Die Büchse der PanDORA

Die EU-Verordnung zur digitalen Resilienz und ihre Auswirkungen für IT-Firmen

HSW | RECHTSANWÄLTE
HARDER SEDLMEIER WEITZEL

Begriffsklärung

... oder eher Warm-Up

Wer kennt Doro?

Queen of Heavy Metal

Und wer kennt DORA?

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsaktes an die nationalen Parlamente,

Zahlen, Daten, Fakten:

- 79 Seiten
- 106 Erwägungsgründe
- 64 Artikel
- Direkt betroffene Unternehmen:
  - In EU rund 22.000
  - In Deutschland 1.600 oder 3.600 (je nach Schätzung)
- Indirekt betroffene IT-Firmen:
  - In D rund 20.000 Firmen

Warum sollte Sie das interessieren?

Lizenz zum Geldverdienen!

Zertifizierte/-r DORA-IKT-Risikomanager/-in (DVA)

Erfolgreiches Management von IKT-Risiken im Versicherungsunternehmen

BUCHUNG

WEB-CODE **V7614**

PREIS

1.350 € MwSt.-frei

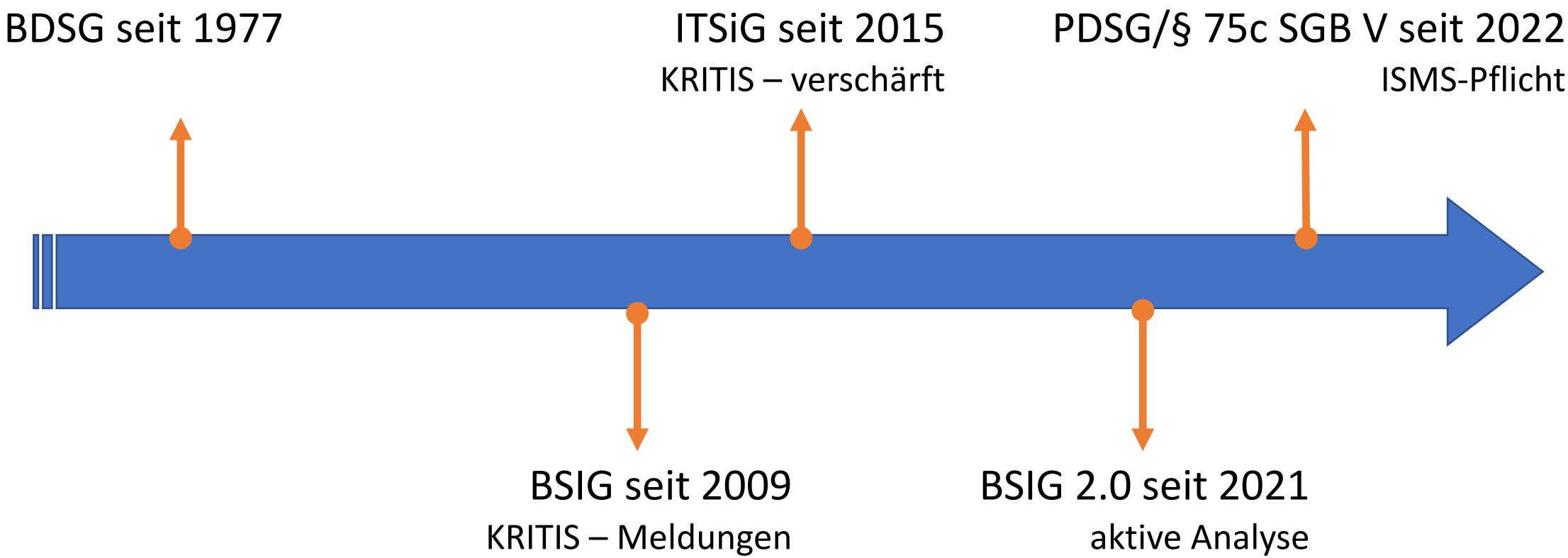
Die Prüfungsgebühr (200,00€) ist im Lehrgangspreis enthalten.

KONZEPT | ZIELE / NUTZEN | INHALTE | TEILNAHMEINFOS | PRÜFUNG

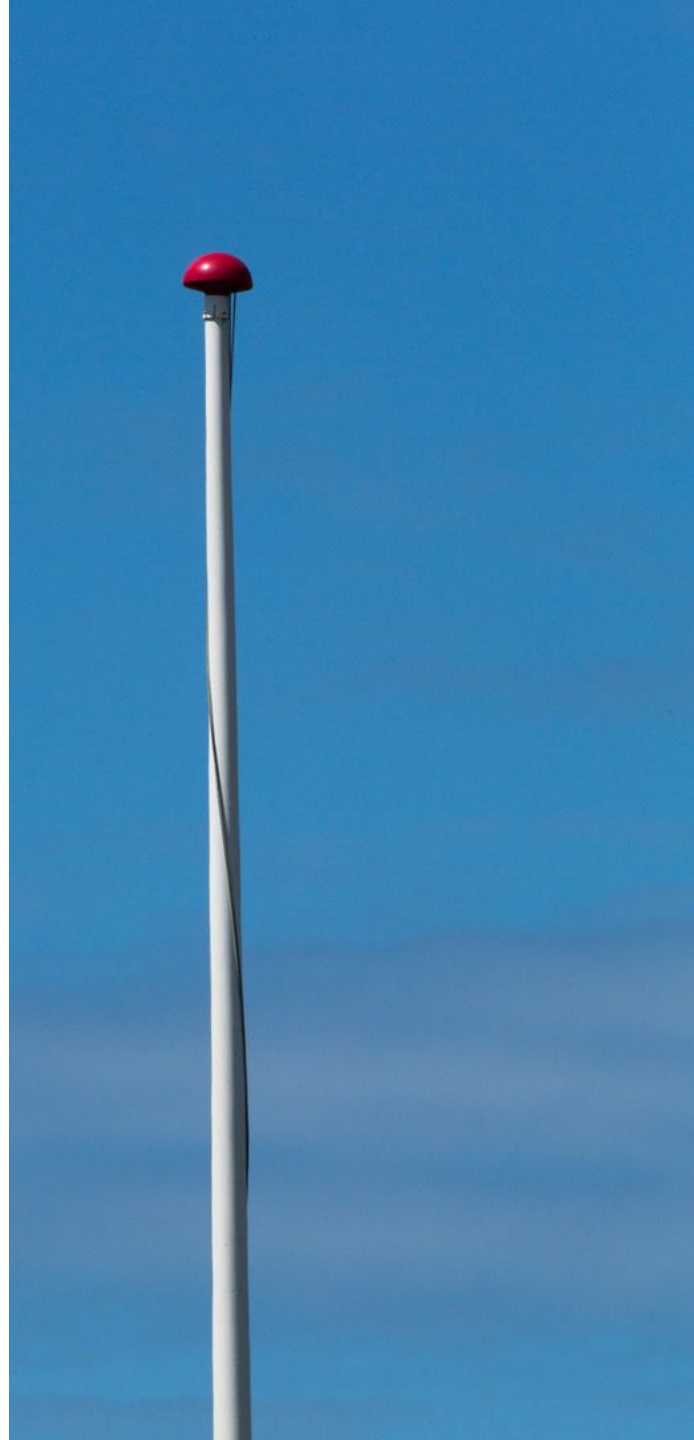
Durch die immer weiter fortschreitende Digitalisierung in Versicherungsunternehmen, sind deren

HSW | RECHTSANWÄLTE HARDER SEDLMEIER WEITZEL

Schritt für Schritt immer schärfer



Mit DORA endlich erreicht?



DORA – hat das Boot nicht längst abgelegt?!

Ein Schnellstart sieht anders aus …

Der ursprüngliche Plan:

- Zwei Jahre gesetzliche Vorbereitungsfrist ab 17.1.2023 sollten ausreichen
- Verordnung ist am 17.1.2025 anwendbar geworden

Der langsame Start:

- In europäischen Firmen meist schon 2023 begonnen
- In D meist ab Sommer oder Herbst 2024 erste hektische Vorbereitung

Als Reaktion dann die erste Terminverschiebung:

- Frist zur Einreichung des IKT-Informationsregisters bei BaFin mehrfach verschoben
- Zum 28. April 2025 musste dann alle hochgeladen sein
- Seitdem: Still ruht der See … oder doch nicht?

Jetzt geht es los ...

... mit der Nachverhandlung der IT-Dienstleister

Halt, Sprachpolizei!

... mit der Nachverhandlung der **IT-Dienstleister**

Jetzt geht es los ...

... mit der Nachverhandlung der **IKT-Drittdienstleister**

Interessante Erfahrungen

Aus DORA-Einführungsprojekten

Wer bietet an?

- Entweder die ganz Großen
  - Big Four mit ihren Beratungssparten
  - Großkanzleien bei großen Versicherung
- Oder ganz kleine Krauter
  - Beispiel Ausschreibung IT-Consultant mit juristischer Beratung

- In der SW-Industrie:
  - Die Großen tun sich schwer
  - Die Kleinen aus anderen Gründen
  - Die meisten sind unendlich teuer

servicenow

Doria

ARTEMEON

Datenflut beim Informationsregister

- Unnütze Dry Run Exercise der EU (07-08/24)
  - Nur Trockenlauf mit wenigen Einträgen
  - Und in Deutschland einer Handvoll Beteiligten
- Bei vielen CIFs, Tochtergesellschaften oder Zweigstellen bis zu vierstellige Zahl an Funktionskennungen
- Bei großen Finanzinstituten hunderttausende bis Millionen Zeilen im Register
  => Excel hoffnungslos überfordert
  => Manche DORA-Tools auch, da kommen laufend Updates

Neue Querschnittsfunktionen/mehr Personal:

- Unabhängige Kontrollfunktion
  - Eigenständige Funktion aufgrund der **drei Verteidigungslinien**
- Einkauf, Risiko-Management und unabhängige Kontrollfunktion brauchen für die **vielen neuen Aufgaben** mehr Personal

  → Braucht 5 bis 10 % Personalaufstockung in mittelgroßen Unternehmen

- Liebgewonnene Bequemlichkeit muss aufgegeben werden:
  - CRO kann nicht länger nur überwachen und Leitlinien setzen

  → muss seine Organisation in **operatives Risiko-Management** einbinden
- Abläufe bei rasch benötigter IT-Beschaffung **viel aufwendiger** und **langwieriger**


Was befürchten
die Dienstleister?

Befürchtungen der IKT-Dienstleister

- Finanzinstitute werden im Windschatten zwingender DORA-Änderungen weitreichende oder inakzeptable Änderungen der Verträge „durchdrücken“.
- Rasche Ausstiegsmöglichkeit dank zwingender neuer Kündigungsklauseln
  - Wie bekommen wir das durch die Subunternehmer-Kette durchgereicht?
  - Wie können wir ein US-Unternehmen zur Anpassung laufender Verträge bewegen?
- Was bedeutet die Pflicht zur Aufnahme einer Aktualisierungsklausel in SLA?
  - Beispiel: *„Die Parteien erörtern einmal pro Jahr, ob und inwiefern die Dienstleistungsgüte an aktuelle Bedarfe angepasst werden kann.“*

  => Was ist, wenn der Dienstleister das nicht will oder kann?

  => Was ist mit der Vergütung?

Entwicklung bei DORA-Vertragsnachträgen

- Erste Dokumente Herbst 2024:
  - Meist noch kurz, oft deutlich überzogen
  - Ansage: Friss oder stirb!
  - Versuch, Verträge nachzuschärfen oder bessere Leistungen zu gleichem Preis einzukaufen
- Unrühmliche Höhepunkte durch Großkanzleien:
  - 28 Seiten bei Allianz (Ashhurst), 34 Seiten bei Züricher (andere Großkanzlei)
- Entwicklung bis März:
  - Komplexität wird wieder reduziert, manchmal bis hin zu 4-Seitern
  - Berater-Kanzleien rudern bei überzogenen Mustern zurück
  - Viele Nachtragsdokumente belegen/erläutern inzwischen Notwendigkeit durch DORA-Verweise in jeder Klausel
  - Bei Wunsch nach Verhandlung/Veränderung erfolgt oft Rückstufung auf non-CIF1
- Noch deutlicher seit April:
  - Bereitschaft zur echten Nachverhandlung (externe Berater mit Schema F sind von Bord)
  - Kulantere Lösungen
  - Vorgefertigte Klauseln für Plan B/Nachverhandlung

Butter bei die Fische!

Aus DORA-Vertragsnachträgen

HSW | RECHTSANWÄLTE
HARDER SEDLMEIER WEITZEL

Aktuelle Entwicklungen

Plumpe Umgehung

- Klausel-Beispiel:

  „The agreed service level descriptions, including updates and revisions thereof including the quantitative and qualitative performance targets for the ICT Services provided under the Framework Agreement, are set out in Rahmenbedingungen für Dienstleistungen, incl. Vertragsgegenstand.“

Hat der wer nachgedacht?

- Klausel-Beispiel:

  „Die Durchführung der Leistungen sowie die Verarbeitung der Daten, einschließlich der Speicherung, erfolgt durch den Auftragnehmer und ggf. seine Unterauftragnehmer ausschließlich an den in dem zugrundeliegenden Vertrag aufgeführten Standorten (Regionen und/oder Länder).

  *Der Auftraggeber ist vorab mindestens in Textform **zu informieren**, wenn der Auftragnehmer oder sein Unterauftragnehmer eine Änderung dieser Standorte beabsichtigt.“*

Aktuelle Entwicklungen

„Schweineklauseln“ (1/3)

- *„Der Auftragnehmer gewährleistet, die IKT-Dienstleistungen in voller Übereinstimmung **mit allen rechtlichen, regulatorischen** und behördlichen Bestimmungen sowie relevanter Rechtsprechung zu erbringen, die **auf den Auftraggeber bzw. dessen VU** anwendbar sind und zum direkten Leistungsumfang des Auftragnehmers gehören.“*
- *„Der Auftragnehmer ist verpflichtet, den Auftraggeber bei einem IKT-Vorfall, der mit der für Auftraggeber bereitgestellten IKT-Dienstleistungen in Verbindung steht, ohne **zusätzliche Vergütung jede erforderliche Unterstützung** zu leisten.“*
- *„Der Auftragnehmer verpflichtet sich, alle vertragsgegenständlichen Daten und Konfigurationen sowohl in den Produktions- als auch in den Back-Up-Umgebungen zu speichern sowie **zusätzlich eine dritte**, logisch und **physisch getrennte Speicherung** der vertragsgegenständlichen Daten und Konfigurationen vorzunehmen.“*

Aktuelle Entwicklungen

„Schweineklauseln“ (2/3)

- *„Der Auftragnehmer ist in Bezug auf die geschuldeten Dienstleistungen zur laufenden internen Kontrolle und zur regelmäßigen Berichterstattung an den Auftraggeber sowie zur umgehenden Meldung **jeglicher auftretender Probleme und Fehler** bei der Durchführung des Hauptvertrags und dieser Zusatzvereinbarung verpflichtet.“*
- *„Die Parteien sind sich darüber einig, dass insbesondere bei Vorliegen folgender Umstände der Auftraggeber zur außerordentlichen Kündigung aus wichtigem Grund berechtigt ist:*
  *– sonstige Umstände, welche zu einer **aus Sicht des** Auftraggebers untragbaren **Risikoerhöhung** führen würden“*
- *„Der Auftragnehmer wird den Auftraggeber im Falle einer Beendigung des Hauptvertrags bei der Wiedereingliederung bzw. **Implementierung einer alternativen Lösung** unterstützen und gemeinsam mit dem Auftraggeber **sicherstellen**, dass die Vertragsbeendigung nicht zu Lasten der Kontinuität und Qualität der Dienstleistungen für die Kunden des Auftraggebers geht.“*

Aktuelle Entwicklungen

„Schweineklauseln“ (3/3)

- *„Der Auftragnehmer ist verpflichtet, **alle** unterbeauftragten IKT-Dienstleistungen, welche im Zusammenhang mit der für den Auftraggeber zu erbringenden IKT-Dienstleistung stehen, **fortlaufend** zu überwachen, um **sicherzustellen**, dass seine vertraglichen Verpflichtungen gegenüber dem Auftraggeber **fortlaufend** eingehalten werden.“*
- *„Der Auftragnehmer stellt sicher, u. a. durch eine entsprechende schriftliche Vereinbarung mit dem jeweiligen Unterauftragnehmer, dass der jeweilige Unterauftragnehmer über Notfallpläne und Geschäftsfortführungspläne verfügen, die **mit den im Verhältnis** zwischen Auftraggeber und Auftragnehmer vereinbarten Notfall- und Geschäftsfortführungsplänen **harmonisieren**.“*
- *„Der Auftragnehmer stellt sicher, dass der Unterauftragnehmer über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit verfügt, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch den Auftraggeber im Einklang **mit seinem Rechtsrahmen** bieten.“*

Aktuelle Entwicklungen

Da hat wer nicht ganz aufgepasst ...

- Art. 13 (6) DORA:
  *„**Gegebenenfalls** nehmen die Finanzunternehmen entsprechend Artikel 30 Absatz 2 Buchstabe i auch IKT-Drittdienstleister in ihre einschlägigen Schulungsprogramme auf.“*
- Klausel-Beispiel aus nonCIF-Vertrag:
  *„ Die Parteien **sichern** sich **gegenseitig zu**, dass sie ihr in die Leistungserbringung involviertes Personal im erforderlichen Umfang mit Blick auf die IKT-Sicherheit sensibilisieren und das Wissen durch Schulungen im erforderlichen Umfang aktuell halten.“*
- Zu Subunternehmen:
  *„ Der Auftragnehmer stellt sicher, dass er in dem Vertragsverhältnis mit dem **Unterauftragnehmer** die **zu erreichende Dienstleistungsgüte** vereinbart.“*

Aktuelle Entwicklungen

Absicherung für die Zukunft

- Art. 30 Abs. 4 DORA erwähnt Standardvertragsklauseln der Behörden für bestimmte Dienstleistungen
  - Klausel-Beispiel:
    „Die Parteien vereinbaren daher, dass etwaige nach Vertragsunterzeichnung von Behörden veröffentlichen Standardvertragsklauseln für die in dieser Zusatzvereinbarung vereinbarten IKT-Dienstleistungen ***Anwendung finden*** *werden und* ***Vorrang*** *haben werden vor jeder abweichenden Regelung aus dieser Zusatzvereinbarung. “*
- Verordnungen können sich ändern …
  - Klausel-Beispiel:
    „Soweit sich die DORA-Anforderungen während der Laufzeit des zugrundeliegenden Vertrags ändern oder eine Anpassung dieses DORA-Nachtrags erforderlich machen, werden die Parteien diesen ***nach Treu und Glauben*** *entsprechend* ***anpassen****, um den DORA-Anforderungen zu genügen.“*

Aktuelle Entwicklungen

Moderate Rücksichtnahme

- Klausel-Beispiele:
  - *„The Third Party Service Provider shall participate in NIBC´s ICT security awareness programmes and digital operational resilience training in case such is reasonably considered appropriate by NIBC. NIBC **may take into account** whether the Third Party Service Provider has its own such programmes and trainings.“*
  - *Eine Anforderung zur IKT-Qualifizierung kann der Auftragnehmer nur zurückweisen, wenn er **nachweist**, dass das eingesetzte Personal in den vergangenen zwölf Monaten an einer IKT-Qualifizierung mit vergleichbarem Inhalt **teilgenommen hat**."*
- Ganz neu: mit wenigen Anpassungen akzeptable Vertragsnachträge

Der große Streitpunkt

- Nach wie vor: Wer zahlt?
- Art. 30 (2) lit. f) DORA:
  *„die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, **ohne** zusätzliche Kosten **oder** zu vorab festzusetzenden Kosten Unterstützung zu leisten“*
- Art. 30 (2) lit. g) DORA
  *„die Verpflichtung des IKT-Drittdienstleisters, **vollumfänglich** mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden **zusammenzuarbeiten**, einschließlich der von diesen benannten Personen“*

Alles gut soweit?

So könnte man meinen ...

Was bleibt bislang auf der Strecke (1/2)?

- Service Level Agreements / detaillierte Leistungsbeschreibungen
  - Kosten Zeit und Mühe
  - Müsste Einkauf zeitaufwendig aus Fachabteilungen beschaffen
- Einstufung von Verträgen zur Unterstützung wichtig/kritischer Funktionen
  - Bei genauer Nachfrage/Prüfung plötzlich alles non-CIF
  - Weil dafür den Einkäufern mehr Großzügigkeit eingeräumt wird

Was bleibt bislang auf der Strecke (2/2)?

- DORA-konforme Neuverträge oder spezielle AGB:
  - Alle seit 17.1.2025 geschlossene Neuverträge müssten genaue Leistungsbeschreibung, SLA, Hinterlegung und von DORA vorgeschriebenen Klauseln enthalten
  - Bislang kaum Änderung bisheriger Praxis erkennbar
- Echte Stärkung der digitalen Resilienz erfordert:
  - Nicht bloß Beschränkung auf Zusatzklauseln nach Art. 30 (2) und (3) DORA
  - Realistische Notfallplanung
  - Auswechselung von IKT-Dienstleistern, die Anforderungen nicht erfüllen
  - Überprüfung von IT-Sicherheit gelieferter Software
  - Ausfallsicherung für SaaS
  - Ausfallsicherung für Crypt Keys (auch in HSM!)

Was könnte helfen?

Wird tatsächlich so heiß gegessen, wie die EU kocht?

Hilfreiche Normen

- Oft übersehen: Art. 42 Abs. 8 DORA
  - *„Die zuständigen Behörden gewähren Finanzunternehmen den **erforderlichen Zeitraum**, damit sie die vertraglichen Vereinbarungen mit **kritischen IKT-Drittdienstleistern** anpassen können, um nachteilige Auswirkungen auf ihre digitale operationale Resilienz zu vermeiden und ihnen die Anwendung der in Artikel 28 genannten Ausstiegsstrategien und Übergangspläne zu ermöglichen.“*

- Noch unklar:
  - Weshalb nur für kritische Dienstleister?
  - Zu welchen Zwecken genau?

HSW | RECHTSANWÄLTE
HARDER SEDLMEIER WEITZEL