Deutsche Bank

Kontrollpflichten Dritter

Eine Nichteinhaltung von Bestimmungen in diesem Dokument kann zu Disziplinarmaßnahmen bis hin zur Kündigung führen. Bedenken in Bezug auf Verletzungen der Bestimmungen sind gemäß der „Richtlinie zur Äußerung von Bedenken (einschließlich Hinweisgeben) – Deutsche-Bank-Konzern" zu eskalieren.

Inhaltsverzeichnis

1. Einleitung

In diesem Dokument geht es um Hinweise zu den Kontrollpflichten für Dritte, die gegenüber der Deutschen Bank (DB) Dienstleistungen erbringen. Auch wenn vertragliche Vereinbarungen Vorrang haben, kann dieses Dokument von solchen Dritten als Referenzmaterial für die Art der Kontrollen herangezogen werden, die bei Risikobewertungen von Anbietern und Dienstleistungen sowohl beim Onboarding als auch in regelmäßigen Abständen während ihrer Arbeit für die DB zum Einsatz kommen.

1.1. Auslegung

Im Sinne dieses Dokuments versteht man unter einem Lieferanten, Anbieter oder externen Dienstleister einen Dritten, der einem Mitglied des Deutsche-Bank-Konzerns Produkte oder Dienstleistungen bereitstellt („Lieferant"), einschließlich seiner Eigentümer, leitenden Angestellten, Vorstandsmitglieder, Mitarbeiter, Berater, verbundenen Unternehmen, Auftragnehmer und Unterauftragnehmer, und jeder in diesem Dokument enthaltene Verweis auf Personal gilt für dessen eigenes Personal sowie für das Personal von jeglichen Unterauftragnehmern.

1.2. Anwendungsbereich

Dieses Dokument sollte als Vorgabe der DB erachtet werden, wenn ein Lieferant auf eine Aufforderung zur Angebotsabgabe antwortet oder auf ein sonstiges Angebot zur Lieferung von Waren an sowie zur Erbringung von Dienstleistungen für die Deutsche Bank reagiert. Von den Lieferanten wird erwartet, die in diesem Dokument festgelegten Kontrollpflichten einzurichten und deren Einhaltung in regelmäßigen Abständen weiter zu überwachen. Bei Widersprüchen zwischen diesem Dokument und jeglichen lokalen rechtlichen und regulatorischen Anforderungen bzw. jeglichen Vereinbarungen mit der Deutschen Bank haben die jeweils lokalen rechtlichen und regulatorischen Anforderungen bzw. die Vereinbarung Vorrang. Jeweils zu Beginn einer Zusammenarbeit mit der Deutschen Bank sollten die Lieferanten ihrem Personal, das mit dem Risikomanagement für die Waren und Dienstleistungen betraut ist, eine Kopie dieses Dokuments zur Verfügung stellen und sie entsprechend schulen. Hierzu sollte erwähnt werden, dass die Bereitstellung der in diesem Dokument beschriebenen Dokumentation an die DB im Rahmen des Risikomanagementprozesses für Dritte jeweils vom Risikoprofil der für die DB erbrachten Dienstleistung abhängig gemacht wird.

1.3. Compliance

Vorsorglich wird darauf hingewiesen, dass die Deutsche Bank stets von ihren Lieferanten verlangt, alle geltenden Gesetze und Vorschriften in den Ländern, in denen sie tätig sind, umfassend einzuhalten. Die Deutsche Bank erwartet von ihren Lieferanten, dass sie dieses Dokument ggf. auch im Rahmen der Zollgesetze und des lokalen Rechts des Landes beachten, in dem sie tätig sind. Die Lieferanten haben jegliche Bedenken oder vermuteten Verstöße gegen geltendes Recht oder Vorschriften, die mit der Deutschen Bank im Zusammenhang stehen, unverzüglich zu melden.

Obwohl dieses Dokument an sich nicht rechtsverbindlich sein soll, möchte die Deutsche Bank die Lieferanten in Bezug auf die bei ihr geltenden Risikomanagementstandards, deren Einhaltung von den Lieferanten erwartet wird, entsprechend sensibilisieren. Jegliche Nichteinhaltung dieser Kontrollpflichten

hat zur Folge, dass sich die Möglichkeiten für eine Zusammenarbeit mit der Deutschen Bank einschränken werden. Die zwischen der Deutschen Bank und den Lieferanten geltenden rechtlichen Verpflichtungen sind stets im Vertrag zwischen diesen Parteien zu finden.

1.4. Umsetzung

Die Deutsche Bank verlangt von ihren Lieferanten den Abschluss einer Vereinbarung über Verpflichtungen, mit denen sich die in diesem Dokument aufgeführten Kontrollpflichten erfüllen lassen. Vorsorglich wird darauf hingewiesen, dass dieses Dokument weder eine vollständige noch eine abschließende Liste der zu erfüllenden Anforderungen enthält. Die Deutsche Bank wird durch dieses Dokument auch nicht daran gehindert oder in ihrem Recht eingeschränkt, zusätzliche Risiken zu ermitteln und die Einhaltung zusätzlicher Pflichten einzufordern.

Lieferanten haben am Lieferantenrisikomanagement-Prozess der Deutschen Bank teilzunehmen und Nachweise über die bei ihnen geltenden Kontrollpflichten vorzulegen, die den in diesem Dokument dargelegten Anforderungen entsprechen.

2. Bekämpfung der Wirtschaftskriminalität (Anti-Financial Crime, AFC)

Je nach Faktoren wie der Art des Lieferanten und den von ihm erbrachten Dienstleistungen können zur Minderung des Risikos finanzieller Straftaten, das im Rahmen des bei der DB durchgeführten Risikobewertungsprozesses für Dritte ermittelt wurde, folgende Kontrollen zur Anwendung kommen.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Verhaltenskodex (Code of Business Conduct)	Der Lieferant verpflichtet sich, seine Geschäfte nach rechtlichen und ethischen Grundsätzen zu führen, die in den Richtlinien bzw. dem Verhaltenskodex des Lieferanten niedergelegt sind.
Richtlinie zur Bekämpfung der Wirtschaftskriminalität (Anti-Financial Crime Policy)	Beim Lieferanten gilt ein Verbot für die Beteiligung an Finanzkriminalität, einschließlich Bestechung und Korruption, Geldwäsche, Terrorismusfinanzierung und Proliferationsfinanzierung und von ihm werden die Sanktionsvorschriften und -anforderungen erfüllt, die in den Richtlinien oder dem Verhaltenskodex des Lieferanten dargelegt sind.
Anonyme Meldung von Verstößen	In der Richtlinie des Lieferanten sollten zumindest Kanäle genannt sein, über die seine Mitarbeiter anonym Bedenken hinsichtlich vermuteter oder tatsächlicher Verstöße gegen Gesetze, Vorschriften, Unternehmensrichtlinien oder Fehlverhalten äußern können, und die ihnen die Möglichkeit eröffnen, solche Bedenken zu äußern und vermutete oder tatsächliche Verstöße gegen Gesetze, Vorschriften, Unternehmensrichtlinien oder Fehlverhalten von Mitarbeitern anonym zu melden.
Schulung zur Bekämpfung der Wirtschaftskriminalität	Zur Gewährleistung, dass die Mitarbeiter alle geltenden Verpflichtungen in Bezug auf Bestechungs- und Korruptionsbekämpfung, Schutz vor Betrug und Geldwäsche, Bekämpfung von Steuerhinterziehung und Sanktionen sowie die Kanäle zur Meldung von jeglichen Missständen kennen, über die sie ihre Bedenken anonym äußern können, haben die

	AFC-Schulungen der Lieferanten solche Themen zu umfassen. Damit soll sichergestellt werden, dass die Mitarbeiter Finanzkriminalität erkennen und verhindern können und wissen, an wen sie sich ggf. wenden können.
Bekämpfung der Ermöglichung von Steuerhinterziehung	Zur Minderung des Risikos der Steuerhinterziehung ist in den Richtlinien des Lieferanten verankert, dass die einschlägigen Steuergesetze in den Ländern, in denen der Lieferant tätig ist und Dienstleistungen für die DB erbringt, einzuhalten sind.
Interaktionen mit staatlichen Stellen, Regierungsbeamten oder politisch exponierten Personen (PEP) im Auftrag der DB	Zur Ermittlung und Steuerung möglicher Risiken im Zusammenhang mit Finanzkriminalität, insbesondere Bestechung und Korruption, die bei der Erbringung von Dienstleistungen für die DB entstehen können, hat der Lieferant alle gegebenenfalls bestehenden Interaktionen mit staatlichen Stellen, Regierungsbeamten oder politisch exponierten Personen offenzulegen.
Frühere oder aktuelle Verbindungen mit, Eigentum an oder Beteiligung in jeglicher Form an der DB, ihren Tochtergesellschaften oder verbundenen Unternehmen	Zur Ermittlung und Steuerung möglicher Finanzkriminalitätsrisiken hat der Lieferant offenzulegen, ob seine Geschäftsführung mit der DB, ihren Tochtergesellschaften oder verbundenen Unternehmen in jeglicher Form verbunden ist, an solchen ein Eigentum bzw. eine Beteiligung hält.
Verbindungen zu aktuellen oder ehemaligen Amtsträgern in den letzten sieben Jahren	Zur Ermittlung und Steuerung möglicher Finanzkriminalitätsrisiken, insbesondere Bestechung und Korruption, hat der Lieferant alle Verbindungen offenzulegen, die er oder seine Geschäftsführung in den letzten sieben (7) Jahren mit aktuellen oder ehemaligen Amtsträgern unterhalten haben.
An der Erbringung von Dienstleistungen beteiligte Länder	Der Lieferant hat für die Dienstleistungen, die er gegenüber der DB erbringt, eine Liste derjenigen Länder vorzulegen, in bzw. ausgehend von denen er seine Dienstleistungen für die DB erbringen wird, damit sich mögliche Finanzkriminalitätsrisiken im Zusammenhang mit einer Geschäftstätigkeit in risikoreichen Ländern bewerten lassen.
Transaktionsüberwachungskontrollen	Solche kommen ggf. zum Einsatz, um mögliche Geldwäschehandlungen (einschließlich Steuerhinterziehung) sowie Sanktions- und Embargorisiken zu ermitteln, zu erkennen und mindern zu können, indem sichergestellt wird, dass Richtlinien- und Verfahrensdokumente vorhanden sind und darin mindestens Folgendes geregelt wird: 1. Überprüfung von Kunden, Aktivitäten und Produkten („Due Diligence“) 2. Prüfungen der Transaktionsstruktur 3. Filterung nach Risiko 4. Dokumentationsprozess, einschließlich anwendbare Gesetze und Vorschriften 5. Eskalationsweg für „entdeckte Ergebnisse“
Know Your Client-Kontrollen (KYC)	Sofern dies zur Minderung möglicher Finanzkriminalitätsrisiken erforderlich ist, hat der Lieferant KYC-Kontrollen nachzuweisen. Diese sollten mindestens Folgendes umfassen:

	1. Kundensorgfaltspflichten: a) Definition von Risikofaktoren zu Kunden, Produkten und geografischen Regionen b) Prozess zur Identifizierung der Vertragspartei c) Ermittlung des Verifizierungsprozesses d) Kontrollen zur Art des Kundengeschäfts
Handlungen zur Anbieter-/Kundenüberprüfung	Gegebenenfalls hat der Lieferant zur Gewährleistung, dass eine angemessene Überprüfung des Anbieters/Kunden erfolgt und die Ergebnisse angemessen berücksichtigt werden, Unterlagen zur Verfügung zu stellen, aus denen die Handlungen im Rahmen der Anbieter-/Kundenüberprüfung hervorgehen. Diese sollten mindestens Folgendes umfassen: 1. schriftliche Verfahren 2. Prozessablauf zur Abbildung während des Überprüfungsprozesses 3. Eskalationsverfahren 4. eingesetzte Überprüfungsliste(n) wurden mit DB abgestimmt 5. Verifizierung der entdeckten Ergebnisse 6. Abhilfemaßnahmen für entdeckte Ergebnisse wurden eingeleitet 7. Einzelheiten der erforderlichen Genehmigungen bei einem entdeckten Vorfall 8. Anforderungen an die regelmäßige Berichterstattung

3. Geschäftskontinuitätsmanagement (Business Continuity Management)

Folgende Kontrollen greifen, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte ein mögliches Risiko in Bezug auf die Reaktion auf Betriebsunterbrechungen und ein Wiederherstellungsrisiko bei den für die DB zu erbringenden Dienstleistungen ermittelt wurde.

Bezeichnung der Kontrolle	**Beschreibung der Kontrolle**
Krisenmanagementorganisation/-modell	Zur Gewährleistung einer zeitnahen und koordinierten Reaktion auf Krisensituationen bzw. störende Ereignisse hat der Lieferant über ein(e) Krisenmanagementorganisation/-modell zu verfügen.
Geschäftskontinuitätsplan (Business Continuity Plan, BCP)	Für die Sicherstellung einer wirksamen Wiederherstellung nach Betriebsunterbrechungen hat der Lieferant für alle Prozesse im Zusammenhang mit der Transaktion über einen BCP zu verfügen, der die folgenden Mindestanforderungen erfüllt: - Planung anhand der Szenarien des Geschäftskontinuitätsplans - Definition von Funktionen und Verantwortlichkeiten zur Aufrechterhaltung des Geschäftskontinuitätsplans

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
	- Dokumentation der Vorgaben für die Wiederherstellungszeit (Recovery Time Objectives, RTOs) für die im Leistungsumfang enthaltenen Dienstleistungen
Anforderungen an den Geschäftskontinuitätsplan (BCM-Test)	Zur Gewährleistung, dass der Geschäftskontinuitätsplan in der Praxis funktioniert und eine effektive Wiederherstellung nach Betriebsunterbrechungen ermöglicht, führt der Lieferant einen BCM-Test (Wiederherstellungs-Test/Test des BCM-Plans) durch, der folgende Mindestanforderungen erfüllt: - alle Wiederherstellungsstrategien des Geschäftskontinuitätsplans wurden in der Praxis getestet - die Rollen und Verantwortlichkeiten für den BCM-Test sind dokumentiert - die Testergebnisse sind dokumentiert - der Test wurde in den letzten 12 Monaten durchgeführt
Anrufbaum (oder vergleichbare Kommunikationskanäle)	Zur Gewährleistung, dass die Mitarbeiter des Lieferanten über Störungsereignisse und die damit verbundene Einleitung von Wiederherstellungslösungen informiert werden, um nach Störungsereignissen eine effektive Wiederherstellung zu ermöglichen, hat der Lieferant über einen aktuellen Anrufbaum (oder vergleichbare Kommunikationskanäle) zu verfügen, der innerhalb der letzten 12 Monate getestet wurde und die folgenden Mindestanforderungen erfüllt: - im Anrufbaum sind alle Mitarbeiter aufgeführt, die für die im Leistungsumfang enthaltenen Dienstleistungen relevant sind - der Anrufbaum wurde in den letzten 12 Monaten getestet - die Ergebnisse des Anrufbaums sind dokumentiert - der Anrufbaum und der Anrufbaumtest umfassen alle Vertreter der DB (alternativ wurde der Ansprechpartner bei DB in den letzten 12 Monaten separat getestet)
BCM-Schulung	Zur Gewährleistung, dass die Mitarbeiter des Lieferanten im Falle von Betriebsunterbrechungen mit der Anwendung von Wiederherstellungslösungen vertraut sind, hat der Lieferant innerhalb der letzten 12 Monate eine BCM-Schulung für all diejenigen Mitarbeiter durchgeführt, die an den für die DB erbrachten Dienstleistungen beteiligt sind.

4. Konzern-Datenschutz (Group Data Privacy, GDP)

Folgende Kontrollen greifen, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte festgestellt wurde, dass für die Bereitstellung von Waren oder Dienstleistungen gegenüber der DB personenbezogene Daten relevant sind.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Verarbeitung personenbezogener Daten aus der EU in einem Drittland (außerhalb der EU)	Zur Gewährleistung der Datenschutz-Grundverordnung der EU wird der Lieferant um eine Bestätigung gebeten, ob im Rahmen seiner Dienstleistungen personenbezogene Daten der EU durch den Lieferanten, verbundene Unternehmen oder Unterauftragnehmer in einem Drittland (außerhalb der EU), zu dem keine von der EU-Kommission ausgestellte Erklärung zur Angemessenheit des Datenschutzes vorliegt, verarbeitet und/oder gespeichert werden. Sofern die vorstehende Frage mit „Ja“ beantwortet wurde, wird der Lieferant um eine Bestätigung gebeten, dass mit jeglichen verbundenen Unternehmen oder Unterauftragnehmern die EU-Standardvertragsklauseln vereinbart wurden und eine Bewertung des Übertragungsrisikos erfolgt ist.
Personenbezogene Daten aus der EU, die Gegenstand eines Auskunftsersuchens der Strafverfolgungsbehörden oder der Regierung sind	Sofern die vorstehende Frage mit „Ja“ beantwortet wurde, wird der Lieferant um eine Bestätigung gebeten, ob er in den letzten drei Jahren Gegenstand eines Auskunfts- bzw. Offenlegungsersuchens der Strafverfolgungsbehörden oder der Regierung in Bezug auf personenbezogene Daten aus der EU war. Der Lieferant wird ggf. um eine Stellungnahme gebeten, ob solche Ersuchen abgelehnt oder angefochten wurden.
Hochrisiko-Szenarien	Für die Gewährleistung einer verhältnismäßigen Sorgfaltspflicht bei allen Hochrisiko-Szenarien wird der Lieferant um eine Bestätigung dahingehend gebeten, ob der Lieferant, ein verbundenes Unternehmen oder ein Unterauftragnehmer: - im Rahmen der Dienstleistungen personenbezogene Daten der EU physisch außerhalb der 27 EU-Mitgliedstaaten speichern wird - im Zusammenhang mit Ermittlungen zur Bekämpfung von Geldwäsche und damit zusammenhängenden Unterlagen, Analysen von E-Mail-Inhalten, strafrechtlichen Verurteilungen und Straftaten von außerhalb der 27 EU-Mitgliedstaaten Zugang zu personenbezogenen Daten der EU hat - für Anwendungen, die personenbezogene Daten der EU aus einem Drittland (außerhalb der EU) enthalten, für das von der EU-Kommission keine Erklärung zur Angemessenheit des Datenschutzes vorgelegt wurde, über eine Root-Zugriffsverwaltung verfügt

5. Daten und Unterlagen

Folgende Kontrollen greifen, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte ein mögliches Risiko in Bezug auf Daten und Unterlagen ermittelt wurde.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Erstellung von Unterlagen	Sofern vom Lieferanten im Auftrag der DB Unterlagen erstellt und/oder aufbewahrt werden, wird der Lieferant um eine Bestätigung gebeten, dass solche Unterlagen den Anforderungen im Dokument „Records Management and Continued Retention Requirements for Third Parties“ (Unterlagenmanagement und fortlaufend geltende Aufbewahrungsanforderungen für Dritte) entsprechen, das während des Sourcing-Prozesses übermittelt wird. Dies gilt insbesondere für: • Unterlagen, die vom Lieferanten im Auftrag der DB erstellt werden; dafür ist eine Liste der Unterlagentypen, einschließlich ihrer Aufbewahrungsorte und -fristen (ggf. einschließlich auslösender Ereignisse) und der Art der für diese Unterlagen erbrachten Dienstleistungen (Erstellung, Aufbewahrung, Abruf, Bereitstellung) vorzulegen.
Aufbewahrung von Unterlagen	Sofern eine Aufbewahrung erfolgt, hat der Lieferant zu bestätigen, dass: • elektronische Datensätze in einem von der DB zertifizierten Enterprise Approved Electronic Archive (EAEA) oder in einem zertifizierten In-Place-Archiv (einem intern entwickelten Bankprodukt, das die Archivierung in die Unterlagen einbringt) archiviert werden; • physische Aufzeichnungen in Übereinstimmung mit dem vorstehend genannten Dokument aufbewahrt werden.
Abfrage von Unterlagen	Der Lieferant bestätigt, dass für die vom Lieferanten im Auftrag der DB aufbewahrten Unterlagen ein Vertrag über den genauen und rechtzeitigen Abruf der Unterlagen besteht, und die entsprechende Dokumentation der DB zur Verfügung gestellt wird.
Entsorgung von Unterlagen	Der Lieferant bestätigt, dass für Unterlagen, die der Lieferant im Auftrag der DB aufbewahrt, ein Unterlagen-Entsorgungsansatz dokumentiert ist, und der DB der Nachweis erbracht wird, dass die Entsorgung in Übereinstimmung mit dem vorstehend genannten Dokument erfolgen kann.
Speicherung und/oder Verarbeitung von Daten	Der Lieferant bescheinigt, dass er vor der Speicherung bzw. Verarbeitung von Daten der DB in oder von einem neuen Standort bzw. vor der Durchführung neuer Verarbeitungshandlungen die Genehmigung der DB über den Änderungsantragsprozess im Rahmen des Drittanbietermanagements einholt. Auf Verlangen sorgt der Lieferant für umfassende Transparenz und legt alle Standorte offen, an denen er Daten der DB speichert oder verarbeitet; dasselbe gilt für alle Verarbeitungstätigkeiten, die er an Daten der DB durchführt.

6. Compliance

Folgende Kontrollen greifen , wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte ein mögliches Compliance-Risiko ermittelt wurde.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Richtlinie/Verfahren für die Beschwerdebehandlung	Wenn der Lieferant mit Kunden interagiert oder an der Transaktionsberichterstattung beteiligt ist bzw. Kundengelder verwaltet oder an Wertpapierhandel, Einlagenaufnahme, Kredit- oder Kreditvergabetätigkeiten beteiligt ist, hat der Lieferant eine Richtlinie/ein Verfahren zur Bearbeitung von Beschwerden vorzuhalten, in der/dem der Begriff Beschwerden definiert und der Prozesses zur Bearbeitung von Kundenbeschwerden erläutert wird.
Beschwerdeprotokoll/-unterlagen	Sofern die vorstehende Frage mit „Ja“ beantwortet wurde, hat er (ein) Beschwerdeprotokoll/-unterlagen zu führen, in dem/denen alle von Kunden eingegangenen Beschwerden sowie die in Bezug auf solche Beschwerden ergriffenen Maßnahmen dokumentiert sind.
Statusbericht zur Verpflichtung der regulatorischen Berichterstattung und der diesbezüglichen Leistung	Sofern der Lieferant Dienstleistungen erbringt, die zur Erfüllung bestimmter gesetzlicher Berichtspflichten bzw. der Berichtspflichten nach einer Verordnung einer nationalen, internationalen oder supranationalen Organisation, der ARM, APA oder einer Regierungsbehörde, die für die finanzielle oder nichtfinanzielle Aufsicht, Überwachung oder Regulierung der Aktivitäten der Bank verantwortlich ist, vorgeschrieben sind, kann der Lieferant regelmäßig einen Überblick über den Status der Berichterstattung geben, einschließlich (u. a.) Verstöße, verspätete/geänderte Offenlegungen, Geldbußen und Fehler. Vorlage regelmäßiger Statusberichte, um einen Überblick über den Status der Berichterstattung zu geben, einschließlich Verstöße, Anzahl verspäteter/geänderter Offenlegungen, Bußgelder, Fehler und anderer Angelegenheiten, die zur Gewährleistung erforderlich sind, dass die erbrachte Dienstleistung die gesetzlich vorgeschriebenen Berichtspflichten bzw. die Berichtspflichten nach einer Verordnung einer nationalen, internationalen oder supranationalen Organisation, der ARM, APA oder einer Regierungsbehörde, die für die finanzielle oder nichtfinanzielle Aufsicht, Überwachung oder Regulierung der Aktivitäten der Bank verantwortlich ist, erfüllt.
Eskalationsrahmen	Sofern der Lieferant an Positionsmeldungen und/oder regulatorischen Meldungen beteiligt ist, hat er über einen etablierten Eskalationsrahmen zu verfügen, über den Meldeverletzungen behandelt werden, einschließlich der Eskalation an die Geschäftsführung und ggf. der Benachrichtigung von Aufsichtsbehörden.
Umgang mit Kundeninformationen	Sofern der Lieferant Zugang zu vertraulichen Kundeninformationen hat, verfügt er über schriftliche Richtlinien und Verfahren, in denen die Mindestanforderungen für den angemessenen Umgang mit vertraulichen Kundeninformationen und/oder firmeneigenen Informationen der DB verankert sind.
Eskalation von Verstößen	Sofern der Lieferant im Rahmen einer Dienstleistungen Zugriff auf vertrauliche Kundeninformationen und/oder firmeneigene Informationen der DB hat, verfügt er über ein Verfahren zur Eskalation von Verstößen im Zusammenhang mit dem versehentlichen Verlust oder Missbrauch vertraulicher Kundeninformationen und/oder firmeneigener Informationen

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
	der DB, in dem im Falle eines Verstoßes mindestens die Dokumentation der Verstöße und die Übermittlung von Mitteilungen an die DB gefordert wird.
Getrennte Aufbewahrung von Vermögenswerten der Kunden	Sofern die Dienstleistungen des Lieferanten das Halten von bzw. den Umgang mit Kundengeldern und/oder die Entgegennahme von Einlagen umfassen, verfügt der Lieferant über schriftliche Verfahren, in denen der Prozess der getrennten Aufbewahrung von Vermögenswerten der Kunden (Gelder oder Wertpapiere) dokumentiert ist, einschließlich (u. a.) der korrekten Ermittlung dieser Vermögenswerte, ihrer angemessenen getrennten Aufbewahrung und des Umgangs mit diesen Vermögenswerten gemäß den geltenden Gesetzen, Regeln und Vorschriften.
Vermögenswerte der Kunden	Sofern der Lieferant Kundengelder verwaltet oder hält, führt der Lieferant Unterlagen über jegliche Vermögenswerte des Kunden, die von ihm direkt oder indirekt gehalten bzw. verwaltet werden.
Kommunikations- und Marketingmaterial	Sofern zu den Dienstleistungen des Lieferanten die Durchführung von Marketingaktivitäten für Kunden gehört, hat er einen regelmäßigen Überprüfungsprozess eingerichtet, um sicherzustellen, dass Kommunikations- und Marketingmaterialien den gesetzlichen und regulatorischen Anforderungen entsprechen und deutlich, fair und nicht irreführend sind.

7. Finanzen

Folgende Kontrollen werden anwendbar, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte Dienstleistungen ermittelt werden, bei denen Lieferanten und/oder deren Unterauftragnehmer einen wesentlichen Einfluss auf die Finanzen der DB haben könnten.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
SOC 1 Typ II-Bericht (ISAE 3402-Bericht) für Lieferanten und Unterauftragnehmer + Bridge Letter, sofern der vorstehende Bericht nicht das gesamte Jahr behandelt	Zur Bewertung, ob die internen Kontrollen des Lieferanten in geeigneter Weise konzipiert sind und effektiv funktionieren, um die gewünschten Dienstleistungen zu erbringen, hat der Lieferant einen SOC 1-Bericht vorzulegen, um Sicherheit für alle internen Kontrollen der Finanzberichterstattung sowie für alle Kontrollprozesse/Dienstleistungen zu gewinnen, die der Lieferant im Auftrag der DB durchführt.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Probleme im SOC 1 Typ II-Bericht (ISAE 3402-Bericht) für Lieferanten und Unterauftragnehmer	Der Lieferant hat alle im SOC 1-Bericht enthaltenen Kontrollprobleme oder -lücken zu bestätigen, die Abhilfemaßnahmen bzw. sogar einer Risikoakzeptanz unterliegen.

8. Sicherheit Dritter (Third Party Security, TPS)

Die Kontrollanforderungen für die bei der Deutschen Bank geltenden Third-Party Security (Sicherheit Dritter) sind an den internationalen Standard ISO/IEC 27001 angelehnt.

9. Modellrisiko

Folgende Kontrollen greifen, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte ein mögliches Modellrisiko beim Einsatz von mathematischen Modellen in den Dienstleistungen für die DB ermittelt wurde, einschließlich der AI-Modelle.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Bereitstellung hinreichender Informationen und Dokumente	Der Lieferant stellt der DB ausreichende Informationen und Unterlagen zur Verfügung, damit die Ergebnisse der modellgestützten/nicht-modellgestützten Schätzung von einer entsprechend qualifizierten Validierungsfunktion repliziert werden können.
Testergebnisse der modellgestützten/nicht-modellgestützten Schätzung	Für eine Überprüfung der Genauigkeit und Robustheit des Modells, zur Bewertung potenzieller Einschränkungen sowie der Auswirkungen von Annahmen im Rahmen verschiedener Szenarien hat der Lieferant Folgendes bereitzustellen: A. Zugang einer bei der DB eingerichteten unabhängigen Validierungsfunktion zum System des Lieferanten für die Durchführung unabhängiger Tests der modellgestützten/nicht-modellgestützten Schätzung ODER B. Bereitstellung der Ergebnisse der Tests zu den modellgestützten/nicht-modellgestützten Schätzungen für eine Überprüfung durch die bei der DB eingerichteten unabhängigen Validierungsfunktion; einschließlich der Testszenarien, die von der bei der DB eingerichteten unabhängigen Validierungsfunktion vorgegeben werden
Ansprechpartner für KMU zur Bearbeitung von Anfragen	Der Lieferant hat einen geeigneten Ansprechpartner für KMU bereitzustellen, der die während der Validierung oder des laufenden Lebenszyklusmanagements von modellgestützten/nicht-modellgestützten Schätzungen aufkommenden Fragen beantworten kann.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Bewertung der modellgestützten/nicht-modellgestützten Schätzungen durch Dritte	Zur Gewährleistung, dass die modellgestützte/nicht-modellgestützte Schätzung validiert wird, um bestätigen zu können, dass das Modell wie erwartet und im Einklang mit seinen Entwurfszielen und seiner geschäftlichen Verwendung funktioniert, und um mögliche Einschränkungen des Modells ermitteln zu können, wird der Lieferant um eine Bestätigung gebeten, dass entweder: A. die modellgestützte/nicht-modellgestützte Schätzung einer internen, aber trotzdem unabhängigen Validierung unterliegt, bei der deren Entwicklung, Umsetzung und Nutzung anhand vereinbarter Standards und Anforderungen überwacht und wirksam hinterfragt wird ODER B. die modellgestützte/nicht-modellgestützte Schätzung von einem unabhängigen (externen) Lieferanten validiert wird.
Weitergabe aller Validierungsergebnisse des Lieferanten an die DB	Der Lieferant hat die Ergebnisse und Resultate jeder Validierung an die bei der DB eingerichtete unabhängige Validierungsfunktion weiterzugeben, einschließlich: A. Annahmen und Mängel (Einschränkungen und Schwächen), die auf klaren Leitlinien zu Fähigkeiten, Beschränkungen und Unsicherheiten basieren und B. Weiterer Nachweise (z. B. Informationen zu Eingabedaten/Parametern usw.) zur Untermauerung des Validierungsergebnisses.
Weitergabe von Nachweisen über die SAS 70-/SSAE 16-/SOC 1-Validierung (nur in den USA)	Der Lieferant hat gegenüber der bei der DB eingerichteten unabhängigen Validierungsfunktion einen Nachweis zu erbringen (eine SAS70-/SSAE 16-Prüfung (nur in den USA) durch eine unabhängige Partei kann hierfür ausreichen), aus dem Einzelheiten zu folgenden Punkten hervorgehen: A. Es bestehen laufende Prozesskontrollen für Dateneingaben, die Auswirkung auf die Ausgabe haben und B. Es bestehen angemessene und geeignete Methodikkontrollen, die als Teil der Entwicklung und Tests gelten und C. Die Umsetzung erfolgt anhand genau definierter und dokumentierter Testhandlungen D. Es bestehen angemessene Kontrollen, um unbefugte Änderungen/Nutzungen zu verhindern.

10. Physische Sicherheit

Folgende Kontrollen greifen, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte mögliche physische Sicherheitsrisiken ermittelt wurden.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Audit der physischen Sicherheit	Der Lieferant hat nachzuweisen, dass er und relevante Unterauftragnehmer, die auf vertrauliche/streng vertrauliche Daten und/oder Vermögenswerte der DB zugreifen/diese speichern/damit umgehen, robuste physische Sicherheitsstandards einhalten und diese anhand eines relevanten Kontrollsystemstandards wie SSAE18 oder ISAE3402 geprüft werden. Dafür

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
	kann die Vorlage eines Auditberichts, wie SOC 2 Typ II, PCI-DSS oder eine andere vergleichbare unabhängige Bewertung, aus der keinerlei sicherheitsrelevante Ergebnisse hervorgehen, als ausreichend erachtet werden. ODER Sofern keine SOC 2 Typ II-Berichte vorliegen, die für alle Standorte gelten, an denen vertrauliche/streng vertrauliche Daten gespeichert werden, hat der Lieferant für alle Standorte (einschließlich der Standorte von Unterauftragnehmern), an denen vertrauliche/streng vertrauliche Daten gespeichert werden, Risikobewertungen, Sicherheitsrichtlinien und -konzepte, Berichte zu Sicherheitsaudits und/oder einschlägige Branchenzertifizierungen (z. B. ISO 27001:2013) vorzulegen.
Berechtigungen und Lizenzen	Sofern die Dienstleistungen die Lagerung von Vermögenswerten der DB außerhalb der Räumlichkeiten der DB umfassen, hat der Lieferant (einschließlich der Unterauftragnehmer, die der DB zugewiesen sind) Nachweise über die von den zuständigen lokalen Gesetzgebungsbehörden ausgestellten entsprechenden Genehmigungen in Bezug auf die physische Sicherheit, das Personal und die Fahrzeuge (sofern sie am Transport/dem Umgang mit Vermögenswerten der DB beteiligt sind) vorzulegen.
TRM-Richtlinien der MAS	Sofern bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte ermittelt wurde, dass die Dienstleistungen kritische Systeme im Sinne der Definition der Währungsbehörde von Singapur (Monetary Authority of Singapore, MAS) umfassen, wird der Lieferant um die Vorlage eines Nachweises gebeten, dass diese alle behördlichen Anforderungen erfüllen, die in den TRM-Richtlinien der MAS über die physischen Sicherheits- und Umweltkontrollen niedergelegt sind. Einzelheiten zu den TRM-Richtlinien der MAS sind verfügbar unter: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf.

11. Nachhaltigkeit

Folgende Kontrollen greifen, wenn bei einer Bewertung der inhärenten Risiken im Rahmen des bei der DB intern durchgeführten Risikobewertungsprozesses für Dritte mögliche Nachhaltigkeitsrisiken ermittelt wurden.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
EcoVadis oder ein äquivalentes Umwelt-, Sozial- und Governance-Rating (ESG)	Der Lieferant hat ein EcoVadis- oder ein gleichwertiges ESG-Rating vorzulegen.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Menschenrechtsrisiken	Zur Gewährleistung, dass der Lieferant die Menschenrechtsstandards, einschließlich der Verhinderung und Behebung nachteiliger Auswirkungen, auch im Einklang mit den Anforderungen des deutschen Lieferkettensorgfaltspflichtengesetzes (LkSG) erfüllt, sollte der Lieferant über Richtlinien oder ein Programm zum Umgang mit Menschenrechtsrisiken verfügen, in dem folgende Bereiche geregelt sind: - Maßnahmen zur Bewertung und Steuerung von Risiken innerhalb des Betriebs und der Lieferkette - Maßnahmen zur Verhinderung von Zwangs-, Pflichtarbeit, Schuldknechtschaft, unfreiwilliger Arbeit oder Schwarzarbeit - Maßnahmen zur Verhinderung von Kinderarbeit im Betrieb und in der Lieferkette - Gesundheits- und Sicherheitsrichtlinie, -verfahren bzw. -praktiken - Maßnahmen zur Gewährleistung einer gerechten und rechtzeitigen Lohnzahlung - Maßnahmen zur Gewährleistung, dass Arbeitnehmer Gewerkschaften, Arbeitnehmerräten oder anderen Tarifverhandlungsorganisationen beitreten können - Maßnahmen zur Förderung inklusiver Arbeitspraktiken, einschließlich der Gewährleistung, dass keinerlei Diskriminierung aufgrund von Rasse, Klasse, Nationalität, Religion, Alter, Behinderung, Geschlecht, Familienstand, sexueller Orientierung, Gewerkschaftszugehörigkeit oder politischer Zugehörigkeit erfolgt - Vorhandensein eines Beschwerdemechanismus, auf den Mitarbeiter, Lieferanten und andere Personen, mit denen der Lieferant über seinen Betrieb interagiert (z. B. Mitglieder der Gemeinschaft), problemlos zugreifen können - Verfahren oder Mechanismen zur Ermittlung und Reaktion auf Menschenrechtsverletzungen innerhalb des Betriebs oder der Lieferkette
Umweltrisiken	Zur Ermittlung, Bewertung und Eindämmung von Umweltrisiken im Zusammenhang mit den durchgeführten Tätigkeiten sollte der Lieferant, auch im Einklang mit den Anforderungen des Lieferkettensorgfaltspflichtengesetzes (LkSG), über Richtlinien oder ein Programm zum Umgang mit Umweltrisiken verfügen, in dem folgende Bereiche geregelt sind: - Maßnahmen zur Bewertung und zum Management von Umweltrisiken innerhalb des Betriebs und der Lieferkette - Verfahren zum Umgang mit und zur Entsorgung von gefährlichem Material (sofern vorhanden)

12. Unterauftragnehmer

Der Lieferant wird gebeten, im Rahmen des Risikobewertungsprozesses eine Erklärung zum Einsatz von Unterauftragnehmern abzugeben. Für Transaktionen mit höherem Risiko gelten die folgenden Kontrollen. Der Lieferant wird zudem gebeten, Einzelheiten über die Unterauftragnehmer mitzuteilen, die in Verbindung mit dem Risikomanagementrahmen für Dritte eingesetzt werden.

Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Untervergabe jeglicher Rechte oder Pflichten	Der Lieferant hat die DB in Kenntnis zu setzen, sofern er die Absicht verfolgt, seine in dieser Vereinbarung vorgesehenen Rechte oder Pflichten an einen anderen Lieferanten unterzuvergeben. Der Lieferant bleibt gegenüber der DB jederzeit für die Erfüllung der Vereinbarung verantwortlich.
Risikomanagementprozess oder -rahmen beim Lieferanten	Der Lieferant hat nachzuweisen, dass er über einen Risikomanagementrahmen für Dritte verfügt, in dem ggf. Dinge, wie die Festlegung der Wichtigkeit seiner Lieferanten, die Sorgfaltspflichten, das Risikomanagement, eine laufende Überwachung, das Management, die Übergangs-, Austritts-/Kündigungspläne und -strategien geregelt sind.
Prüfungen der Integritätsbewertung der eingesetzten Dritten	Der Lieferant hat nachzuweisen, dass er in seiner eigenen Lieferkette Integritätsbewertungen durchführt, in deren Rahmen Dinge wie negative Medien, Sanktionen, Embargos, politisch exponierte Personen und Interessenkonflikte berücksichtigt werden.
Überprüfungen der finanziellen Stabilität für eingesetzten Dritten	Zur Gewährleistung, dass die Lieferkette finanziell stabil ist und keine Gefahr für Unterbrechungen der gegenüber der DB erbrachten Dienstleistungen besteht, hat der Lieferant nachzuweisen, dass er in seiner eigenen Lieferkette Finanzstabilitätsprüfungen durchführt.
Anforderungen an wesentliche Unterauftragnehmer	Ein Unterauftragnehmer gilt dann als wesentlich, wenn: • an diesen Kunden- oder Mitarbeiterdaten der DB bzw. andere sensible Daten der DB (z. B. Finanzdaten) weitergegeben werden oder • dieser lizenzierte Finanzdienstleistungstätigkeiten in Bezug auf die für die DB erbrachten Dienstleistungen durchführt (z. B. Handeln nach oder Treffen von Entscheidungen bzw. Verpflichtungen im Namen der DB, direkte Kundeninteraktionen) oder • die Dienstleistungen direkt an den Unterauftragnehmer weitergegeben werden oder ein mit einem Unterauftragnehmer zusammenhängendes Problem unmittelbar zu einer Unterbrechung eines messbaren Teils der Gesamtdienstleistungen führen würde oder • dieser unbeaufsichtigten Zugang zu Einrichtungen der DB oder Zugang zu Produktionssystemen der DB hat. Der Lieferant ist aufgefordert, für jeden wesentlichen Unterauftragnehmer Folgendes nachzuweisen: • Einhaltung der lokalen Datenschutzgesetze und -vorschriften (DSGVO) • Vorhandensein eines Rahmens für die Bekämpfung der Finanzkriminalität (AFC) • Verpflichtung zur Durchführung einer Mitarbeiter-Hintergrundüberprüfung (durch das Personalwesen) und • Umsetzung der und Tests zu den Geschäftskontinuitätsplänen (BCM).

RECHTLICHE HINWEISE

Auch wenn der Inhalt dieses Dokuments der Deutschen Bank als zuverlässig gilt und aus Quellen stammt, die als zuverlässig gelten, wird selbiges ausschließlich zu spezifischen Informationszwecken bereitgestellt und „wie besehen“ ohne Gewährleistung oder Zusicherung jeglicher Art vorgelegt. Die DB gibt keinerlei Zusicherungen oder Gewährleistungen dafür, dass das Dokument (i) richtig, aktuell, vollständig oder fehlerfrei ist, (ii) individuelle Anforderungen des Empfängers, einschließlich in Bezug auf Fairness oder Angemessenheit, erfüllt oder (iii) für den internen Zweck des Empfängers geeignet ist. Die DB gibt keine ausdrücklichen oder stillschweigenden (gesetzlichen oder sonstigen) Zusicherungen, Gewährleistungen oder Bedingungen in oder durch die Bereitstellung dieses Dokuments ab, und alle derartigen Zusicherungen, Gewährleistungen und Bedingungen sind ausgeschlossen, soweit ihr Ausschluss gesetzlich zulässig ist.

Dieses Dokument ist Ausdruck der aktuellen Situation der Mindeststandards für Anbieter, die ausschließlich im Hinblick auf die Erwartungen an die Kontrollpflichten Dritter gelten. Diese Situation kann durch die DB ohne Vorankündigung oder Haftung geändert werden, einschließlich in Bezug auf rechtliche, regulatorische, interne Richtlinien oder andere Technologie- oder Marktpraktiken. Es besteht keine Verpflichtung zur Aktualisierung, Modifizierung oder Änderung dieses Dokuments bzw. zur sonstigen Benachrichtigung eines Empfängers, falls sich eine hierin genannte Angelegenheit ändert oder später unrichtig wird.

Nichts auf oder in diesem Dokument gilt als Angebot oder Zusage, die von einem Empfänger angenommen bzw. als Aufforderung zur Angebotsabgabe verstanden werden darf, um vertragliche Verpflichtungen ohne weiteres Handeln der DB zu begründen. Die DB handelt nicht und gibt nicht vor, in irgendeiner Weise als Berater oder in treuhänderischer Funktion zu handeln, und das Dokument stellt keine Aufforderung zur Abgabe oder die Bereitstellung von Investitions-, Finanz-, Buchhaltungs-, Rechts-, Regulierungs- oder Steuerberatung dar und sollte nicht als Ersatz für die Einholung eigener Ratschläge von einem in dem jeweiligen Land zugelassenen Sachverständigen verwendet werden; Letzteres wird von der DB empfohlen. Alle Angebote oder möglichen Transaktionen, die sich auf den Gegenstand dieses Dokuments beziehen, erfolgen auf Grundlage separater und gesonderter Unterlagen, und in einem solchen Fall treten solche Unterlagen vollständig an die Stelle der in diesem Dokument enthaltenen Informationen oder Daten.