aringer herbst winklbauer

Sie kommen zu Recht.

IT-Services im Finanzsektor –
EBA Leitlinien zu Auslagerungen und andere Rechtsvorschriften für IT Services im Finanzsektor

15. Österreichischer IT-Rechtstag

5.5.2021

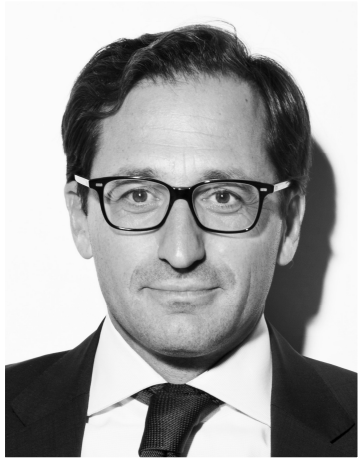
Axel Anderl, Stephan Winklbauer

DORDA

Ansprechpartner

Dr Axel Anderl, LL.M.

- Managing Partner bei DORDA
- Leiter der IT/IP und Datenschutz sowie der Digital Industries Group
- Absolvent der Universität Wien (Dr iur 2005) und des Universitätslehrgangs für Informationsrecht und Rechtsinformation der Universität Wien(IT-Law) (LL.M. 2001)
- Fachliche Schwerpunkte: IT-Recht, insb E-Commerce, Outsourcing, IT-Projektverträge, Datenschutzrecht, Urheberrecht
- ILO Clients Choice Award für E-Commerce 2012 und 2013
- ILO Clients Choice Award für Information Technology 2014, 2015, 2016, 2017, 2018 und 2019
- Seit Jahren als führender Anwalt in IT-Recht in "Chambers Europe" und "Legal 500"empfohlen
- Legal500 Hall of Fame TMT
- Autor zahlreicher Fachpublikationen in den Bereichen IT-, IP-Urheber- und Wettbewerbsrecht
- Vortragender an diversen Hochschulen und Fachhochschulen
- Autor zahlreicher Fachpublikationen, zuletzt NISG Kommentar (Manz), #Blockchain (lexisnexis) und IP Recht in der Praxis (Manz)



Dr. Stephan Winklbauer, LL. M.
aringer herbst winklbauer
rechtsanwälte

- Partner bei aringer herbst winklbauer
- Absolvent der Universität Wien (Dr iur 1994) und des Masterstudiums für Europarecht der Donauuniversität Krems (LL.M.1998)
- Fachliche Schwerpunkte: IT-Recht, insb Outsourcing, Softwareprojekt- und -wartungsverträge, Datenschutzrecht, IT-Litigation
- Autor und Vortragender

Agenda

I. Einleitung – Rechtliche Ausgangslage

II. Anwendungsbereich

- Adressatenkreis
- Definition Auslagerung

III. Pflichten – Gliederung und Aufbau

- Vor der Auslagerung
- Vertragliche Verpflichtungen
- Während der Auslagerung: Monitoring und Exit

IV. Exkurs: ESMA Leitlinien

V. Praxistipps

EBA Guidelines – Historie und Bedeutung

- Leitlinien der European Banking Authority (EBA)
  - Grundlage in Art 16 EBA-VO
  - Ziel: Schaffung kohärenter, effizienter und wirksamer Aufsichtspraktiken
- Guidelines on outsourcing arrangements – EBA/GL/2019/02
  - Vorgänger:
    - CEBS Guidelines vom 14.12.2006
    - EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03)
- am 25.2.2019 erlassen – seit 30.9.2019 in Kraft
  - für alle ab diesem Datum abgeschlossenen Auslagerungsverträge
  - Übergangsfrist für bestehende Verträge bis 31.12.2021

EBA Guidelines – rechtliche Wirkung

- Direkte Adressaten:
  - Institute
  - Zahlungsinstitute
  - E-Geld-Institute
- Art 16 Abs 3 EBA-VO
  - Erfordernis, "*alle erforderlichen Anstrengungen unternehmen*"
  - Zielt bei Auslagerung auf Bindung Dritter (Provider) ab
  - Überbindung der Anforderungen erforderlich
- Leitlinien in der Praxis der **wichtigste Prüfmaßstab der FMA**
- Sanktionen bei Nichteinhaltung durch FMA
  - Auftrag zur Herstellung des rechtskonformen Zustandes (Bescheid)
  - Zwangsstrafe bis zu EUR 30.000,-
  - Untersagung der Geschäftsführung; Konzessionsentzug

Anwendungsbereich

- Auslagerung
  - eines Prozesses;
  - Erbringung einer Dienstleistung; oder
  - Erbringung einer Tätigkeit durch einen Dritten, der normalerweise im Anwendungsbereich des Instituts selbst liegt
  - tatsächliche Wahrnehmung in der Vergangenheit nicht erforderlich
- Negativabgrenzung – keine Auslagerung bei
  - Tätigkeit Dritte aufgrund Rechtsvorschriften (zB Abschlussprüfungen)
  - Marktinformationsdienste
  - Nutzung globaler Netzinfrastrukturen (zB Visa, Mastercard)
  - Dienstleistungen, die normalerweise nicht vom Institut erbracht werden (zB Erstellung Rechtsgutachten; Beratung eines Architekten; nicht: IT Services per se)

Anwendungsbereich

Unterscheidung – unwesentliche und wesentliche Auslagerung

- Anzeigepflicht bei kritischer (wesentlicher) Auslagerung
- Abgrenzung schwierig; entscheidende Parameter:
  - unzureichende oder unterlassene Wahrnehmung führt zu wesentlicher Beeinträchtigung der:
    - kontinuierlichen Einhaltung der Zulassungsbedingungen bzw (regulatorischen) Pflichten
    - finanziellen Ergebnisse
    - Solidität oder Kontinuität der Bank- und Zahlungsdienste und –geschäfte
  - Auslagerung operationeller Aufgaben von internen Kontrollfunktionen
    - außer unzureichende Wahrnehmung zieht keine negativen Folgen nach sich
  - Auslagerung von Funktionen des Bankgeschäfts oder Zahlungsdienste
    - wenn Zulassung der zuständigen Behörde erforderlich

Abgrenzung in der Praxis

- wichtige Faktoren zur Einordnung wesentlicher Auslagerungen
  - unmittelbarer Zusammenhang mit Erbringung von Bankgeschäften und Zahlungsdiensten
  - Auswirkung einer Störung der ausgelagerten Funktion
    - Finanzielle Widerstandsfähigkeit und Tragfähigkeit
    - Geschäftsfortführung
    - Operationelles und Reputationsrisiko
    - Sanierungs- und Abwicklungsplanung; Fortführung des Geschäftsbetriebs
  - Potentielle Auswirkungen der Auslagerung
  - Folgen für die Kunden
  - Größe und Komplexität des Geschäftsbetriebs
  - Möglichkeit der (raschen) Wiedereingliederung (Insourcing)
  - Schutz der Daten und Folgen einer Verletzung

EBA Guidelines

Allgemeine Pflichten vor Auslagerung

- Angemessenheit und Anwendung im Konzern
  - risikobasierter Ansatz für unterschiedliche Funktionen
  - wesentliche oder kritische Funktionen strenger beurteilt
- Rahmen für Governance
  - umfassendes Risikomanagement
  - keine Auslagerung der Management Verantwortung
  - klare Verantwortlichkeiten
  - ausreichend finanzielle Mittel für Compliance
  - effektive Aufsichtsbefugnisse und Dokumentationsanforderungen
  - Auslagerungsrichtlinien
  - Interne Revision
  - **Berücksichtigung von Interessenkonflikten**

EBA Guidelines

Allgemeine Pflichten vor Auslagerung

- Bewertung der bestehenden Auslagerungsvereinbarungen
  - Auslagerung oder nicht? (zB Netzwerkinfrastruktur)
  - Dokumentation: kritische oder wesentliche Vereinbarungen? (Beeinträchtigung des Tagesgeschäfts, Finanzausstattung, Verstöße gegen Aufsichtsrecht etc)
- Auslagerungsprozess
  - Analyse der Auslagerung
  - Benachrichtigungserfordernis der Aufsichtsbehörde
    - Auslagerung kritischer oder wesentliche Funktionen
  - Risikobewertung und Due Diligence bei Auswahl des Dienstleister
  - Implementierung der vorgegebenen Vertragsinhalte
- Leitlinie für zuständige Aussichtsbehörden

EBA Guidelines

Neue Verpflichtungen

- Dokumentation aller Auslagerungen ("Auslagerungsverzeichnis")
- Identifikation von wesentlichen oder kritischen Funktionen
- Benachrichtigung von Aufsichtsbehörden
- Dokumentierter Due Diligence Prozess bei Auswahl Provider
- Verbindliche Vertragsklauseln (inkl Exit Strategie)

→ **zwingender Verhandlungsbedarf in der Praxis**

EBA Guidelines – Implementierung in der Praxis

Zwingende vertragliche Bestandteile

- **klare Beschreibung der ausgelagerten Funktionen**
- Start und Enddatum der Vereinbarung
- anwendbares Recht & Speicherort der Daten
- **Zulässigkeit von Weiterverlagerungen (Sub-Auslagerung)?**
  - Kontrolle bei Weiterverlagerung
  - Verpflichtung zur Überbindung des gesamten Vertrages
- Sicherung Verfügbarkeit, Integrität, Vertraulichkeit und Sicherheit der ausgelagerten Daten
- **Monitoring und Auditrechte**
- **Service Level**
  - Sollen Steuerung ermöglichen

EBA Guidelines – Implementierung in der Praxis

Zwingende vertragliche Bestandteile

- Reporting Verpflichtungen Provider über relevante Änderungen der Rahmenbedingungen
- Verpflichtung zur Implementierung und Testung von Notfallplänen
- Vorkehrungen für eine Insolvenz des Providers (insb Zugriffsrechte)
- **Verpflichtung zu Kooperation mit Aufsichtsbehörden**
- **besondere Beendigungsrechte**
  - Beendigungsunterstützung
  - Nachwirkung
- Sofern anwendbar: Vorgaben über den Abschluss einer Versicherung und entsprechende Deckungshöhe

EBA Guidelines – Implementierung in der Praxis

Sonderthema Subauslagerung

- Dokumentation der Weiterverlagerung
- **Schriftliche Zustimmung**
- Ausschluss besonders kritischer oder wesentlicher Funktionen
- **Überbindung Gesamtvertrag**
- Aufsichtspflichten (insb für primären Provider)
- Informationspflichten über wesentliche Änderungen
- Widerspruchs- und Beendigungsrechte insb bei Veränderungen des Risikoprofils
- Audit Rechte auch bei Weiterverlagerungen

Schutz und Sicherheit

- Zusicherung angemessener Sicherheitsstandards im Hinblick auf IT
- Definition von Sicherheitsanforderungen
  - laufendes Monitoring der Anforderungen
- risikobasierter Ansatz hinsichtlich geographischer Aspekte der ausgelagerten Funktion (insb Speicherort)
  - EuGH E Max Schrems II
- angemessene und effektive Geheimhaltungsklauseln

EBA Guidelines – Implementierung in der Praxis

Zutritts-, Informations- und Auditrechte

Bei **kritischen oder wesentlichen** Funktionen

- **Vereinbarung eines unbeschränkten Auditrechts**
  - Eine dauerhafte Auslagerung der Auditrechte ist nicht möglich!

- unbeschränkter Zugriff auf Betriebsgelände, inkl IT-Infrastruktur mit entsprechender Vorlaufzeit

Zutritts-, Informations- und Auditrechte

Bei allen anderen Funktionen

- risikobasierter Ansatz
  - mögliche Auswirkungen auf operative Ebene, Ruf, Skalierbarkeit, Performance des Kreditinstituts.
- Achtung: Funktionen können auch nachträglich kritisch werden
- Pool-Audits bzw Zertifizierungen unter besonderen Voraussetzungen
  - richtiger Scope (Key Systems bzw passend zur ausgelagerten Funktion)
  - gründliche Prüfung der Audits Reports
  - Eignung der Auditgesellschaft (Rotation, Expertise etc)
  - Audits basierend auf Branchenstandards (zB ISO)
  - vertragliches Recht auf anlassbezogene Erweiterung des Audit-Scopes
  - Recht auf individuelle Audits für wesentliche oder kritische Funktionen

EBA Guidelines – Implementierung in der Praxis

Zutritts-, Informations- und Auditrechte

- Durchführung von Penetration Tests
- zeitgerechte Ankündigung
- besondere Sicherheitsvorkehrungen für Multi-Client Environments
- angemessene technische Kenntnisse bei den Mitarbeitern des auditierten Unternehmens

Sonderkündigungsrechte

- Verstoß gegen geltendes Recht durch Dienstleister
- Funktionseinbußen
- maßgebliche Änderungen betreffend die Out-Sourcing Vereinbarung oder den Dienstleister
- Mängel im Hinblick auf Datensicherheit
- Anweisung der zuständigen Behörde
- Weitergabe oder Re-Integration der Funktion im Rahmen der Beendigung (Übergangsperioden, Kooperationsverpflichtungen für Service Provider)

EBA Guidelines – Inhouse Pflichten

Exit Strategien

- Auslagerungsrichtlinien und Geschäftsfortführungspläne
- dokumentierte Exit Strategie für den Fall von
  - Beendigung der Auslagerungsvereinbarung
  - Ausfall des Dienstleisters
  - Abfall der Qualität der Services bzw konkrete Unterbrechungen
  - materielle Risiken für die angemessene und dauerhafte Anwendung der Funktion
- Zielsetzung: Beendigung der Auslagerungsvereinbarung ohne
  - Störung des Geschäftsbetriebs
  - Beeinträchtigung von Compliance und
  - Beeinträchtigung der Kontinuität und Qualität der Erbringung von Dienstleistungen.

Exkurs – Was gibt es noch?

ESMA Leitlinien für Cloud Service Provider

- European Securities and Markets Authority (ESMA)
  - für die Auslagerung an Cloud Service Provider
- Komplexer, aber viele inhaltliche Parallelen
- Zusätzliche Anforderungen:
  - tiefergreifendere und genauere Pre-Outsourcing Analyse
    - inkl Wiederholung der Due-Diligence bei Nachlassen der Leistung
  - zusätzliche Bestimmungen für Incident-Management
    - insb Meldung bei Vorfällen
  - Meldung an Aufsichtsbehörde bei Auslagerung von wichtigen und kritischen Funktionen in die Cloud
  - erweiterte Zugriffs- und Auditrechte

Planung

- Am Beginn steht die interne Outsourcing Policy …
  - Darstellung des allgemeinen Auslagerungsansatzes
  - Eckpunkte der Erstellung konkreter Auslagerungsstrategien
  - Darstellung des einzuhaltenden Auslagerungsprozesses
  - Darstellung der Anforderungen an Auslagerungsverträge
- … dann kommt der Outsourcing-Vertrag:
  - Prüfung der Eignung des Dienstleisters (Due Diligence)
  - wechselseitige geschäftliche Verpflichtungen klar vereinbaren
  - regelmäßige Kontrollen, zB Jour Fixe mit Dienstleister und laufende Berichte

Praxistipps

Awareness schaffen

- Ergänzungs- und Überarbeitungsbedarf
  - Vertragsmuster des Anbieters bildet in der Praxis oft weder aufsichts- noch datenschutzrechtliche Besonderheiten ab
  - zusammengehörige Verträge gemeinsam verhandeln
- klare Bestimmungen, bewährtes Wording
  - Vertragsaufbau
  - Themen klar angesprochen
  - **WICHTIG**: Frühzeitig erkennen und Verständnis schaffen!
- gilt auch für Intra-Group Verträge
  - gleicher Sorgfaltsmaßstab

Praxistipps

Stolpersteine

- unterschiedliche Auslegung der Definitionen
  - Institut vs Dienstleister
  - Was ist kritisch und wesentlich?
  - Institute vorsichtiger → weite Auslegung
- Entwicklung zum Marktstandard
  - Auch in sonstigen Branchen
- Überbindung von regulatorischen Anforderungen
  - BWG, WAG, VAG, BörseG, etc
  - Provider meist zurückhaltend
    - Argument: nicht direkt auf den Dienstleister anwendbar
    - Gegenargument: genau deshalb ist dies vertraglich zu überbinden

Dr Axel Anderl, LLM

DORDA Rechtsanwälte GmbH

T: +43 1 533 47 95 – 23

E: axel.anderl@dorda.at

Dr Stephan Winklbauer, LLM

aringer herbst winklbauer rechtsanwälte

T: +43 1 890 90 17 – 0

E: winklbauer@ahwlaw.at