AXA GRUPPE
Verbindliche unternehmensinterne Regelungen (BINDING CORPORATE RULES)

Hintergrund

Die AXA Gruppe hat sich der vertraulichen Behandlung von Daten, die sie im Rahmen ihrer Geschäftstätigkeiten erhält sowie der Einhaltung der anwendbaren Gesetze und Vorschriften bezüglich der Behandlung von Personenbezogenen und Besonderen Arten Personenbezogener Daten verpflichtet.

Die AXA Gruppe hat eine globale Datenschutz-Organisation/Governance eingeführt mit (i) einem vom Management Committee beschlossenen Datenschutz-Governancemodell, (ii) einem Gruppen-Datenschutzbeauftragten, (iii) einem Gruppen-Datenschutz-Steuerungsausschuss, (iv) einem weltweiten Netzwerk an lokalen Datenschutzbeauftragten die vom Gruppen-Datenschutzbeauftragten koordiniert werden, und (v) einer Gruppen-Datenschutzrichtlinie.

Die AXA-Gruppe hat beschlossen, verbindliche unternehmensinterne Regelungen (Binding Corporate Rules – „BCR") einzuführen, um angemessene Sicherheitsmaßnahmen einzurichten, damit sichergestellt ist, dass Personenbezogene Daten geschützt sind, während sie innerhalb der AXA Gruppe von einer AXA Gesellschaft mit Sitz innerhalb des Geregelten Zuständigkeitsbereiches (wie im folgenden Artikel I definiert) an eine AXA Gesellschaft mit Sitz in einem anderen Geregelten Zuständigkeitsbereich übermittelt werden, wo diese Übermittlung und jede spätere Weiterübermittlung dieser Daten nicht anderweitig durch das anwendbare Recht erlaubt ist.

ARTIKEL I - DEFINITIONEN

Soweit sie in den verbindlichen unternehmensinternen Regelungen, ihren Anhängen und der gruppeninternen Vereinbarung (Intra Group Agreement) verwendet werden, haben folgende Begriffe und Ausdrücke, sofern mit einem Großbuchstaben geschrieben, die unten aufgeführten Bedeutungen:

„Artikel-29-Datenschutzgruppe" besteht aus Repräsentanten der Datenschutzbehörden aus jedem EU-Mitgliedsstaat, dem Europäischen Datenschutzbeauftragten und der Europäischen Kommission. Die Arbeitsgruppe ist unabhängig und wird in beratender Funktion tätig.

„AXA BCR Steuerungsausschuss" ist ein Ausschuss, der speziell den BCR gewidmet ist, bestehend aus Repräsentanten der AXA Gruppengeschäftsleitung und Datenschutzbeauftragten aus ausgewählten BCR AXA Gesellschaften.

„AXA Gesellschaften" heißt AXA, Société Anonyme, mit einem Vorstand mit Hauptsitz in 25, avenue Matignon, 75008 Paris, eingetragen im Handelsregister von Paris unter der Nummer 572 093 920; und (i) jede andere Gesellschaft, die von der AXA beherrscht wird bzw. die AXA beherrscht, wobei eine Gesellschaft dann als beherrschende Gesellschaft einer anderen gilt, wenn: (a) sie direkt oder indirekt einen Teil des Kapitals hält, der sie zur Mehrheit der Stimmrechte bei Hauptversammlungen der Aktionäre dieser Gesellschaft berechtigt; (b) sie die Mehrheit der Stimmrechte an dieser Gesellschaft nur aufgrund einer mit anderen Gesellschaftern oder Aktionären geschlossenen Vereinbarung hält, die nicht den Interessen der Gesellschaft widerspricht; (c) sie de facto,

durch Stimmrechte, die sie hält, über die Entscheidungen während der Hauptversammlungen der Aktionäre dieser Gesellschaft bestimmt; (d) auf jeden Fall, wenn sie direkt oder indirekt einen Anteil an Stimmrechten hält, der größer ist als 40% und wenn kein anderer Gesellschafter oder Aktionär einen Anteil hält, der größer ist als ihr eigener; (ii) jede wirtschaftliche Interessengruppe, bei der sich AXA bzw. eine oder mehrere der AXA Gesellschaften an mindestens 50% der Betriebskosten beteiligt; (iii) in den Fällen, wo durch ein auf eine Gesellschaft anwendbares Gesetz die Stimmrechte oder die Beherrschungsverhältnisse eingeschränkt werden (wie hier oben definiert), wird diese Gesellschaft als Gesellschaft der AXA Gruppe betrachtet, wenn die Stimmrechte an Hauptversammlungen oder die Beherrschung, die eine Gesellschaft der AXA Gruppe ausübt, die vom besagten anwendbaren Gesetz festgelegte Höchstgrenze erreichen; und (iv) alle AXA Gesellschaften, welche die "AXA Gruppe" bilden.

„AXA-Mitarbeiter" sind alle Mitarbeiter der AXA Gesellschaften einschließlich leitende Angestellte, Auszubildende, Praktikanten und Personen mit vergleichbarem Status.

„AXA Gruppe" bedeutet insgesamt die AXA SA und alle AXA Gesellschaften.

„BCR AXA Gesellschaften" sind alle AXA Gesellschaften, die eine gruppeninterne Vereinbarung (IGA) in ihrer Eigenschaft entweder als Datenexporteur oder als Datenimporteur unterzeichnet haben.

„BCR AXA Hubs" bedeutet die wesentlichen transversalen und/oder lokalen AXA Gesellschaften bzw. andere AXA Organisationen, die sich in Zusammenarbeit mit dem GDPO an der Umsetzung der BCR zum Schutz der Personenbezogenen Daten innerhalb der AXA-Gruppe sowie in Bezug auf den Transfer von Personenbezogenen Daten aus Mitgliedstaaten des Europäischen Wirtschaftsraums ("EWR") innerhalb und außerhalb des EWRs beteiligen.

„Binding Corporate Rules" oder "BCR" meint die vorliegenden verbindlichen, unternehmensinternen Regelungen, die von und zwischen AXA SA sowie allen BCR AXA Gesellschaften abgeschlossen werden.

„Daten-Controller" bedeutet eine BCR AXA Gesellschaft, die allein oder mit anderen zusammen die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten bestimmt.

„Datenexporteur" meint jeden Daten-Controller oder Datenverarbeiter innerhalb des Geregelten Zuständigkeitsbereiches, der Personenbezogene Daten im Namen eines Daten-Controllers verarbeitet, der Personenbezogene Daten nach außerhalb des Geregelten Zuständigkeitsbereiches, wo er ansässig ist, übermittelt und eine IGA unterzeichnet hat.

„Datenimporteur" meint jeden Daten-Controller oder Datenverarbeiter, der Personenbezogene Daten im Namen eines Daten-Controllers verarbeitet, der die Personenbezogenen Daten von einem Datenexporteur im Rahmen einer Relevanten Übermittlung oder einer Weiterübermittlung erhält und der eine gruppeninterne Vereinbarung unterzeichnet hat.

„Datenschutzbeauftragter" (Data Privacy Officer" oder "DPO") bedeutet die Person innerhalb einer AXA Gesellschaft, die jeweils für die Koordination mit dem GDPO und die Sicherstellung der Einhaltung der BCR sowie der anwendbaren lokalen rechtlichen Bestimmungen und behördlichen Regelungen seitens der AXA Gesellschaft zuständig ist.

„Datenverarbeiter" bedeutet eine BCR AXA Gesellschaft, die Personenbezogene Daten im Namen eines Daten-Controllers verarbeitet.

„Datenschutzbehörde" bedeutet die administrative Behörde, die in jedem Land, in dem die AXA Gruppe präsent ist, offiziell für Datenschutz zuständig ist (in Frankreich zum Beispiel die Commission Nationale de l'Informatique et des Libertés; in Spanien, die Agencia Espanola de Proteccion de Datos, usw.). Zur Klarstellung: der Begriff "Datenschutzbehörde" schließt auch jeden Ersatz bzw. Nachfolger einer Datenschutzbehörde ein.

„Betroffene Person" bedeutet jede natürliche Person, die sich direkt oder indirekt mit Mitteln, die mit hinreichender Wahrscheinlichkeit von einer natürlichen oder juristischen Person verwendet werden, identifizieren lässt, insbesondere durch Bezugnahme auf eine Identifikationsnummer, Standortdaten, Online-Identifikationsdaten oder auf einen Faktor bzw. auf Faktoren, die für die physische, physiologische, genetische, geistige, wirtschaftliche, kulturelle oder soziale Identität dieser Person spezifisch sind.

„EWR" oder **„Europäischer Wirtschaftsraum"** bedeutet den europäischen Wirtschaftsraum, der die Länder der Europäischen Union und die Mitgliedstaaten der EFTA (European Free Trade Association = Europäische Freihandelsassoziation) vereint. Ab 2012 umfasst er Österreich, Belgien, Bulgarien, Zypern, Tschechien, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Island, Irland, Italien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, die Niederlande, Norwegen, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Schweden und das Vereinigten Königreich.

„EWR-Datenexporteur" meint jeden in der EWR ansässigen Daten-Controller oder Datenverarbeiter, der Personenbezogene Daten im Namen eines Daten-Controllers verarbeitet, der die Personenbezogenen Daten nach außerhalb des EWR (ob über einen Datenverarbeiter oder einen dritten Datenverarbeiter) übermittelt und der eine IGA unterzeichnet hat.

„Betroffene Person/EWR" bedeutet eine Betroffene Person, die zum Zeitpunkt, als ihre Personenbezogenen Daten erhoben wurden, innerhalb des EWRs ansässig war.

„EU-Standardvertragsklauseln" sind die standardisierten vertraglichen Klauseln, die von der Europäischen Kommission herausgegeben werden und welche ausreichende Schutzmaßnahmen anbieten, wie von der Europäischen Verordnung für den Transfer von Personenbezogenen Daten zu dritten Ländern gefordert, welche kein angemessenes Schutzniveau für den Datenschutz entsprechend der Europäischen Kommission haben.

„Europäische Verordnung" bedeutet die gegenwärtigen und künftigen anwendbaren Regelungen und Verordnungen in Bezug auf Datenschutz, die in den Ländern des EWRs gültig sind.

„Gruppendatenschutzbeauftragter" (**„Group Data Privacy Officer"** oder **„GDPO"**) bedeutet die Person, die für die Gesamtkontrolle dieser verbindlichen unternehmensinternen Regelungen (BCR) durch ein Netzwerk an lokalen Datenschutzbeauftragten zuständig ist.

„Gruppeninterne Vereinbarung" (**„Intra Group Agreement"** oder **„IGA"**) bedeutet die als Anhang 1 beigefügte BCR-Vereinbarung und/oder jede Annahmeerklärung der BCR der AXA Gruppe, die von BCR AXA Gesellschaften unterzeichnet wurden oder werden.

„Weiterübermittlung“ meint die Weiterübermittlung von zuvor exportierten Personenbezogenen Daten entweder aufgrund einer Relevanten Übermittlung oder einer Übermittlung in der US Safe-Harbor-Regelung, jeweils:

(i) zu einer anderen BCR AXA Gesellschaft, die in einem Gebiet ist, welches (doch für den Betrieb der BCR) kein angemessenes Schutzniveau bietet, wie von dem Datenschutzgesetz des relevanten Geregelten Zuständigkeitsbereiches am Ursprung der relevanten Übermittlung gefordert,

(ii) die nicht unter eine der zulässigen Ausnahmen oder Bedingungen im Datenschutzrecht des jeweiligen Geregelten Zuständigkeitsbereichs fallen (was die Zustimmung der Betroffenen Person, bestehenden vertraglichen Schutz, die Eintragung in die Safe-Harbor-Regelung und/oder Einrichtung in einem von der Europäischen Kommission anerkannten Land nach Art. 25 (6) der Richtlinie 95/46/EU, enthalten kann).

„Personenbezogene Daten” bedeutet alle Daten bezüglich einer individuellen natürlichen Person, die entweder anhand dieser Daten oder anhand dieser Daten zusammen mit weiteren Informationen identifizierbar ist.

„Verarbeitung” ist jede im Zusammenhang mit Daten unternommene Handlung, wie z.B. Erheben, Registrieren, Kopieren, Vervielfältigen, Übertragen, Suchen, Sortieren, Speichern, Trennen, Kreuzen, Zusammenführen, Modifizieren, Bereitstellen, Verwenden, Veröffentlichen, Verbreiten, Verwahren, Organisieren, Speichern, Anpassen, Abrufen, Offenbaren durch Übermitteln oder sonstiges Zugänglich-Machen, Verstecken, Bewegen und sonstiges Unzugänglich-Machen sowie die Durchführung anderer Handlungen im Zusammenhang mit den Daten, egal, ob die Handlung automatisch, halb-automatisch oder auf sonstige Weise durchgeführt wird.

„Geregelter Zuständigkeitsbereich“ meint jeden Zuständigkeitsbereich innerhalb des EWR und Andorra, Schweiz, Faröer Inseln, Guernsey, Isle of Man und Jersey.

„Betroffene Person/Geregelter Zuständigkeitsbereich“ meint jede Betroffene Person, die zum Zeitpunkt, als ihre Personenbezogenen Daten erhoben wurden, innerhalb des Geregelten Zuständigkeitsbereiches ansässig war.

„Relevante Übermittlung“ meint eine Übermittlung von Personenbezogenen Daten (in dem Maße, wie Personenbezogene Daten nicht zuvor Gegenstand einer Relevanten Übermittlung oder Weiterleitung waren):

(i) von einer BCR AXA Gesellschaft, die ein Datenexporteur für eine andere BCR AXA Gesellschaft ist, welche in einem Gebiet ist, welches (doch für den Betrieb der BCR) kein angemessenes Schutzniveau bietet, wie von dem Datenschutzgesetz des relevanten Geregelten Zuständigkeitsbereiches des Datenexporteurs verlangt; und

(ii) die nicht unter eine der zulässigen Ausnahmen oder Bedingungen im Datenschutzrecht des jeweiligen Geregelten Zuständigkeitsbereichs fallen (was die Zustimmung der Betroffenen Person, bestehenden vertraglichen Schutz, die Eintragung in die US Safe-Harbor-Regelung und/oder Einrichtung in einem von der Europäischen Kommission anerkannten Land nach Art. 25 (6) der Richtlinie 95/46/EU, enthalten kann).

„Besondere Arten Personenbezogene Daten“ meint solche Daten, wie in Art. IV Abs. 2 beschrieben.

„Andere Partei” bedeutet jede natürliche oder juristische Person (einschließlich der AXA Gesellschaften/BCR AXA Gesellschaften), öffentliche Behörde, jedes Amt und jede andere Körperschaft außer der Betroffenen Person, dem Daten-Controller, dem Datenverarbeiter und Personen die unter der direkten Aufsicht des Daten-Controllers oder des Datenverarbeiters ermächtigt sind, die Personenbezogene Daten einer Betroffenen Person zu verarbeiten.

ARTIKEL II - ZWECK

Zweck der BCR ist es, ein angemessenes Schutzniveau für die Personenbezogenen Daten, die aufgrund einer Relevanten Übermittlung oder einer Weiterübermittlung von einer im Geregelten Zuständigkeitsbereich ansässigen AXA Gesellschaft zu einer in einem anderen Zuständigkeitsbereich sitzenden AXA Gesellschaft sicherzustellen.

ARTIKEL III - GELTUNGSBEREICH

1. Geographischer Geltungsbereich

Die AXA Gruppe ist in mehr als 50 Ländern präsent und mehr als 150.000 AXA-Mitarbeiter und Vertriebskräfte sind verpflichtet Millionen von Kunden zu betreuen.

Die vorliegenden BCR gelten ausschließlich für die Übermittlung Personenbezogener Daten von innerhalb des Geregelten Zuständigkeitsbereichs ansässigen Datenexporteuren an in anderen Zuständigkeitsbereichen ansässige Datenimporteure sowie für Weiterübermittlungen, Rückgriffe gegen Verstöße von Drittbegünstigungsrechten sowie die Beschwerde- und Haftungsbestimmungen dieser BCR (wie in Artikeln VII, VIII und IX dieser BCR dargelegt) beschränken sich auf Betroffene Personen/Geregelter Zuständigkeitsbereich.

Auch wenn die BCR AXA Gesellschaften Prozesse, die für die Einführung der BCR erforderlich sind, überall eingeführt haben, übernehmen BCR AXA Gesellschaften keine BCR-Garantien für Personenbezogene Daten, die nicht dem Datenschutz des Geregelten Zuständigkeitsbereichs unterliegen, d.h. die nicht aus dem Geregelten Zuständigkeitsbereich übertragen werden, z.B.:

- wenn eine in den US ansässige AXA Gesellschaft ihre Personenbezogenen Daten an eine in Indien ansässige AXA Gesellschaft übermittelt, dann unterliegt diese Übermittlung und damit verbundene Verarbeitung nicht den BCR, oder

- wenn eine in Japan ansässige AXA Gesellschaft ihre Personenbezogenen Daten an eine in Singapur ansässige AXA Gesellschaft übermittelt, dann unterliegt diese Übermittlung und damit verbundene Verarbeitung nicht den BCR.

2. Materieller Geltungsbereich

    a. Geltungsbereich unter den BCR AXA Gesellschaften und Durchsetzbarkeit gegenüber AXA-Mitarbeitern

Die vorliegenden BCR binden alle AXA Gesellschaften, die die BCR angenommen haben, indem sie eine gruppeninterne Vereinbarung ("Intra-Group Agreement“, “IGA”) unterschrieben haben, die ihre Akzeptanz der BCR darlegt und zum Ausdruck bringt.

Jede AXA Gesellschaft, die eine IGA unterzeichnet, wird am Tag der Unterzeichnung oder (wenn später) zum Stichtag, der in der jeweiligen IGA festgelegt ist, zur BCR AXA Gesellschaft.

Nach Maßgabe des anwendbaren Arbeitsrechts werden die vorliegenden BCR für die AXA-Mitarbeiter aller BCR AXA Gesellschaften durch eine der folgenden Vereinbarungen in der jeweiligen BCR AXA Gesellschaft verbindlich und durchsetzbar:

- durch eine bindende interne AXA-Richtlinie, oder
- durch einen bindenden Tarifvertrag, oder
- durch eine Klausel im Arbeitsvertrag, oder
- durch andere geeignete Mittel, um die BCR verbindlich für AXA-Mitarbeiter in dem jeweiligen Land zu machen.

Nach Maßgabe des anwendbaren Arbeitsrechts sowie ihrer eigenen internen Regeln und Arbeitsverträge kann jede BCR AXA Gesellschaft disziplinarische Maßnahmen gegenüber ihren eigenen AXA-Mitarbeitern ergreifen, insbesondere in folgenden Fällen:

- Verletzung dieser BCR durch einen AXA-Mitarbeiter,
- Nichtbefolgung der Empfehlungen und Ratschläge, die erteilt wurden, nachdem die jeweiligen Datenschutzbeauftragten („DPO“) die Einhaltung geprüft haben,
- Unterlassung der Zusammenarbeit bei der Prüfung der BCR-Einhaltung durch den jeweiligen DPO, bzw. mit den jeweiligen für Datenschutz zuständigen Behörden.

b. Personenbezogene Daten und Verarbeitungsumfang

Der Zweck oder die Zwecke der Übermittlung von Personenbezogenen Daten und die Verarbeitung nach der Übermittlung unterstützen und vereinfachen AXAs Geschäftstätigkeit.

AXAs Kernkompetenzen spiegeln sich in einer Reihe von Produkten und Dienstleistungen wider, angepasst an die Bedürfnisse jedes Kunden in den drei wichtigsten Sparten: Schaden- und Unfallversicherung, Produkte für die private Altersvorsorge sowie Vermögensverwaltung:

- Die Schaden- und Unfallversicherung umfasst die Sach- und Haftpflichtversicherung. Es deckt eine breite Palette von Produkten und Dienstleistungen ab, konzipiert für unsere Einzel- und Geschäftskunden einschließlich Assistance-Leistungen und internationale Versicherungen für Großkunden wie Marine und Luftfahrt.
- Unsere Einzel- und Gruppenlebensversicherung beinhaltet beides: Spar- und Altersvorsorgeprodukte auf der einen Seite und auf der anderen Seite Krankenversicherungs- und Personenschadenprodukte. Spar- und Altersvorsorgeprodukte erfüllen die Notwendigkeit Kapital zur Finanzierung der Zukunft, ein spezielles Projekt oder den Ruhestand beiseite zu legen. Personenschadenprodukte decken die Risiken im Zusammenhang mit einer individuellen körperlichen Unversehrtheit, Gesundheit oder Leben. AXA bietet zudem seinen Einzelkunden in einigen Ländern eine einfache Auswahl von Bankdienstleistungen und -produkten, die die Versicherungsangebote ergänzen.
- Das Vermögensverwaltungsgeschäft umfasst die Investition und Verwaltung von Vermögenswerten für die Versicherungsgesellschaften der Gruppe und deren Kunden, genauso wie für Dritte, Privatanleger sowie institutionelle Kunden.

Serviceabwicklung von AXAs Geschäftsaktivitäten umfasst:

- Visionierung (definieren langfristiger Unternehmensvision, Geschäftsstrategie entwickeln, verwalten einer strategischen Initiative, Fortschritte kontrollieren)

- Gestaltung (Produktstrategie entwickeln, Risikopolitik etablieren, Gestalten, Entwickeln und Einführen eines Produktes, pflegen bestehender Produktportfolios)
- Vertrieb (entwickeln einer Vertriebsstrategie, verwalten und kontrollieren von Vertriebsnetzen, Marketing-Aktivitäten ausführen, Kundenbeziehung verwalten, Angebotsgestaltung, verkaufen, Verkaufsumsätze belohnen)
- Herstellung (zeichnen, verwalten einer Police, Prämien sammeln, Policen-Portfolio überwachen)
- Serviceabwicklung (Katastrophenbewältigung, Schadenabwicklung, Dienstleistungen anbieten, Hilfsstoffe verwalten, Betrug aufdecken, Forderungsübergang verwalten und Gelder aus dem Rückversicherungsgeschäft wiederherstellen, Wrack-Bergungen verwalten, Schadenbearbeitung kontrollieren)
- Verwaltung Finanzen (Planung und Steuerung von Finanzen, Investitionen verwalten, Unternehmensfinanzierungen verwalten, Transaktionen durchführen, Kapitalanlagen verwalten, Finanzen analysieren, Zahlungsmittel verwalten, Geldgeschäfte und Zahlungsmittel verwalten, Steuern verwalten, Vorschriften einhalten, um Rückversicherung kümmern)
- Verwaltung IT (IT-Kundenbeziehungen verwalten, Lösungen liefern und vorhalten, IT-Dienstleistungen liefern und unterstützen, IT-Infrastruktur verwalten, IT-Organisation verwalten, IT-Sicherheit verwalten)
- Personalwesen entwickeln und verwalten (Personalentwicklung verwalten und leiten, Personalwesen führen, Personalkommunikation durchführen, soziale Partner und den Betriebsrat verwalten)
- Verwaltung Kauf (Lieferanten und Verträge verwalten, Waren und Dienstleistungen liefern und erhalten, Lieferantenrechnungen verwalten, Zahlungen genehmigen und validieren, Beschaffungsreporting und Performance-Analysen durchführen)
- Verwaltung Risiken (finanzielle Risiken verwalten, Investitionsrisiken verwalten, operationale Risiken verwalten, Prognosen erstellen, risikobereinigte Profitabilität berechnen)
- Andere Unterstützungsfunktionen (externe Kommunikation durchführen, rechtliche Unterstützung, Verbesserungen und Veränderungen verwalten, Innenrevision, zentrale Funktionen)

Alle Arten und Kategorien von Personenbezogenen Daten, die von den BCR AXA Gesellschaften in Ausübung ihrer Tätigkeit verarbeitet werden, sollen unter den Anwendungsbereich dieser BCR fallen. Solche Arten und Kategorien beinhalten: Personenbezogene Daten, die von Kunden, Antragstellern, Anspruchstellern, AXA-Mitarbeitern, Bewerbern, Vertretern, Lieferanten und anderen Dritten erhoben werden.

Die BCR umfassen sowohl maschinelle als auch manuelle Arten der Verarbeitung.

ARTIKEL IV - GRUNDSÄTZE DER VERARBEITUNG

Bei jeder Verarbeitung Personenbezogener Daten nach Maßgabe von Artikel III – GELTUNGSBEREICH werden die im Folgenden dargelegten Verarbeitungsgrundsätze beachtet.

1. Hauptgrundsätze

Jede der BCR AXA Gesellschaften sichert zu und verspricht, dass es die Anforderungen des anwendbaren Gesetzes und der zuständigen lokalen Datenschutzbehörde für die ursprüngliche Verarbeitung der Personenbezogenen Daten erfüllt, die anschließend im

Rahmen einer Relevanten Übermittlung oder einer Weiterübermittlung gemäß den BCR übermittelt werden.

Jede der BCR AXA Gesellschaften sichert zu, dass die unter ihrer Kontrolle durchgeführte Verarbeitung Personenbezogener Daten, einschließlich der Datenübermittlung, weiterhin nach Maßgabe der Bestimmungen dieser BCR und insbesondere folgender Mindestvorschriften erfolgen wird:

- Personenbezogene Daten müssen ordnungsgemäß und rechtmäßig erhoben werden unter Beachtung des Rechts der Betroffenen Person auf Auskunft, es sei denn, eine solche Auskunft ist aufgrund rechtlicher Ausnahmen nicht erforderlich; und dürfen nur mit vorheriger eindeutiger Einwilligung der Betroffenen Person, oder falls die Verarbeitung sonst durch anwendbares Recht erlaubt ist, verarbeitet werden.

- Personenbezogene Daten dürfen nur zu bestimmten, ausdrücklichen und rechtmäßigen Zwecken erhoben und nicht auf eine Weise weiterverarbeitet werden, die diesem Zweck oder diesen Zwecken nicht entspricht. Personenbezogene Daten werden Dritten nur zu solchen Zwecken zur Verfügung gestellt oder wie anderweitig durch das anwendbare Recht gestattet.

- Angemessene Kontrollen sowie technische und organisatorische Prozesse müssen eingeführt werden, um die Sicherheit der Personenbezogenen Daten zu gewährleisten und nicht autorisierte Zugriffe oder Veröffentlichung, potenzielle Schäden, die durch Änderung entstehen könnten, versehentliche oder kriminelle Zerstörung oder versehentlichen Verlust der Daten zu verhindern sowie alle anderen gesetzeswidrigen Arten der Verarbeitung. Unter Berücksichtigung der Rechtsvorschriften, der bewährten Verfahrensweisen und der durch ihre Umsetzung entstehenden Kosten sollen die Sicherheitsmaßnahmen ein Niveau an Sicherheit gewährleisten, das für die durch die Verarbeitung und die Art der zu schützenden Daten dargestellten Risiken angemessen ist.

- Die erhobenen Personenbezogenen Daten müssen richtig, vollständig für den betreffenden Zweck und erforderlichenfalls ständig aktuell sein.

- Die erhobenen Personenbezogenen Daten müssen angemessen, erheblich und verhältnismäßig sein im Verhältnis zu dem Zweck/den Zwecken, für die sie erhoben und/oder weiterverarbeitet werden.

- Personenbezogene Daten dürfen nicht länger aufbewahrt werden als nötig ist für den Zweck/die Zwecke, für die sie erhoben und/oder verarbeitet wurden.

- Prozesse sind einzuführen zur Sicherstellung zeitnaher Antworten auf Anfragen von Betroffenen Personen, um zu gewährleisten, dass sie ihre Rechte auf Auskunft, Berichtigung und den Widerspruch gegen die Verarbeitung ordnungsgemäß wahrnehmen können (sofern das anwendbare Recht nichts anderes vorsieht).

Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine solche Verarbeitung rechtlich begründet ist, einschließlich z. B. wenn:

- die Betroffene Person ihre eindeutige Einwilligung erteilt hat; oder

- die Verarbeitung für die Erfüllung eines Vertrags, den die Betroffene Person geschlossen hat, notwendig ist, oder zur Einleitung von Schritten vor Abschluss eines Vertrags auf Antrag der Betroffenen Person hin; oder
- die Verarbeitung zur Einhaltung einer rechtlichen Verpflichtung, der der Daten-Controller unterliegt, notwendig ist; oder
- die Verarbeitung zum Schutz der lebenswichtigen Interessen der Betroffenen Person notwendig ist; oder
- die Verarbeitung zur Erfüllung einer im öffentlichen Interesse durchzuführenden Aufgabe notwendig ist oder in der Ausübung einer offiziellen Vollmacht, die dem Daten-Controller bzw. einem Dritten, dem die Personenbezogene Daten offenbart wurden, erteilt worden ist; oder
- die Verarbeitung für die legitimen Interessen des Daten-Controllers oder des Dritten bzw. -parteien, denen die Personenbezogenen Daten offenbart wurden, notwendig ist, außer in Fällen, wo die Interessen oder Grundrechte und Freiheiten der Betroffenen Person Vorrang vor solchen Interessen haben.

Wenn die Verarbeitung von Personenbezogenen Daten allein auf einer automatisierten Verarbeitung basiert, die bestimmte persönliche Aspekte bezüglich der Betroffenen Person bewerten sollen (so wie Leistung bei der Arbeit, Kreditwürdigkeit, Zuverlässigkeit, Verhalten, usw.) und erzeugt sie rechtliche Folgen für sie oder beeinträchtigt diese sie erheblich, hat die Betroffene Person das Recht der Verarbeitung zu widersprechen, es sei denn eine solche Verarbeitung:

- im Rahmen des Abschlusses oder der Erfüllung eines Vertrags erfolgt, sofern der Antrag der Betroffenen Person auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde oder es angemessene Maßnahmen zur Wahrung ihrer legitimen Interessen gibt, etwa Regelungen, damit sie ihre Meinung äußern kann; oder
- durch ein Gesetz autorisiert wird, das außerdem Maßnahmen zur Wahrung der legitimen Interessen der Betroffenen Personen vorschreibt.

2. Besondere Arten Personenbezogener Daten

Für die Zwecke dieser BCR umfassen Besondere Arten Personenbezogener Daten alle Personenbezogenen Daten in Bezug auf:

- die Rasse oder ethnische Herkunft, die politischen Meinungen oder den religiösen oder philosophischen Glauben der Betroffenen Person,
- Mitgliedschaft der Betroffenen Person in einer Gewerkschaft,
- den physischen oder psychischen Gesundheitszustand oder das Sexualleben der Betroffenen Person,
- bestimmte Daten, die nach geltendem Recht und bestimmten Regeln als Besondere Arten Personenbezogener Daten gelten (z.B. medizinische Daten),
- das Begehen oder vermeintliche Begehen einer Straftat durch die Betroffene Person, oder
- jedes Verfahren wegen einer von der Betroffenen Person begangenen oder vermeintlich begangenen Straftat, den Abschluss eines solchen Verfahrens oder das Urteil von einem Gericht in einem solchen Verfahren.

Obige Liste darf keinesfalls als vollständige Aufzählung Besonderer Arten Personenbezogener Daten betrachtet werden, da die lokale Gesetzgebung zusätzliche Kategorien vorsehen kann, die in solchen und auch in anderen Fällen vom Datenexporteur und vom Datenimporteur als Besondere Arten Personenbezogener Daten zu beachten sind.

Die Verarbeitung Besonderer Arten Personenbezogener Daten ist mit Ausnahme folgender Fälle verboten:

1. die Betroffene Person hat ihre ausdrückliche Einwilligung für die Verarbeitung solcher Besonderer Arten Personenbezogener Daten erteilt, und eine solche Einwilligung ist als gültig erachtet worden gemäß den anwendbaren Gesetzen und Vorschriften; oder
2. die Verarbeitung ist für die Zwecke der Wahrnehmung der Pflichten und spezifischen Rechte des Daten-Controllers im Bereich des Arbeitsrechts notwendig, soweit sie vom nationalen Recht, das für angemessene Sicherheit sorgt, autorisiert wird; oder
3. die Verarbeitung ist zum Schutz der lebenswichtigen Interessen der Betroffenen Person, bzw. einer anderen Person notwendig, wenn die Betroffene Person körperlich oder rechtlich nicht in der Lage ist, ihre Einwilligung zu erteilen; oder
4. die Verarbeitung wird im Rahmen seiner legitimen Aktivitäten durchgeführt mit angemessenen Gewährleistungen einer Stiftung, eines Verbands oder einer anderen gemeinnützigen Organisation mit einer politischen, philosophischen, religiösen oder gewerkschaftlichen Orientierung und vorausgesetzt, dass die Verarbeitung ausschließlich im Zusammenhang mit den Mitgliedern des Verbands oder den Personen, die in Bezug auf dessen Zwecke regelmäßigen Kontakt dazu haben, stattfindet, und dass die Personenbezogenen Daten nicht ohne die Einwilligung der Betroffenen Personen an Dritte offenbart werden; oder
5. die Verarbeitung bezieht sich auf Besondere Arten Personenbezogener Daten, die von der Betroffenen Person erkennbar veröffentlicht wurden; oder
6. die Verarbeitung Besonderer Arten Personenbezogener Daten ist für die Erhebung, Geltendmachung oder Abwehr gesetzlicher Ansprüche notwendig; oder
7. die Verarbeitung der Besonderen Arten Personenbezogenen Daten ist für die Zwecke präventiver Medizin, medizinischer Diagnose, Pflege oder Behandlung oder der Verwaltung von Gesundheitsdienstleistungen notwendig; und wo diese Besonderen Arten Personenbezogener Daten verarbeitet werden
   - von einem qualifizierten Gesundheitsdienstmitarbeiter, der durch die geltenden Gesetze oder Regeln der zuständigen nationalen Behörden der beruflichen Schweigepflicht unterliegt, oder
   - einer anderen Person, die ebenfalls einer äquivalenten Schweigepflicht unterliegt; oder
8. die Verarbeitung ist ansonsten nach dem geltenden Recht des Landes erlaubt, in welchem der Datenexporteur sitzt.

3. Unterbeauftragungen von Verarbeitern

Wenn die Verarbeitung im Namen eines Datenimporteurs von einem Subunternehmen durchgeführt wird, wählt Letzterer ein Subunternehmen, das ausreichende technische Sicherheitsmaßnahmen und organisatorische Maßnahmen für die durchzuführende Verarbeitung gewährt, um sicherzustellen, dass die Verarbeitung in Übereinstimmung mit den BCR erfolgt und der Datenimporteur muss sicherstellen, dass das Subunternehmen diese Maßnahmen erfüllen wird. Der Datenimporteur, der den Subunternehmer wählt, sichert und vereinbart solche technischen Sicherheitsmaßnahmen und organisatorischen Maßnahmen schriftlich mit dem jeweiligen Subunternehmer und macht insbesondere zur

Bedingung, dass der Subunternehmer nur auf Anweisungen des Datenimporteurs handeln soll.

4. Datenübermittlungen

1. Datenübermittlungen innerhalb der AXA Gruppe

Es dürfen keine Personenbezogenen Daten zu einem Datenimporteur außerhalb des EWR übermittelt werden (oder im Falle des Exports aus einem anderen Geregelten Zuständigkeitsbereich, dieser Geregelte Zuständigkeitsbereich), bis der Datenexporteur festgestellt hat, dass der Datenimporteur gebunden ist an:

- diese BCR,
- andere Maßnahmen, welche die Übermittlung Personenbezogener Daten nach Maßgabe des anwendbaren Rechts erlauben (z.B. EU-Standardvertragsklauseln).

Wie unter den Begriffen „Relevante Übermittlung“ und „Weiterübermittlung“ wiedergegeben, finden diese BCR nur Anwendung bei Übermittlungen die nicht schon von anderen Maßnahmen gedeckt sind, welche eine Übermittlung erlauben, sofern nichts anderes schriftlich zwischen dem Datenexporteur und dem Datenimporteur vereinbart ist.

2. Datenübermittlungen außerhalb der AXA Gruppe

In Bezug auf jede Übermittlung an eine dritte Gesellschaft außerhalb des EWR (im Falle des Exports aus dem EWR und sonst außerhalb des relevanten Geregelten Zuständigkeitsbereiches), die nicht an diese BCR gebunden ist, verpflichtet sich jeder Datenexporteur zu Folgendem:

- wenn die Übermittlung an einen Datenverarbeiter erfolgt, Unterzeichnung einer Datenverarbeitungs-Vereinbarung mit dem datenverarbeitenden Dritten, um nach europäischen Standards genügenden Schutz der verarbeiteten Daten sicherzustellen, indem z.B. die anwendbaren EU-Standardvertragsklauseln der Europäischen Kommission oder eine andere Vereinbarung, durch die mindestens eine äquivalente Verpflichtung eingegangen wird, verwendet werden; oder
- Durchführung aller weiteren notwendigen Sicherheitsmaßnahmen, die nach Maßgabe des anwendbaren Rechts für die Übermittlung Personenbezogener Daten erforderlich sind (z.B. EU-Standardvertragsklauseln).

ARTIKEL V - RECHTE AUF INFORMATION, AUSKUNFT, BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN

Im Fall einer Übermittlung Personenbezogener Daten an einen Datenimporteur sind Betroffene Personen/Geregelter Zuständigkeitsbereich nach schriftlichem Antrag dazu berechtigt,

- eine Kopie der für die Öffentlichkeit bestimmten Version der BCR von der AXA Internetseite, der AXA Intranet Webseite oder dem DPO nach Antrag und innerhalb eines angemessenen Zeitraums zu erhalten;
- Informationen über gespeicherte Personenbezogene Daten anzufordern, einschließlich Informationen in Bezug darauf, wie Personenbezogene Daten erhoben wurden;
- die Liste der Empfänger oder Kategorien der Empfänger, an die ihre Personenbezogenen Daten übermittelt werden;
- Auskünfte zum Zweck der Erhebung der Personenbezogenen Daten sowie der Übermittlung einzuholen;

- ihre Personenbezogenen Daten zu berichtigen, falls sie unrichtig sind;
- der Verarbeitung ihrer Personenbezogenen Daten aus zwingenden, legitimen Gründen bezüglich ihrer spezifischen Situation zu widersprechen, wenn nicht durch das anwendbare Recht anders vorgesehen;
- die Löschung ihrer Personenbezogenen Daten durchzusetzen, wenn dies rechtlich möglich und begründet ist;
- alle weiteren Auskünfte, die nach dem anwendbaren lokalen Gesetz notwendig wären, einzuholen,

in jedem Fall ist Speichern in dem Umfang nach dem Datenschutzrecht des Geregelten Zuständigkeitsbereichs erlaubt in welchem die Betroffene Person/Geregelter Zuständigkeitsbereich ansässig war zu dem Zeitpunkt an dem ihre Personenbezogenen Daten erhoben wurden.

ARTIKEL VI - MAßNAHMEN ZUR EINFÜHRUNG DER BCR

1. Schulungsprogramme

BCR AXA Gesellschaften verpflichten sich Schulungsprogramme über den Schutz Personenbezogener Daten für AXA-Mitarbeiter einzuführen, die an der Verarbeitung Personenbezogener Daten beteiligt sind und Werkzeuge zu entwickeln, um die Personenbezogenen Daten zu verarbeiten im Hinblick auf die in diesen BCR enthaltenen Grundsätze.

Die allgemeinen Grundsätze für Schulung und Awareness werden zentral in einem Dokument erarbeitet und praktische Beispiele werden geteilt, während die finale Entwicklung und Einführung der Schulungs- und Awarenesssitzungen (e-learning, face-to-face, …) von jeder BCR AXA Gesellschaft nach Maßgabe der jeweils anwendbaren Gesetze und Prozesse erfolgt.

Jede AXA Gesellschaft soll definieren, wie sie die Kontrolle über den erfolgreich abgeschlossenen Ausbildungsstand ausführt. Außerdem wird jede AXA Gesellschaft die Intervalle von Auffrischungsschulungen, die Schulung über den Schutz Personenbezogener Daten neu angestellter AXA-Mitarbeiter als ein Teil ihrer Einführungsveranstaltung über den Beitritt zu einer BCR AXA Gesellschaft bestimmen, wie auch die Schulung, die sich speziell an AXA-Mitarbeiter richtet, die an kritischen Aspekten von Personenbezogenen Daten enger beteiligt sind.

2. BCR Governance

3. Verantwortlichkeiten für die BCR und BCR Compliance-Kontrollprogramm

4. Zugang zu den BCR und Mitteilung an Betroffene Personen/Geregelter Zuständigkeitsbereich

Die Unterrichtung von Betroffenen Personen/Geregelter Zuständigkeitsbereich, die keinen Zugang zu der AXA Intranet Webseite haben, wie Kunden, die ihnen gleichgestellte Personen (Anspruchsteller, Unfallopfer und andere Bezugsberechtigte einer Versicherungspolice, die diese nicht abgeschlossen haben), Bewerber und Zulieferer über die BCR ist erfüllt durch die Veröffentlichung der für die Öffentlichkeit bestimmten Version der BCR auf der öffentlichen AXA Internetseite.

Die Unterrichtung von Betroffenen Personen/Geregelter Zuständigkeitsbereich, welche Zugang zu der AXA Intranet Webseite haben, so wie AXA-Mitarbeiter und die ihnen

gleichgestellte Personen (Makler, Repräsentanten, …) über die BCR ist erfüllt durch die Veröffentlichung der für die Öffentlichkeit bestimmten Version der BCR auf der AXA-Intranet Webseite.

Weitere optionale Wege die Kunden, Provider und AXA-Mitarbeiter in den jeweiligen BCR AXA Gesellschaften zu informieren, sind: das Informieren von Kunden über verschiedene Themen innerhalb eines Schreibens/einer Mitteilung, das Informationen von Kunden über eine Agentur - z.B. durch den Zugriff eines Vermittlers auf das Intranet sowie das Informieren von AXA-Mitarbeitern über Betriebsräte oder sonstige zuständige Mitarbeitervertreter. Es ist nicht möglich (da übermäßig schwierig und teuer) einen persönlichen Brief an alle Kunden zu schicken, wie z. B. Anspruchsteller, Unfallopfer oder Bezugsberechtigte einer Police, welche nicht versichert sind oder diese nicht abgeschlossen haben.

ARTIKEL VII - RECHTE DRITTBEGÜNSTIGTER

Es ist die Absicht aller Datenexporteure den Betroffenen Personen/Geregelter Zuständigkeitsbereich Drittbegünstigungsrechte unter diesen BCR einzuräumen in Bezug auf Relevante Übermittlungen und Weiterübermittlungen. Dementsprechend ist es von jedem Datenexporteur ausdrücklich anerkannt und akzeptiert, dass Betroffene Personen/Geregelter Zuständigkeitsbereich unter Beachtung von Relevanten Übermittlungen und Weiterübermittlungen dazu berechtigt sind ihre Rechte auszuüben gemäß der Bestimmungen der Artikel IV.1, IV.2, IV.4, V, VII, VIII, IX, X, XII.3 und XIII dieser BCR und dass die Unterlassung jedes Datenexporteurs mit den Verpflichtungen dieser Artikel übereinzustimmen unter diesen Umständen Anlass geben wird dies zu beheben und, wenn erforderlich und soweit nach anwendbarem Recht vorgesehen, Entschädigungsrechte (wie es der Fall sein kann unter Berücksichtigung der begangenen Verletzung und dem erlittenen Schaden) für die Betroffenen Personen/Geregelter Zuständigkeitsbereich beeinflusst.

Es ist ausdrücklich vereinbart, dass die oben erwähnten an Dritte gewährten Rechte ausschließlich für Betroffene Personen/Geregelter Zuständigkeitsbereich in Bezug auf Relevante Übermittlungen und Weiterübermittlungen gelten und keinesfalls auf Betroffene Personen außerhalb des Geregelten Zuständigkeitsbereichs ausgeweitet oder ausgelegt werden dürfen oder auf andere Übermittlungen Personenbezogener Daten.

ARTIKEL VIII - BESCHWERDEN

Es ist die Verantwortlichkeit jeder BCR AXA Gesellschaft, einen internen Bearbeitungsprozess einzurichten. Im Falle eines Disputs können Betroffene Personen/Geregelter Zuständigkeitsbereich nach Maßgabe der jeweiligen lokalen Regelungen eine Beschwerde über eine etwaige illegale oder unangemessene Verarbeitung ihrer Personenbezogenen Daten, die in irgendeiner Hinsicht diesen BCR nicht entspricht, bei folgenden Stellen einlegen:

- dem Datenschutzbeauftragten,
- der zuständigen Datenschutzbehörde, und
- den örtlich zuständigen Gerichten des Landes in welchem der Datenexporteur seinen Sitz hat. Sofern Letzterer seinen Sitz nicht im EWR hat, aber Personenbezogene Daten einer Betroffenen Person/EWR innerhalb des EWR verarbeitet, soll die zuständige Gerichtsbarkeit in dem Land sein, wo eine solche Verarbeitung stattfindet. Wo Personenbezogene Daten von Betroffenen Personen/EWR von einem EWR-Datenexporteur stammen, soll die zuständige Gerichtsbarkeit der Ort der Niederlassung des EWR-Datenexporteurs sein.

Zur Vermeidung von Zweifeln ist es selbstverständlich, dass die Betroffene Person/Geregelter Zuständigkeitsbereich, wenn sie nicht zufrieden ist mit den Antworten des Datenschutzbeauftragten, das Recht hat eine Beschwerde vor der zuständigen Datenschutzbehörde und/oder der zuständigen Gerichtsbarkeit des Landes gemäß vorstehendem Absatz einzureichen.

Jede BCR AXA Gesellschaften weist auf Ihrer Internet-Webseite daraufhin, wo Betroffene Personen/Geregelter Zuständigkeitsbereich ihre Beschwerden einlegen können, und macht mindestens eine der folgenden Angaben:

- Link zu einem Beschwerdeformular
- E-Mail-Adresse
- Telefonnummer
- Postanschrift.

Außer in den Fällen, wo es besonders schwierig ist, die zur Überprüfung notwendigen Informationen herauszufinden, sind Beschwerden innerhalb eines (1) Monats ab Einreichung der Beschwerde zu überprüfen.

ARTIKEL IX - HAFTUNG

1. Allgemeine Position

Jede BCR AXA Gesellschaft trägt die alleinige Verantwortung für alle Verletzungen der BCR gegenüber anderen, wie es der Fall sein kann, AXA BCR Gesellschaften, zuständigen Datenschutzbehörden des Geregelten Zuständigkeitsbereichs und Betroffenen Personen/Geregelter Zuständigkeitsbereich, soweit nach anwendbarem Recht und Vorschriften vorgesehen.

Soweit nach anwendbarem Recht und Vorschriften und vorbehaltlich Artikel IX (2) und IX (3), haftet jeder Datenexporteur persönlich für erlittene Schäden aufgrund einer Verletzung der BCR einer Betroffenen Person/Geregelter Zuständigkeitsbereich, die er selbst oder durch einen Datenimporteur begangen hat, der die Personenbezogenen Daten aus einem Geregelten Zuständigkeitsbereich gemäß einer Relevanten Übermittlung oder einer Weiterübermittlung stammend von dem verbundenen Datenexporteur bekommen hat.

Soweit nach anwendbarem Recht und Vorschriften und vorbehaltlich Artikel IX (2) und IX (3), wo Personenbezogene Daten von Betroffenen Personen/EWR von einem EWR-Datenexporteur stammen, haftet jeder EWR-Datenexporteur persönlich für Schäden, die eine Betroffene Person/EWR erleidet aufgrund einer durch sich selbst oder durch eine vom Datenimporteur begangen Verletzung der BCR, der Personenbezogene Daten durch eine Übermittlung aus dem EWR aufgrund einer Relevanten Übermittlung oder einer Weiterübermittlung von dem verbundenen EWR-Datenexporteur bekommen hat.

Vorbehaltlich Artikel IX (2) und (3), ist jede BCR AXA Gesellschaft verantwortlich für den Verlust oder Schaden infolge seiner eigenen Verletzung der BCR soweit nach anwendbarem Recht und Vorschriften vorgesehen. Keine BCR AXA Gesellschaft haftet für die Verletzung, die durch eine andere BCR AXA Gesellschaft begangen wurde, außer in dem Fall der Verletzung durch einen Datenimporteur wo ein Datenexporteur die Betroffene Person/Geregelter Zuständigkeitsbereich zunächst erstatten kann (gem. Artikel IX (2) und (3)), und dann die Erstattung vom Datenimporteur begehrt, z.B. wenn ein Datenimporteur die BCR verletzt und der Datenexporteur Entschädigung an die Betroffene Person/Geregelter Zuständigkeitsbereich zahlt im Hinblick auf eine solche

Verletzung, dann ist der Datenexporteur verpflichtet dem Datenimporteur zurückzuerstatten.

Der Datenexporteur dessen Haftung als Folge einer Verletzung durch einen Datenimporteur entstanden ist, kann die notwendigen Maßnahmen treffen, um diese Handlungen des Datenimporteurs zu beheben und, unter Berücksichtigung der Verletzung und des erlittenen Schadens der Betroffenen Person/Geregelter Zuständigkeitsbereich, eine Entschädigung zahlen an die Betroffene Person/Geregelter Zuständigkeitsbereich in Übereinstimmung mit dem geltenden Recht und den lokalen Standards. Danach kann der Datenexporteur versuchen Regress gegen den Datenimporteur für die Verletzung der BCR zu erhalten. Der Datenexporteur kann entweder teilweise oder vollständig entlastet werden, wenn er nachweisen kann, dass er nicht verantwortlich ist für die Ursache solcher Schäden.

Eine Betroffene Person/Geregelter Zuständigkeitsbereich hat das Recht auf angemessenen Schadenersatz für Schäden, die von einem Datenimporteur in Bezug auf vom Datenexporteur übermittelte Personenbezogene Daten verursacht wurden unter Berücksichtigung der Verletzung gemäß dem anwendbarem Recht und den lokalen Standards und unter Berücksichtigung des (nachweislich) erlittenen Schadens. Soweit die Betroffene Person/Geregelter Zuständigkeitsbereich durch die geltende Gerichtsbarkeit dazu berechtigt ist, kann sie den Anspruch vor der Datenschutzbehörde oder der zuständigen Gerichtsbarkeit des Landes, in welchem der Datenexporteur seinen Sitz hat, bringen. Wo Letztere nicht in dem EWR ansässig ist, aber Personenbezogene Daten einer Betroffenen Person/EWR innerhalb des EWR verarbeitet, soll die zuständige Gerichtsbarkeit in dem Land sein, in dem die Verarbeitung stattfindet. Wo Personenbezogene Daten der Betroffenen Person/EWR von einem EWR-Datenexporteur stammen, ist die zuständige Gerichtsbarkeit der Ort der Niederlassung des ersten EWR-Datenexporteurs.

2. Zusätzliche Bestimmungen, wo der Datenimporteur ein Daten-Controller ist

Die folgenden Bestimmungen gelten nur dann, wenn der Datenimporteur als Daten-Controller handelt und legen die einzigen Umstände fest, wenn ein Anspruch von einer Betroffenen Person/Geregelter Zuständigkeitsbereich gegen einen solchen Datenimporteur oder seinen Unterauftragsverarbeiter erhoben werden kann.

In Situationen, in denen Beschwerden eingereicht werden, wonach der Datenimporteur seinen Verpflichtungen aus den BCR nicht nachgekommen ist, muss die Betroffene Person/Geregelter Zuständigkeitsbereich zuerst fordern, dass der entsprechende Datenexporteur angemessene Schritte unternimmt, um den Fall zu untersuchen und (wenn eine Verletzung vorliegt) die Schäden zu beheben, die aus der angeblichen Verletzung entstanden sind und die die Betroffene Person/Geregelter Zuständigkeitsbereich erlitt und seine Rechte gegenüber dem Datenimporteur behaupten, der die BCR verletzte. Sollte der Datenexporteur diese Schritte nicht in einer angemessenen Zeit unternehmen (normalerweise 1 Monat), ist die Betroffene Person/Geregelter Zuständigkeitsbereich berechtigt ihre Rechte gegen den Datenimporteur unmittelbar geltend zu machen. Eine Betroffene Person/Geregelter Zuständigkeitsbereich ist ebenso berechtigt Maßnahmen direkt gegen den Datenexporteur geltend zu machen, der es unterlassen hat zumutbare Anstrengungen zu unternehmen, egal ob der Datenimporteur in der Lage ist, die Verpflichtungen aus diesen BCR in dem Umfang wie vorgesehen und in Übereinstimmung mit anwendbarem Recht zu erfüllen.

3. Zusätzliche Bestimmungen, wo der Datenimporteur ein Datenverarbeiter ist

Die folgenden Bestimmungen gelten nur dann, wenn der Datenimporteur als Datenverarbeiter handelt und legen die einzelnen Umstände fest, wann ein Anspruch von einer Betroffenen Person/Geregelter Zuständigkeitsbereich gegen einen solchen Datenimporteur oder seinen Unterauftragsverarbeiter erhoben werden kann.

Wenn es einer Betroffenen Person/Geregelter Zuständigkeitsbereich nicht möglich ist, einen Schadenersatzanspruch gegen den Datenexporteur geltend zu machen, der sich aus einer Verletzung des Datenimporteurs oder seines Unterauftragsverarbeiters ergibt, weil der Datenexporteur faktisch verschwunden ist oder aufgehört hat rechtlich zu existieren oder insolvent wurde, stimmt der Datenimporteur zu, dass die Betroffene Person/Geregelter Zuständigkeitsbereich einen Anspruch geltend machen kann gegen den Datenimporteur so als wäre es der Datenexporteur, es sei denn, ein Rechtsnachfolger hat die gesamten rechtlichen Verpflichtungen des Datenexporteurs durch Vertrag oder von Rechts wegen übernommen, in diesem Fall kann die Betroffene Person ihre Ansprüche gegen dieses Unternehmen durchsetzen. Der Datenimporteur kann bei einer Verletzung durch den Unterauftragsverarbeiter nicht auf seine Verpflichtung vertrauen, um seine eigene Verantwortung zu vermeiden.

Wenn es einer Betroffenen Person/Geregelter Zuständigkeitsbereich nicht möglich ist, einen Anspruch gegen den Datenexporteur oder den Datenimporteur geltend zu machen, der sich aus einer Verletzung einer ihrer Verpflichtungen aus diesen BCR durch eine unterauftragsverarbeitende BCR AXA Gesellschaft ergibt, weil beide, der Datenexporteur und der Datenimporteur faktisch verschwunden sind oder aufgehört haben rechtlich zu existieren oder insolvent wurden, stimmt die unterauftragsverarbeitende BCR AXA Gesellschaft zu, dass die Betroffene Person/Geregelter Zuständigkeitsbereich einen Anspruch gegen die unterauftragsverarbeitende BCR AXA Gesellschaft geltend machen kann im Hinblick auf seine eigene Verarbeitung als wäre es der Datenexporteur und der Datenimporteur, es sei denn, ein Rechtsnachfolger hat sämtliche rechtliche Pflichten des Datenexporteurs oder Datenimporteurs durch Vertrag oder von Rechts wegen angenommen, wobei die Betroffene Person/Geregelter Zuständigkeitsbereich seine Rechte gegenüber diesen Unternehmen geltend machen. Die Haftung der unterauftragsverarbeitenden BCR AXA Gesellschaft soll auf seine eigene Verarbeitung Personenbezogener Daten beschränkt werden.

ARTIKEL X - GEGENSEITIGE UNTERSTÜTZUNG UND ZUSAMMENARBEIT MIT DATENSCHUTZBEHÖRDEN

1. Zusammenarbeit mit Datenschutzbehörden

Die BCR AXA Gesellschaften arbeiten mit ihrer jeweiligen Datenschutzbehörde in Bezug auf alle Fragen hinsichtlich der Auslegung der BCR zusammen, soweit es dem anwendbaren Recht und den Vorschriften entspricht und ohne Verzicht auf dem Daten-Controller zur Verfügung stehende Einreden und/oder Rechtsmittel:

- durch Bereitstellung der erforderlichen Mitarbeiter für den Dialog mit den Datenschutzbehörden;
- durch eine aktive Prüfung und Betrachtung aller von den Datenschutzbehörden gefällten Entscheidungen sowie der Ansichten der Artikel-29-Datenschutzgruppe in Bezug auf die BCR,
- durch Mitteilung aller wesentlichen Änderungen der BCR an die jeweilige Datenschutzbehörde,
- durch Antworten auf Auskunftsanforderungen oder Beschwerden der Datenschutzbehörden,

- durch Befolgung relevanter Empfehlungen oder Ratschläge von ihrer jeweiligen Datenschutzbehörde bezüglich der Beachtung der BCR durch die BCR AXA Gesellschaften.

Die BCR AXA Gesellschaften kommen überein, sich an eine formelle Entscheidung der zuständigen Datenschutzbehörde bezüglich der Auslegung und Anwendung dieser BCR zu halten, vorausgesetzt, dass eine solche Entscheidung nicht gegen lokale Gesetze oder Vorschriften verstößt und ohne Verzicht auf dem Daten-Controller zur Verfügung stehende Einreden und/oder Rechtmittel.

2. Verhältnis zwischen anwendbarem Recht und den BCR

BCR AXA Gesellschaften müssen stets lokale Gesetze einhalten. Dort, wo keine Datenschutzgesetze existieren, werden Personenbezogene Daten nach Maßgabe der BCR verarbeitet. Dort, wo die lokalen Gesetze ein höheres Niveau an Schutz Personenbezogener Daten vorsehen als die BCR, werden die lokalen Gesetze befolgt. Dort, wo die lokalen Gesetze ein niedrigeres Niveau an Schutz Personenbezogener Daten vorsehen als die BCR, werden die BCR befolgt.

Im Falle, dass eine BCR AXA Gesellschaft einen Grund hat zu glauben, dass die anwendbaren rechtlichen/regulatorischen Anforderungen die BCR AXA Gesellschaft daran hindern, die BCR zu befolgen, informiert die BCR AXA Gesellschaft sofort ihren DPO, und der DPO informiert den DPO des Daten-Exporteurs und den GDPO.

Soweit bestimmte Teile dieser BCR den anwendbaren Gesetzen/aufsichtsrechtlichen Bestimmungen widersprechen, haben die gesetzlichen/aufsichtsrechtlichen Bestimmungen Vorrang, bis die jeweiligen Konflikte auf eine Weise, die den gesetzlichen Vorschriften entsprechen, gelöst worden sind. Der GDPO und/oder der DPO kann die zuständige Datenschutzbehörde kontaktieren, um mögliche Lösungen zu besprechen.

ARTIKEL XI - DATUM DES INKRAFTTRETENS UND DAUER DER BCR

Die BCR treten am 15.01.2014 für eine unbestimmte Zeitdauer in Kraft.

Die BCR werden für jede BCR AXA Gesellschaft am Datum des Inkrafttretens der gruppeninternen Vereinbarung (IGA), die sie jeweils in Bezug auf diese BCR abschließt, wirksam. Die BCR werden für eine bestimmte BCR AXA Gesellschaft unwirksam, sobald entweder (i) die BCR schriftlich durch den GDPO an die koordinierende Datenschutzbehörde (die CNIL) und jede BCR AXA Gesellschaft gekündigt werden; oder (ii) die von ihr eingegangene IGA nach Maßgabe der in der IGA festgelegten Bedingungen gekündigt worden ist.

ARTIKEL XII - ANWENDBARES RECHT

1. Rechtswahl

Diese BCR (einschließlich jeder BCR Vereinbarungen) bestimmen sich nach und sind in Übereinstimmung mit dem französischem Recht.

2. Streitigkeiten zwischen dem Datenimporteur und dem Datenexporteur

Jede Streitigkeit unter diesen BCR zwischen dem Datenimporteur und dem Datenexporteur soll vor der zuständigen Gerichtsbarkeit des Landes des

Datenexporteurs entschieden werden, sofern nicht lokale Gesetze etwas anderes vorschreiben.

3. Andere Streitigkeiten zwischen den BCR AXA Gesellschaften

Jede andere Streitigkeit zwischen den BCR AXA Gesellschaften unter diesen BCR (einschließlich jeder BCR Vereinbarung) werden von den Gerichten der zuständigen Gerichtsbarkeit in Paris entschieden werden, es sei denn ein zwingendes Erfordernis der anwendbaren Rechtsvorschriften sieht etwas anderes vor.

4. Streitigkeiten mit Betroffenen Personen/Geregelter Zuständigkeitsbereich

Soweit nach geltender Gerichtsbarkeit und den Bestimmungen nach diesen BCR zu Rechten Dritter zulässig, ist eine Betroffene Person/Geregelter Zuständigkeitsbereich berechtigt einen Anspruch geltend zu machen

(i) vor der zuständigen Behörde des Landes in welchem der Datenexporteur seinen Sitz hat. Wo Letzterer seinen Sitz nicht im EWR hat, aber die Personenbezogenen Daten der Betroffenen Personen/EWR im EWR verarbeitet, ist die zuständige Gerichtsbarkeit in dem Land, wo die Verarbeitung stattfindet. Wo Personenbezogene Daten der Betroffenen Personen/EWR von einem EWR-Datenexporteur stammen, ist die zuständige Behörde am Ort der Niederlassung des ersten EWR-Datenexporteurs; oder

(ii) die Gerichte von Paris.

ARTIKEL XIII - AKTUALISIERUNG DER REGELN

Der GDPO stellt eine regelmäßige Überprüfung und Aktualisierung der BCR sicher, zum Beispiel als Folge wesentlicher Änderungen der Unternehmensstruktur und im aufsichtsrechtlichen Umfeld.

Alle BCR AXA Gesellschaften erkennen ausdrücklich an und stimmen zu, dass:

- Wesentliche Änderungen dieser BCR, die die Anforderungen an die BCR AXA Gesellschaften deutlich erhöhen, können in einer Entscheidung des AXA BCR Steuerungsausschusses beschlossen werden nach einem (1) Monat Beratung per E-Mail der BCR AXA Gesellschaften über E-Mails-Adressen der DPOs, die dem GDPO bekannt sind; und

- Unwesentliche Änderungen dieser BCR, welche alle anderen Änderungen sind, dürfen durch einen Beschluss des AXA BCR Steuerungsausschusses auch ohne Abstimmung mit irgendwelchen BCR AXA Gesellschaften angenommen werden.

Der GDPO ist dafür zuständig, die BCR AXA Gesellschaften aufzulisten und den Überblick zu behalten und jede Aktualisierung der BCR und der BCR AXA Gesellschaften festzuhalten. Der GDPO kommuniziert jedes Jahr solche aktualisierten BCR AXA Gesellschaften und jede wesentliche Änderung der BCR zu der koordinierenden Datenschutzbehörde und, außerdem, jeder anderen relevanten Datenschutzbehörde auf Anfrage. Der DPO kommuniziert solche aktualisierten für die Öffentlichkeit bestimmten Versionen der BCR an die Betroffenen Personen/Geregelter Zuständigkeitsbereich auf Anfrage.

VERZEICHNIS DER ANHÄNGE:

Anhang 1: BCR Vereinbarung
Anhang 2: Compliance-Kontrollprogramm