



Unterstützung der  
Banken durch IBM  
im Zusammenhang  
mit den Empfehlungen  
der Europäischen  
Bankenaufsichtsbehörde  
über Cloud-Computing

# Einführung

Die Europäische Bankenaufsichtsbehörde (EBA) gab den „Abschlussbericht über Empfehlungen zur Auslagerung an Cloud-Anbieter“, anwendbar seit 1. Juli 2018, heraus, um zusätzliche Beratung für EU-Kreditinstitute und Investmentfirmen (im Allgemeinen als Finanzinstitute, FIs, bezeichnet) im Zusammenhang mit den „Richtlinien über Outsourcing vom Ausschuss der Europäischen Aufsichtsbehörden für das Bankwesen“ (CEBS-Richtlinien) über das Outsourcing an Cloud-Service-Anbieter (CSP) zu bieten.

Zusätzlich zu den ehemaligen CEBS-Richtlinien konzentrieren sich die EBA-Richtlinien auf sechs Hauptaspekte für EU-Finanzinstitute:

1. Bewertung der Materialität des Cloud-Outsourcing und Information der Regulierungsbehörden
2. Recht auf Zugriff und Recht auf Prüfung für Institute und befugte Behörden
3. Sicherheit der verwendeten Daten und Systeme
4. Ort der Datenverarbeitung
5. Ketten-Outsourcing
6. Notfallpläne und Ausstiegsstrategien.

IBM® begrüßte die Initiative der Europäischen Bankenaufsichtsbehörde und nahm aktiv am Beratungsprozess teil, um ein gemeinsames behördliches Rahmenwerk zum Outsourcing zu Cloud-Service-Anbietern zum Nutzen aller Parteien zu erstellen. IBM glaubt, dass die Empfehlungen der EBA für den Einsatz der Cloud von Nutzen sind und ihn unterstützen. Außerdem ermöglichen sie eine weitere Annäherung der Praktiken und Erwartungen von FIs und Überwachungsbehörden. IBM verpflichtet sich, FIs beim Lösen der Herausforderungen des Cloud-Outsourcing zu unterstützen.

Durch unser Expertenwissen der globalen Finanzdienstleistungs-Industrie sowie unsere tiefgreifenden Kenntnisse über Outsourcing versteht IBM die Bedürfnisse und Anforderungen der FIs und verfügt über eine breite Perspektive davon. Wir haben diese Anforderungen in unsere Cloud-Plattform integriert und können nie da gewesene Funktionen für Kern- und Peripherie-Workloads anbieten.

Diese Funktionen werden durch unser vertragliches Rahmenwerk ergänzt, in dem die besonderen Schwerpunkte, die in den EBA-Empfehlungen unterstrichen werden, behandelt werden. So können Finanzinstitute bessere Vorteile aus der Cloud ziehen und gleichzeitig ihre geschäftlichen Kontrollen und geltende Regelungen einhalten.

Zusammenfassend bietet IBM Cloud eine Umgebung, die es outsourcenden Institutionen ermöglichen, die EBA-Empfehlungen über Cloud-Outsourcing einzuhalten während sie IBM Cloud für materielle und nicht-materielle Aktivitäten nutzen.

# IBM geht auf die Anforderungen von Cloud-Service-Anbietern ein

FIs erfahren viel Druck, die Erwartungen von Kunden und Aktionären zu erfüllen und gleichzeitig die wachsenden behördlichen Anforderungen einzuhalten. IBM nutzt seine tiefgreifenden Branchenkenntnisse, um seine Cloud-Umgebung zu entwickeln, zu liefern und ständig zu aktualisieren, um den Anforderungen der Finanzdienstleistungsindustrie gerecht zu werden. Dazu zählen die Empfehlungen der EBA über das Outsourcing zu CSPs. IBM, als CSP, nimmt seine Verpflichtungen folgendermaßen wahr.

## **Materialität von Cloud-Outsourcing zur Information der berechtigten Behörden**

*Gemäß CEBS-Richtlinien fordert die EBA von outsourcenden Instituten, die Materialität von Aktivitäten zu prüfen und die berechtigten Autoritäten zu informieren. Darüber hinaus fordert sie, dass outsourcende Institute ein Verzeichnis materieller und nicht-materieller ausgegliederter Aktivitäten pflegen.*

Obwohl die Durchführung einer Materialitätsbewertung und die folgende Information der überwachenden Behörden weiterhin in der Verantwortung des outsourcenden Instituts liegt, kann IBM helfen, die notwendigen Anforderungen zu unterstützen, damit FIs erfolgreich ihre Geschäftsziele und regulatorische Position einhalten können.

Jeder IBM Cloud Service verfügt über eine klar umrissene Servicebeschreibung, die genau die Details dieses Service in Unterstützung der Anforderung von Materialitätsbewertung beschreibt. IBM kann Unternehmen dabei helfen, die Materialität von Aktivitäten und outgesourceten Informationen zu bewerten und zu dokumentieren, um sie zur EBA zu senden.

## **Recht auf Prüfung für Institute und befugte Behörden**

*Gemäß EBA- und CEBS-Richtlinien sollten outsourcende Institute und befugte Behörden sicherstellen, dass sie vollen Zugriff auf die CSP-Geschäftseinrichtungen sowie uneingeschränktes Recht auf Inspektion und Prüfung im Zusammenhang mit den outgesourceten Services haben.*

Die Liste der EBA-Empfehlungen unterstützt den Ansatz von IBM, global anerkannte und akzeptierte Zertifizierungen und Berichte von unabhängigen Dritten als verhältnismäßigen und risikobasierten Ansatz im Hinblick auf Sorgfaltspflicht und weitere ständige Überwachung zu nutzen. IBM pflegt eine umfassende Liste von Compliance-Zertifizierungen und Prüfberichten.

Eine vollständige Liste ist auf der [IBM Cloud Compliance-Website](#) verfügbar, gemeinsam mit Anweisungen darüber, wie Exemplare von bestimmten Berichten gefunden werden können.

IBM Cloud ist, von einer Sicherheits- und Zuverlässigkeitsperspektive für kritische sowie nicht-kritische Workloads entwickelt und gebaut. Dies zeigen auch unsere [Zertifizierungen](#) sowie das Vertrauen der FIs: sowohl globale als auch europäische FIs haben IBM zur Innovationsförderung auf prozess- und infrastrukturelevanter Technologieebene gewählt, wobei sowohl materielle als auch nicht materielle Aktivitäten zur IBM Cloud outgesourcet werden.

IBM hat ein „Cloud Addendum für den Finanzsektor“ erstellt, indem die vertraglichen Verpflichtungen, einschließlich im Hinblick auf Prüf- und Zugriffsrechte für Kunden im Einklang mit den EBA-Empfehlungen, festgelegt werden.

Seit 2016 verfügt IBM über einen Beratungsausschuss über Cloud Compliance (CCAB) für FIs. Dieser Ausschuss trifft sich vierteljährlich, um Probleme und Sorgen im Hinblick auf individuelle und globale regulatorische Anforderungen zu besprechen. Die Teilnahme am CCAB bietet zudem Einsichten über den internen Kontrollbewertungs-Prozess von IBM, was den Umfang der umfangreichen externen Zertifizierungen und Auditberichte noch vergrößert.

## Sicherheit von Daten und Systemen

*Die EBA empfiehlt, dass outsourcende Institute diejenigen Aktivitäten, die an den Cloud-Service-Anbieter gesendet werden sollen, klassifizieren, um ein angemessenes Niveau zu erhalten im Hinblick auf: Schutz der Vertraulichkeit der Daten, Kontinuität der outgesourcten Aktivitäten sowie Integrität und Verfolgbarkeit von Daten und Systemen im Kontext des beabsichtigten Cloud-Outsourcing.*

IBM Cloud bietet FIs einzigartige Funktionen im Zusammenhang mit der Sicherheit für Daten und Systeme, unter anderem die Fähigkeit, die anspruchsvollsten Workloads aufzunehmen. Das Dokument „[Datensicherheits- und Vertraulichkeitsprinzipien für IBM Cloud Services](#)“ beschreibt die Sicherheitsprinzipien hinter den technischen und organisatorischen Maßnahmen, die in allen IBM Cloud Services implementiert sind. Spezifische technische und organisatorische Maßnahmen, die von IBM für alle IBM Cloud Services-Produkte eingesetzt werden, sind im [Datenblatt über Cloud-Services](#) beschrieben.

Von Umgebungsisolierung bis hin zu Datenverschlüsselung und sogar dedizierter physikalischer Infrastruktur können FIs aus einer großen Bandbreite von Sicherheitsoptionen wählen, um ihre Workloads einzusetzen.

Wenn zusätzliche Sicherheitsfunktionen notwendig sind, kann IBM mit der FI zusammen an weiteren Sicherheitslösungen arbeiten, um erweiterte Anforderungen für die Cloud-Umgebung einzuhalten.

## Ort der Daten und Datenverarbeitung

*Outsourcing-Institutionen sollten vor allem bei Outsourcing-Vereinbarungen außerhalb der EBA achtsam sein, da eine Möglichkeit von Datenschutz-Risiken besteht. Die EBA empfiehlt outsourcing-Institutionen, einen risikobasierten Ansatz für die Orte von Daten und Datenverarbeitung zu wählen, der auch rechtliche Risiken und Compliance-Probleme umfasst.*

IBM Cloud Services sind von einer Vielzahl von Orten verfügbar und gehostet (die vollständige Liste finden Sie [hier](#)), sodass FIs ihren bevorzugten Einsatzort für IBM Cloud Services wählen können, und sicher sein können, dass ihr Cloud Service und ihre Daten innerhalb des ausgewählten Orts bleiben.

Für jeden IBM Cloud Service steht ein spezifisches Datenblatt mit detaillierten Informationen zu Hosting- und Verarbeitungsorten von IBM zur Verfügung. Die Datenblätter finden Sie [hier](#), herausgegeben zur Einhaltung der allgemeinen Datenschutzbestimmungen und unterstützt durch das IBM-Addendum über Datenverarbeitung. Falls Teil eines IBM Cloud Service außerhalb der EBA zur Verfügung gestellt wird, ermöglicht es IBM seinen Kunden, die [Modellklauseln der Europäischen Union \(EUMC\)](#) anzuwenden, wodurch sicher gestellt wird, dass IBM Datenimporteure über angemessene Sicherheitsmaßnahmen im Hinblick auf Datenschutz sowie Grundrechte und Freiheiten von Einzelpersonen verfügen. Außerdem ist IBM Mitglied der europäischen Generalversammlung über den [Cloud Code of Conduct](#).

## Ketten-Outsourcing

*Institutionen sollten die Risiken in Verbindung mit dem so genannten Ketten-Outsourcing beachten: Konsistenz der Pflichten müssen in der gesamten Subunternehmer-Kette garantiert werden, Mitteilungen müssen sofort herausgegeben werden, wenn wichtige Veränderungen in der Subunternehmer-Kette geplant werden, und klare Verantwortlichkeiten müssen in der Outsourcing-Vereinbarung zugeteilt werden.*

Wie durch die CEBS gefordert, und von den EBA-Empfehlungen unterstützt, haben Drittparteien, die IBM zum Anbieten von Cloud-Services in IBM Cloud Rechenzentren nutzt, die gleichen Verpflichtungen wie diejenigen, die zwischen IBM und der FI festgelegt sind. Außerdem wird IBM von seinen Subprozessoren mit Zugriff auf Kundeninhalte verlangen, technische und organisatorische Sicherheitsmaßnahmen zu erhalten, durch die IBM seine Verpflichtungen für Cloud-Services einhalten kann. Eine aktuelle Liste der Subprozessoren und ihrer Rollen wird auf Anfrage bereit gestellt. Institute können die Liste der externen Subprozessoren (soweit es sie gibt) für IBM Cloud Services im Datenblatt jedes Service einsehen.

Es ist wichtig, zu beachten, dass IBM mit der FI vertraglich eine Mitteilungsfrist für Veränderungen in der Subunternehmer-Kette festlegen wird, damit der Kunde seine interne Risikoanalyse durchführen kann.

## Notfallplan und Ausstiegsstrategien

*Die EBA empfiehlt outsourcenden Instituten, Vorkehrungen zu planen und zu treffen, um die Geschäftskontinuität zu garantieren, und eine Klausel über Kündigung und Ausstiegsmanagement einzufügen. Der Cloud-Service-Anbieter muss im Fall einer Vertragskündigung den Transfer von Aktivitäten zu einem anderen Service-Anbieter oder zur direkten Verwaltung durch das outsourcende Institut unterstützen.*

IBM Cloud legt einen Business-Continuity-Plan pro IBM Cloud Service fest, gemäß dem Dokument [Datensicherheits- und Vertraulichkeitsprinzipien für IBM Cloud Services](#). Darüber hinaus werden bilden Business-Continuity-Pläne für jeden Service Teil jedes [Datenblatts zu IBM Cloud Services](#).

*Die Vereinbarung über IBM Cloud Services* umfasst die Option, einen IBM Cloud Service zu kündigen, wenn die FI aus rechtlichen Gründen Veränderungen am IBM Cloud Service nicht akzeptieren kann. Außerdem wird im Cloud-Addendum für Finanzdienstleistungen die EBA-Empfehlung, dass der CSP das outsourcende Institut beim Transfer zu einem anderen Service-Anbieter unterstützen sollte, behandelt.

# Zusammenfassung

FIs können IBM Cloud nutzen, um materielle Outsourcing-Aktivitäten zu implementieren. IBM Cloud geht auf die EBA-Empfehlungen über das Outsourcing zu Cloud-Service-Anbietern für FIs ein. Die Industriekenntnisse von IBM, in Zusammenspiel mit unseren Cloud-Fähigkeiten, kann FIs Vorteile im Hinblick auf Kosten, Flexibilität und Geschwindigkeit bieten, wobei sie stets Kontrolle über die outgesourceten Aktivitäten behalten, wie von der EBA gefordert. IBM kann FIs bei jedem Schritt ihres Wegs zur Cloud unterstützen – von Entwicklung zu Migration, wobei Cloud-Services genutzt werden, die für hochgradig regulierte Workloads ausgestattet sind.

## Haftungsausschluss

Der Kunde ist selbst für die Einhaltung verschiedener Gesetze und Richtlinien verantwortlich. Kunden müssen sich hinsichtlich der Ermittlung und Interpretation geltender Gesetze und Vorschriften, die die Geschäfte des Unternehmens betreffen, auf eigenen Antrieb hin rechtlich beraten lassen – auch inklusive der Maßnahmen, die sie ergreifen müssen, um alle Gesetze und Vorschriften einzuhalten. IBM bietet weder rechtliche, buchhalterische noch revisionsbezogene Beratung an. Des Weiteren übernimmt IBM keine Garantie dafür, dass die von IBM bereitgestellten Services oder Produkte die Einhaltung gesetzlicher Bestimmungen oder Vorschriften durch den Kunden sicherstellen. Obwohl jeder Versuch unternommen wurde, die Genauigkeit dieses Dokuments zu sichern, können die hierin angegebenen Informationen unvollständig oder fehlerhaft sein, und keinerlei Repräsentation oder Garantie über die Richtigkeit, Zuverlässigkeit oder Vollständigkeit des Dokuments gegeben.

## Nützlicher Link:

[www.ibm.com/cloud/banking/security](http://www.ibm.com/cloud/banking/security)

### Erstellt von:

Nicolò Lorenzoni  
IBM Cloud Architect Leader FSS

Giovanni Boniardi Senior  
Infrastructure Consultant

Luis Lara Pezzi  
Cloud Platform FSS Industry Lead  
for Europe

### Gepüft von:

Heather Hinton  
Hybrid Cloud CISO

David Cass  
Cloud and SaaS CISO

Carlo Comporti  
Promontory Financial Group -  
Managing Director

Mafalda Garcia  
Counsel

IBM Deutschland GmbH  
IBM-Allee 1  
71139 Ehningen  
[ibm.com/de](http://ibm.com/de)

IBM Österreich  
Obere Donaustraße 95  
1020 Wien  
[ibm.com/at](http://ibm.com/at)

IBM Schweiz  
Vulkanstrasse 106  
8010 Zürich  
[ibm.com/ch](http://ibm.com/ch)

IBM, das IBM Logo, [ibm.com](http://ibm.com) und IBM Cloud sind eingetragene Marken der International Business Machines Corporation in vielen Ländern weltweit. Weitere Produkt- und Servicennamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Website „Copyright and trademark information“ unter <http://www.ibm.com/legal/us/en/copytrade.shtml>

Dieses Dokument ist aktuell zum Datum der Veröffentlichung und kann von IBM jederzeit ohne Vorankündigung geändert werden. Nicht alle Angebote sind in jedem Land verfügbar, in dem IBM vertreten ist.

Alle in diesem Dokument enthaltenen Informationen werden „ohne Gewähr“ und ohne ausdrückliche oder implizite Gewährleistung bereitgestellt, einschließlich der implizierten Gewährleistung für Handelbarkeit oder die Eignung für einen bestimmten Zweck oder die Nichtverletzung der Rechte Dritter.

Für IBM Produkte gelten die Gewährleistungen gemäß den AGB der Vereinbarungen, nach denen sie bereitgestellt werden.

Erklärung zum Sicherheitsverfahren: Die Sicherheit von IT-Systemen beinhaltet den Schutz von Systemen und Daten durch Verhinderung, Erkennung und Abwehr von unbefugten Zugriffsversuchen (die interner oder externer Art sein können). Unbefugte Zugriffe können dazu führen, dass Daten manipuliert, zerstört oder widerrechtlich entwendet werden. Zudem ist eine Beschädigung oder missbräuchliche Nutzung der Systeme möglich, einschließlich Angriffen auf andere Systeme. Kein IT-System oder IT-Produkt sollte als vollkommen sicher betrachtet werden. Kein Produkt und keine Sicherheitsmaßnahme können unbefugte Zugriffe stets verhindern. IBM Systeme und Produkte basieren auf einem umfassenden Sicherheitsansatz, der zwingend zusätzliche Betriebsprozeduren vorschreibt und möglicherweise andere Systeme, Produkte oder Services voraussetzt, um maximale Effektivität bieten zu können. IBM garantiert nicht, dass Systeme und Produkte vor dem böswilligen oder illegalen Verhalten anderer Parteien sicher sind.

© Copyright IBM Corporation 2018

79020079DEDE-02