Branchenstandard für das Auslagerungsmanagement

A. Präambel

Der Verband deutscher Kreditplattformen und die ihm angeschlossenen Mitglieder stehen für die professionelle, integre und transparente Betreibung ihrer Marktplätze sowie die Erfüllung höchster Qualitätsstandards im Interesse von Schuldnern, Investoren und Geschäftspartnern. Mit der Verabschiedung der „Allgemeinen Verbandsgrundsätze und Verhaltensregeln“ durch die Mitgliederversammlung am 04.06.2019 wurde dieser Selbstanspruch kodifiziert. Satzungsgemäß verpflichtet sich jedes Ordentliche Mitglied zur Einhaltung dieser Grundsätze und Regeln.

Per Vorstandsbeschluss vom 29.05.2020 wurde entschieden, diese durch die Entwicklung von Einzelstandards zu konkretisieren und damit Maßstäbe für die gesamte Branche zu setzen. Die Kompetenz zur Annahme als „Branchenstandards“ liegt bei der Mitgliederversammlung.

Gegenstand des vorliegenden Standards ist die Konkretisierung des Abschnitts II/1/B der Allgemeinen Verbandsgrundsätze und Verhaltensregeln. Dieser lautet:

> B.
>
> Die Mitglieder tragen dafür Sorge, dass interne Kontrollsysteme für ein effektives Risikomanagement vorhanden sind und diese verlässlich arbeiten.

Ziel des Standards ist die Entwicklung und Förderung eines branchenweiten Verständnisses für die Qualität der Steuerung und internen Kontrolle von ausgelagerten Aktivitäten und Prozessen.

Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung verschiedener Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

B. Definitionen

I. Auslagerung: Auslagerung ist die Beauftragung eines Dritten zur Wahrnehmung von Aufgaben, die im direkten Zusammenhang mit der Durchführung der Hauptgeschäftstätigkeit des Mitglieds stehen und ebenso von diesem selbst erbracht werden könnten.

II. wesentliche Auslagerung: Wesentlich ist eine Auslagerung in Abgrenzung zur einfachen Auslagerung, wenn deren unzureichende oder unterlassene Durchführung die Einhaltung von Gesetzen, die finanzielle Leistungsfähigkeit oder auch die Solidität bzw. Kontinuität der Hauptgeschäftstätigkeit erheblich beeinträchtigen würde.

III. sonstiger Fremdbezug: Das sind Aktivitäten durch Dritte, die mit der Wahrnehmung von Aufgaben beauftragt werden, die in keinem direkten Zusammenhang mit der Durchführung der Hauptgeschäftstätigkeit des Mitglieds stehen.

C. Verbandsgrundsatz für das Auslagerungsmanagement (Allgemeiner Teil)

Abhängig von Art, Umfang, Komplexität und Risikogehalt einer Auslagerung von Aktivitäten auf Dritte, die für die Durchführung von bestimmten Aspekten der Hauptgeschäftstätigkeit beauftragt werden, hat das Mitglied angemessene Vorkehrungen zu treffen, um zusätzliche mit der Auslagerung verbundene Risiken zu vermeiden. Sie darf weder die ordnungsgemäße Durchführung der Geschäfte noch die Geschäftsorganisation des Mitglieds beeinträchtigen. Als Teil einer gesunden Risikokultur trägt ein professionelles Auslagerungsmanagement zur Weiterentwicklung des eigenen Unternehmens und der gesamten Branche bei.

Das Mitglied soll auf der Grundlage einer nachvollziehbaren Analyse die für eine Auslagerung relevanten Prozesse und die mit ihnen jeweils verbundenen Risiken identifizieren. Im Anschluss sind diese als wesentlich oder unwesentlich zu bewerten. Die Risikoanalyse ist in angemessenen Abständen, jedoch mindestens einmal jährlich, oder anlassbezogen durchzuführen.

Insbesondere in den Blick genommen werden sollen neben finanziellen, operationellen, rechtlichen, (geo-) politischen und reputierlichen Risiken auch der Datenschutz und Cyber Risks. Ebenso Berücksichtigung finden soll die Konzentration von Risiken für den Fall, dass mehrere Aspekte der Hauptgeschäftstätigkeit an einen einzelnen Dritten ausgelagert werden.

Die von einer Auslagerung tangierten Organisationseinheiten sind in den Prozess der Identifikation einzubinden, jedoch nicht in die Bewertung.

Bei der geplanten Nutzung von Cloud-Diensten ist zusätzlich ein Augenmerk auf die mit der Migration verbundenen Risiken und ihre Überwachung zu legen.

Die Speicherung von personenbezogenen Daten in der Cloud muss unter Berücksichtigung des einschlägigen Datenschutzrechts erfolgen.

Die Ergebnisse von Risikoanalysen sollen in das vom Compliance-Beauftragten alle zwei Jahre durchzuführende Compliance Risk Assessment einfließen. Weitere Einzelheiten zum Compliance-Beauftragten sind dem Branchenstandard für die Compliance-Organisation zu entnehmen.

Es darf die Unterscheidung zwischen Auslagerungsaktivitäten im Zusammenhang mit der Hauptgeschäftstätigkeit (Auslagerung) und sonstigem Fremdbezug getroffen werden. Letzterer unterliegt nicht direkt den in diesem Branchenstandard beschriebenen Vorgaben für das Auslagerungsmanagement. Da Fremdbezug jedoch auch risikobehaftet sein kann, ist dieser jedenfalls unter dem allgemeinen Gesichtspunkt der Ordnungsgemäßheit des Geschäftsbetriebes zu überwachen.

D. Verbandsgrundsatz für das Auslagerungsmanagement (Besonderer Teil)

Bei der Umsetzung des Verbandsgrundsatzes sind im Einzelnen folgende Anforderungen zu beachten:

I. Prozesse und Auslagerungsvertrag

Die Mitglieder haben alle angemessenen organisatorischen und vertraglichen Vorkehrungen zu treffen, um Risiken zu vermeiden, die durch Auslagerungen entstehen können. Ziel ist eine verantwortliche und effiziente Organisation des Auslagerungsmanagements. Hierfür sind die Grundsätze und Verfahren, das Berichtswesen sowie die Kontrollen durch Prozessanweisungen so umfassend zu beschreiben, dass ihre harmonische Wirksamkeit gewährleistet ist. Sie sind deshalb mit der bestehenden internen Prozesslandschaft auf Friktionen hin zu überprüfen.

Insbesondere bei wesentlichen Auslagerungen ist im Auslagerungsvertrag mit dem Dritten sicherzustellen, dass die Informations- und Überwachungsmöglichkeiten des Mitglieds in keiner Weise eingeschränkt werden.

Der Fall der Beendigung einer Auslagerungsvereinbarung ist durch die Vereinbarung von ordentlichen und außerordentlichen Kündigungsmöglichkeiten ausdrücklich zu regeln. Auch ist der Notfall zu adressieren. Es sind vertragliche und interne prozessuale Vorkehrungen zu treffen, die die Kontinuität des ordnungsgemäßen Geschäftsbetriebs sicherstellen. Die Handlungsoptionen sind regelmäßig und anlassbezogen zu überprüfen.

II. Weiterverlagerung

Verlagert der Dritte seinerseits weiter auf andere Parteien (Subunternehmer), ändert das nichts an der Letztverantwortlichkeit des Mitglieds für die Steuerung und Überwachung aller mit der Auslagerungskette verbundenen Risiken. Das Mitglied soll für die Fälle, in denen die Weiterverlagerung von Aktivitäten erfolgt, die als wesentliche Auslagerung eingestuft werden, in dem Vertrag mit dem Dritten sicherstellen, dass die Beauftragung von Subunternehmern mindestens dem gleichen Steuerungs- und Kontrollniveau unterliegt wie die Erstauslagerung. Einschränkungen, insbesondere solche, nach der nur ähnliche Verpflichtungen oder etwa gestufte Berichts- und Überwachungsverfahren in den Vertrag mit dem Subunternehmer übernommen werden, sind unzulässig.

Bei der Weiterverlagerung gelten die gleichen inhaltlichen Anforderungen an den Vertrag, wie sie oben unter Punkt D.I. im Zusammenhang mit der Erstauslagerung genannt sind.

III. Organisation und Überwachung

Für die Umsetzung und Überwachung des Auslagerungsmanagements trägt die Geschäftsleitung die Gesamtverantwortung. Sie kann sich von einem zentralen Auslagerungsmanager unterstützen lassen. Die Aufgabe kann sie auch dem Compliance-Beauftragten übergeben; weitere Einzelheiten zum Compliance-Beauftragten sind dem Branchenstandard für die Compliance-Organisation zu entnehmen. Der zentrale Auslagerungsmanager erhält die notwendigen Informationen von den mit der jeweiligen Auslagerung tangierten Organisationseinheiten. Hierzu können in der jeweiligen Organisationseinheit dezentrale Auslagerungsmanager bestimmt werden, die dem zentralen Auslagerungsmanager als direkter Ansprechpartner dienen.

Die Geschäftsleitung trägt Sorge dafür, dass im Unternehmen hinreichend Kenntnisse und Erfahrungen vorhanden sind, die eine wirksame Überwachung der von einem Dritten bzw. Subunternehmer konkret erbrachten Dienstleistungen erlauben.

Der Auslagerungsmanager trägt die Verantwortung dafür, dass ein der Art, dem Umfang und der Komplexität der konkreten Auslagerungsaktivitäten angemessenes System zur Überwachung implementiert und weiterentwickelt wird. Ein besonderes Augenmerk soll auf der Vermeidung von Interessenkonflikten liegen sowie auf einer vertraglich zu vereinbarenden Möglichkeit, Dritten und Subunternehmern ggf. Weisungen in Bezug auf die ausgelagerten Aktivitäten zu erteilen, um die wirksame Steuerung der Auslagerung (-skette) sicherzustellen.

Es ist ein elektronisch gestütztes System zur Erfassung, Bearbeitung und systematischen Auswertung von Auslagerungen sowie Auslagerungsketten (Auslagerungsregister) einzurichten und zu führen. Alle wesentlichen für die Überwachung relevanten Dokumente, Verfahrensschritte, Erkenntnisse und Bewertungen sind dort – geschützt vor dem unbefugten Zugriff Dritter – unverzüglich abzulegen. Das System ist gegen sachlich nicht gebotene Änderungen zu schützen, muss nachträgliche Änderungen oder Ergänzungen erkennen lassen und eine ungehinderte Einsichtnahme für den Auslagerungsmanager gewährleisten. Dem Compliance-Beauftragten ist auf Nachfrage uneingeschränkt Systemzugang zu gewähren.

Die gespeicherten Daten sind vorbehaltlich abweichender gesetzlicher Vorgaben mindestens fünf Jahre aufzubewahren.

E. Auslagerungsbericht

Der Auslagerungsmanager berichtet mindestens einmal jährlich sowie anlassbezogen in Textform an die Geschäftsleitung über seine Überwachungs- und Kontrollhandlungen (Auslagerungsbericht). Darin sind mindestens die folgenden Punkte aufzuführen:

- Darstellung aller Auslagerungen, jeweils einschließlich der Einordnung als einfache oder wesentliche Auslagerung (sonstiger Fremdbezug ist nicht aufzuführen)
- Darstellung und Bewertung, ob die vertraglich vereinbarte Qualität sowie die Leistungsziele (Service Level Agreements) erreicht wurden; Störungen sind hervorzuheben, ebenso ist der Ablauf zur Beseitigung durch den Support darzustellen.
- Bewertung, ob die ausgelagerten Aktivitäten und Prozesse angemessen gesteuert und überwacht werden konnten; jeder Mangel an Kooperation ist hervorzuheben und zu beschreiben.
- Erklärung, dass einschlägige datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen berücksichtigt wurden; Störungen sind hervorzuheben und der Ablauf zur Beseitigung ist darzustellen.
- Darstellung, ob risikomindernde Maßnahmen für die Zukunft ergriffen werden sollten.
- Jegliche Kontaktaufnahme mit oder durch Aufsichtsbehörden im Zusammenhang mit wesentlichen Auslagerungen ist im Detail darzustellen und zu erklären, ob die Fragen zur Zufriedenheit der Beamten abschließend geregelt werden konnten.

Die Geschäftsleitung hat einen förmlichen Beschluss über die Kenntnisnahme des Auslagerungsberichts zu fassen. Darüber hinaus sollte der Bericht auch dem Aufsichtsorgan übermittelt werden, wenn ein solches vorhanden ist.

F. Fortbildung des Auslagerungsbeauftragten; Schulung von Mitarbeitern

Alle Mitarbeiter werden anlassbezogen in den Grundsätzen und Verfahren des Auslagerungsmanagements beschult.

G. Kontrollen

Das Mitglied hat Pläne zur regelmäßigen Kontrolle der Einhaltung der Bestimmungen dieses Branchenstandards und legt die Aufgabenverteilung fest. Zur Gewährleistung der Wirksamkeit der Kontrolle ist sie durch den Compliance-Beauftragten durchzuführen. Die Ergebnisse können der Geschäftsleitung auch im Auslagerungsbericht dargestellt werden.

H. Key Performance und Risk Indikatoren

Das Mitglied entwickelt Key Performance Indikatoren (KPI) und Key Risk Indikatoren (KRI) zur regelmäßigen, risikobasierten Messung und Beurteilung der Leistung des Dritten bzw. eines Subunternehmers.

I. Abweichungen von den Bestimmungen dieses Branchenstandards

Von den Bestimmungen dieses Branchenstandards soll grundsätzlich nicht abgewichen werden. In begründeten Fällen sind Abweichungen jedoch ausnahmsweise möglich. Hierfür ist ein begründeter Antrag in Textform an den Vorstand zu richten. Die Entscheidung wird gemäß Satzung mit qualifizierter Mehrheit getroffen.

Einem Mitglied, dass das Gütesiegel verliehen bekommen hat, kann das Recht zum Tragen von der Mitgliederversammlung mit einfacher Mehrheit entzogen werden, wenn das Mitglied von den Bestimmungen dieses Branchenstandards abweicht, ohne zuvor die Geschäftsstelle über die Abweichungen rechtzeitig informiert zu haben.

I. Revisionsklausel

Dieser Branchenstandard ist im Abstand von zwei Jahren einer Revision durch den Ausschuss für Risiko- und Compliance-Management zu unterziehen. Allfällige Änderungen und/oder Ergänzungen verabschiedet die Mitgliederversammlung mit qualifizierter Mehrheit.