



IBM unterstützt Banken
bei der Umsetzung
von Empfehlungen
der European Banking
Authority bezüglich des
Cloud-Computing

Einleitung

Die Europäische Bankenaufsichtsbehörde (EBA) veröffentlichte ihre Empfehlungen im Bericht *Empfehlungen zur Auslagerung an Cloud-Anbieter*, die ab 1. Juli 2018 anzuwenden sind. Sie bieten eine Anleitung/Klarstellung für Kreditinstitute und Investmentgesellschaften in der EU, die unter der Bezeichnung Finanzinstitute zusammengefasst werden, bezüglich der Umsetzung der 'Committee of European Banking Supervisors guidelines on outsourcing' („CEBS-Richtlinien“). Diese befassen sich mit dem Thema „Outsourcing an Cloud-Service-Provider“ (CSP).

Zusätzlich zu den früheren CEBS-Richtlinien konzentrieren sich die EBA-Empfehlungen für Finanzinstitute in der EU auf die folgenden sechs Hauptbereiche:

1. Bewertung der Wesentlichkeit von Auslagerungen / Cloud-Outsourcing und Informationen an Regulierungsbehörden
2. Das Zutritts- und Prüfungsrecht für Finanzinstitute und zuständige Behörden
3. Die Sicherheit der Daten und die dafür verwendeten Systeme
4. Standort der Datenverarbeitung
5. Weiterverlagerung
6. Der Plan für unvorhersehbare Ereignisse und Kündigungsmodalitäten

IBM begrüßte die Initiative der Europäischen Bankenaufsichtsbehörde und beteiligte sich aktiv am Konsultationsprozess mit dem Ziel, einen gemeinsamen regulatorischen Rahmen für das Outsourcing an Cloud-Service-Provider zum Nutzen aller Beteiligten festzulegen. IBM ist der Auffassung, dass die Empfehlungen der EBA die Einführung von Cloud Technologien unterstützen und die Konvergenz der Praktiken von Finanzinstituten mit den Praktiken und Erwartungen der Aufsichtsbehörden fördern.

IBM unterstützt Finanzinstitute aktiv dabei, die Herausforderungen im Bereich Cloud-Outsourcing zu bewältigen.

Durch unser globales Know-how in der Finanzdienstleistungsbranche, kombiniert mit unserer weltweiten Erfahrung im Bereich Outsourcing, haben wir bei IBM ein gutes Verständnis für die Bedürfnisse und Anforderungen von Finanzinstituten. Wir haben diese Anforderungen in unserer Cloud-Plattform umgesetzt und können damit herausragende Möglichkeiten zur Abbildung von Kernprozessen und sonstigen Workloads anbieten.

Diese Fähigkeiten werden durch unseren vertraglichen Rahmen ergänzt, der die spezifischen Schwerpunkte der EBA-Empfehlungen abdeckt und es Finanzinstituten ermöglicht, die Vorteile der Cloud zu nutzen, gleichzeitig revisionssicher zu sein und die geltenden Vorschriften einzuhalten.

Zusammenfassend lässt sich sagen, dass die IBM Cloud eine Umgebung bietet, die es Finanzinstituten ermöglicht, die EBA-Empfehlungen zum Cloud-Outsourcing einzuhalten, wenn sie die IBM Cloud sowohl für wesentliche, als auch für sonstige Auslagerungen, nutzen.

IBM adressiert die Anforderungen an Cloud-Services-Provider

Finanzinstitute stehen derzeit unter großem Druck, die Erwartungen von Kunden und Eigentümern zu erfüllen und gleichzeitig den steigenden regulatorischen Anforderungen gerecht zu werden. IBM nutzt sein umfassendes Branchenwissen, um seine Cloud-Umgebung zu gestalten, bereitzustellen und kontinuierlich zu aktualisieren, damit sie den Anforderungen der Finanzdienstleistungsbranche gerecht wird und gleichzeitig den Empfehlungen der EBA zum Outsourcing an Cloud-Service-Provider genügt. IBM als Cloud-Service-Provider kommt diesen Verpflichtungen wie folgt nach.

Bewertung der Wesentlichkeit von Cloud-Outsourcing-Aktivitäten und Informationen an die zuständigen Behörden

Gemäß den CEBS-Richtlinien verlangt die EBA von Finanzinstituten, die Wesentlichkeit von Auslagerungen zu bewerten und die zuständigen Behörden zu informieren. Zusätzlich sind Finanzinstitute verpflichtet, ein Verzeichnis sowohl der wesentlichen, als auch der sonstigen ausgelagerten Tätigkeiten zu führen.

Obwohl die Durchführung einer Wesentlichkeitsbewertung und die anschließende Unterrichtung der Aufsichtsbehörden in der Verantwortung der Finanzinstitute verbleiben, wird IBM dazu beitragen, die Anforderungen zu erfüllen, sodass die Finanzinstitute ihre Geschäftsziele erreichen und ihre regulatorischen Verpflichtungen erfolgreich erfüllen können. Jeder IBM Cloud Service hat eine klar umrissene Servicebeschreibung, in der die Details dieses Services eindeutig formuliert sind, sodass die Anforderungen der Wesentlichkeitsbewertung erfüllt werden. IBM unterstützt Firmen bei der Bewertung und Dokumentation der Wesentlichkeit von Auslagerungen und Informationen zum Outsourcing, die an den Regulator geschickt werden müssen.

Prüfungsrecht der Institutionen und zuständigen Behörden

Gemäß den Leitlinien von EBA und CEBS müssen Outsourcing-Institutionen und zuständige Behörden sicherstellen, dass sie uneingeschränkter Zugang zu den CSP-Geschäftsräumen und uneingeschränkte Prüfungs- und Auditrechte im Zusammenhang mit den per Outsourcing ausgelagerten Services haben.

Die Liste der EBA-Empfehlungen fördert den IBM Ansatz, Zertifizierungen und Berichte unabhängiger, weltweit anerkannter Dritter einzusetzen, als verhältnismäßiger und risikobasierter Ansatz zur Durchführung der Sorgfaltspflicht und der anschließenden laufenden Überwachung. IBM führt eine umfassende Liste von Compliance-Zertifizierungen und Auditberichten. Die vollständige Liste ist auf der [Webseite IBM Cloud Compliance](#) einsehbar, wo auch Anweisungen zum Herunterladen bestimmter Berichte verfügbar sind.

Die IBM Cloud wurde für kritische und nicht kritische Workloads mit dem Blick auf die Sicherheit und Ausfallsicherheit entwickelt und erstellt. Dies wird durch unsere [Zertifizierungen](#) und das Vertrauen der Finanzinstitute belegt: Sowohl weltweite als auch Europäische Finanzinstitute haben sich dafür entschieden, dass IBM sie bei der Förderung von Innovationen auf den Ebenen von Prozessen und Infrastrukturtechnologie unterstützen soll, und lagern sowohl wesentliche als auch sonstige Aktivitäten per Outsourcing in die IBM Cloud aus.

IBM hat ein Cloud Addendum für den Finanzdienstleistungssektor entwickelt, zu dessen vertraglichen Verpflichtungen unter anderem die Bereitstellung von Audit- und Zugriffsrechten für seine Kunden gemäß den EBA-Empfehlungen gehört.

IBM hat seit dem Jahr 2016 einen Cloud Compliance Advisory Body (CCAB) für Finanzinstitute. Dieses Gremium tagt vierteljährlich und befasst sich mit Problemen und Fragen individueller und globaler regulatorischer Anforderungen. Die Teilnahme am CCAB bietet auch Einblicke in den Beurteilungsprozess der internen Kontrollen von IBM und vergrößert die Reichweite durch umfangreiche externe Zertifizierungen und Auditberichte weiter.

Sicherheit von Daten und Systemen

Die EBA empfiehlt den Finanzinstituten, die Aktivitäten zu klassifizieren, die an den Cloud-Service-Provider zu übertragen sind, um pro Aktivität den erforderlichen Level festzulegen für: Schutz der Vertraulichkeit von Daten, Kontinuität der per Outsourcing ausgelagerten Aktivitäten sowie Integrität und Rückverfolgbarkeit von Daten und Systemen im Rahmen des beabsichtigten Cloud Outsourcing.

Die IBM Cloud bietet Finanzinstituten einzigartige Funktionen in Bezug auf die Sicherheit von Daten und Systemen und bietet die Möglichkeit, höchst anspruchsvolle Workloads zu hosten. Das Dokument [Data Security and Privacy Principles for IBM Cloud Services](#) beschreibt die Sicherheitsregeln, die den technischen und organisatorischen Maßnahmen zugrunde liegen, die für alle IBM Cloud-Services greifen. Spezifische technische und organisatorische Maßnahmen, die von IBM für jedes IBM Cloud Services-Produkt ergriffen werden, werden beschrieben in den [Cloud Services Data Sheets](#).

Von der Mandatenfähigkeit über die Datenverschlüsselung bis hin zur dedizierten physischen Infrastruktur können Finanzinstitute aus einer Vielzahl von Sicherheitsoptionen wählen, um ihre Workloads je nach ihren spezifischen Anforderungen einzusetzen.

Wenn zusätzliche Sicherheitsfunktionen erforderlich sind, kann IBM mit dem Finanzinstitut zusammenarbeiten, um zusätzliche Sicherheitslösungen anzubieten, die alle erhöhten Anforderungen an die Cloud-Umgebung erfüllen.

Speicherort von Daten und Standort der Datenverarbeitung

Finanzinstitute müssen bei der Unterzeichnung von Outsourcing-Vereinbarungen, die außerhalb des EWR getroffen werden, wegen möglicher Datenschutzrisiken besondere Sorgfalt walten lassen. Die EBA empfiehlt Finanzinstituten, einen risikobasierten Ansatz für Daten- und Datenverarbeitungsstandorte zu wählen, der rechtliche Risiken und Compliance-Fragen einschließt.

Verfügbare IBM Cloud-Services werden an einer Vielzahl an Standorten gehostet. Die vollständige Liste ist [hier](#) einsehbar. Finanzinstitute wählen aus der Liste ihren bevorzugten Standort für die Implementierung eines IBM Cloud-Services aus. Dabei können sie sicher sein, dass ihr Cloud-Service und ihre Daten am ausgewählten Standort bleiben.

Für jeden IBM Cloud-Service wird ein spezielles Datenblatt zur Verfügung gestellt, das die Informationen zu den IBM Hosting- und IBM Verarbeitungsstandorten beschreibt. Das Repository der Datenblätter kann [hier](#) eingesehen werden. Alle sind gemäß der allgemeinen Datenschutzanforderungen und des IBM Data Processing Addendums ausgestellt. Falls ein Teil eines IBM Cloud-Services außerhalb des EWR erbracht wird, gelten für die IBM Kunden die [European Union Model Clauses \(EUMC\)](#). Diese stellen sicher, dass IBM Datenimportprogramme mit geeigneten Sicherheitseinrichtungen ausgestattet sind, Datenschutz und die Persönlichkeitsrechte betreffend. Außerdem ist IBM Mitglied im Verhaltenskodex [European Cloud Code of Conduct](#).

Weiterverlagerung

Die Institute müssen die mit der Weiterverlagerung verbundenen Risiken berücksichtigen: Die Konsistenz der Verpflichtungen entlang der Kette der Unterauftragnehmer muss gewährleistet sein. Es muss eine unverzügliche Benachrichtigung erfolgen, wenn wesentliche Änderungen in der Kette der Unterauftragnehmer geplant sind, und es müssen klare Verantwortlichkeiten im Rahmen der Outsourcing-Vereinbarung zugewiesen werden.

Wie vom CEBS gefordert und durch die EBA-Empfehlungen bekräftigt, muss jeder von IBM zur Bereitstellung von Cloud-Services in IBM Cloud-Rechenzentren eingesetzte Dritte die gleichen Verpflichtungen erfüllen, die zwischen IBM und dem Finanzinstitut vereinbart wurden. Darüber hinaus verlangt IBM von Unterauftragnehmern mit Zugriff auf Kundeninhalte, technische und organisatorische Sicherheitsmaßnahmen zu treffen, die es IBM ermöglichen, seinen Verpflichtungen für einen Cloud-Service nachzukommen. Eine aktuelle Liste von Unterauftragnehmern und deren Rollen wird auf Anfrage zur Verfügung gestellt. Die Institute können die Liste der Unterauftragnehmer von Dritten (falls zutreffend) für IBM Cloud-Services im Datenblatt jedes Services einsehen.

Es ist wichtig zu beachten, dass IBM mit dem Finanzinstitut eine Benachrichtigungsfrist für Änderungen in der Kette der Unterauftragnehmer vertraglich vereinbart, damit der Kunde seine interne Risikobewertung durchführen kann.

Der Plan für unvorhersehbare Ereignisse und Ausstiegsstrategien

Die EBA empfiehlt Finanzinstituten, Vorkehrungen zu treffen, um die Kontinuität ihrer Geschäftstätigkeit zu wahren und eine Kündigungs- und Ausstiegsklausel einzuführen. Der Cloud-Services-Provider muss die Übertragung der Aktivität auf einen anderen Service-Provider oder im Falle der Beendigung der Vereinbarung in die direkte Verantwortung der Finanzinstitute unterstützen.

Die IBM Cloud definiert einen Business-Continuity-Plan pro IBM Cloud-Service, wie es in den [Data Security and Privacy Principles for IBM Cloud Services](#) festgelegt wurde. Außerdem werden für jeden Service Business-Continuity-Pläne als Teil des [IBM Cloud Service Data Sheet](#) bereitgestellt.

[Das IBM Cloud Services Agreement](#) umfasst die Option, einen IBM Cloud-Service zu beenden, wenn das Finanzinstitut Änderungen an einem IBM Cloud-Service aus rechtlichen Gründen nicht akzeptieren kann. Darüber hinaus unterstreicht das Cloud Addendum for Financial Services die EBA-Anforderung, dass der CSP eine Outsourcing-Institution bei der Übertragung auf einen anderen Service Provider unterstützt.

Zusammenfassung

Finanzinstitute nutzen die IBM Cloud für wesentliche Auslagerungen. Die IBM Cloud trägt zur Erfüllung der EBA-Anforderungen an die Finanzinstitute bezüglich Outsourcings an Cloud-Services-Providers bei. Das Branchenwissen von IBM, kombiniert mit den IBM Cloud-Funktionalitäten, bringt Finanzinstituten Vorteile in Bezug auf Kosten, Agilität und Geschwindigkeit. IBM trägt zur Kontrolle über die ausgelagerten Aktivitäten bei, wie sie von der EBA gefordert wird. IBM unterstützt Finanzinstitute bei jedem Schritt auf ihrem Weg in die Cloud, von der Entwicklung bis zur Migration. IBM bietet Cloud-Services, die für stark regulierte Workloads vorbereitet sind.

Haftungsausschluss

Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein den Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Auslegung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die ihre Geschäftstätigkeit und die von ihnen eventuell einzuleitenden Maßnahmen zur Einhaltung dieser Gesetze und Bestimmungen betreffen. IBM erteilt keine Rechts- oder Steuerberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen und gesetzlichen Bestimmungen. Trotz des Bestrebens, die Richtigkeit dieses Dokuments zu gewährleisten, können die hierin enthaltenen Informationen unvollständig oder ungenau sein. Es wird keine Gewährleistung irgendeiner Art hinsichtlich seiner Genauigkeit, Verlässlichkeit oder Vollständigkeit übernommen.

Nützlicher Link:

ibm.com/cloud/banking/security

Vorbereitet von:

Nicolò Lorenzoni
IBM Cloud Architect Leader FSS

Giovanni Boniardi
Senior Infrastructure Consultant

Luis Lara Pezzi
Cloud Platform FSS Industry Lead
for Europe

Geprüft 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

IBM Österreich

Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz

Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:

ibm.com

IBM, das IBM Logo, ibm.com und Watson sind eingetragene Marken oder Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter ibm.com/legal/us/en/copytrade.shtml

Dieses Dokument ist zum Datum seiner Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle IBM Angebote sind in jedem Land, in welchem IBM tätig ist, verfügbar.

Die Informationen in diesem Dokument werden auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt, einschließlich, aber nicht beschränkt auf die Gewährleistungen für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter.

Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

Erklärung zu geeigneten Sicherheitsvorkehrungen: Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Angriffen. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme oder Produkte vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

© Copyright IBM Corporation 2019

79020079-DEDE-03