OPITZ CONSULTING

DSGVO, SCHREMS, CLOUD ACT & CO.

Worauf Behörden bei der Digitalisierung bauen können

Dr. Hans Markus Wulf
Thomas Unterbörsch
Thomas Buch

04.11.2022 Webinar Digitaler Staat online

AGENDA

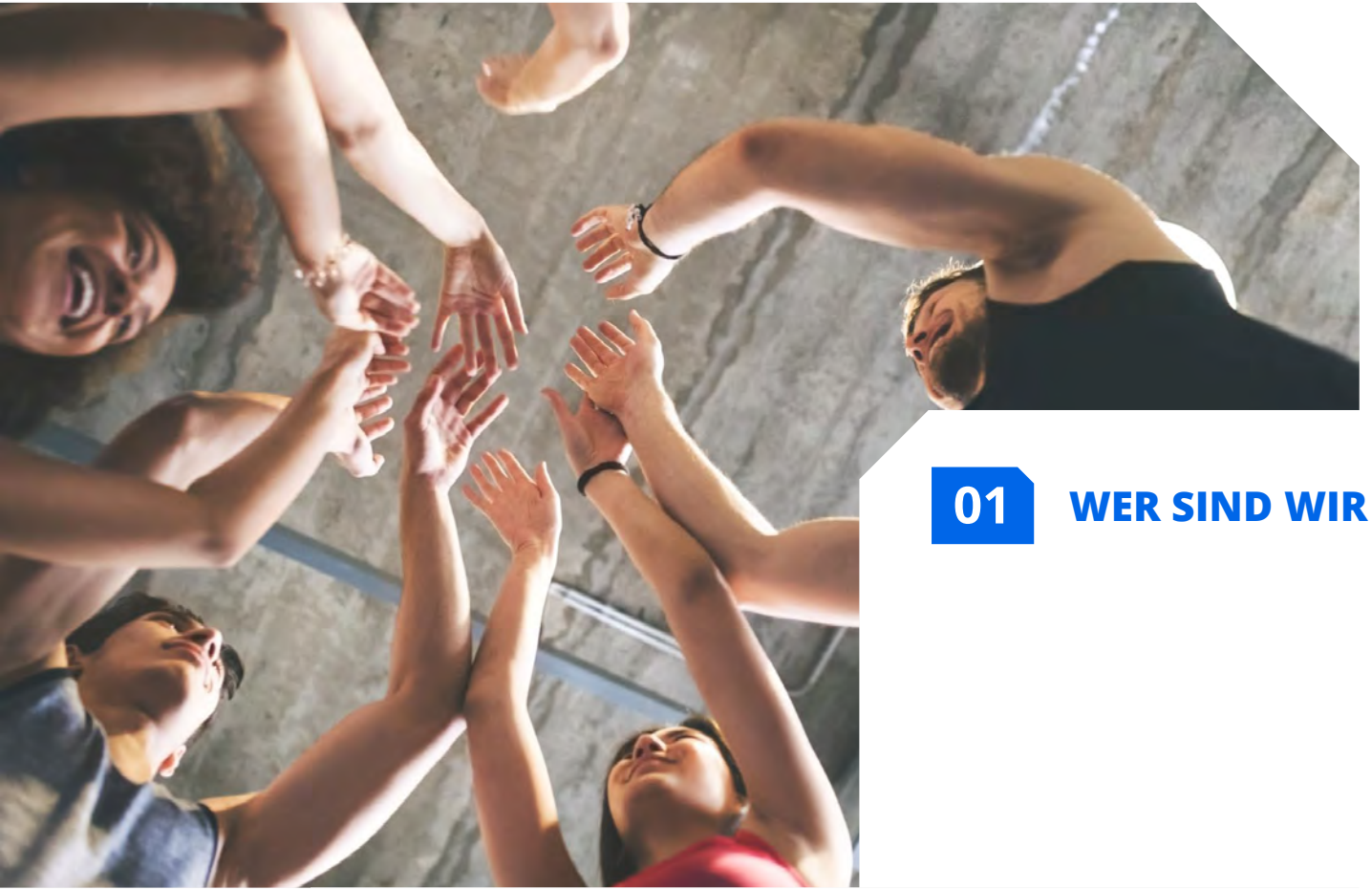
01
WER SIND WIR

02
HERAUSFORDERUNG

03
RECHTLICHER RAHMEN

04
LÖSUNGSANSÄTZE

05
ZUSAMMENFASSUNG / FAZIT



01 WER SIND WIR

HEUKING KÜHN LÜER WOJTEK

RECHTSANWÄLTE UND STEUERBERATER

Überblick zur Sozietät

414 Rechtsanwälte

20 Praxisgruppen

57 Anwälte in der Praxisgruppe IP, Media & Technology

9 eigene Standorte

98 **weltweite** Standorte von Partnerkanzleien

22 Sprachen

OPITZ CONSULTING #DIGITALE SERVICE MANUFAKTUR

Mehr als 30 Jahre Erfahrung
für den Erfolg unserer Kunden

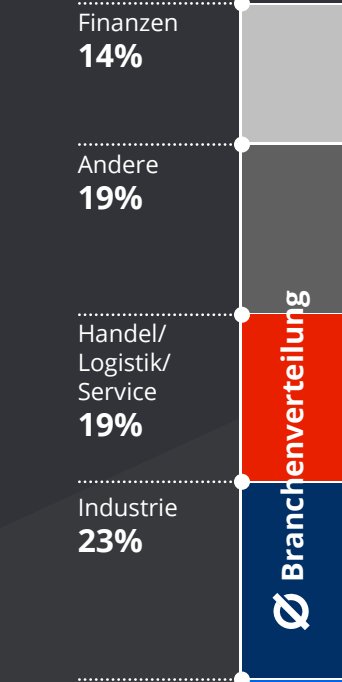
Auf Augenhöhe
Partner für den gehobenen Mittelstand, Konzerne & **Öffentliche Auftraggeber**

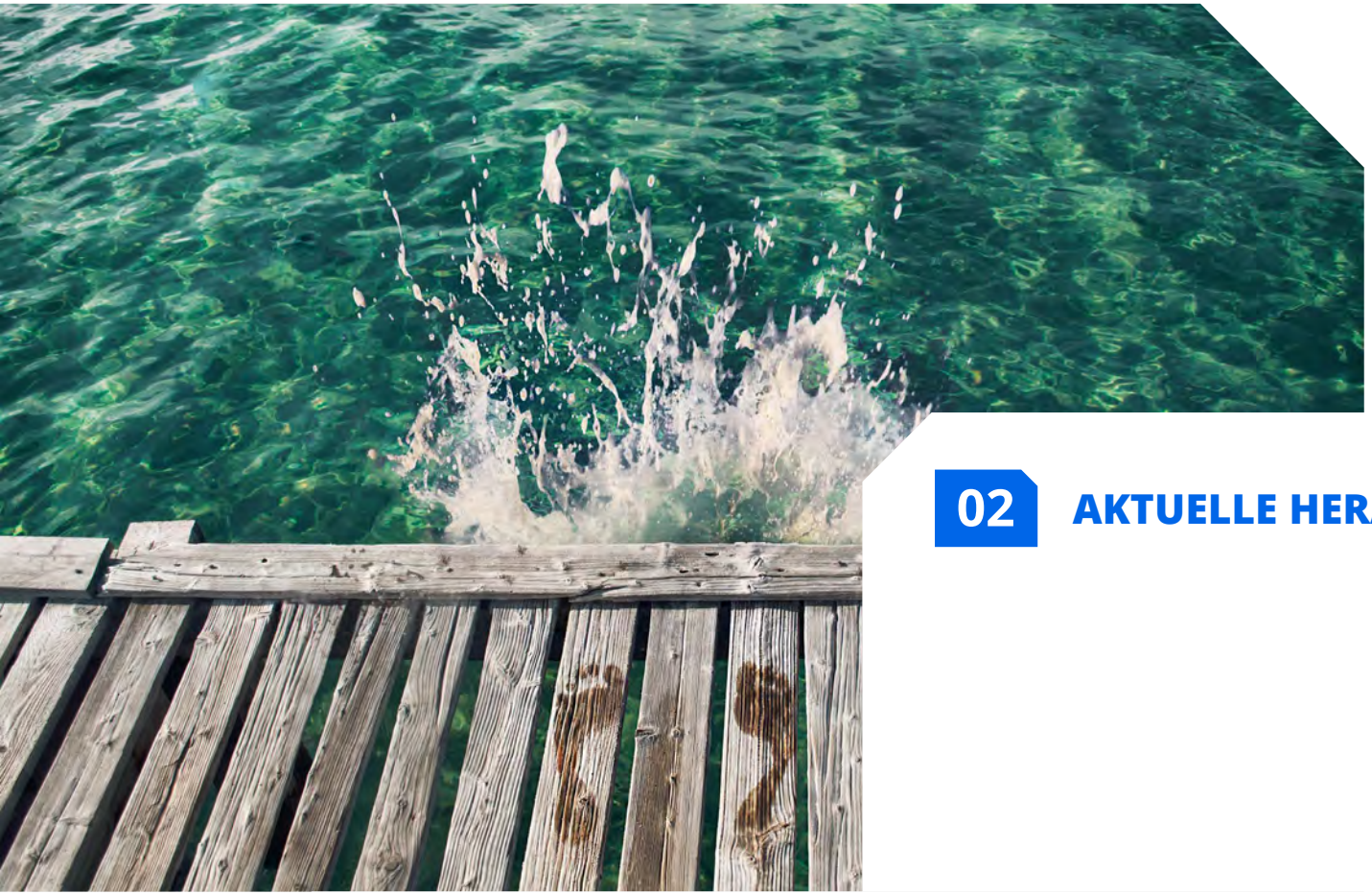
Innovation & Technology
Intelligent Automation,
Moderne IT-Landschaften,
Systemintegration
Sichere Infrastructure / Cloud

Experten vor Ort
505 Mitarbeiter **8+2** Standorte
56 Mio. Umsatz (2021)

End-to-end Service
IT Consulting, Individuelle Applikationsentwicklung
Managed Services & Betrieb

Strategische Technologie-Partner
AWS, IONOS, Oracle, Microsoft





02 AKTUELLE HERAUSFORDERUNGEN

AKTUELLE HERAUSFORDERUNGEN

Quelle: BSI

Energie: Analysen, Vorhersagen, automatisierte Entscheidungen, Verhaltensmuster/Modelle

Digitalisierung: Verfahren, Anträge, Digitale Bürgerdienste, Online-Zugangsgesetz, e-Akte,...

Logistik-/Zulieferketten: Berechnung, Planung, Nachverfolgung Transportwege (Wasser, Luft, Land), vernetztes Fahren

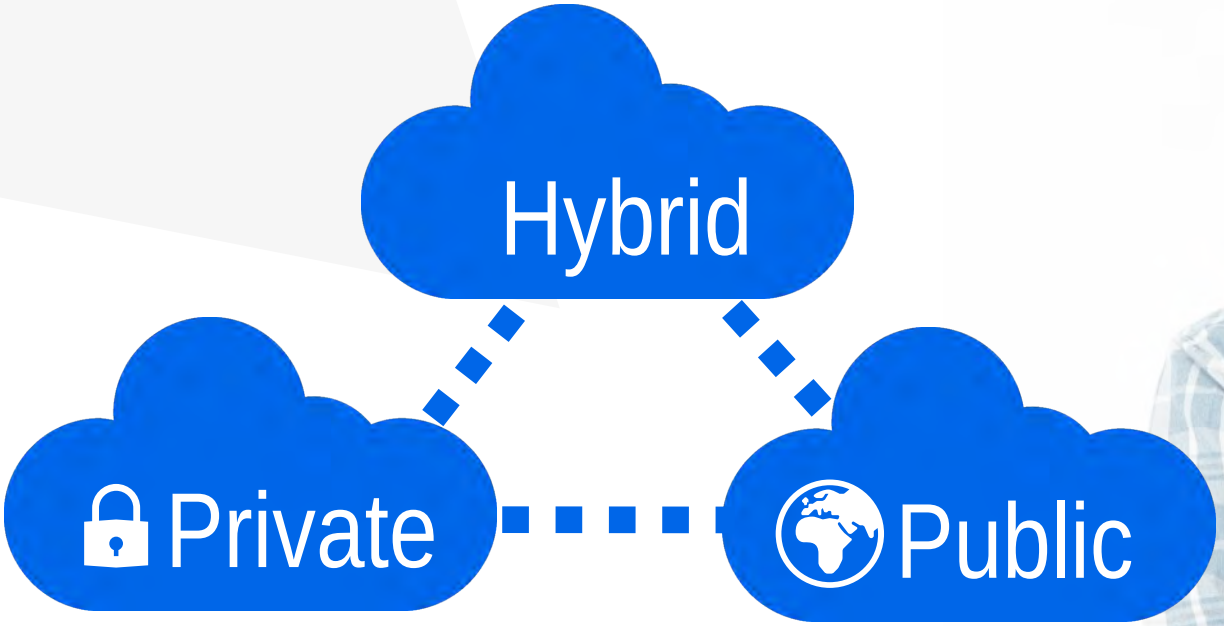
Smart City: digitaler Bürger, digitale Stadt, digitaler Staat, entsprechende Auswertungen und Angebote

BSI - Leitfaden zur Nutzung der Cloud
BSI – Cloud Risiken und Sicherheitstipps

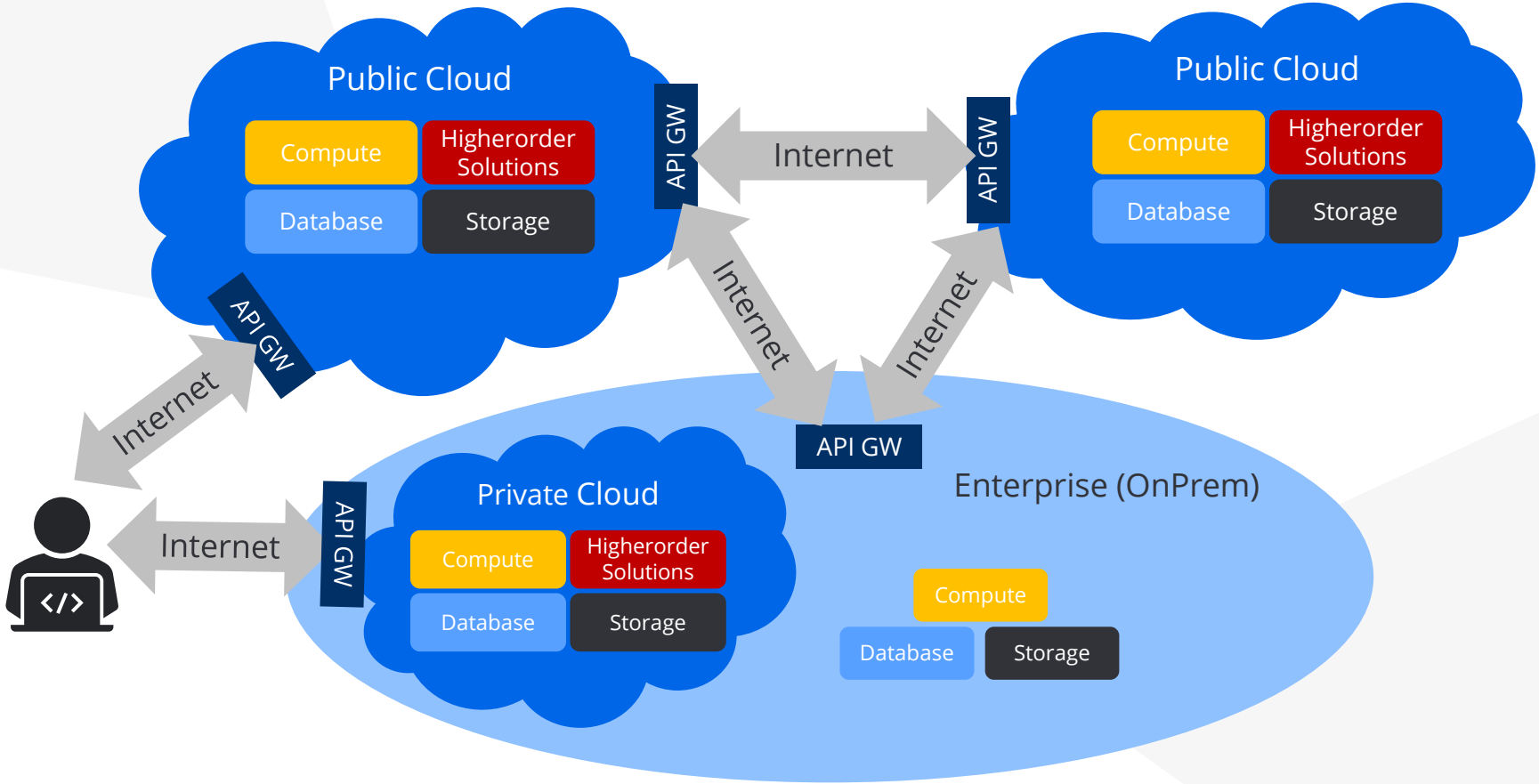
UNSICHERHEITEN AUF DER BEDARFSTRÄGERSEITE

- „Meine Private Cloud im Rechenzentrum kann nicht unbegrenzt skalieren“.
- „Kurzfristige Anpassungen kann ich mit meinen IT-Mitarbeitenden nur begrenzt umsetzen.“
- „Die zunehmenden Homeoffice-Zugriffe haben unserer IT schwer zu schaffen gemacht.“
- „Die Lieferzeiten bei IT-Hardware verzögern den Ausbau unseres Rechenzentrums.“
- „Cloud, Hybrid Cloud, MultiCloud? Wie sieht der rechtliche Rahmen hierzu jeweils aus?“
- „Was soll ich beschaffen? Welche Urteile gibt es? Wie bin ich rechtlich auf der sicheren Seite?“
- „Ich setzte nur Cloud-Anbieter mit C5-Testat oder mit EU-Niederlassung ein. Ist das sicher?“
- „Ständig habe ich Diskussionen mit den Datenschutzbeauftragten. Wie kann ich den Schwierigkeiten beim Umgang mit personenbezogenen Daten in der Cloud begegnen?“

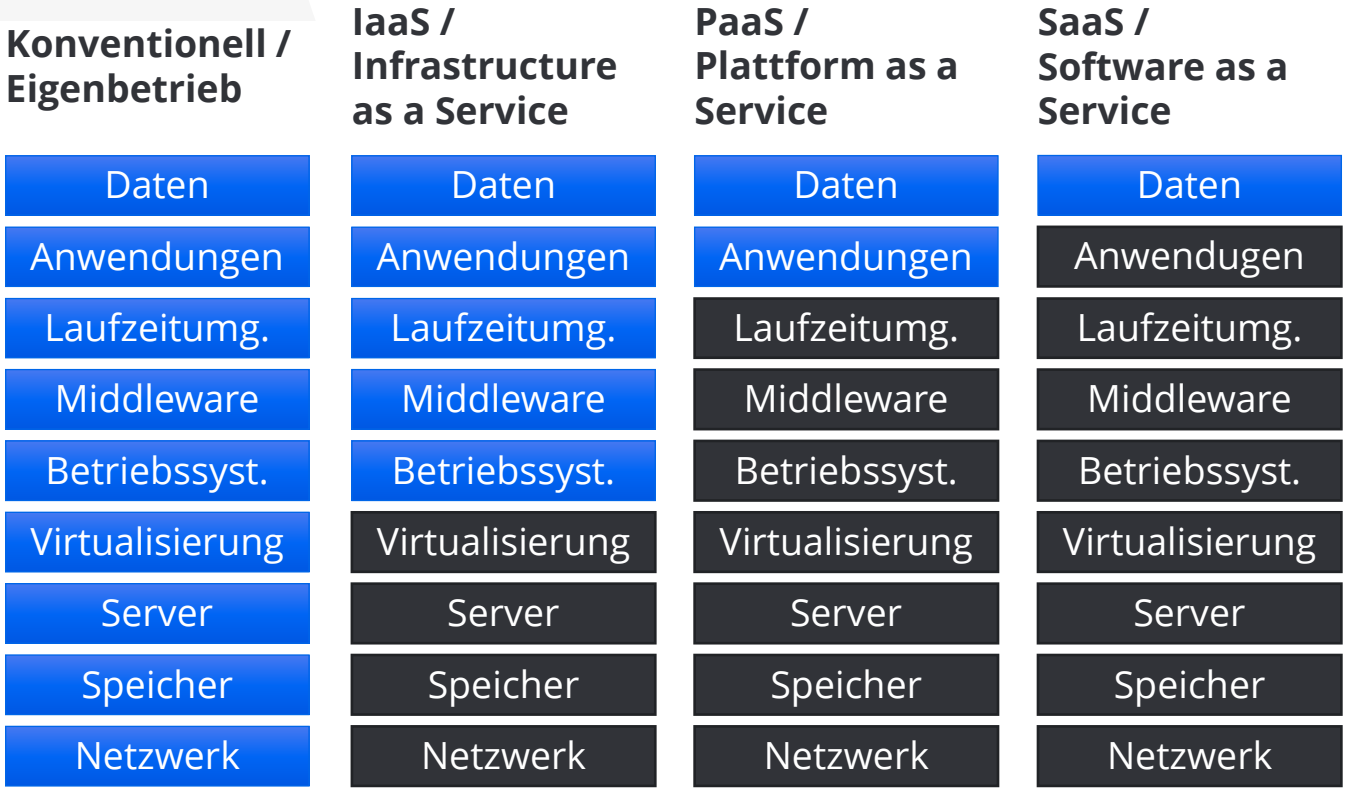
DIE VERSCHIEDENEN CLOUD-MODELLE – CHANCEN FÜR DIE ÖFFENTLICHE VERWALTUNG

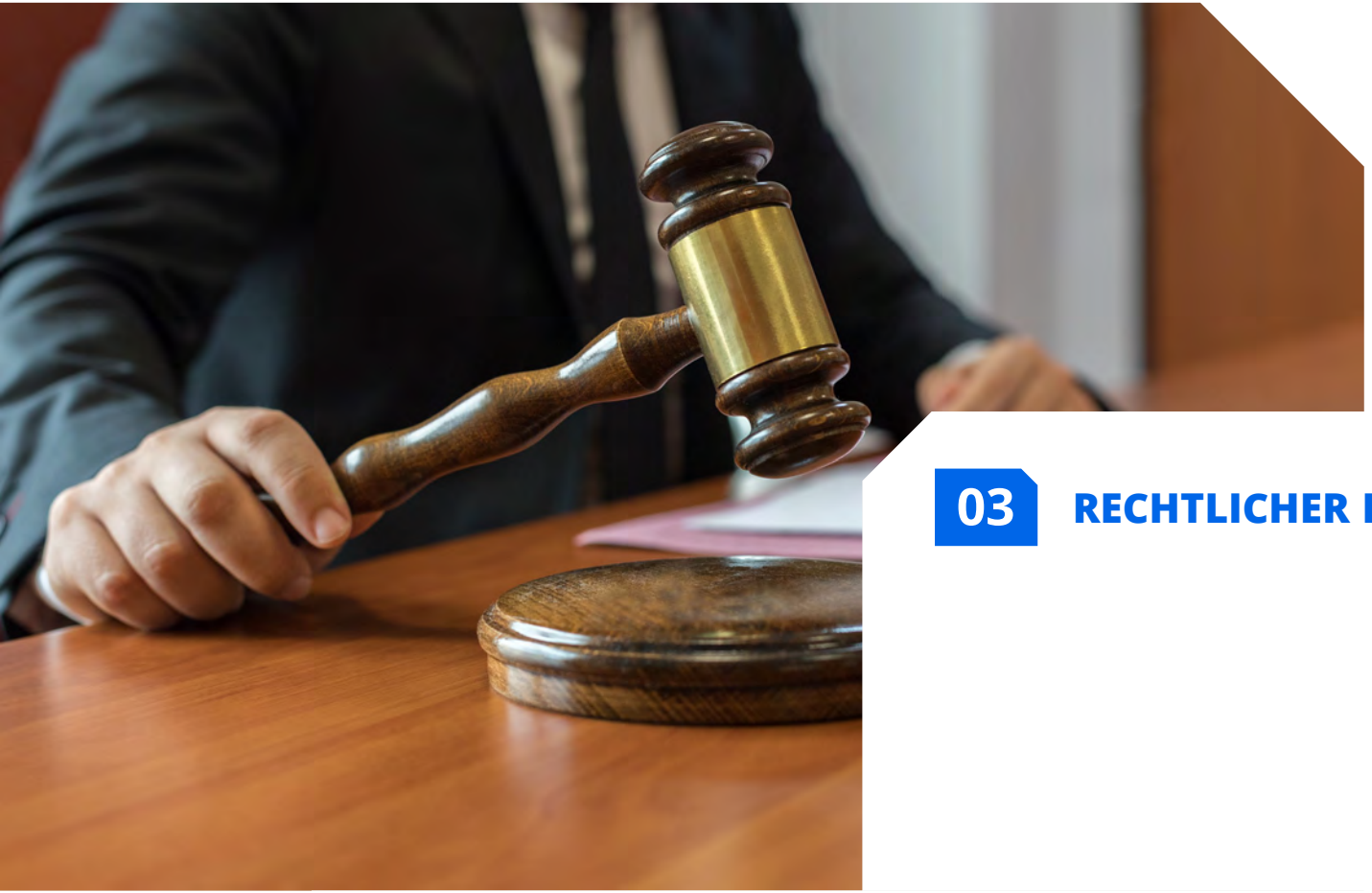


HYBRIDE MODELLE SINNVOLL NUTZEN



NUTZUNGSMODELLE CLOUD ARCHITEKTUR: „SHARED RESPONSIBILITY MODEL“ – WER IST VERANTWORTLICH?





03 RECHTLICHER RAHMEN

BESONDERE ANFORDERUNGEN FÜR DRITTLANDTRANSFERS

- Jede Datenübermittlung in ein Land, das nicht zur EU oder dem Europäischen Wirtschaftsraum gehört

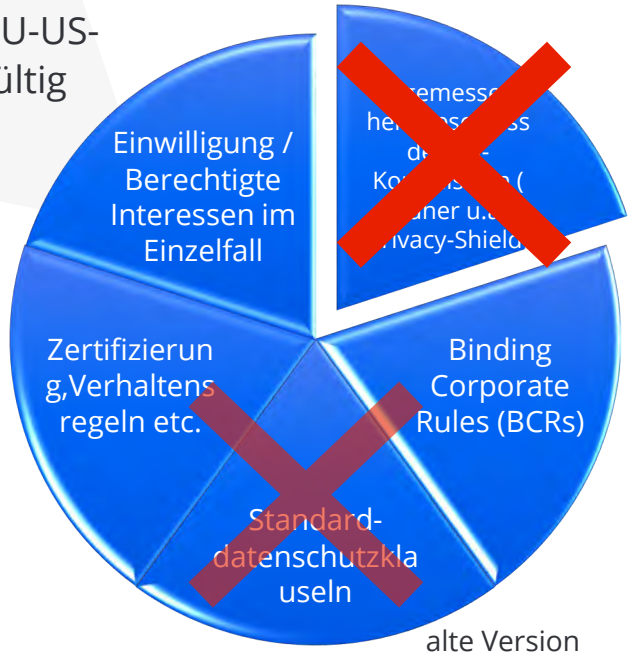
- Grundsätzlich nur auf Grundlage geeigneter Garantien zulässig, Art. 45, 46 DSGVO

→

RECHTSLAGE BEI US-TRANSFER NACH SCHREMS II

Aber:

In dem Urteil *Schrems II* (EuGH C-311/18) wurde der EU-US-Privacy-Shield für ungültig erklärt



alte Version ungenügend

Lösung?

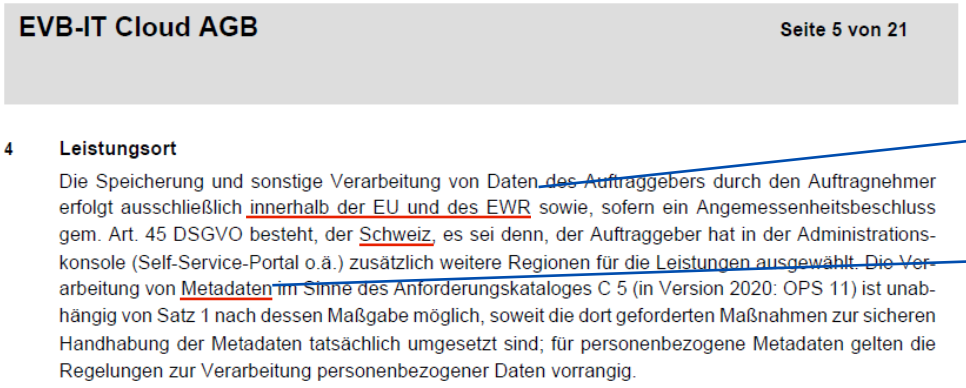
(neue) **Standard Contractual Clauses (SCC)**

Verantwortlicher muss Datenschutzniveau trotzdem selbst überprüfen

ggf. weitere technische und organisatorische / vertragliche Maßnahmen

TIA (Transfer Impact Assessment)

WEICHENSTELLUNG DES EVB-IT-CLOUDVERTRAGES



EVB-IT Cloud AGB Seite 5 von 21

4 Leistungsort

Die Speicherung und sonstige Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer erfolgt ausschließlich innerhalb der EU und des EWR sowie, sofern ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht, der Schweiz, es sei denn, der Auftraggeber hat in der Administrationskonsole (Self-Service-Portal o.ä.) zusätzlich weitere Regionen für die Leistungen ausgewählt. Die Verarbeitung von Metadaten im Sinne des Anforderungskataloges C 5 (in Version 2020: OPS 11) ist unabhängig von Satz 1 nach dessen Maßgabe möglich, soweit die dort geforderten Maßnahmen zur sicheren Handhabung der Metadaten tatsächlich umgesetzt sind; für personenbezogene Metadaten gelten die Regelungen zur Verarbeitung personenbezogener Daten vorrangig.

Datenverarbeitung in der Cloud grundsätzlich nur in EU, EWR und Schweiz

Nur Metadaten ohne Personenbezug dürfen auch in anderen Drittländern verarbeitete werden

Ausnahmsweise Modifikation über den Kriterienkatalog zum EVB-IT Cloudvertrag:

- ✓ Erweiterung auf andere Staaten mit Angemessenheitsbeschluss (Art. 45 DSGVO)
- ✓ Ausnahmen möglich für:
  - Daten ohne Personenbezug
  - Support und Wartung
- ✓ Einschränkungen möglich:
  - Beschränkung auf Deutschland oder
  - Beschränkung auf bestimmte Rechenzentren oder Leistungsort

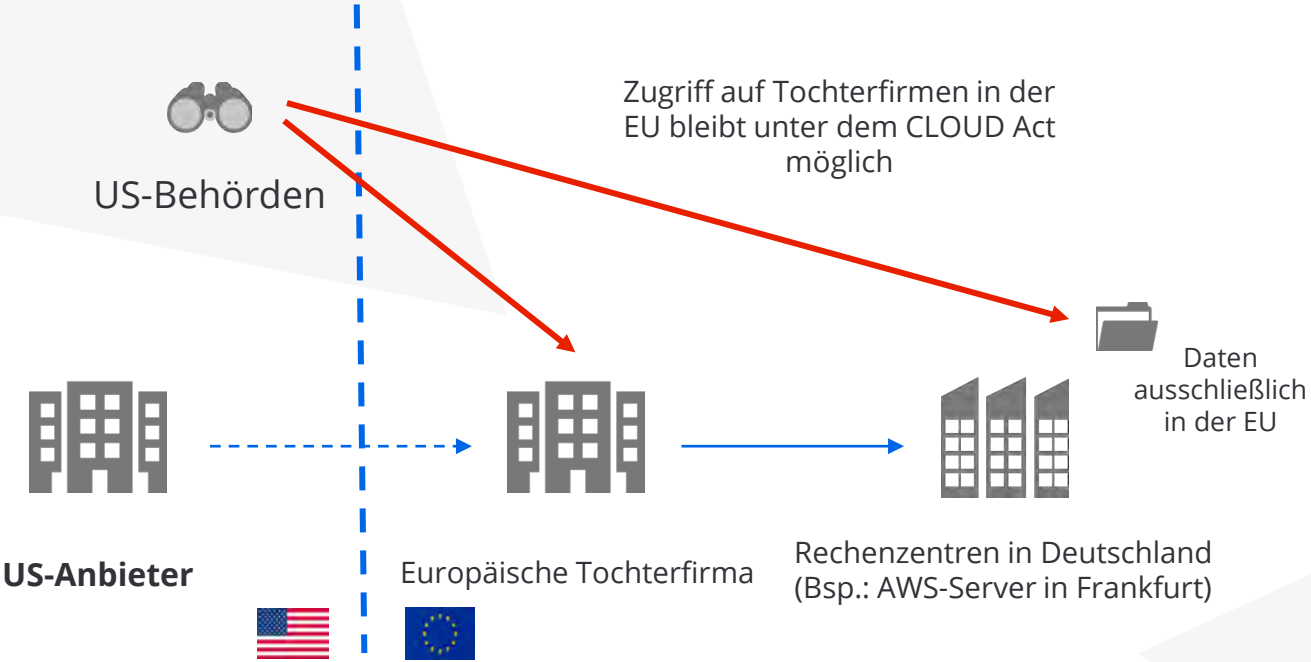
RISIKO: US CLOUD ACT
(CLARYFYING LAWFUL OVERSEAS USE OF DATA ACT)

- Datenherausgabe ohne gerichtliche Entscheidung
- Herausgabe von Daten außerhalb Europas
- Grundsätzlich auch gegen das Recht anderer Staaten
- § Rechtsschutz nur bei Verletzung des Rechts qualifizierter Staaten

18 U.S. Code § 2713. Required preservation and disclosure of communications and records

„A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

CLOUD ACT ERLAUBT ZUGRIFF DER US-BEHÖRDEN



Ist das zulässig?

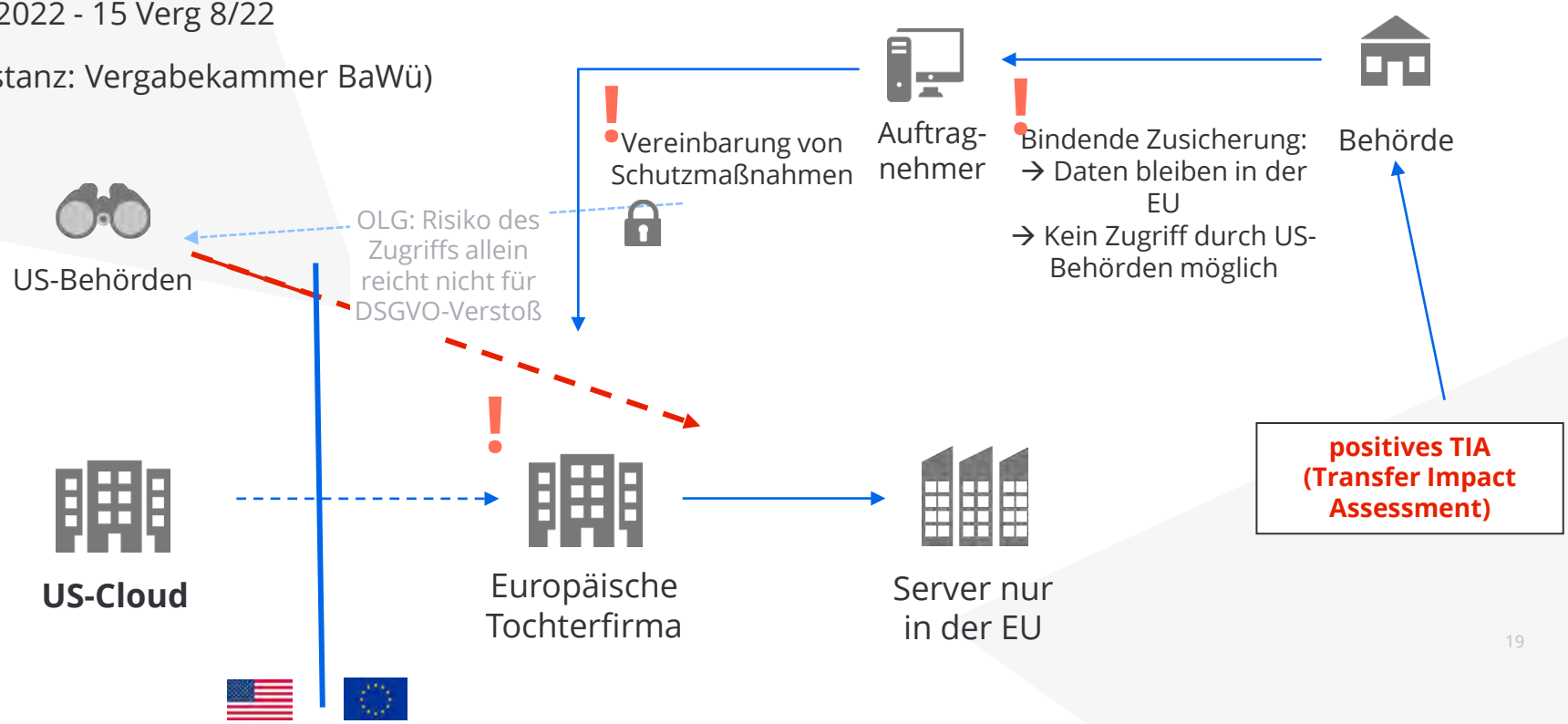
Vergabekammer BaWü:
Latentes Zugriffs-Risiko ist Datenschutzverstoß

aber…

OLG KARLSRUHE: ZUGRIFFSRISIKO ALLEIN NOCH KEIN VERSTOß

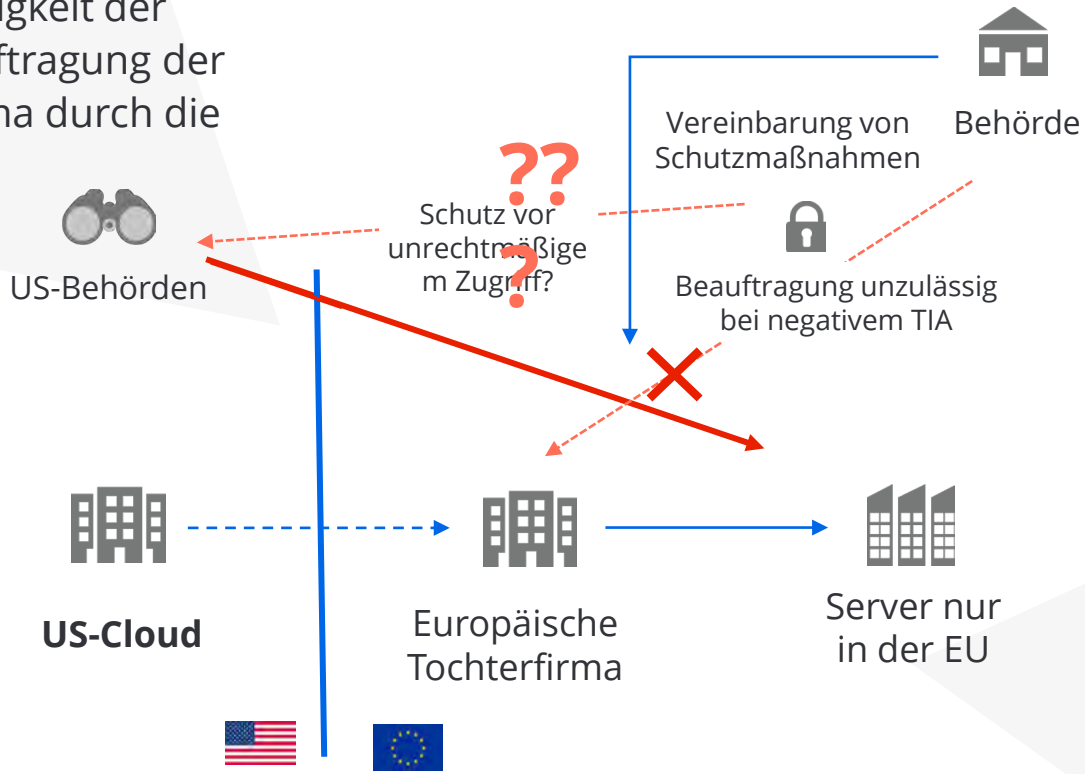
- 07.09.2022 - 15 Verg 8/22

  (Vorinstanz: Vergabekammer BaWü)

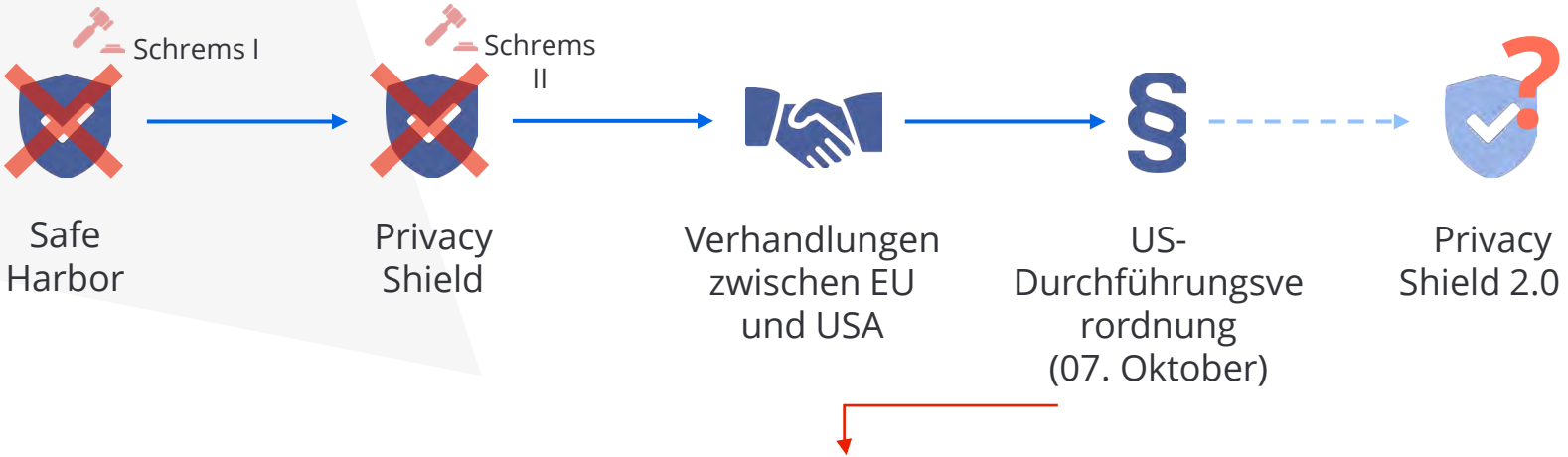


OLG KARLSRUHE: DIREKTE BEAUFTRAGUNG OFFEN

Unklar: Zulässigkeit der direkten Beauftragung der EU-Tochterfirma durch die Behörde



EINGESCHRÄNKTER US-ZUGRIFF? DIE US-DURCHFÜHRUNGSVERORDNUNG



Zweistufiger Rechtsbehelfsmechanismus:

- Beschwerdemöglichkeit beim Civil Liberties Protection Officer
- Anfechtung der Entscheidungen vor dem Data Protection Review Court

KEINE RECHTSSICHERHEIT TROTZ DURCHFÜHRUNGSVERORDNUNG:

Privacy Shield II frühestens im Frühjahr 2023

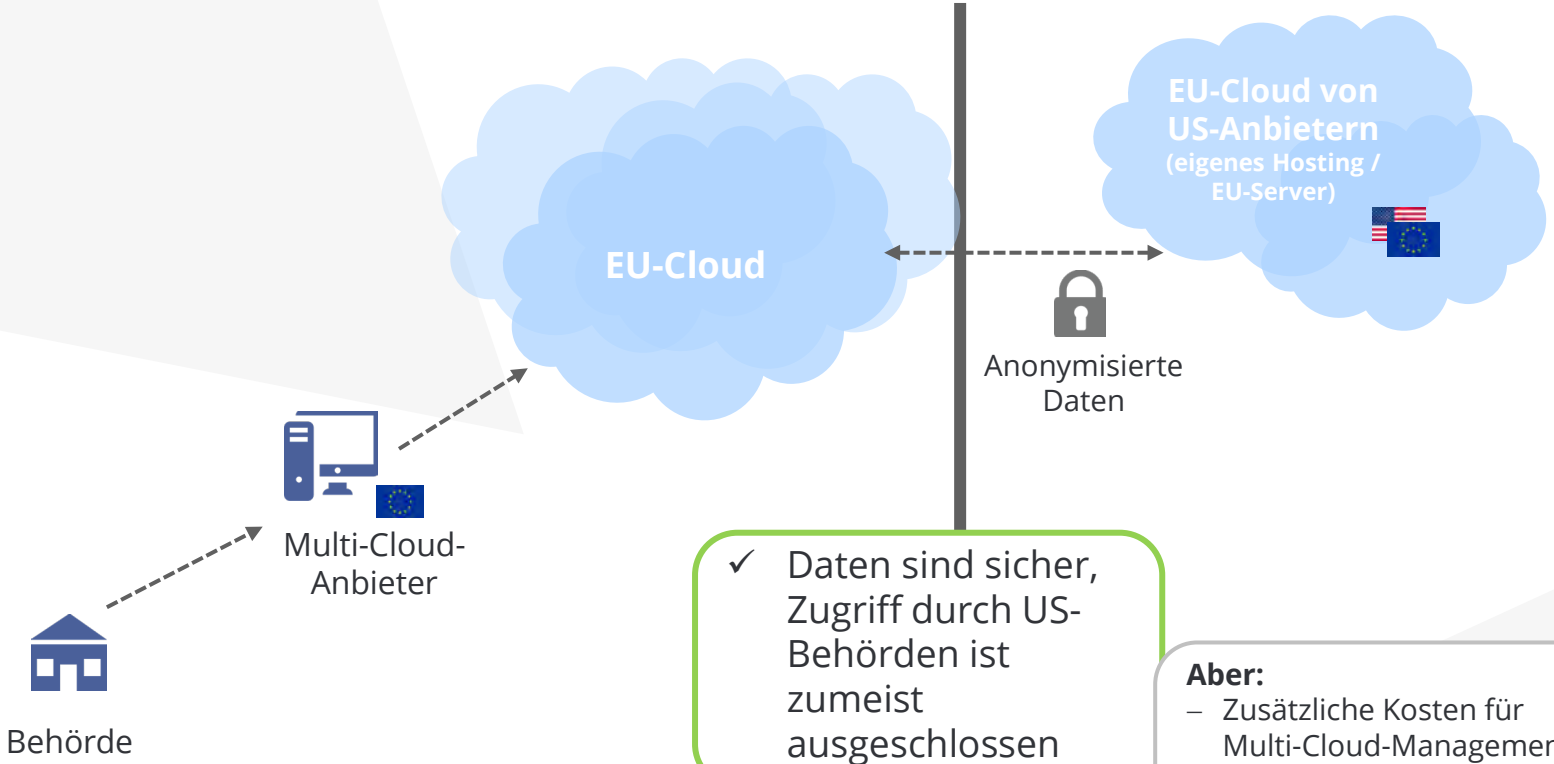
Datenschützer wollen auch hiergegen vorgehen

Kritik der Datenschutzbehörden:

- Kein Parlamentsgesetz
- Für EU-Bürger:innen nicht einklagbar
- Verhältnis zum Cloud Act unklar
- Auslegung von *Verhältnismäßigkeit*
- Data Protection Review Court gehört voraussichtlich zu Exekutive

Rechtsunsicherheit bei Nutzung von US-Clouds + DE-Servern bleibt!

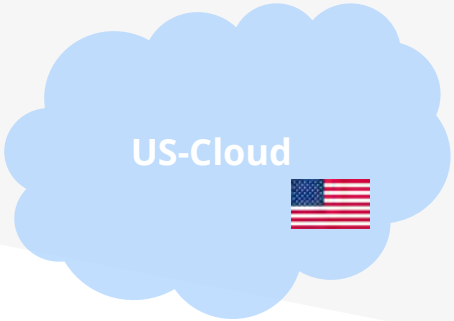
DIE MULTI-CLOUD ALS ALTERNATIVE

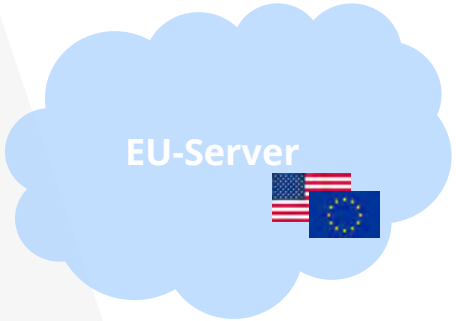


✓ Daten sind sicher, Zugriff durch US-Behörden ist zumeist ausgeschlossen

Aber:
- Zusätzliche Kosten für Multi-Cloud-Management
- Noch keine Behördenstatements
- Größere IT-Angriffsfläche

FAZIT





Hohe Anforderungen:

- SCC & TIA zwingend
- Privacy Shield 2.0 unsicher
- Datenzugriff kann nicht ausgeschlossen werden
- Viel Abstimmungsbedarf und Rechtsunsicherheit

Besser:

- Verringertes Risiko für US-Datenzugriff
- Kann laut dem OLG Karlsruhe zulässig sein bei Zusicherung durch US-Provider
- Aber: Rechtslage weiter unklar

Guter Zwischenweg:

- US-Datenzugriff zumeist ausgeschlossen
- Heute kaum funktionale Einschränkungen mehr
- Aber: Technische Umsetzung ist kompliziert und Compliance stark hiervon abhängig

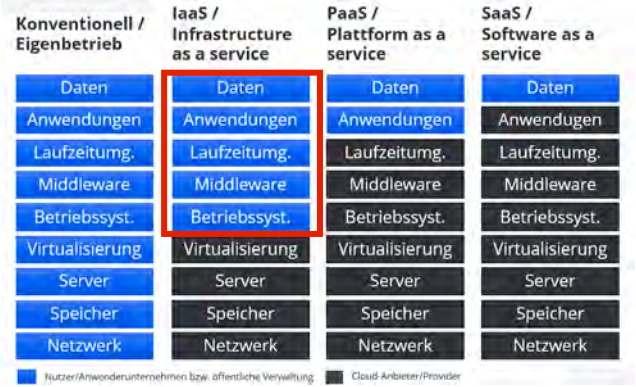
Sicher und einfach:

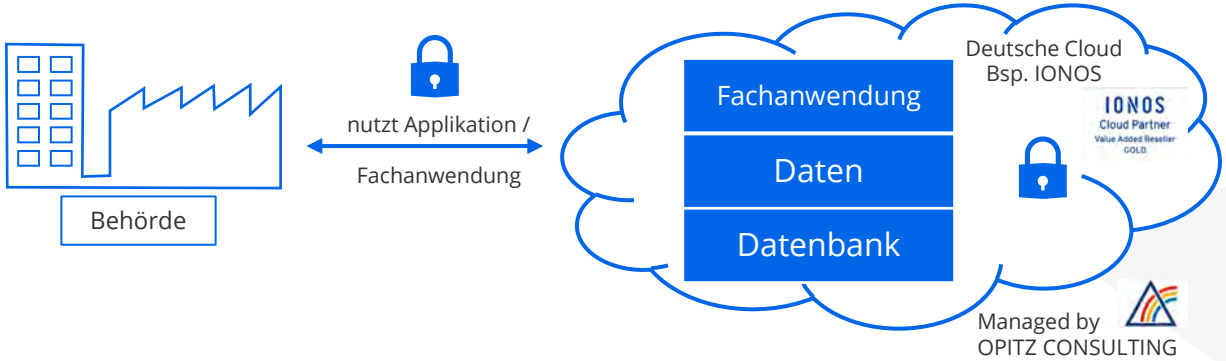
- Kein Drittlandtransfer, daher nur Anforderungen der Auftragsverarbeitung zu erfüllen
- Keine weiteren Sicherungsmechanismen notwendig

04 LÖSUNGSANSÄTZE

FALL1 – CLOUD MADE IN GERMANY

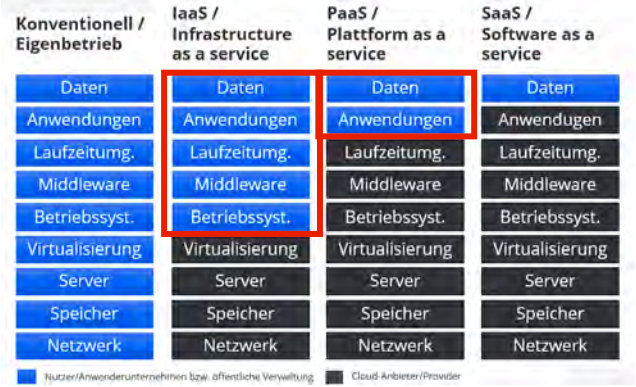
- Verbindungen verschlüsselt
- Speicherung von personenbezogenen Daten nach DSGVO „Made in Germany“
- Durch jeglichen Fremdzugriff geschützt
- Anwendung und Infrastruktur einfach erweiter- und skalierbar
- Entwicklung und Betrieb z. B. durch OPITZ CONSULTING

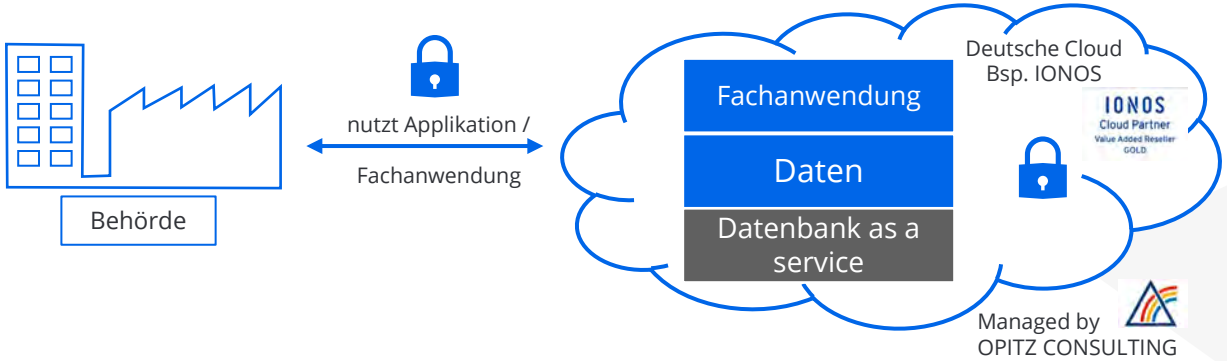




FALL2 – CLOUD MADE IN GERMANY + CLOUD SERVICES

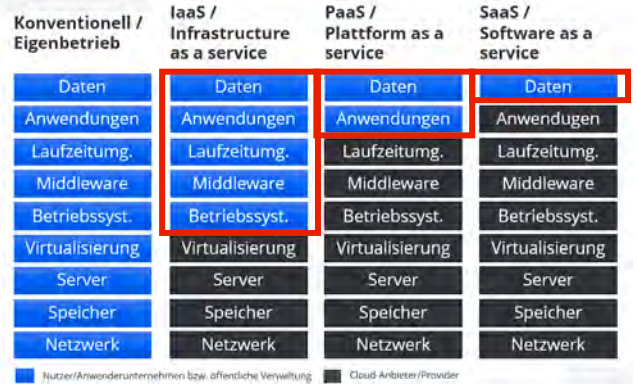
- Verbindungen verschlüsselt
- Speicherung von personenbezogenen Daten nach DSGVO „Made in Germany“
- Durch jeglichen Fremdzugriff geschützt
- Anwendung und Infrastruktur einfach erweiterbar/skalierbar
- Entwicklung/Betrieb z.B. von Opitz Consulting Deutschland

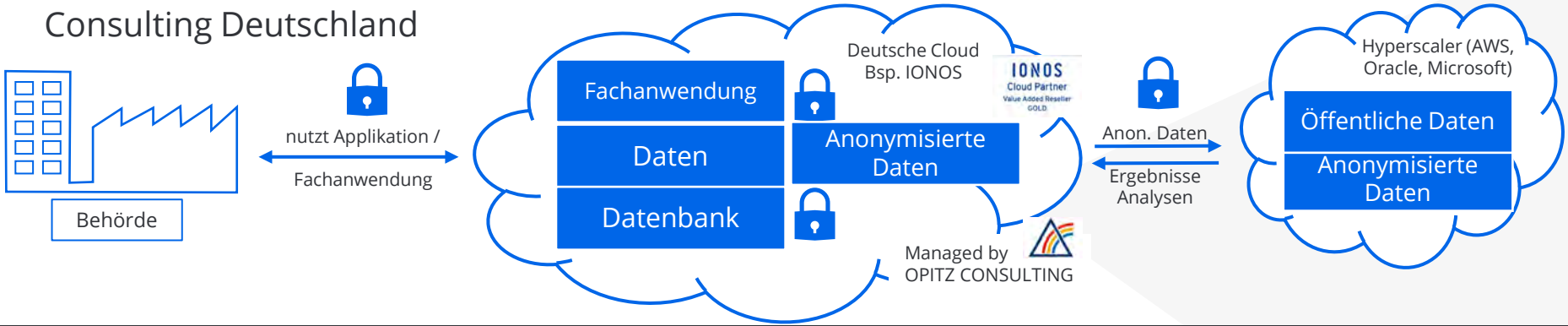




FALL3 – KOMBINATION DEUTSCHE CLOUD & HYPERSCALER

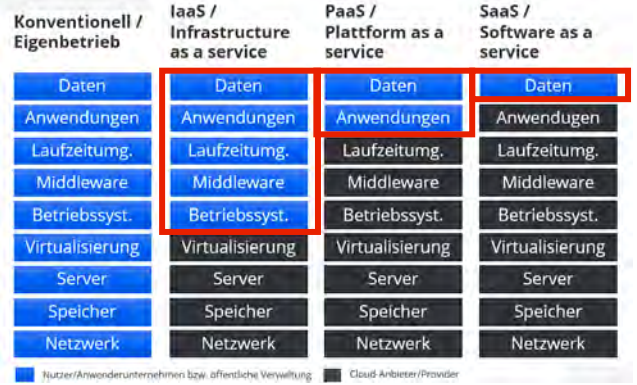
- Personenbezogene Daten werden zur Weiterverarbeitung anonymisiert oder pseudonymisiert.
- Nutzung von Services eines Hyperscalers wie (AWS, Oracle, Azure) nur auf anonymisierten Datensätzen.
- Rückfluss / Ergebnisse der Analysen für den Anwender / Fachanwendung. Ggf. Treuhänderprinzip
- Entwicklung, Betrieb, Anonymisierung z.B. durch Opitz Consulting Deutschland

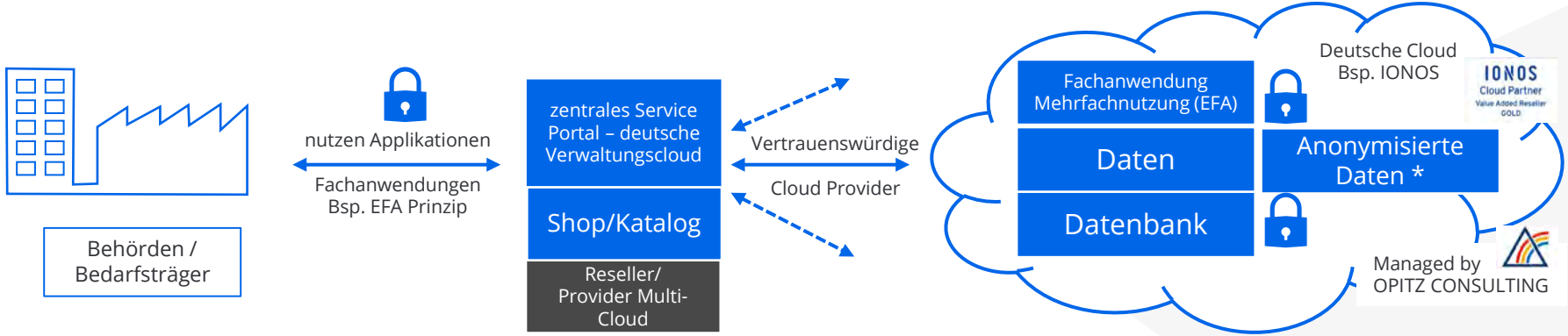




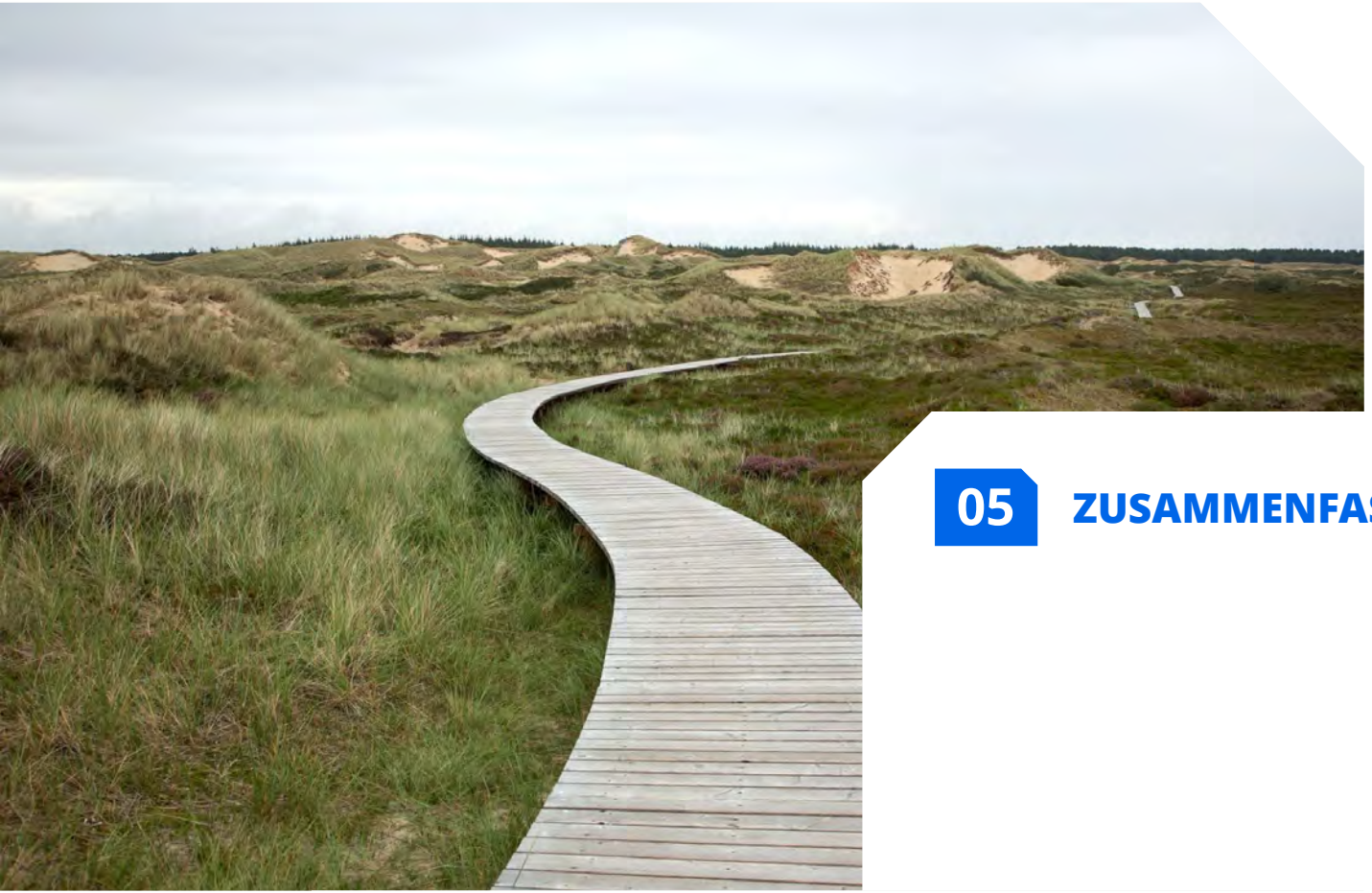
FALL4 – VERTRAUENSWÜRDIGE CLOUD PROVIDER ÜBER PORTAL

- **Zukunft:** Deutsche Verwaltungscloud als zentraler Service
- Shop/Katalog - Zugänglich für Bedarfsträger
- Auswahl Services/Applikationen vertrauenswürdiger Cloud Provider oder RZ Betreiber; Nutzung ggf. nach EfA
- Hosting jeweils in darunterliegender CSP (Cloud Service Provider) Infrastruktur / RZ-Betreiber





* nach Datenklassifizierung



05 ZUSAMMENFASSUNG/FAZIT

FAZIT: INANSPRUCHNAHME VON CLOUD-DIENSTEN

- ✓ Keine Compliance-Probleme: Inanspruchnahme von EU-Anbietern mit ausschließlicher Nutzung von EU-Servern
- ✓ US-Hyperscaler: Inanspruchnahme von US-Servern vermeiden
- ✓ US-Hyperscaler: Inanspruchnahme von EU-Servern mit dem Risiko der Untersagung durch Aufsichtsbehörden möglich, sofern TIA, SCC und ergänzende Schutzmaßnahmen dokumentiert sind. Bestenfalls Anonymisierung oder Multi-Cloud von EU-Anbietern.

FAZIT: WAS MÜSSEN BEHÖRDEN BEI AUSSCHREIBUNGEN BEACHTEN?

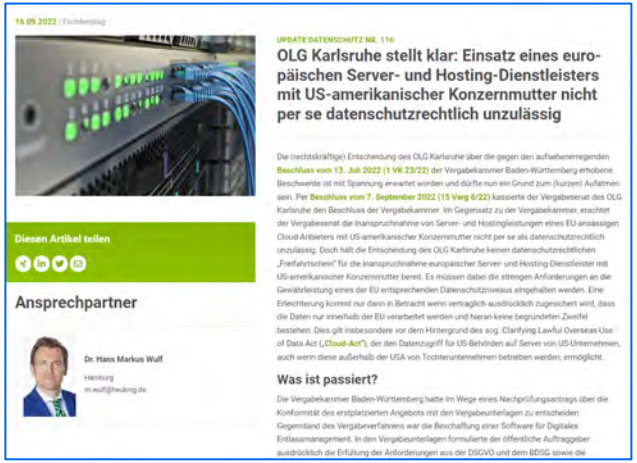
- ✓ Festlegen, welche Arten von Daten ausgelagert werden sollen.
- ✓ Prüfen, ob technische Verschlüsselung vor der Datenübermittlung möglich ist.
- ✓ Durchführen einer Datenschutz-Folgenabschätzung.
- ✓ Verwendung eines strengen Vertrags zur Auftragsverarbeitung.

Bei Einbindung von US-Hyperscalern:

- ✓ SCC vereinbaren (auch bei Reduzierung auf EU-Server),
- ✓ Zusicherung einholen (sowohl des Providers als auch des US-Hyperscalers), dass US-Datenzugriff ausgeschlossen ist (vgl. Urteil des OLG Karlsruhe);
- ✓ Informationspflicht einbinden bei Herausgabeverlangen von US-Behörden

NÜTZLICHE LINKS

[Eine moderne Verwaltung mit OPITZ CONSULTING (www.opitz-consulting.com)]



KONTAKT

Dr. Hans Markus Wulf

Rechtsanwalt und Partner bei Heuking Kühn Lüer Wojtek

m.wulf@heuking.de

Thomas Unterbörsch

Director Business Development – Corporate Development

thomas.unterboersch@opitz-consulting.com

Thomas Buch

Senior Manager Sales

Öffentliche Auftraggeber

thomas.buch@opitz-consulting.com