Garantieerklärung

der DZ BANK AG, Deutsche Zentral-Genossenschaftsbank, Frankfurt am Main (im Folgenden DZ BANK AG) bezüglich der Verarbeitung personenbezogener Daten durch die rechtlich unselbstständigen Niederlassungen

Die DZ BANK AG unterhält folgende rechtlich unselbstständige Niederlassungen (im Folgenden unter dem Begriff Niederlassungen zusammengefasst) außerhalb der Europäischen Union:

Hong Kong Branch, Tower II, 9th Floor, Admiralty Centre, 18 Harcourt Road, Hong Kong, Central

New York Branch, One Vanderbilt, New York, NY 10017, USA

Singapore Branch, 50 Raffles Place #43-01, Singapore Land Tower, Singapore 048623

London Branch, 150 Cheapside, London EC2V 6ET, UK (bei Wegfall des Angemessenheitsbeschlusses der EU-Kommission)

Zur Erfüllung ihrer Aufgaben greifen diese auch auf bei der DZ BANK AG in Deutschland gespeicherte personenbezogene Daten zu. Zur Sicherstellung eines angemessenen Datenschutzniveaus und zur Gewährung ausreichender Garantien für die betroffenen Personen erklärt die DZ BANK AG hiermit als einseitiges Garantieversprechen, was folgt:

§ 1 Sicherstellung eines angemessenen Datenschutzniveaus in den Niederlassungen

Die DZ BANK AG hat ihre vorgenannten unselbständigen Niederlassungen durch verbindliche unternehmensinterne Regelungen auf die Einhaltung der dieser Erklärung als Anlage beigefügten Standardvertragsklauseln (Modul 1 – Verantwortlicher an Verantwortlicher) gemäß dem Durchführungsbeschluss der Europäischen Kommission (EU) 2021/914 vom 04. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (DSGVO) verpflichtet.

Darüber hinaus müssen die vorgenannten unselbständigen Niederlassungen der DZ BANK AG aufgrund verbindlicher unternehmensinterner Vorgaben uneingeschränkt die Bestimmungen der EU-Datenschutz-Grundverordnung beachten und einhalten.

Auch die in den unselbständigen Niederlassungen tätigen Mitarbeiter wurden auf die Einhaltung der in den Standardvertragsklauseln enthaltenen Regelungen und der Bestimmungen der EU-Datenschutz-Grundverordnung verpflichtet.

§ 2 Verbindlichkeit gegenüber allen betroffenen Personen

Die Regelungen der Standardvertragsklauseln sind — im Wege der Drittbegünstigung — auch gegenüber allen betroffenen Personen verbindlich. Die DZ BANK AG ist für die Bearbeitung aller geltend gemachten Rechtsansprüche zuständig.

Die betroffenen Personen sind berechtigt, die Einhaltung ihrer drittbegünstigenden Rechte durch die DZ BANK AG, durch eine Beschwerde bei einer Datenschutzaufsichtsbehörde ihrer Wahl oder durch die Geltendmachung eines Rechtsbehelfs bei den für die DZ BANK AG zuständigen Gerichten durchzusetzen. Sie können sich jederzeit auch an den Datenschutzbeauftragten der DZ BANK AG wenden.

§ 3 Verantwortlichkeit bei Verstößen

Im Falle eines Verstoßes gegen die Regelungen der Standardvertragsklauseln durch eine der vorgenannten unselbständigen Niederlassungen bleibt die DZ BANK AG gegenüber den betroffenen Personen verantwortlich. Den betroffenen Personen stehen in diesen Fällen gegenüber der DZ BANK AG dieselben Rechte zu, wie wenn der Verstoß von der DZ BANK AG in Deutschland begangen worden wäre und nicht von einer der unselbständigen Niederlassungen im Drittland.

Die betroffenen Personen können von der DZ BANK AG Wiedergutmachung und gegebenenfalls Schadensersatz verlangen.

§ 4 Überprüfung der Einhaltung der Standardvertragsklauseln

Die DZ BANK AG wird durch geeignete Maßnahmen sicherstellen, dass die Einhaltung eines angemessenen Datenschutzniveaus nach Maßgabe dieser Standardvertragsklauseln in ihren unselbständigen Niederlassungen außerhalb der Europäischen Union regelmäßig kontrolliert wird.

Kommt eine Überprüfung zu dem Ergebnis, dass Abhilfemaßnahmen wegen eines Verstoßes gegen die Standardvertragsklauseln zu treffen sind, wird die DZ BANK AG auch für eine Umsetzung der erforderlichen Abhilfemaßnahmen Sorge tragen.

§ 5 Änderungen von rechtlichen Bestimmungen am Sitz der Niederlassungen

Die Niederlassungen beobachten die Rechtsentwicklung in den Ländern, in denen diese ihren Sitz haben.

Soweit sich die jeweils geltenden rechtlichen Bestimmungen dahingehend verändern, dass Nachteile für diejenigen Garantien entstehen können, die die in den unselbständigen Niederlassungen außerhalb der Europäischen Union für verbindlich erklärten Standardvertragsklauseln bieten, wird diese Information an die DZ BANK AG weitergegeben. Diese prüft umgehend mögliche Konsequenzen, die sich aus den veränderten rechtlichen Rahmenbedingungen für die Gewährleistung eines angemessenen Datenschutzniveaus ergeben.

***

Frankfurt, 30.03.2022

Ulrike Brouzi
Vorstand

Frankfurt, 30.03.2022

Dr. Michael Lange
Bereichsleiter Compliance

ANHANG

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

b) Die Parteien:

i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)"), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur"), und

ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur"),

haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") einverstanden erklärt.

c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.

d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie – in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter – Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3

Drittbegünstigte

a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:

i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7

ii) Klausel 7 – Klausel 7.5 Buchstabe e und Klausel 7.9 Buchstabe b

iii) Klausel 10 – Klausel 10 Buchstaben a und d

iv) Klausel 11

v) Klausel 13.1 Buchstaben c, d und e

vi) Klausel 14 Buchstabe e

vii) Klausel 16 – Klausel 16 Buchstaben a und b

b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4

Auslegung

a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6

Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 7

Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur – durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen – in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

7.1 Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e) der Übermittlung. Er darf die personenbezogenen Daten nur dann für einen anderen Zweck verarbeiten,

i) wenn er die vorherige Einwilligung der betroffenen Person eingeholt hat,

ii) wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder

iii) wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.

7.2 Transparenz

a) Damit betroffene Personen ihre Rechte gemäß Klausel 8 wirksam ausüben können, teilt der Datenimporteur ihnen entweder direkt oder über den Datenexporteur Folgendes mit:

i) seinen Namen und seine Kontaktdaten,
ii) die Kategorien der verarbeiteten personenbezogenen Daten,
iii) das Recht auf Erhalt einer Kopie dieser Klauseln,
iv) wenn er eine Weiterübermittlung der personenbezogenen Daten an Dritte beabsichtigt, den Empfänger oder die Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), den Zweck und den Grund einer solchen Weiterübermittlung gemäß Klausel 7.7.

b) Buchstabe a findet keine Anwendung, wenn die betroffene Person bereits über die Informationen verfügt, einschließlich in dem Fall, wenn diese Informationen bereits vom Datenexporteur bereitgestellt wurden, oder wenn sich die Bereitstellung der Informationen als nicht möglich erweist oder einen unverhältnismäßigen Aufwand für den Datenimporteur mit sich bringen würde. Im letzteren Fall macht der Datenimporteur die Informationen, soweit möglich, öffentlich zugänglich.

c) Die Parteien stellen der betroffenen Person auf Anfrage eine Kopie dieser Klauseln, einschließlich der von ihnen ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, können die Parteien Teile des Textes der Anlage vor der Weitergabe einer Kopie unkenntlich machen; sie legen jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für

die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen.

d) Die Buchstaben a bis c gelten unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

7.3 Richtigkeit und Datenminimierung

a) Jede Partei stellt sicher, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Der Datenimporteur trifft alle angemessenen Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Hinblick auf den/die Zweck(e) der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

b) Stellt eine der Parteien fest, dass die von ihr übermittelten oder erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet sie unverzüglich die andere Partei.

c) Der Datenimporteur stellt sicher, dass die personenbezogenen Daten angemessen und erheblich sowie auf das für den/die Zweck(e) ihrer Verarbeitung notwendige Maß beschränkt sind.

7.4 Speicherbegrenzung

Der Datenimporteur speichert die personenbezogenen Daten nur so lange, wie es für den/die Zweck(e), für den/die sie verarbeitet werden, erforderlich ist. Er trifft geeignete technische oder organisatorische Maßnahmen, um die Einhaltung dieser Verpflichtung sicherzustellen; hierzu zählen auch die Löschung oder Anonymisierung der Daten und aller Sicherungskopien am Ende der Speicherfrist.

7.5 Sicherheit der Verarbeitung

a) Der Datenimporteur und – während der Datenübermittlung – auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffene Person gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

b) Die Parteien haben sich auf die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen geeinigt. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

c) Der Datenimporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

d) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

e) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, meldet der Datenimporteur die Verletzung unverzüglich sowohl dem Datenexporteur als auch der gemäß Klausel 11 festgelegten zuständigen Aufsichtsbehörde. Diese Meldung enthält i) eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), ii) ihre wahrscheinlichen Folgen, iii) die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und iv) die Kontaktdaten einer Anlaufstelle, bei der weitere Informationen eingeholt werden können. Soweit es dem Datenimporteur nicht möglich ist, alle Informationen zur gleichen Zeit bereitzustellen, kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

f) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Datenimporteur ebenfalls die jeweiligen betroffenen Personen unverzüglich von der Verletzung des Schutzes personenbezogener Daten und der Art der Verletzung, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur, unter Angabe der unter Buchstabe e Ziffern ii bis iv genannten Informationen, es sei denn, der Datenimporteur hat Maßnahmen ergriffen, um das Risiko für die Rechte oder Freiheiten natürlicher Personen erheblich zu mindern, oder die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. Im letzteren Fall gibt der Datenimporteur stattdessen eine öffentliche Bekanntmachung heraus oder ergreift eine vergleichbare Maßnahme, um die Öffentlichkeit über die Verletzung des Schutzes personenbezogener Daten zu informieren.

g) Der Datenimporteur dokumentiert alle maßgeblichen Fakten im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, einschließlich ihrer Auswirkungen und etwaiger ergriffener Abhilfemaßnahmen, und führt Aufzeichnungen darüber.

7.6 Sensible Daten

Sofern die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Datenimporteur spezielle Beschränkungen und/oder zusätzliche Garantien an, die an die spezifische Art der Daten und die damit verbundenen Risiken angepasst sind. Dies kann die Beschränkung des Personals, das Zugriff auf die personenbezogenen Daten hat, zusätzliche Sicherheitsmaßnahmen (wie Pseudonymisierung) und/oder zusätzliche Beschränkungen in Bezug auf die weitere Offenlegung umfassen.

7.7 Weiterübermittlungen

Der Datenimporteur darf die personenbezogenen Daten nicht an Dritte weitergeben, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union ansässig sind (im Folgenden „Weiterübermittlung"), es sei denn, der Dritte ist im Rahmen des betreffenden Moduls an diese Klauseln gebunden oder erklärt sich mit der Bindung daran einverstanden. Andernfalls ist eine Weiterübermittlung durch den Datenimporteur nur in folgenden Fällen zulässig:

i) Sie erfolgt an ein Land, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt;

ii) der Dritte gewährleistet auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung,

iii) der Dritte geht mit dem Datenimporteur ein bindendes Instrument ein, mit dem das gleiche Datenschutzniveau wie gemäß diesen Klauseln gewährleistet wird, und der Datenimporteur stellt dem Datenexporteur eine Kopie dieser Garantien zur Verfügung,

iv) die Weiterübermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich,

v) die Weiterübermittlung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, oder

vi) – falls keine der anderen Bedingungen erfüllt ist – der Datenimporteur hat die ausdrückliche Einwilligung der betroffenen Person zu einer Weiterübermittlung in einem speziellen Fall eingeholt, nachdem er sie über den/die Zweck(e), die Identität des Empfängers und die ihr mangels geeigneter Datenschutzgarantien aus einer solchen Übermittlung möglicherweise erwachsenden Risiken informiert hat. In diesem Fall unterrichtet der Datenimporteur den Datenexporteur und übermittelt ihm auf dessen Verlangen eine Kopie der Informationen, die der betroffenen Person bereitgestellt wurden.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

7.8 Verarbeitung unter der Aufsicht des Datenimporteurs

Der Datenimporteur stellt sicher, dass jede ihm unterstellte Person, einschließlich eines Auftragsverarbeiters, diese Daten ausschließlich auf der Grundlage seiner Weisungen verarbeitet.

7.9 Dokumentation und Einhaltung der Klauseln

a) Jede Partei muss nachweisen können, dass sie ihre Pflichten gemäß diesen Klauseln erfüllt. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die unter seiner Verantwortung durchgeführten Verarbeitungstätigkeiten.

b) Der Datenimporteur stellt der zuständigen Aufsichtsbehörde diese Aufzeichnungen auf Verlangen zur Verfügung.

Klausel 8

Rechte betroffener Personen

a) Der Datenimporteur bearbeitet, gegebenenfalls mit Unterstützung des Datenexporteurs, alle Anfragen und Anträge einer betroffenen Person im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte gemäß diesen Klauseln unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang der Anfrage oder des Antrags. Der Datenimporteur trifft geeignete Maßnahmen, um solche Anfragen und Anträge und die Ausübung der Rechte betroffener Personen zu erleichtern. Alle Informationen, die der betroffenen Person zur Verfügung gestellt werden, müssen in verständlicher und leicht zugänglicher Form vorliegen und in einer klaren und einfachen Sprache abgefasst sein.

b) Insbesondere unternimmt der Datenimporteur auf Antrag der betroffenen Person folgende Handlungen, wobei der betroffenen Person keine Kosten entstehen:

i) Er legt der betroffenen Person eine Bestätigung darüber vor, ob sie betreffende personenbezogene Daten verarbeitet werden, und, falls dies der Fall ist, stellt er ihr eine Kopie der sie betreffenden Daten und die in Anhang I enthaltenen Informationen zur Verfügung; er stellt, falls personenbezogene Daten weiterübermittelt wurden oder werden, Informationen über die Empfänger oder Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), an die die personenbezogenen Daten weiterübermittelt wurden oder werden, sowie über den Zweck dieser Weiterübermittlung und deren Grund gemäß Klausel 7.7 bereit; er informiert die betroffene Person über ihr Recht, gemäß Klausel 9 Buchstabe c Ziffer i bei einer Aufsichtsbehörde Beschwerde einzulegen;

ii) er berichtigt unrichtige oder unvollständige Daten über die betroffene Person;

iii) er löscht personenbezogene Daten, die sich auf die betroffene Person beziehen, wenn diese Daten unter Verstoß gegen eine dieser Klauseln, die Rechte als Drittbegünstigte gewährleisten, verarbeitet werden oder wurden oder wenn die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützt, widerruft.

c) Verarbeitet der Datenimporteur die personenbezogenen Daten für Zwecke der Direktwerbung, so stellt er die Verarbeitung für diese Zwecke ein, wenn die betroffene Person Widerspruch dagegen einlegt.

d) Der Datenimporteur trifft keine Entscheidung, die ausschließlich auf der automatisierten Verarbeitung der übermittelten personenbezogenen Daten beruht (im Folgenden „automatisierte Entscheidung"), welche rechtliche Wirkung für die betroffene Person entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen würde, es sei denn, die betroffene Person hat hierzu ihre ausdrückliche Einwilligung gegeben oder eine solche Verarbeitung ist nach den Rechtsvorschriften des Bestimmungslandes zulässig und in diesen sind angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person festgelegt. In diesem Fall muss der Datenimporteur, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur,

i) die betroffene Person über die geplante automatisierte Entscheidung, die angestrebten Auswirkungen und die damit verbundene Logik unterrichten und

ii) geeignete Garantien umsetzen, die mindestens bewirken, dass die betroffene Person die Entscheidung anfechten, ihren Standpunkt darlegen und eine Überprüfung durch einen Menschen erwirken kann.

e) Bei exzessiven Anträgen einer betroffenen Person – insbesondere im Fall von häufiger Wiederholung – kann der Datenimporteur entweder eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten für die Erledigung des Antrags verlangen oder sich weigern, aufgrund des Antrags tätig zu werden.

f) Der Datenimporteur kann den Antrag einer betroffenen Person ablehnen, wenn eine solche Ablehnung nach den Rechtsvorschriften des Bestimmungslandes zulässig und in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele zu schützen.

g) Beabsichtigt der Datenimporteur, den Antrag einer betroffenen Person abzulehnen, so unterrichtet er die betroffene Person über die Gründe für die Ablehnung und über die Möglichkeit, Beschwerde bei der zuständigen Aufsichtsbehörde einzulegen und/oder einen gerichtlichen Rechtsbehelf einzulegen.

Klausel 9

Rechtsbehelf

a) Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,

i) eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 11 einzureichen,

ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 16 zu verweisen.

d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.

e) Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.

f) Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 10

Haftung

a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

b) Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.

c) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

d) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe c haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

e) Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

Klausel 11

Aufsicht

a) Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

ABSCHNITT III – LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 12

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich

Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien,

iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.

f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der

Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 13

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

13.1 Benachrichtigung

a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,

i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).

d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

e) Die Buchstaben a bis c gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 12 Buchstabe e und Klausel 14, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

13.2 Überprüfung der Rechtmäßigkeit und Datenminimierung

a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 12 Buchstabe e.

b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.

c) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV – SCHLUSSBESTIMMUNGEN

Klausel 14

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 12 Buchstabe f.

c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

   ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

   iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

d) Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 15

Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von *Deutschland* ist.

Klausel 16

Gerichtsstand und Zuständigkeit

a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

b) Die Parteien vereinbaren, dass dies die Gerichte von *Deutschland* sind.

c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.

d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANLAGE

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur(e):

1. Name: DZ BANK AG, Zentral-Genossenschaftsbank, Frankfurt am Main (im Folgenden DZ BANK AG)

Anschrift: Platz der Republik, 60325 Frankfurt am Main

Name, Funktion und Kontaktdaten der Kontaktperson: Datenschutzbeauftragte der DZ BANK AG, E-Mail: datenschutz@dzbank.de, Tel.: +49 69 744794101

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Tätigkeiten zur Abwicklung des Geschäftsbetriebs

Unterschrift und Datum: ... (30.03.2022)

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Datenimporteur(e):

1. Name: Rechtlich unselbstständige Niederlassung DZ BANK AG, New York Branch

Anschrift: One Vanderbilt, New York, NY 10017, USA

Name, Funktion und Kontaktdaten der Kontaktperson: Local Privacy Officer der DZ BANK AG, New York Branch, Telefon: +1 212 745-1400, Telefax: +1 212 745-1550, E-Mail: new.york@dzbank.de

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Tätigkeiten zur Abwicklung des Geschäftsbetriebs

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

2. Name: Rechtlich unselbstständige Niederlassung DZ BANK AG, Hong Kong Branch

Anschrift: Tower II, 9th Floor, Admiralty Centre, 18 Harcourt Road, Hong Kong, Central

Name, Funktion und Kontaktdaten der Kontaktperson: Local Privacy Officer der DZ BANK AG, Hong Kong Branch, Telefon: +852 28 643 100, Telefax: +852 28 643 160, E-Mail: hongkong@dzbank.de

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Tätigkeiten zur Abwicklung des Geschäftsbetriebs

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

3. Name: Rechtlich unselbstständige Niederlassung DZ BANK AG, Singapore Branch

Anschrift: 50 Raffles Place #43-01, Singapore Land Tower, Singapore 048623

Name, Funktion und Kontaktdaten der Kontaktperson: Local Privacy Officer der DZ BANK AG, Singapore Branch, Telefon: +65 6 427 8388, Telefax: +65 6 223 0082

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Tätigkeiten zur Abwicklung des Geschäftsbetriebs

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

4. Name: Rechtlich unselbstständige Niederlassung DZ BANK AG, London Branch

Anschrift: 150 Cheapside, London EC2V 6ET, UK

Name, Funktion und Kontaktdaten der Kontaktperson: Local Privacy Officer der DZ BANK AG, London Branch, Telefon: +44 20 7776 6000, Telefax: +44 20 7776 6100, E-Mail: london@dzbank.de

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Tätigkeiten zur Abwicklung des Geschäftsbetriebs

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

Kunden, Beschäftigte, Interessenten, Lieferanten, Ansprechpartner

Kategorien der übermittelten personenbezogenen Daten

Beschäftigtenstammdaten, Kundenstammdaten, Kontodaten, Transaktionsdaten, Lieferantenstammdaten, Kommunikationsdaten, Systemkennungen

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

keine

Häufigkeit der Übermittlung

Kontinuierlich

Art der Verarbeitung

Die Daten werden in den IT-Systemen der Verantwortlichen gespeichert und im entsprechend der Zulässigkeitsvoraussetzungen nach Art. 6 DSGVO erforderlichen Umfang automatisiert verarbeitet und nach dem Ende von Aufbewahrungsfristen gelöscht.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Erfüllung der Funktionen der Niederlassungen in den einzelnen Ländern im Auftrag der DZ BANK AG, Frankfurt

- *Verarbeitung zu Zwecken der Erbringung und Vermittlung von Bankgeschäften, Finanzdienstleistungen, Risikosteuerung, Geldwäsche- und Betrugsprävention sowie aller mit dem Betrieb und der Verwaltung eines Kredit- und Finanzdienstleistungsinstituts erforderlichen Tätigkeiten*

Begründung und Vollzug von vertraglichen Beauftragungen von lokalen Personen, die für die Niederlassungen tätig werden, unter Beachtung des anwendbaren (lokalen) Rechts.

Austausch von Daten in Zusammenhang mit der Aufnahme und Abwicklung von Geschäften durch die DZ BANK AG

- *Lesen und Pflege von Kundendaten, Geschäftsanbahnung, Abschluss und Abwicklung von Verträgen;*
- *Übermittlung von Daten an Aufsichtsbehörden, IT-Systempflege, Kommunikation, Erstellung von Abschlüssen*

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Die Speicherdauer der personenbezogenen Daten richtet sich nach dem Löschkonzept der jeweiligen Anwendung.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Von uns eingesetzte Auftragsverarbeiter (Art. 28 DSGVO) können zu den oben genannten Zwecken Daten erhalten. Hierbei handelt es sich um Unternehmen in den Kategorien

kreditwirtschaftliche Leistungen, IT-Dienstleistungen, Druckdienstleistungen, sowie Vertrieb und Marketing.

Vertraglich sind diese Unternehmen dazu verpflichtet die Daten zu löschen, wenn das Auftragsverhältnis beendet wurde oder Aufbewahrungsfristen abgelaufen sind.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 11

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

ANHANG II – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1.1 Maßnahmen zur Zutrittskontrolle

Unter Zutrittskontrolle versteht man Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Umgesetzte Maßnahmen:

Zutrittskontrolle in Rechenzentren:

- Kameraüberwachung des Rechenzentrums (24x7x365)
- Alarmgesicherte, stets verschlossene Serverräume
- Vergaberichtlinien für Zutrittsberechtigungen
- Zutritt besteht nur für autorisierte Mitarbeiter und ggf. vorher angemeldete Dienstleister / Personen nach Ausweiskontrolle. Der Zutritt wird nur wenigen zuvor ausgewählten Personen gewährt.
- Zusätzlich kartengestütztes Zugangskontrollsystem mit Aufzeichnung für die Rechenzentrumsflächen. Kartenausgabe bzw. Berechtigungsvergabe nach Genehmigung durch Vorgesetzten bzw. RZ-Verantwortlichen.

Zutrittskontrolle in Büroräumen:

- Richtlinie zu physischen Maßnahmen zur Zutrittskontrolle
- Kartengestützte personalisierte Zutrittskontrollsysteme mit Zutrittsberechtigung nur für autorisierte Mitarbeiter
- Dienstanweisungen zur Handhabung von Zutrittskontrollen
- Richtlinie zur Begleitung von Gästen im Gebäude
- Gebäudesicherung überwiegend mit Einbruchmeldeanlage, Wachdienst mit Kontrollgängen und Kameraüberwachung
- Abgeschottete Bereiche über zusätzliche Rechtevergabe mit definiertem internen Genehmigungsverfahren, regelmäßige Überprüfung der vergebenen Rechte

1.2 Maßnahmen zur Zugangskontrolle

Unter Zugangskontrolle versteht man Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Umgesetzte Maßnahmen:

- Authentifizierungsinformationen werden bei Übertragung nach dem Stand der Technik verschlüsselt
- Passwörter, PINs und dergleichen werden während der Eingabe maskiert
- Arbeitsplatzrechner mit automatischer Bildschirmsperre
- Sperrung von Nutzerkonten nach mehrfach fehlgeschlagenen Anmeldeversuchen

- Zentrales Verfahren zur Passwortrücksetzung mit Protokollierung
- Richtlinie für Passwortkomplexität und –wechselintervalle
- Verschlüsselung von Festplatten in Laptops und anderer mobiler Datenträger

1.3 Maßnahmen zur Zugriffskontrolle

Unter Zugriffskontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umgesetzte Maßnahmen:

- Berechtigungen werden über dokumentierte Berechtigungsprozesse nach dem Minimalprinzip vergeben
- Umgesetzte Berechtigungen unterliegen der regelmäßigen Prüfung (Rezertifizierung)
- Einrichtung der Benutzerberechtigungen erfolgt getrennt von der Genehmigung

1.4 Maßnahmen zur Trennungskontrolle

Unter Trennungskontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umgesetzte Maßnahmen:

- Beachtung der gängigen Standards zur sicheren Datenverarbeitung. Die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen werden gewährleistet.
- Trennung von zu unterschiedlichen Zwecken erhobenen Daten durch Speicherung in physisch oder logisch getrennten Datenbanken bzw. Systemen

2. Integrität (Art. 32 Abs.1 lit. b) DSGVO)

2.1 Maßnahmen zur Weitergabekontrolle

Unter Weitergabekontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Umgesetzte Maßnahmen:

- Generelle Absicherung des internen Netzwerks durch Firewall, Virenfilter, Internetzugriff nur über Proxy-Server.
- Internes Netzwerk über dedizierte Verbindungen, wo nötig als VPN ausgeführt.
- Zentral administrierte Schnittstellenkontrolle für Schreiben auf USB und CD/DVD-Writer gemäß Berechtigungsprozess
- Festlegung von Archivierungs- und Löschfristen für personenbezogene Daten
- Verbindliches Verfahren zur Datenträgervernichtung bzw. -außerdienststellung mit Löschung oder Vernichtung durch Dienstleister
- Zugangsgesicherte Aufbewahrung von Backup- und Archivdatenträgern

- Dokumentation sämtlicher Schnittstellen zur Datenübertragung
- Austausch sensibler Daten über dedizierte oder verschlüsselte Leitungen
- Verschlüsselung von E-Mails bei Serververbindungen nach Stand der Technik

2.2 Maßnahmen zur Eingabekontrolle

Unter Eingabekontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umgesetzte Maßnahmen:

- Nutzung personalisierter Nutzerkennungen wo möglich
- Grundsatz, dass nur diejenigen Mitarbeiter mit personenbezogenen Daten umgehen, die gemäß organisatorischer Aufstellung mit der jeweiligen Aufgabe betraut sind
- Protokollierung aller Änderungen im Nutzerverwaltungssystem
- Protokollierung des Zugangs zu Systemen und Anwendungen
- Mitarbeiter sind auf Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten verpflichtet
- Protokollierung sämtlicher Eingaben, die von privilegierten Benutzerkonten getätigt wurden.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs.1 lit. b) und c) DSGVO)

Unter Verfügbarkeitskontrolle versteht man Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Umgesetzte Maßnahmen:

- Sicherstellung des IT-Betriebs über zwei entfernte, ausfallsichere Rechenzentren mit gespiegelter Datenhaltung sowie unterbrechungsfreier Stromversorgung und jeweils redundanter Netzwerkanbindung.
- Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Backup-Datenträger in entfernten Rechenzentren.
- Archivierung von Daten gemäß den gesetzlichen und aufsichtsrechtlichen Vorgaben mit redundanter Datenhaltung an zwei getrennten Standorten mit besonderer Zutrittssicherung; regelmäßige Prüfung der Lesbarkeit der archivierten Daten.
- Einsatz von Schutzmaßnahmen wie Virenscannern, Firewalls, SPAM-Filter, entsprechend detaillierte Konzepte zu ihrem Einsatz
- Regelmäßige Prüfung und Übung relevanter Ausfallszenarien

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 lit. Abs.1 d) DSGVO, Art. 25 Abs. 1 DSGVO)

Umgesetzte Maßnahmen:

- Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Regelmäßige Prüfungen der Innenrevision.

- Mitarbeiter sind zum Datenschutz informiert und geschult sowie zur Einhaltung der Vertraulichkeit verpflichtet. Es bestehen Organisationsanweisungen zum Datenschutz.
- Es besteht ein Verfahren zur regelmäßigen Schutzbedarfseinstufung für die Verarbeitungen von personenbezogenen Daten einschließlich Unterlegung mit geeigneten Schutzmaßnahmen.
- Löschungen in den für die Verarbeitung eingesetzten Systemen können durchgeführt werden (Löschfähigkeit).
- Es werden nur die gemäß Vorgaben des Auftraggebers erforderlichen Daten verarbeitet.
- Die Verträge mit weiteren Auftragnehmern gemäß Art.28 DSGVO (Verarbeitung personenbezogener Daten im Auftrag) enthalten die vorgeschriebenen Angaben und Vereinbarungen.
- Die Verträge mit weiteren Auftragnehmern enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- Die Verträge mit weiteren Auftragnehmern enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Sorgfältige Auswahl und Kontrollen von weiteren Auftragnehmern.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.

Der Verantwortliche stellt in seinen (Unter-)Auftragsverhältnissen sicher, dass hinreichende Garantien geboten sind, um die Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen entsprechend den Anforderungen der DSGVO zu gewährleisten.