TaylorWessing

IT-Outsourcing von Versicherungsunternehmen

TW Insurance Day in Kooperation mit der VVB e.V.

18.04.2024 | RA Leonard Raphael und RA Ingo Vinck, Taylor Wessing

IT-Outsourcing von VU

Überblick

1 | Europas digitale Dekade bis 2030

TaylorWessing

1 > Europas digitale Dekade bis 2030

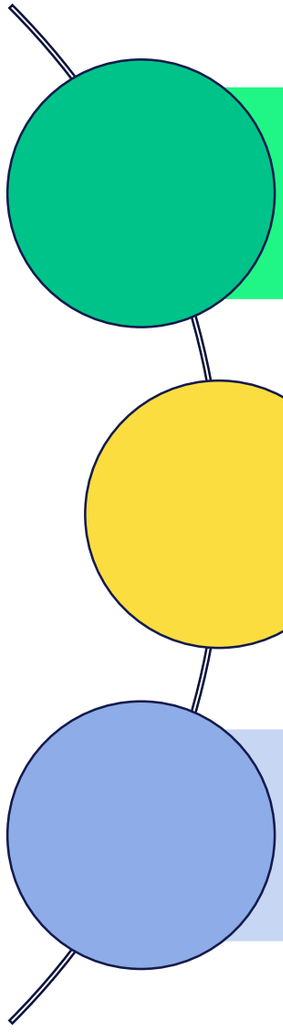
„Europas digitale Dekade bis 2030“

EU-Kommission entwickelt am 9. März 2021 während Corona-Pandemie „Eine europäische Datenstrategie“ vom 19.02.2020 weiter:

- **Eine offene, demokratische und nachhaltige Gesellschaft:** digitale Bildung und digitale Identität mit Zugang für alle EU-Bürger:innen, Medien mit hochwertigen Inhalten / Medienpluralismus, Kreislaufwirtschaft für Geräte
- **Eine faire und wettbewerbsfähige Wirtschaft:** europäische Datenstrategie zur Stärkung der globalen Wettbewerbsfähigkeit der EU-Wirtschaft, Schaffung eines Daten-Binnenmarkts, Überprüfung der Eignung der EU-Wettbewerbsregeln für das digitale Zeitalter
- **Technologie im Dienste der Menschen:** 5G- und 6G-Netze, Cybersicherheit, Super- und Quantencomputer, Quantenkommunikation und Blockchain, *Entwicklung und Einsatz von künstlicher Intelligenz*, EU-Rechenzentren/-Cloudkapazitäten, EU-eigne Chip-Produktion, Normungsvereinheitlichung (z.B. ein Ladekabel mit USB-C-Anschluss für alle Geräte)

1 > Europas digitale Dekade bis 2030

Aktueller Status:



Datenschutz / Datenaustausch

- DSG-VO (EU) 2016/679 v. 27.04.2016: gültig seit 18.05.2018
- Data Governance Act VO (EU) 2022/868 v. 30.05.2022: gültig seit 24.09.2023
- Data Act v. 27.11.2023: gültig ab 12. September 2025
- Plan: Einführung digitale Identität / Common EU Data Spaces

Fairness / Wettbewerb

- Digital Markets Act VO (EU) 2022/1925 v. 14.09.2022: gültig seit 02.05.2023
- Digital Services Act VO (EU) 2022/2065 vom 19.10.2022: gültig seit 17.02.2024

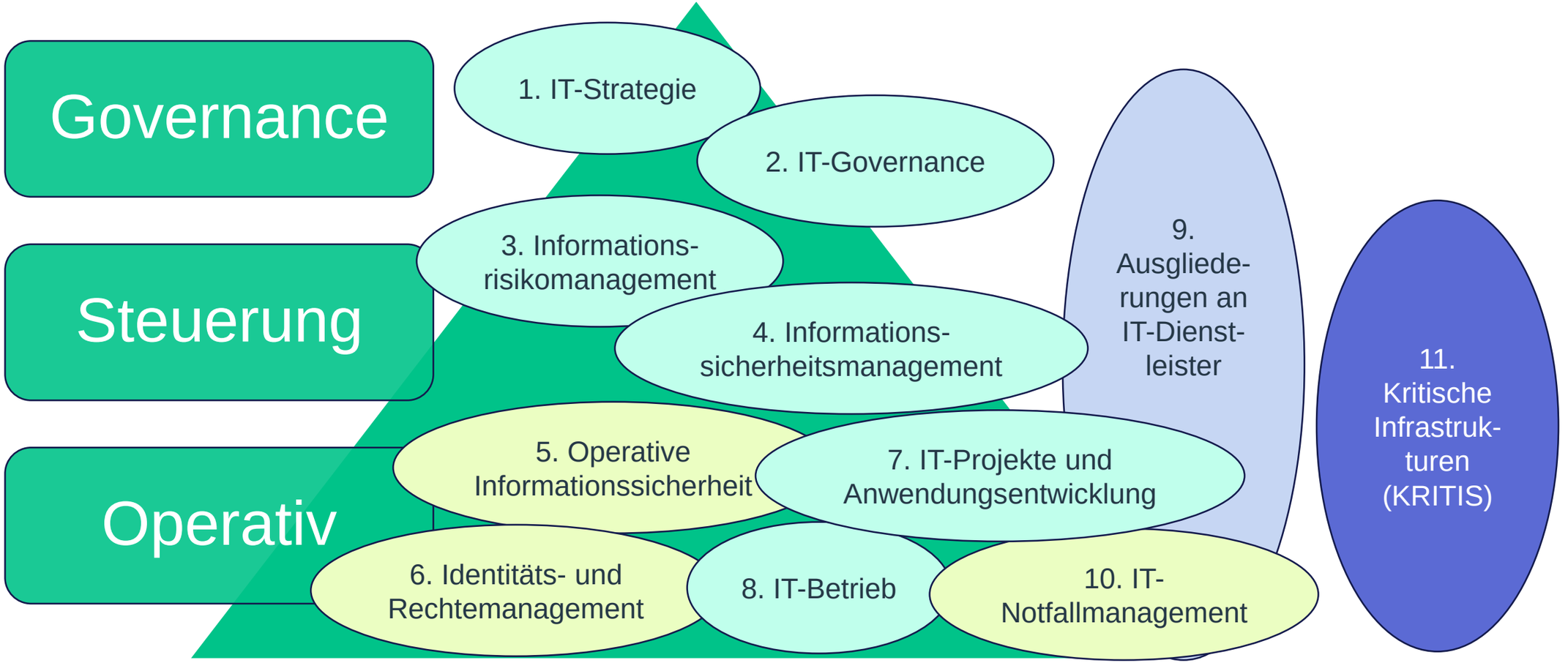
Technologie

- EU Chips Act v. 25.07.2023: gültig seit 21.09.2023
- Rili (EU) 2022/2380 v. 23.11.2022: gültig ab 28.12.2024 bzw. 2026
- NIS-2 Rilis (EU) 2022/2555 + 2557 v. 14.12.2022: gültig ab18.10.2024
- DORA VO (EU) 2022/2554 + Rili (EU) 2022/2556 v. 14.12.2022: gültig ab 17.01.2025
- Vorschlag für KI-VO v. 21.01.2024
- Vorschlag KI-Haftungs-Rili v. 28.09.2022:

2 | Digitale Resilienz von VU (VAIT, DORA)

2 > Digitale Resilienz von VU (VAIT, DORA)

VAIT – BaFin-Rs 10/2018 i.d.F. v. 3. März 2022



2 > Digitale Resilienz von VU (VAIT, DORA)

DORA – digitale Resilienz im Finanzdienstleistungssektor

IKT-Risikomanagement (Kap. II Art. 5 ff. DORA)	**Berichterstattung über Vorfälle** (Kap. III Art. 17 ff., 45 DORA)	**Testen der digitalen operationalen Resilienz** (Kap. IV Art. 24 ff. DORA)	**Management von IKT-Drittrisiken** (Kap. IV Art. 24 ff. DORA)
▪ GL-Verantwortung ▪ Solider, umfassender und gut dokumentierter IKT-Risikomanagement-rahmen (Strategie, Richtlinien, Verfahren, IKT-Protokolle) ▪ Erkennungs-Tools ▪ geeignete Reaktions- und Wiederherstellungs-strategien und Weiter-entwicklung	▪ Vorfalls-Managementpro-zess: IKT-bezogene Vor-fälle / erhebliche Cyber-bedrohungen erkennen, verwalten und melden ▪ Dokumentation und Meldung "schwerwie-gender" Vorfälle an GL und ggfs. an BaFin und Kunden ▪ Austausch von Infos und Erkenntnissen über Cyber-bedrohungen (z.B. GDV)	▪ solides umfassendes Programm für Testen und Schließen von erkannten Schwachstellen als Bestandteil des IKT-Risikomanagements ▪ Tests durch **sachver-ständige unabhängige Parteien** (intern / extern) ▪ mind. 1x jährlich Test und alle 3 Jahre besonderer Penetrationstest (TLPT)	▪ **Vertrag** mit Dritt-Dienst-leistern hat Mindest-inhalte zu regeln ▪ Aktuelles Informations-register mit allen Verträ-gen, 1x jährlich an BaFin nennen ▪ geplante Verträge mit IKT-Dritt-Dienstleister über **kritische oder wichtige Funktionen** vorab an BaFin

Rechtsakte zur Durchführung werden noch folgen: Regulatory + Implementing Technical Standards (RTS + IST)

Aktuell: BaFin/Buba-Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter vom 1. Februar 2024

3 Aufsichtsmitteilung zum Cloud-Outsourcing

TaylorWessing

3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Wesentliches – Prüfungs-, Kontroll- und Weisungsrechte, Risikomanagement, Vertragsklauseln

- Die Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter vom Februar 2024 ist eine Überarbeitung des früheren Merkblatts der BaFin und der Deutschen Bundesbank mit dem Titel „Orientierungshilfe zu Auslagerungen an Cloud Anbieter“, vom November 2018
- § 32 Abs. 2 Satz 1 VAG: **Prüfungs- und Kontrollrechte der BaFin** dürfen durch die Ausgliederung nicht beeinträchtigt werden. Das ausgliedernde Unternehmen hat hinsichtlich der von der Ausgliederung betroffenen Funktionen sicherzustellen, dass
  - das Unternehmen selbst, seine Abschlussprüfer und die Aufsichtsbehörde auf alle Daten zugreifen können,
  - der Dienstleister mit der Aufsichtsbehörde zusammenarbeitet und
  - die Aufsichtsbehörde Zugangsrechte zu den Räumen des Dienstleisters erhält, die sie selbst oder durch Dritte ausüben kann.
- § 32 Abs. 4 Satz 1 VAG: Das ausgliedernde VU hat sich die erforderlichen **Auskunfts- und Weisungsrechte vertraglich zu sichern** und die ausgegliederten Funktionen in sein **Risikomanagement** einzubeziehen
- Die neue Aufsichtsmitteilung ist als Orientierungshilfe zu verstehen, in der BaFin und Deutsche Bundesbank ihre Einschätzung zu Auslagerungen an Cloud-Anbieter mitteilen.
- Durch die Aufsichtsmitteilung soll insbesondere die aufsichtliche Bewertung von **Vertragsklauseln** transparent gemacht, sowie Hinweise zur Überwachung und Kontrolle von Cloud-Auslagerungen und zu den durch die beaufsichtigten Unternehmen sicherzustellenden Anforderungen gegeben werden.
- Die Aufsichtsmitteilung gibt einen Ausblick auf die Anforderungen an Verträge über die Nutzung von **Informations- und Kommunikationstechnologien (IKT)** gemäß DORA

3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Vorbereitende Handlungen und Governance-Rahmen für die Cloud

- **Strategische Überlegungen**: Das beaufsichtigte Unternehmen soll Überlegungen zur Nutzung von Cloud-Diensten in seiner IT-Strategie abbilden. Daneben soll es einen Prozess entwickeln und dokumentieren, der alle für die Strategie über die Migration in die Cloud bis hin zur Ausstiegsstrategie abdeckt.
- **Analyse und Wesentlichkeitsbewertung**: Zunächst ist zu prüfen, ob eine Auslagerung vorliegt und ob sie als wesentlich einzustufen ist. Bei der Risikoanalyse sollen alle für das beaufsichtigte Unternehmen relevanten Aspekte im Zusammenhang mit der Auslagerung auf Cloud-anbieter berücksichtigt werden. Die Aufsichtsmitteilung enthält detaillierte Vorgaben für die Punkte, die bei der **Risikoanalyse** zu berücksichtigen sind, z.B.
  - Kritikalität des Outsourcings
  - Bewertung der finanziellen und operationellen Risiken (Systemausfall, Sabotage), der rechtlichen Risiken (z.B. Risiken der Rechtsdurchsetzung, Datenschutz), der Reputationsrisiken
  - Bewertung der Eignung des Cloud-Anbieters (Fähigkeiten, Infrastruktur, wirtschaftliche Situation)
  - Bewertung des Standortes, an dem Daten abgespeichert werden
- **Interne Vorgaben für die Nutzung der Cloud**: Das beaufsichtigte Unternehmen soll für die Nutzung der Cloud geeignete Vorgaben im Einklang mit der IT-Strategie und dessen Leit- und Richtlinien zur Informationssicherheit formulieren
- **Ressourcenausstattung und Qualifikation**: Beaufsichtigte Unternehmen sollen für die Nutzung der Cloud ausreichend quantitative und qualitative Ressourcen bereitstellen und organisatorisch verankern (personelle, finanzielle und sonstige Ressourcen). Dies betrifft insbesondere Governance, Risikomanagement und Auslagerungsmanagement

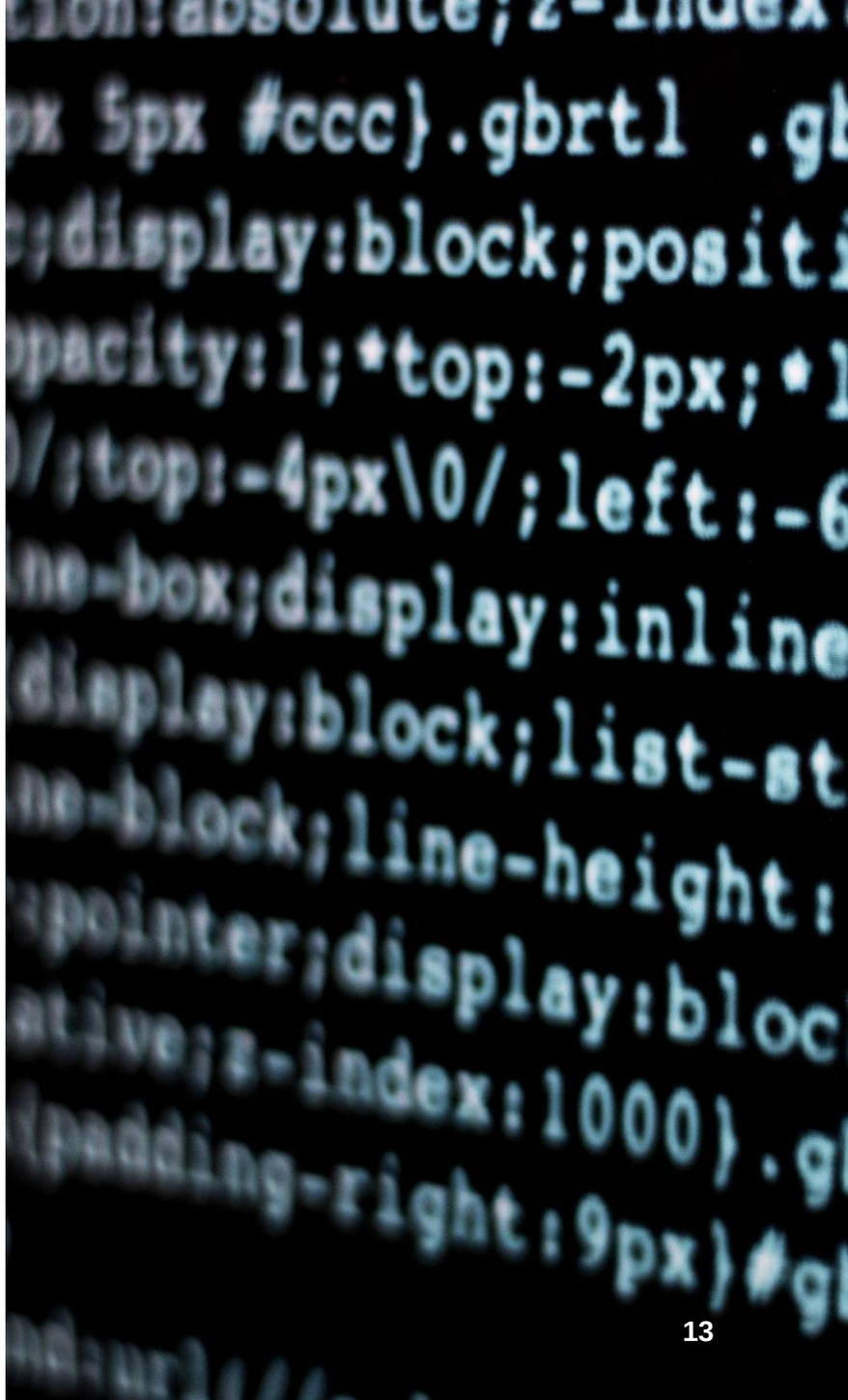
3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Vertragsgestaltung - Überblick

3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Vertragsgestaltung – Bestimmung der Leistungen

- **Leistungsgegenstand**: Im Vertrag soll eine Spezifizierung der von Cloud-Anbieter zu erbringenden Leistung erfolgen:
  - Der auszulagernde Sachverhalt und dessen Umsetzung
  - Anpassungsmöglichkeiten im Falle einer Bedarfsänderung
  - Unterstützungsleistungen (Support)
  - Zuständigkeiten, Mitwirkungs- und Bereitstellungspflichten (z.B. bei Updates)
- Ort der Leistungserbringungen, der Datenverarbeitung und Speicherung (z.B. Standorte der Rechenzentren)
- Beginn und ggf. Ende des Auslagerungsvertrages
- Kennzahlen zur fortlaufenden Überprüfung der Dienstleistungsgüte



3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Vertragsgestaltung – Informations- und Prüfungsrechte des VU

- **Informations- und Prüfungsrechte** sowie **Kontrollmöglichkeiten** des beaufsichtigten Unternehmens dürfen vertraglich nicht eingeschränkt werden. Es ist sicherzustellen, dass das beaufsichtigte Unternehmen zeitnah diejenigen Informationen erhält, die es für die angemessene Steuerung und Überwachung der Auslagerungsrisiken benötigt. Fünf Jahre Aufbewahrung.
- Zur Gewährleistung der Informations- und Prüfungsrechte soll folgendes vereinbart werden:
  - die Gewährung uneingeschränkten Zugriffs auf Informationen und Daten sowie **Zutritts zu den Geschäftsräumen des Cloud-Anbieters**, einschließlich aller Rechenzentren, Geräte, Systeme und Netzwerke, die zur Erbringung der ausgelagerten Sachverhalte eingesetzt werden; hierzu gehören die damit in Zusammenhang stehenden Prozesse und Kontrollen,
  - effektive Kontroll- und Prüfungsmöglichkeiten sowie die Möglichkeit von **Vor-Ort-Prüfungen beim Cloud-Anbieter**.
- Bezogen auf wesentliche Weiterverlagerungen soll sichergestellt werden, dass gleichwertige Informations- und Prüfungsrechte für die gesamte Auslagerungskette vereinbart sind.
- **Keine (mittelbare) Einschränkung der Informations- und Prüfungsrechte**
  - Unzulässig ist z.B. die Vereinbarung gestufter Informations- und Prüfverfahren, z.B. die Verpflichtung zunächst auf Prüfberichte oder Zertifikate zurückzugreifen.

3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Vertragsgestaltung – Informations- und Prüfungsrechte der BaFin

- **Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten** der Aufsicht dürfen vertraglich oder durch interne Umsetzungsrichtlinien des Cloudanbieters nicht eingeschränkt werden.
- Die Aufsicht muss den ausgelagerten Sachverhalt beim Cloud-Anbieter genau kontrollieren können, wie bei dem beaufsichtigen Unternehmen.
- Es muss vertraglich vereinbart werden, dass die Aufsicht ihre Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten ausüben kann.
- Das gilt auch für die Personen, welche die Aufsicht für Prüfungen und Kontrolle einschaltet.

Zur Gewährleistung der Informations- und Prüfungsrechte der Aufsicht soll insbesondere folgendes vereinbart werden:

- Verpflichtung des Cloud-Anbieters zur uneingeschränkten Zusammenarbeit
- Gewährung uneingeschränkten Zugriffs auf Informationen und Daten sowie Zutritt zu den Geschäftsräumen des Cloud-Anbieters, einschließlich Rechenzentren
- Effektive Kontroll- und Prüfungsmöglichkeiten sowie die Möglichkeit der Durchführung von Vor-Ort-Prüfungen beim Cloud-Anbieter
- Unzulässig sind (direkte oder mittelbare) Einschränkungen dieser Informations- und Prüfungsrechte

3 > Aufsichtsmitteilung zum Cloud-Outsourcing

Vertragsgestaltung – Weisungsrechte, Datensicherheit, Kündigung

- **Weisungsrechte**: Es sollen Weisungsrechte der beaufsichtigten Unternehmen vereinbart werden. Diese Weisungsrechte sollen sicherstellen, dass alle erforderlichen und zur Erfüllung der vereinbarten Dienstleistung notwendigen Weisungen erteilt werden können (Einflussnahme- und Steuerungsmöglichkeit)
- **Datensicherheit/-schutz (Ort der Leistungserbringung)**: Es sind Regelungen zu vereinbaren, die sicherstellen, dass sowohl datenschutzrechtliche Bestimmungen, als auch aufsichtsrechtliche Anforderungen an die Informationssicherheit eingehalten werden.
  - Der Ort der Leistungserbringung (Standort des Rechenzentrums) soll bekannt sein
  - Die Redundanz der Daten und Systeme entsprechend ihrem Schutzbedarf soll sichergestellt sein
  - Datenschutz und –sicherheit ist innerhalb der gesamten Auslagerungskette zu gewährleisten
- **Kündigungsmodalitäten**: Es sind Kündigungsrechte und angemessene Kündigungsfristen zu vereinbaren.
  - Es soll für das beaufsichtigte Unternehmen insbesondere ein **Sonderkündigungsrecht** vereinbart werden, das die Kündigung aus wichtigem Grund vorsieht, wenn die Aufsichtsbehörde dies verlangt
- **Weiterverlagerung**: Es sind Möglichkeiten über die Weiterverlagerung zu vereinbaren, die sicherstellen, dass aufsichtliche Anforderungen eingehalten werden. Insbesondere ist zu vereinbaren, dass Prüfungs- und Kontrollrechte sowie Kontrollmöglichkeiten im Falle einer Weiterverlagerung auch gegenüber dem Subunternehmen bestehen.
- **Informationspflichten der Cloud-Anbieter** (z.B. Meldung von Störungen oder Informationssicherheitsvorfällen)
- **Deutsches Recht** oder **Recht eines anderen EU Mitgliedstaats**

Europa > Mittlerer Osten > Asien

taylorwessing.com