

# Informationen über die DekaBank Deutsche Girozentrale und ihre Kryptowerte-Dienstleistungen.

Stand 01/2026

The logo for DekaBank, featuring the word "Deka" in a bold, white, sans-serif font on a red background. The "D" is stylized with a vertical bar to its left.

Die DekaBank erbringt gegenüber institutionellen Kunden die Kryptowerte-Dienstleistungen der Verwahrung und Verwaltung von Kryptowerten für Kunden, der Ausführung von Aufträgen über Kryptowerte für Kunden und der Erbringung von Transferdienstleistungen für Kryptowerte für Kunden. Gemäß den Vorgaben aus Art. 75 Abs. 3, 66 Abs. 3, 72 Abs. 2 der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (kurz: MiCAR) erteilt die DekaBank hiermit folgende Informationen im Zusammenhang mit der Erbringung von Kryptowerte-Dienstleistungen:

## **A. Informationen zur Verwahrstrategie und zu den Sicherheitssystemen**

Die DekaBank bietet institutionellen Kunden eine sichere und verlässliche Lösung zur Verwahrung von Kryptowerten an. Dabei steht die Einhaltung höchster Sicherheitsstandards und gesetzlicher Vorgaben, insbesondere der europäischen MiCAR-Verordnung, im Mittelpunkt.

### **1. Unternehmensprofil und Geschäftstätigkeit**

Als zentraler Finanzdienstleister der Sparkassen-Finanzgruppe baut die DekaBank ihr digitales Angebot gezielt aus und integriert die Verwahrung von Kryptowerten als festen Bestandteil ihrer Digitalisierungsstrategie.

Die DekaBank übernimmt für ihre institutionellen Kunden die vollständige Verwahrung und Verwaltung von zugelassenen Kryptowerten. Dabei verwahrt die Bank auch die zugehörigen privaten kryptographischen Schlüssel, die für den Zugriff und die Übertragung dieser Werte notwendig sind. Für die Verwahrung nutzt die DekaBank eigene technische Systeme („warm Wallets“) und wendet höchste Sicherheitsstandards an. Bei der von der DekaBank bereitgestellten Sammelverwahrung werden die Kryptowerte mehrerer Kunden gemeinsam in einer sogenannten Omnibus Wallet verwahrt.

Neben der Verwahrung bietet die DekaBank ihren Kunden auch die Möglichkeit, Transaktionen mit Kryptowerten durchzuführen,

sowohl innerhalb der Bank als auch zu externen Wallets. Dabei bleibt der direkte Zugriff auf die Blockchain der Bank vorbehalten, was zusätzliche Sicherheit bietet. Kunden geben ihre Transaktionsaufträge über das Portal „Deka Easy Access“ (DEA) ein. Die Bank übernimmt daraufhin die technische Umsetzung der Transaktion. Nach dem Kauf eines Kryptowerts durch den Kunden bei einem externen Anbieter werden die Kryptowerte zunächst auf eine speziell erzeugte Proxy Wallet übertragen. Nach erfolgreicher Prüfung erfolgt die Umbuchung in die zentrale Verwahrung der DekaBank. Zum Schutz der Kunden gelten bei Auszahlungen an externe Wallets besonders hohe Sicherheitsstandards. In diesem Fall werden Transaktionen erst freigegeben, nachdem die Identität des Kunden sowie die Zieladresse eindeutig wurde.

### **2. Governance und interne Zuständigkeit**

Die DekaBank hat klare Zuständigkeiten, Zugriffsrechte und Kontrollprozesse für die Kryptoverwahrung definiert. Dazu zählen ein internes Kontrollsystem mit Vier-Augen-Prinzip, rollenbasierte Workflows und automatisierte Abläufe zur Absicherung des Geschäftsbetriebs (zum Beispiel im Falle eines Standort/Infrastrukturausfalls, IT-Ausfalls, Personal- oder Dienstleistungsausfalls). Es bestehen organisatorische Maßnahmen zur Risikovermeidung, etwa durch technische und manuelle Kontrollen, die Einhaltung regulatorischer Vorgaben (z. B. Geldwäscheprävention) sowie regelmäßige Bewertungen der zu berücksichtigenden Risiken. Die DekaBank stellt durch eine sorgfältige Prüfung und Auswahl sicher, dass Drittanbieter über robuste Sicherheits- und Kontrollsysteme verfügen. Zudem werden im Rahmen eines umfassenden Vertragsmanagements (z. B. durch das zentrale Auslagerungsmanagement) klare Anforderungen an Sicherheitsstandards und Berichtspflichten in den Verträgen mit Drittanbietern festgelegt. Alle Mitarbeiter in den relevanten Organisationseinheiten sind zu den regulatorischen, technischen und prozessbezogenen Anforderungen geschult und verfügen über die erforderlichen Qualifikationen.

### **3. Kundenzugang und Kommunikationswege mit dem Kunden**

Die DekaBank stellt ihre Kryptoverwahrung ausschließlich institutionellen Kunden in Deutschland zur Verfügung. Interessierte Unternehmen können über die Website oder über das Kundenportal mit einem zuständigen Ansprechpartner in Kontakt treten. Für bestehende Kunden erfolgt die Kontaktaufnahme direkt über den persönlichen Kundenberater. Bevor ein Kunde die Kryptoverwahrung nutzen kann, durchläuft er ein umfassendes Onboarding. Dazu gehören die vertragliche Vereinbarung aller relevanten Rahmenbedingungen, gesetzlich vorgeschriebene Prüfungen sowie die technische Einrichtung von Benutzerzugängen. Nach Vertragsabschluss erhalten Kunden Zugang zum Kundenportal DEA. Diese browserbasierte Anwendung ermöglicht eine einfache Verwaltung der Kryptowerte, inklusive Auftragserteilung von Transaktionen (Ein- und Auslieferungen) sowie der Bestandsübersicht. Der Zugang ist durch Sicherheitsverfahren wie Multi-Faktor-Authentifizierung geschützt.

Für die Kommunikation mit ihren Kunden nutzt die DekaBank vorrangig das Kundenportal DEA sowie den E-Mail-Kanal. Über diese Wege erfolgt der sichere und nachvollziehbare Austausch von Informationen, Nachrichten und Dokumenten. Ergänzend besteht die Möglichkeit auch telefonisch mit dem jeweiligen Kundenbetreuer in Kontakt zu treten.

### **4. Sicherheitsmechanismen der Kryptoverwahrung und Verwaltung**

Die DekaBank setzt auf ein mehrstufiges Sicherheitskonzept, um ihre Dienstleistungen im Bereich der Kryptoverwahrung technisch, organisatorisch und prozessual abzusichern. Ziel ist es, Kundengelder vor Verlust, Missbrauch und unbefugtem Zugriff zu schützen.

Für die Verwahrung der Kryptowerte nutzt die DekaBank Multi-Signature-Wallets, die für Transaktionen mehrere Signaturen erfordern. Zusätzlich kommen physische Sicherheitsgeräte sowie zertifizierte Hardware Security Module (HSM) zum Einsatz, um die Private Keys sicher zu verwahren. Zur zusätzlichen Absicherung verwendet die DekaBank Proxy-Wallets, die für jede eingehende Transaktion individuell und einmalig erstellt werden. Erst nach eingehender Prüfung über die Zuordnung und die Konformität der Kryptowerte erfolgt die Übertragung in die zentrale Omnibus-Wallet, in denen die Vermögenswerte verschiedener Kunden gemeinsam verwahrt, aber systemseitig den jeweiligen Kunden eindeutig zugeordnet werden.

Jede Blockchain erhält eine eigene Omnibus-Wallet für die Sammelverwahrung, wobei die interne Zuordnung in den Systemen der DekaBank erfolgt. Die Kryptowerte der Kunden werden strikt getrennt von den Eigenbeständen der DekaBank verwahrt. Diese Eigenbestände werden lediglich für die Bezahlung von Netzwerkgebühren verwendet. Die DekaBank tritt ausschließlich als Verwahrstelle auf, ohne Zugriff oder Anspruch auf Kryptowerte des Kunden.

Für den Fall technischer Störungen oder unerwarteter Zwischenfälle hat die DekaBank umfassende Notfall- und Wiederherstellungspläne etabliert. Alle damit einhergehenden Maßnahmen werden regelmäßig auf Aktualität und Geeignetheit geprüft und bei Bedarf angepasst. Darüber hinaus hat die DekaBank Aufzeichnungs- und Archivierungsvorgaben

implementiert, die ebenfalls die Wiederherstellung der Daten sichern. Um die Einhaltung aller Sicherheitsmaßnahmen sicherzustellen, führt die DekaBank jährliche Assessments für operationelle Risiken und Non-Financial Risks durch und überwacht sämtliche Prozesse. Technisch ist die Infrastruktur durch moderne Schutzmaßnahmen, wie Firewalls, Verschlüsselung und Zugriffskontrollen geschützt. Transaktionen unterliegen einem mehrstufigen Freigabeprozess, wobei bei höheren Beträgen oder unbekanntem Empfängern zusätzliche Kontrollstufen angewendet werden.

Die DekaBank informiert ihre Kunden bereits vor Vertragsschluss sowie fortlaufend während der Geschäftsbeziehung über alle relevanten Aspekte der Kryptoverwahrung. Über das Portal DEA erhalten Kunden jederzeit Einsicht in ihre aktuellen Kryptobestände und Transaktionen. Ergänzend dazu wird mindestens vierteljährlich und auf Anfrage ein Bericht über die vom Kunden verwahrten Kryptopositionen und -transfers bereitgestellt. Auf Anfrage erhalten Kunden Zugang zu allen kundenbezogenen Informationen und Daten, die im Zusammenhang mit der Kryptoverwahrung aufgezeichnet werden.

### **5. Hinweis auf Rechtskonformität und Aktualisierungen**

Die DekaBank stellt sicher, dass ihre Dienstleistungen im Bereich der Kryptoverwahrung jederzeit den geltenden gesetzlichen Vorgaben entsprechen. Dafür werden interne Prozesse regelmäßig überprüft und bei Bedarf angepasst. Mithilfe moderner Compliance-Systeme gewährleistet die DekaBank die Einhaltung gesetzlicher Vorgaben und arbeitet dabei eng und transparent mit den zuständigen Aufsichtsbehörden zusammen. Die Strategie zur Kryptoverwahrung wird mindestens einmal pro Jahr aktualisiert oder kurzfristig angepasst, sobald sich rechtliche Rahmenbedingungen wesentlich ändern.

## B. Risikohinweise

Die Investition in Kryptowerte ist mit erheblichen Risiken verbunden, die teilweise außerhalb der Kontrolle der DekaBank liegen. Die nachfolgenden Risikohinweise dienen dem Zweck, Kunden auf die wesentlichen Risiken im Zusammenhang mit der Verwahrung, dem Handel und Transaktionen mit Kryptowerten und kryptografischen Instrumenten hinzuweisen. Diese Auflistung ist nicht abschließend und deckt nicht alle möglichen Risiken ab, die sich durch technologische, regulatorische oder marktwirtschaftliche Veränderungen ergeben können. Kunden wird daher empfohlen, sich eingehend über potenzielle Risiken zu informieren und, falls erforderlich, unabhängigen steuerlichen, rechtlichen und finanziellen Rat einzuholen.

### Blockchain-Technologie

Die Blockchain-Technologie stellt eine noch relativ junge und daher nur begrenzt erprobte technologische Innovation dar. Kryptowerte wie Bitcoin basieren auf dieser Technologie. Es besteht das Risiko, dass die Blockchain-Technologie durch technische Probleme oder äußere Einflüsse in ihrer Funktionsfähigkeit beeinträchtigt wird. Darüber hinaus könnten Fortschritte in der Kryptographie oder technologische Entwicklungen, wie beispielsweise die Einführung von Quantencomputern, die Sicherheit und Integrität von Kryptowerten gefährden. Ein weiteres Risiko besteht darin, dass die zugrunde liegende Software Schwächen oder Fehler aufweist, die im schlimmsten Fall zu einem vollständigen Verlust des Kryptowerts führen können.

### Akzeptanzrisiko

Kryptowerte sind keine gesetzlich anerkannten Zahlungsmittel, und es gibt keine Verpflichtung für Anbieter von Waren und Dienstleistungen oder andere Marktteilnehmer, diese als Zahlungsmittel zu akzeptieren. Die Nutzung von Kryptowerten hängt daher maßgeblich von der Akzeptanz innerhalb der Gesellschaft und der Wirtschaft ab. Sollte die Akzeptanz von Kryptowerten zukünftig abnehmen, könnte dies zu einem erheblichen Wertverlust bis hin zum Totalverlust führen.

### Wertrisiko

Im Gegensatz zu physischen Vermögenswerten wie Edelmetallen besitzen Kryptowerte keinen intrinsischen oder materiellen Wert. Ihr Marktwert wird ausschließlich durch das Verhältnis von Angebot und Nachfrage bestimmt. Ein plötzlicher oder anhaltender Rückgang der Nachfrage kann zu einem drastischen Wertverlust führen, der nicht durch einen inneren Wert begrenzt wird. Dies birgt das Risiko erheblicher Verluste bis hin zum Totalverlust.

### Aufgaberisiko

Die Funktionsfähigkeit der Distributed-Ledger-Technologie, auf der viele Kryptowerte basieren, hängt bei Kryptowährungen wie Bitcoin (BTC), Bitcoin Cash (BCH), Litecoin (LTC) und Dogecoin (DOGE) stark von der Aktivität der sogenannten Miner ab. Diese Miner stellen ihre Rechenleistung für die Erstellung neuer Blöcke zur Verfügung. Sollten Miner ihre Tätigkeit einstellen – sei es aufgrund mangelnder Rentabilität, fehlender Finanzierung oder geringem Interesse – könnte dies die Funktionsfähigkeit der Technologie erheblich beeinträchtigen.

Bei Kryptowerten wie Ether (ETH), Solana (SOL), Cardano (ADA), Algorand (ALGO) oder Polygon (MATIC) besteht zusätzlich das Risiko, dass eine Konzentration von

Eigentümern, die einen großen Teil des Netzwerks kontrollieren (z. B. 50 % des gestakten Wertes), die Netzwerksicherheit gefährdet. Ein solcher Angriff könnte die Validierung von Transaktionen verhindern und die Funktionsfähigkeit des Netzwerks beeinträchtigen.

### Risiko der Unumkehrbarkeit von Kryptoauszahlungen

Transaktionen auf der Blockchain sind grundsätzlich unumkehrbar. Teilnehmer, die Kryptowerte auf eine Blockchain-Adresse auszahlen lassen möchten, müssen sicherstellen, dass die eingegebene Adresse korrekt ist. Fehler bei der Eingabe können dazu führen, dass die Kryptowerte unwiederbringlich verloren gehen. Ebenso besteht bei Einzahlungen das Risiko, dass eine falsche Wallet-Adresse verwendet wird, was ebenfalls zu einem Verlust führen kann. Teilnehmer sollten daher mit äußerster Sorgfalt vorgehen, um solche Fehler zu vermeiden.

### Regulatorische Risiken

Die rechtlichen Rahmenbedingungen für Kryptowerte und die zugrunde liegende Distributed-Ledger-Technologie können sich ändern. Neue gesetzliche Regelungen oder Änderungen bestehender Vorschriften könnten die Nutzung und den Wert von Kryptowerten negativ beeinflussen. Beispielsweise könnten strengere Vorschriften zur Verwahrung oder Nutzung von Kryptowerten dazu führen, dass technische Betreiber ihre Aktivitäten einstellen oder die Akzeptanz von Kryptowerten sinkt. Solche regulatorischen Änderungen können zu einem Wertverlust bis hin zum Totalverlust führen.

### Steuerliche Risiken

Gewinne aus dem Handel mit Kryptowerten können steuerpflichtig sein. Änderungen in der steuerlichen Behandlung oder eine strengere Auslegung durch in- oder ausländische Finanzbehörden könnten die Steuerbelastung erhöhen und die Nettorendite verringern. Teilnehmer sollten sich über die steuerlichen Auswirkungen ihrer Investitionen im Klaren sein und gegebenenfalls steuerlichen Rat einholen.

### Cybersicherheitsrisiko

Trotz der Anwendung hoher Sicherheitsstandards besteht das Risiko, dass Kryptowerte durch Cyberangriffe oder physische Angriffe verloren gehen. Sicherheitsmaßnahmen können keine vollständige Sicherheit garantieren. Ein erfolgreicher Angriff auf die IT-Infrastruktur könnte zu einem Verlust der verwahrten Kryptowerte führen, der bis hin zum Totalverlust reichen kann.

### Manipulationsrisiko

Die Sicherheit der Distributed-Ledger-Technologie basiert auf kryptografischen Verfahren, die Manipulationen verhindern sollen. Sollten diese Verfahren oder deren Implementierungen Schwächen aufweisen, könnten Cyberangriffe oder andere Manipulationen die Funktionsfähigkeit der Technologie beeinträchtigen. Dies könnte zu einem Verlust von Kryptowerten führen, der bis hin zum Totalverlust reichen kann.

### Risiko eines Mehrheitsangriffs

Bei Kryptowerten, die auf Proof-of-Work-Netzwerken basieren, besteht das Risiko eines sogenannten 51-%-Angriffs. Dabei könnten Miner, die mehr als die Hälfte der Rechenleistung kontrollieren, das Netzwerk manipulieren, Transaktionen blockieren oder doppelte Ausgaben („Double Spending“) durchführen. Ein solcher Angriff könnte die Integrität des Netzwerks gefährden und zu einem Wertverlust führen. Ähnliche Risiken bestehen bei Proof-of-Stake-Netzwerken, wenn eine kleine Anzahl von Eigentümern einen Großteil des

Netzwerks kontrolliert.

### **Transferkostenrisiko**

Der Transfer von Kryptowerten zwischen Blockchain-Adressen ist mit Gebühren verbunden. Steigende Transferkosten könnten die Nutzung von Kryptowerten als Zahlungsmittel unattraktiver machen und somit deren Marktwert negativ beeinflussen.

### **Risiko einer missbräuchlichen Nutzung von Zugangsdaten**

Teilnehmer, die ihre Zugangsdaten (z. B. E-Mail-Adresse, Passwort und Mobile-TAN) nicht ausreichend schützen, laufen Gefahr, dass Dritte unbefugt auf ihre Konten zugreifen. Ein solcher Missbrauch könnte zu unautorisierten Transaktionen und erheblichen Verlusten führen. Teilnehmer sollten daher ihre Zugangsdaten und Geräte sorgfältig sichern.

### **Risiko einer Kreditfinanzierung**

Die Finanzierung des Kaufs von Kryptowerten durch Kredite erhöht das Verlustrisiko erheblich. Neben möglichen Verlusten aus der Wertentwicklung müssen auch die Kreditkosten, insbesondere Zinsen, getragen werden. Sollte der Marktpreis der Kryptowerte sinken, könnten Teilnehmer nicht nur Verluste hinnehmen, sondern auch Schwierigkeiten haben, den Kredit zurückzuzahlen.

### **Höhere Risiken bei taggleichen Geschäften (Daytrading)**

Das sogenannte Daytrading, bei dem Kryptowerte innerhalb eines Tages mehrfach gekauft und verkauft werden, birgt erhöhte Risiken. Die hohe Handelsfrequenz kann zu Verlusten führen, insbesondere bei unerwarteten Marktbewegungen oder unzureichender Marktkenntnis.

### **Risiko unvollständiger Informationen**

Entscheidungen über den Kauf oder Verkauf von Kryptowerten sollten auf einer fundierten Informationsbasis getroffen werden. Teilnehmer, die auf unzureichende oder unvollständige Informationen zurückgreifen, laufen Gefahr, Fehlentscheidungen zu treffen, die zu Verlusten oder entgangenen Gewinnen führen können. Es wird empfohlen, zusätzliche Informationsquellen zu nutzen und gegebenenfalls Expertenrat einzuholen.

**Hinweis:** Diese Risikoinformationen sind nicht abschließend. Teilnehmer sollten sich umfassend informieren und bei Bedarf professionelle Beratung in Anspruch nehmen, um fundierte Entscheidungen zu treffen.

## C. Darstellung möglicher Interessenkonflikte

Die DekaBank hat Vorkehrungen getroffen, damit sich mögliche Interessenkonflikte zwischen der DekaBank, ihrer Geschäftsleitung, ihren Beschäftigten oder anderen Personen, die mit der DekaBank direkt oder indirekt durch Kontrolle verbunden sind, und Kunden oder zwischen den Kunden untereinander nicht auf die Kundeninteressen auswirken

Damit sich mögliche Interessenkonflikte zwischen der DekaBank, ihrer Geschäftsleitung, den Beschäftigten oder anderen Personen, die mit ihr direkt oder indirekt durch Kontrolle verbunden sind, und dem Kunden oder zwischen den Kunden untereinander nicht auf die Kundeninteressen, einschließlich ihrer Nachhaltigkeitspräferenzen, auswirken, sind in den Abschnitten I. und II. mögliche Interessenkonflikte dargestellt und unter Abschnitt III. getroffene Maßnahmen zum Schutz von Kundeninteressen.

I. In der DekaBank können Interessenkonflikte zwischen den Kunden und der DekaBank, Beschäftigten der DekaBank oder mit diesen verbundenen relevanten Personen, inklusive der Geschäftsleitung, Personen, die durch Kontrolle mit der DekaBank verbunden sind, und anderen Kunden bei folgenden Kryptowertedienstleistungen auftreten:

- Kryptokommissionshandel (Ausführung von Aufträgen über Kryptowerte für Kunden. Anschaffung oder Veräußerung von Kryptowerten im eigenen Namen auf fremde Rechnung),
- Kryptotransferdienstleistung (Erbringung von Transferdienstleistungen für Kryptowerte)
- Kryptoverwahrung (Verwahrung und Verwaltung von Kryptowerten für andere und damit verbundene Dienstleistungen)

Unter Kryptowerten versteht die DekaBank die digitale Darstellung eines Werts oder eines Rechts, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann. Unter den Begriff Kryptowerte werden gefasst Vermögenswertreferenzierter Token Art. 3 Abs. 1 Nr. 6 MiCAR (Asset-Referenced Tokens, ART), E-Geld-Token Art. 3 Abs. 1 Nr. 7 MiCAR (E-Money Tokens, EMT), und sonstige Token (z.B. Bitcoin, Ethereum)<sup>2</sup> einschließlich Utility-Token Art. 3 Abs. 1 Nr. 9 MiCAR (z. B. Token, die Zugang zu einem spezifischen Produkt oder einer Dienstleistung gewähren).

II. Es können Interessenkonflikte auch dadurch auftreten, dass

- der DekaBank oder einzelnen relevanten Personen der DekaBank Informationen vorliegen, die zum Zeitpunkt eines Kundengeschäfts noch nicht öffentlich bekannt sind,
- Anreize zur Bevorzugung eines bestimmten Kryptowertes vorliegen, zum Beispiel bei Analyse, Beratung, Empfehlung oder Auftragsausführung,
- Grundsätze oder Ziele, die den Umsatz, das Volumen oder den Ertrag der im Rahmen der Anlageberatung empfohlenen Geschäfte unmittelbar oder mittelbar betreffen (Vertriebsvorgaben), aufgestellt werden.

III. Zur weitgehenden Vermeidung dieser Interessenkonflikte ist die DekaBank Teil einer mehrstufigen Organisation mit entsprechender Aufgabenverteilung zwischen Sparkassen, Landesbanken und Dienstleistern.

Die DekaBank als Kryptowertedienstleister selbst wie auch ihre Mitarbeiter sind entsprechend den gesetzlichen Grundlagen verpflichtet, die unter Ziffer I. Kryptowertedienstleistungen ehrlich, redlich und professionell im Interesse der Kunden zu erbringen und Interessenkonflikte, soweit möglich, zu vermeiden. Unabhängig davon hat die DekaBank eine Compliance-Organisation eingerichtet, die insbesondere folgende Maßnahmen umfassen kann:

- Die Einrichtung von Vertraulichkeitsbereichen mit Informationsbarrieren (sogenannten „Chinese Walls“), das heißt virtuelle bzw. tatsächliche Barrieren zur Beschränkung des Informationsflusses.
- Alle Mitarbeiter, bei denen im Rahmen ihrer Tätigkeit Interessenkonflikte auftreten können, sind zur Offenlegung aller ihrer Geschäfte in Kryptowerten verpflichtet.
- Führung von Beobachtungs- bzw. Sperrlisten, in die Kryptowerte, in denen es zu Interessenkonflikten kommen kann, aufgenommen werden. Geschäfte in Kryptowerten aus der Beobachtungsliste bleiben erlaubt, werden aber zentral beobachtet; Geschäfte in Kryptowerten aus der Sperrliste sind untersagt.
- Führung einer Insiderliste. In diese Liste werden alle relevanten Personen der DekaBank, die bestimmungsgemäß Insiderinformationen haben (mit Zeitpunkt und Art der Information), aufgenommen.
- Eine laufende Kontrolle aller Geschäfte der in der DekaBank tätigen relevanten Personen.
- Bei Ausführung von Aufträgen handelt die DekaBank entsprechend der Best-Execution-Policy bzw. der Weisung des Kunden.
- Regelungen über die Annahme von Geschenken und sonstigen Vorteilen.
- Schulung der Mitarbeiter.
- Überwachung der Einhaltung der Kundeninteressen bei Ausgestaltung und Umsetzung von Vertriebsvorgaben.
- Überwachung der Einrichtung, sachgerechten Ausgestaltung und Umsetzung des Vergütungssystems.
- Berücksichtigung der Kundeninteressen im Rahmen unserer Produktfreigabeverfahren und -überwachung.

IV. Sind Interessenkonflikte in Einzelfällen ausnahmsweise nicht durch die obige Aufgabenteilung oder unsere Compliance-Organisation vermeidbar, werden die Kunden entsprechend diesen Grundsätzen darauf hingewiesen. Auf Wunsch des Kunden wird die DekaBank weitere Einzelheiten zu diesen möglichen Interessenkonflikten zur Verfügung stellen.



**DekaBank**  
**Deutsche Girozentrale**  
**Anstalt des Öffentlichen Rechts**  
Große Gallusstraße 14  
60315 Frankfurt  
Telefon: (069) 71 47 - 0  
Telefax: (069) 25 46 - 1376  
[www.deka.de](http://www.deka.de)

Handelsregister:  
Amtsgericht Frankfurt am Main  
HRA 16068  
USt-Id-Nr.: DE 114103563

