

AUSLAGERUNG VON IT-DIENSTLEISTUNGEN

Dr. Oliver Völkel, LL.M.
Bryan Hollmann, Esq., LL.M.
Andreas Pfeil, LL.M.

15. Mai 2019

STADLER VÖLKE
RECHTSANWÄLTE • ATTORNEYS AT LAW

Seilerstätte 24
1010 Wien

+43 (1) 997 1025

office@svlaw.at

VORSTELLUNG

- Vortragende
- Kanzlei (u.a.)
 - Banking, Finance, Capital Markets
 - Data Protection, Privacy
 - FinTech
 - Blockchain-Technology, Virtual Currencies
- Schlagwort IT-Sicherheit
- Bottom-Up Approach



AGENDA

– Bryan Hollmann

– Overview: EBA Guidelines on Outsourcing Arrangements 2019 (EN)

– Andreas Pfeil

– Auslagerung von IT-Dienstleistungen in Österreich (DE)

– Oliver Völkel

– Ausgewählte Fragen im Zusammenhang mit den EBA Guidelines, Q&A (DE)

Overview: EBA Guidelines on Outsourcing Arrangements 2019

OVERVIEW

- Published 25 February 2019
- Enters into force 30 September 2019
- Applies to credit institutions and investment firms (CRR), payment institutions (PSD2) and electronic money institutions (E-Money Directive)
- Main sections:
 - Assessment (Title II)
 - Governance framework (Title III)
 - Outsourcing process (Title IV)
- *Principle of proportionality

ASSESSMENT

What is outsourcing?

– Outsourcing: *"an arrangement of any form between an institution . . . and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution . . . itself."*

Not outsourcing:

- Statutory audit
- Market information services (Bloomberg, Moody's, Standard & Poor's, Fitch)
- Global network infrastructures (Visa, Mastercard)
- Correspondent banking services
- Legal representation

Outsourcing:

- IT services
- Cloud services
- Compliance
- Workplace management
- Etc.

CRITICAL OR IMPORTANT FUNCTIONS

What is a critical or important function?

Defect or failure in performance would materially impair:

- Authorization and regulatory obligations;
- Financial performance; or
- Soundness or continuity of banking and payment services and activities.

Examples:

- IT and data services
- Investment of assets / portfolio management
- Ongoing compliance, internal audit

GOVERNANCE FRAMEWORK

"holistic"

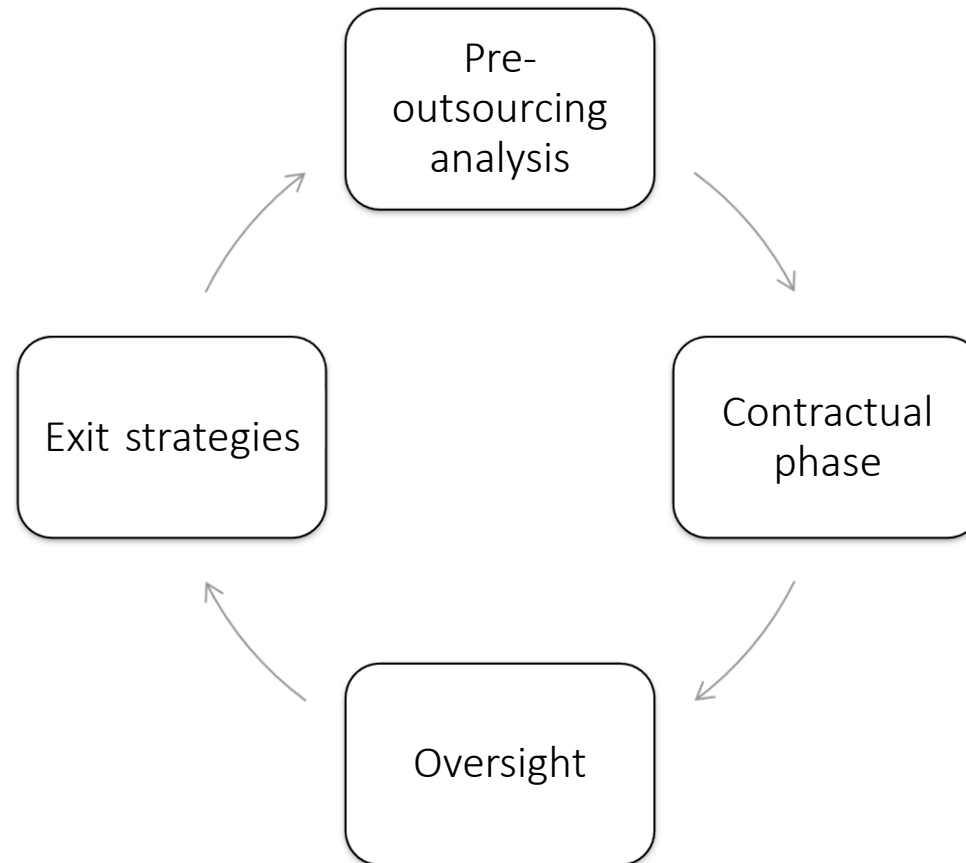
"institution-wide"

"extending across all business lines and internal units."

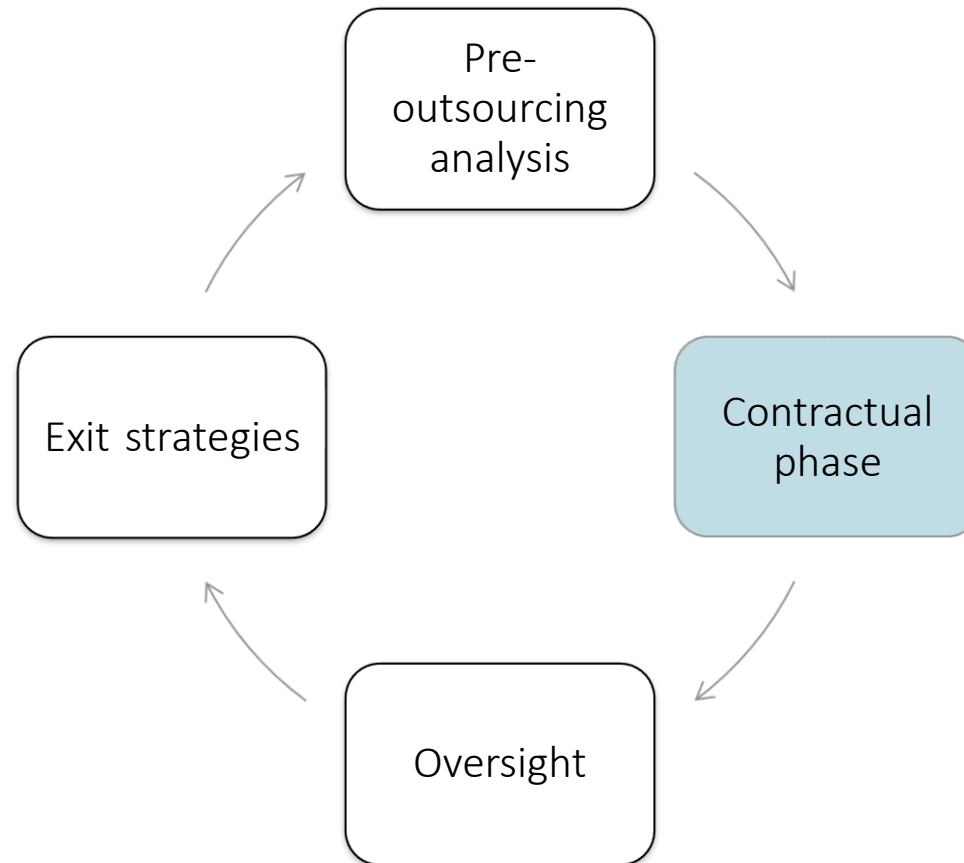
Key considerations:

- No delegation of the management body's responsibilities;
- Clear assignment of responsibilities;
- Written outsourcing policy;
- Register of outsourcing arrangements;
- No 'empty shells' or 'letter-box' entities.

OUTSOURCING PROCESS



OUTSOURCING PROCESS



CONTRACTUAL PHASE

Critical contractual terms

Sub-outsourcing of critical or important functions

Termination rights

IMPLEMENTATION

30 September 2019: entry into force.

31 December 2021: documentation deadline.

- Obligation to inform competent authority if not finalized.

Auslagerung von IT-Dienstleistungen in Österreich

NATIONALE NORMEN

§ 25 BWG:

- (1) Wesentliche bankbetriebliche Aufgaben (Vorkehrungen gemäß Anlage); Auslagerung darf die Qualität der internen Kontrolle des Kreditinstituts nicht beeinträchtigen
- (2) Auslagerung darf nicht:
 - zu einer Delegation der Aufgaben der Geschäftsleitung führen;
 - das Verhältnis und die Pflichten des Kreditinstituts gegenüber seinen Geschäftspartnern und Kunden gemäß BWG verändern;
 - die Einhaltung der in § 69 BWG genannten Bestimmungen behindern oder erschweren und
 - zu einem Entfall oder einer Veränderung der übrigen Voraussetzungen, unter denen dem Kreditinstitut die Konzession erteilt wurde, führen.

§ 21 ZaDiG 2018

DEFINITION I

- Keine nationale Legaldefinition vorhanden
- FMA verweist im Leitfaden IKT-Sicherheit auf CEBS Guidelines
- EBA Guidelines ersetzen CEBS Guidelines
- CEBS Guidelines sind EU *soft law* mit keiner verbindlichen Rechtsqualität
- Seit 2010 sind Kreditinstitute durch EBA-Verordnung angehalten die EBA Guidelines einzuhalten

DEFINITION II

Die EBA versteht unter Outsourcing:

Eine Vereinbarung zwischen einem Institut, einem Zahlungsinstitut oder einem E-Geld-Institut und einem Dienstleister, aufgrund derer dieser Dienstleister einen Prozess, eine Dienstleistung oder eine Tätigkeit ausführt, die ansonsten von dem Institut, dem Zahlungsinstitut oder dem E-Geld-Institut selbst durchgeführt werden müsste.

TATBESTANDSMERKMALE AUSLAGERUNG

- [...] eine Tätigkeit ausführt, die ansonsten von dem Institut, [...] selbst durchgeführt werden müsste.*

* Abschließende Definition

TATBESTANDSMERKMALE EINKAUF I

- Abgrenzungshilfe des Einkaufes der CEBS-Guidelines wurde in den EBA-Guidelines gestrichen, kann aber als nützliche Auslegungshilfe herangezogen werden
- CEBS-Definition Einkauf:

*Unter anderem die Lieferung (i) von Dienstleistungen, Waren oder Einrichtungen, **ohne** dass der Lieferant **Kontrolle über Informationen** über das einkaufende Institut oder über dem Institut gehörende Informationen erhält, **oder** (ii) von **genormten Produkten**, z.B. Marktinformationen oder Büroinventar. (Konzessionierte Rechtsträger sollten sicherstellen, dass ihre Einkäufe zweckdienlich sind.) Die Lieferung von (i) oder (ii) ist kein Outsourcing.**

*Keine abschließende Definition somit kann im Zweifel eher von einem Einkauf ausgegangen werden

TATBESTANDSMERKMALE EINKAUF II

- Definition eröffnet Interpretationsspielraum:
 - Welche Informationen darf der Dienstleister nicht erhalten?
 - Welche Kontrollmöglichkeit des Dienstleisters muss gegeben sein?
 - Was ist unter einem Standardprodukt (*genormtes Produkt*) zu verstehen?

OUTSOURCING I

- Ein Outsourcing liegt dann vor wenn:
 - a) kein Einkauf vorliegt und **b)** die Tatbestandsmerkmale der Definition des Outsourcings erfüllt sind,
 - **1)** Prozess, Dienstleistung oder **Tätigkeit**:
 - mehr als Hilfstätigkeit
 - betriebliche Tätigkeit die vom Unternehmensgegenstand sowie den in § 1 BWG genannten Bankgeschäften umfasst sind
 - eigenständige bankenbetrieblich-operationelle Tätigkeit (§ 25 (1) BWG)

OUTSOURCING II

- Ein Outsourcing liegt dann vor wenn:
 - a) kein Einkauf vorliegt und **b)** die Tatbestandsmerkmale der Definition des Outsourcings erfüllt sind,
 - 1) Prozess, Dienstleistung oder Tätigkeit, **2)** die ansonsten das Institut **selbst durchführen müsste**
 - Ist eine "Auslagerung" von zuvor intern nicht erbrachten Tätigkeiten überhaupt eine tatbestandsmäßige Auslagerung?
 - Wäre die interne Erbringung der Tätigkeit überhaupt rechtlich zulässig?
 - Liegt eine tatbestandsmäßige Auslagerung vor, wenn das Institut die Tätigkeit selbst ausüben dürfte, diese jedoch aufgrund des wirtschaftlich oder technischen Umfanges üblicherweise nicht von Instituten durchgeführt werden?
 - Würde die Tätigkeit überhaupt intern vom Institut (ohne Auslagerung) durchgeführt werden?

IT-OUTSOURCING

- Operationelles Risiko nach § 39 Abs 2b Z 5 BWG
- Proportionalitätsgrundsatz zu beachten
- Standardprodukt oder Individualisierung?
- Laut FMA ist es ausreichend, wenn Kreditinstitute den "*branchentypischen Standardvorgehensweisen zur Informationssicherheit und dem Stand der Informationssicherheit*" entsprechen
- Eigenentwicklung ist kein Outsourcing

PRAXIS

- Durchführung einer vorgelagerten und Prüfung ob überhaupt Outsourcing vorliegt
- Im Zweifelsfall Anzeige an die FMA erstatten
- Interne Strukturen (unter anderem) zur Überwachung der Outsourcing-Dienstleister und deren Tätigkeit schaffen
- Bestehende Outsourcing-Verträge prüfen und diese gegebenenfalls bis spätestens Ende 2021 entsprechend den neuen EBA-Guidelines adaptieren
- IT-Sicherheit als Prüfungsschwerpunkt der FMA für das Jahr 2019 beachten

Ausgewählte Fragen im Zusammenhang mit den EBA Guidelines

BACKGROUND I

24. “[...] Institutions need to consider that receiving services, including IT services, from third parties creates risks, even when those arrangements are not considered to be outsourcing arrangements [...].”

31. “[...] guidelines provide some requirements that apply [...] to all arrangements with third parties, taking into account the application of the proportionality principle.

i.V.m. Prüfungsschwerpunkt der FMA für 2019 „IT-Sicherheit“

Wir empfehlen Prüfung auch bisher allenfalls wenig beachteter Bereiche

–u.a. Auswahl von Hardware und Standardsoftware, Mensch als Teil der IT-Sicherheit, Sicherheit von Standard-Diensten (Internet, Verschlüsselung), Damage Control

BACKGROUND II

27. “[...] Without prejudice to the waivers [...], intragroup outsourcing is subject to the same regulatory framework as outsourcing to service providers outside the group.”

Anordnung grs. eindeutig: Gleiche Anforderungen, sowohl hinsichtlich Auswahl, Vertragsgestaltung, und technischer Einschätzung.

Proportionalitätsgrundsatz

BACKGROUND III

37. “Institutions [...] must ensure that personal data are adequately protected and kept confidential. Institutions and payment institutions fall within the scope of application of [the GDPR] and must comply with it. [...]”

Datenschutz als leitendes Prinzip in allen IT-Prozessen mitüberlegen

Einsatz von E-Mail, Verschlüsselung auf Hardware-Ebene, etc

BACKGROUND IV

44. “It is of particular importance that competent authorities have a comprehensive overview of the outsourcing arrangements of institutions [...]. Institutions [...] should therefore document all their outsourcing arrangements. In addition, institutions [...] should inform competent authorities or engage with competent authorities in a dialogue regarding planned outsourcing arrangements, in particular with regard to critical or important functions.”

Abstimmung mit der Aufsicht nie verkehrt.

AUSGEWÄHLTE ASPEKTE I

14. “Institutions [...] should review and amend accordingly existing outsourcing arrangements with a view to ensuring that these are compliant with these guidelines.”
16. “Institutions [...] should complete the documentation of all existing outsourcing arrangements, other than for outsourcing arrangements to cloud service providers, in line with these guidelines following the first renewal date of each existing outsourcing arrangement, but by no later than 31 December 2021.”
- Klare Zuständigkeit festlegen
 - Prüfprozess definieren
 - Interdisziplinär agieren (allenfalls Arbeitsgruppe)

AUSGEWÄHLTE ASPEKTE II

26. “Institutions and payment institutions should establish whether an arrangement with a third party falls under the definition of outsourcing.”
41. “The management body of an institution [...] that has outsourcing arrangements in place or plans on entering into such arrangements should approve, regularly review and update a written outsourcing policy and ensure its implementation [...].”
- Berücksichtigen der Eckpunkte für die Outsourcing Policy

AUSGEWÄHLTE ASPEKTE III

52. “As part of their risk management framework, institutions [..] should maintain an updated register of information on all outsourcing arrangements at the institution [...] and should appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements.”

– Berücksichtigen der Eckpunkte für das Outsourcing Register

AUSGEWÄHLTE ASPEKTE IV

98. “The outsourcing arrangement should expressly allow the possibility for the institution [...] to terminate the arrangement, in accordance with applicable law, including in the following situations:
[...]”

– Berücksichtigen der Eckpunkte für die Prüfung bestehender Verträge

AUSGEWÄHLTE ASPEKTE V

61. “Before entering into any outsourcing arrangement, institutions [...] should:
- a. assess if the outsourcing arrangement concerns a critical or important function, as set out in Title II;
 - b. assess if the supervisory conditions for outsourcing set out in Section 12.1 are met;
 - c. identify and assess all of the relevant risks of the outsourcing arrangement in accordance with Section 12.2;
 - d. undertake appropriate due diligence on the prospective service provider in accordance with Section 12.3;
 - e. identify and assess conflicts of interest that the outsourcing may cause in line with Section 8.”

STADLER VÖLKE
RECHTSANWÄLTE • ATTORNEYS AT LAW

Dr. Oliver Völkel, LL.M.
oliver.voelkel@svlaw.at

Bryan Hollmann, Esq., LL.M.
bryan.hollmann@svlaw.at

Andreas Pfeil, LL.M.
andreas.pfeil@svlaw.at