bei Auftragsverarbeitung - Modell 1



Absicherung Datenfluss bei Auftragsverarbeitung - Modell 2



Absicherung Datenfluss bei Auftragsverarbeitung - Modell 3



Implikationen

- Erforderlichkeit einer TIA, wenn die SCC genutzt werden?
- DPF als ein gesetzliches beziehungsweise verwaltungsgesetztes TIA
- Praxistipp: Geltungsklausel als Rückfallklausel bzw. doppelte Absicherung im Fall der Ungültigkeit des DPF

Fazit

Fehlende Vorgabe zum Anwendungsbereich des DPF für HR-Data

- Wunsch Aufsichten nach „Doppel-Selbstzertifizierungen“
- Praxis nutzt HR-Data nur bei Controller to Controller in den eigenen Konzernstrukturen
- Weitere Unschärfen durch unklare Reichweite von HR-Data
  - Personalakte
  - Bewerbungen
  - Logdaten
  - Gleichlauf mit § 26 BDSG

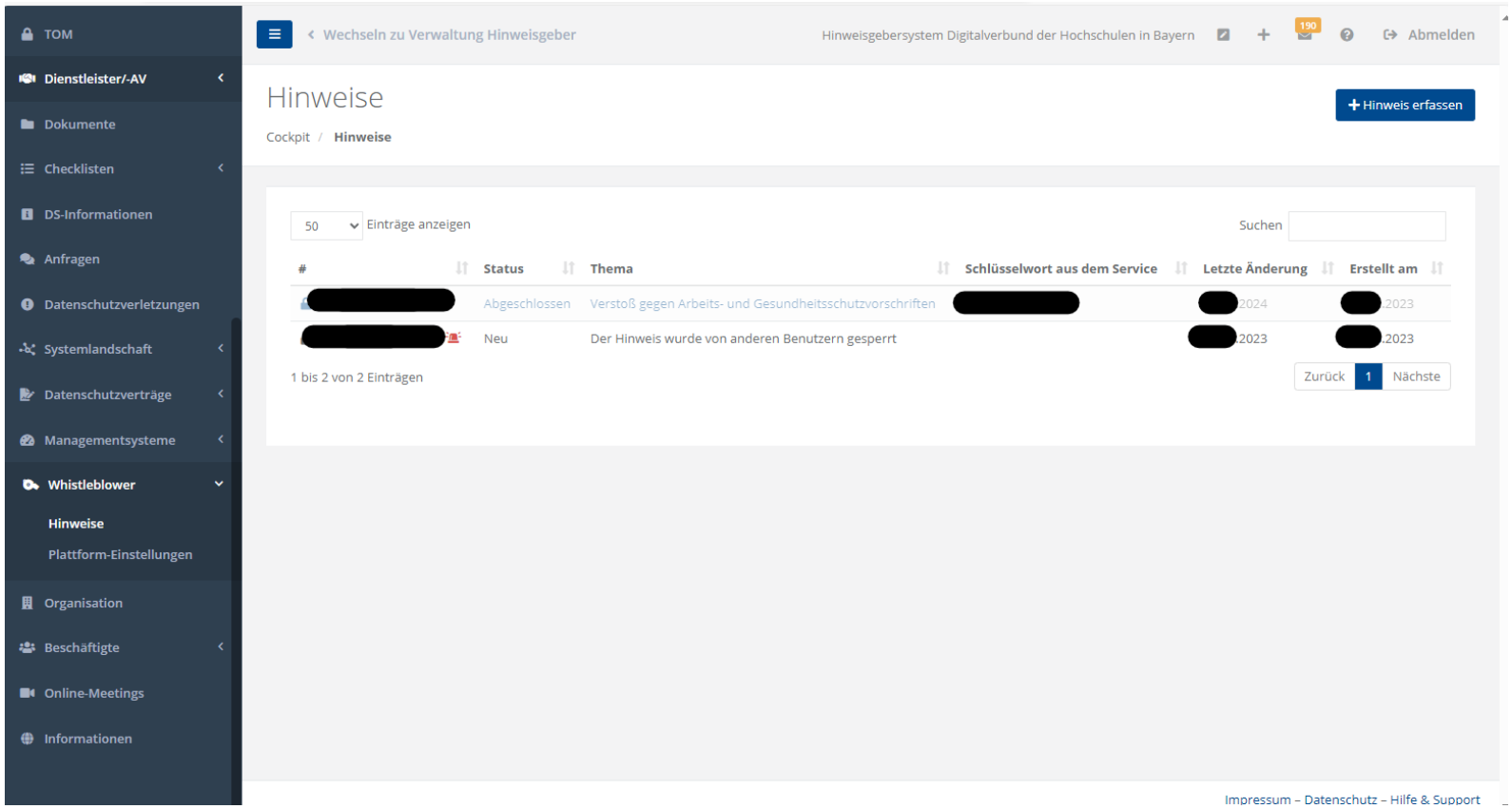
Deutsche Stiftung für Recht und Informatik

Mythen und Praxis des Hinweisgeberschutzes mit Fokus auf öffentliche Stellen

Johannes Nehlsen / Tilmann Fleck
Julius-Maximilians-Universität Würzburg

Herbstakademie 2024

Sehr geringes Anfragevolumen auch bei großen Einrichtungen (hier eine große bayerische Universität)



Einwilligungen oder Freigaben

Was würde das Erfordernis einer Datenschutzrechtlichen Einwilligungen im HinSchG bedeuten?

- Hohe Formerfordernisse
- Hohe Dokumentationserfordernisse
- Jederzeitige Widerrufbarkeit
- Mehr Komplexität in der Datenschutzinformation des Hinweisgeberschutzsystems

Gründe

- HinSchG und RL mischen Begriffe (Einwilligung, Zustimmung)
- Kein Vorrang der Sprachfassungen ➔ englische und französische Fassung hingegen von „consent“ bzw. „consentement“
- Erschwerte Tauglichkeit
- Prozessabsicherung durch Freigabe ausreichend

Weiteres in *Nehlsen/Fleck*, DSB 2024, 12 (13 f.)

Kooperative Meldestellen für öffentliche Stellen

- In der Richtline als Möglichkeit vorgesehen
  - In Bayern können verpflichtete Gemeinden, Bezirke und Landratsämter eine gemeinsame Meldestelle beim Staatsministerium des Innern nutzen
  - Konkrete Umsetzung ggf. mit Interessenskonflikte durch die Vermischung der Aufgaben als Meldestelle und Fach- bzw. Rechts-Aufsicht
  - Markteingriff gegenüber privatwirtschaftlichen Angeboten
- Wurde die bayerische Lösung kopiert?
  - https://eur-lex.europa.eu/legal-content/DE/NIM/?uri=CELEX:32019L1937

Reichweite der Tätigkeit der Meldestelle

- § 3 Abs. 2 Nr. 2:

„Dieses Gesetz gilt außerdem für die Meldung und Offenlegung von Informationen über [...] Verstöße gegen Binnenmarkt-vorschriften im Sinne des Artikels 26 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union, […]“

- Müssen folgende Meldungen bearbeitet werden?
  - nicht barrierefreier Webseiten und mobile Anwendungen öffentlicher Stellen
  - Verstoß gegen Pflichten aus der KI-Verordnung
  - Mobbing am Arbeitsplatz § 3 Abs. 1
  - Diskriminiere Stellenausschreibung § 3 Abs. 1
  - Cannabiskonsum am Arbeitsplatz § 3 Abs. 1

Praxisempfehlungen

- Keine Pflicht-DSFA, da nicht in den Blacklisten, aber freiwillige vertiefte Risikobetrachtung sinnvoll
  - Alternativ-Kurz-DSFA für die Ablage
- Vertrag der externen internen Meldestelle
  - Kombination aus gemeinsamer Verantwortlichkeit und Auftragsverarbeitung
  - Alternativ analog zum externen Datenschutzbeauftragten
- Freigabe der Vertraulichkeitszusicherung für die meldenden Person soweit diese selbst von Meldung betroffen ist
  - Beispiele etwa Unberechtigte Abmahnung oder Arbeitszeitverstöße
- Schadensersatz und Aufhebung der Vertraulichkeit nur bei vorsätzlichen Falschmeldungen empfohlen

Informationen zu den Referenten

Johannes Nehlsen, Regierungsrat

Leiter der Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Externer Datenschutzbeauftragter in Nebentätigkeit

Mail: johannes.nehlsen@uni-wuerzburg.de

Tilmann Fleck

Studentische Hilfskraft der Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Mail: gustav.fleck@uni-wuerzburg.de

Vielen Dank für Ihre Aufmerksamkeit!