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. Wir verlangen von unseren Lieferanten durch vertragliche Vereinbarungen, dass sie ähnliche Standards zum Schutz personenbezogener Daten einhalten wie wir.

Die AXA Gruppe verfügt über eine globale Datenschutzorganisation/-governance mit (i) einem vom Management Committee genehmigten Datenschutz-Governancemodell, (ii) einem Gruppen-Datenschutzbeauftragten, (iii) einem Gruppen-Datenschutz-Steuerungsausschuss, (iv) einem Netzwerk an lokalen Datenschutzbeauftragten, die vom Konzerndatenschutzbeauftragten koordiniert werden, und (v) einer Gruppen-Datenschutzrichtline, der in das konzernweite Risiko-/Compliance-Management eingebettet ist.

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:

„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" bezeichnet zusammen die AXA SA und alle AXA Gesellschaften.

„BCR AXA Unternehmen" sind (i) alle AXA Gesellschaften, die die gruppeninterne Vereinbarung in ihrer Eigenschaft als Datenexporteure oder Datenimporteure unterzeichnet haben, und (ii) Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit mit AXA Gesellschaften ausüben, die die gruppeninterne Vereinbarung in ihrer Eigenschaft als Datenexporteure oder Datenimporteure unterzeichnet haben.

„Mitarbeiter von BCR-Unternehmen" sind alle Mitarbeiter von Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit mit AXA Gesellschaften ausüben, die die konzerninterne Vereinbarung in ihrer Eigenschaft als Datenexporteure oder Datenimporteure 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.

„Datenverletzung" bezeichnet eine Sicherheitsverletzung, die zur unbeabsichtigten oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.

„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.

„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.

„Europäischer Datenschutzrat" ist das Organ der Union, das sich aus dem Leiter einer Kontrollbehörde jedes Mitgliedstaates und dem Europäischen Datenschutzbeauftragten zusammensetzt.

„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 dem 19. März 2024 gehören zum EWR Österreich, Belgien, Bulgarien, Kroatien, Zypern, Tschechien, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Island, Irland, Italien, Lettland, Lichtenstein, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Polen, Portugal, Rumänien, Slowakei, Slowenien Spanien, und Schweden.

„EWR-Datenexporteur" meint jeden in der EWR ansässigen Daten-Controller oder Datenverarbeiter, der Personenbezogene Daten im Auftrag 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 Vorschriften" meint die derzeit und zukünftig anwendbaren Regel und Vorschriften zum Datenschutz, die in den EWR Staaten anzuwenden 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.

„Weiterleitung" bezeichnet die Weitergabe von Personenbezogenen Daten, die zuvor im Rahmen einer Relevanten Übertragung exportiert wurden:

(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) das keiner der zulässigen Ausnahmen oder Bedingungen unterliegt, die im Datenschutzgesetz in der entsprechenden geregelten Gerichtsbarkeit enthalten sind (wozu die Einwilligung der betroffenen Person, bestehende vertragliche Schutzmaßnahmen und/oder die Niederlassung in einer von der Europäischen Kommission gemäß der Europäischen Verordnung genehmigten Gerichtsbarkeit gehören können.

„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" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder Gruppen personenbezogener Daten wie das Erheben, das Speichern, die Organisation, die Strukturierung, die Speicherung, die Anpassung oder die Veränderung, das Auslesen, das Abfragen, die Benutzung, die Trennung, das Überkreuzen, das Zusammenführen, die Änderung, die Bereitstellung, die Nutzung, die Weitergabe, die Verbreitung, die Weitergabe durch Übermittlung, die Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung, die Einschränkung, die Löschung oder die Vernichtung.

„Verarbeiter" bezeichnet eine BCR AXA Gesellschaft, die personenbezogene Daten im Auftrag eines für die Verarbeitung Verantwortlichen verarbeitet.

„Geregelter Zuständigkeitsbereich" bezeichnet jeden Zuständigkeitsbereich innerhalb des EWR und in Andorra, der Schweiz, den Färöer-Inseln, Guernsey, der Isle of Man, Jersey, Singapur, der Türkei und dem Vereinigten Königreich.

„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 und /oder Einrichtung in einem von der Europäischen Kommission anerkannten Land gemäß der Europäischen Verordnung)

„Besondere Datenkategorien" sind solche Daten, die in Artikel IV Abschnitt 2 beschrieben werden.

„Aufsichtsbehörde" oder **„Datenschutzbehörde"** oder **"DPA"** bezeichnet die Verwaltungsbehörde, die offiziell für den Schutz personenbezogener Daten in jeder regulierten Gerichtsbarkeit zuständig ist, in der die AXA Gruppe präsent ist (in Frankreich ist diese Behörde beispielsweise die Commission Nationale de l'Informatique et des Libertés; in Spanien ist es die Agencia Espanola de Proteccion de Datos, usw.). Um Zweifel auszuschließen, schließt der Begriff "Aufsichtsbehörde" jeden Ersatz oder Nachfolger einer Datenschutzbehörde ein.

„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 oder eine Gesellschaft, die eine gemeinsame wirtschaftliche Tätigkeit mit AXA Gesellschaften mit Sitz in einer anderen Gerichtsbarkeit ausübt.

ARTIKEL III – GELTUNGSBEREICH

1. Geografischer 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 relevante Übermittlungen Personenbezogener Daten von innerhalb eines Geregelten Zuständigkeitsbereiches an Datenimporteure mit Sitz in einem anderen Zuständigkeitsbereich und für relevante Übermittlungen von Datenimporteuren mit Sitz in einem anderen Zuständigkeitsbereich zurück an einen Datenexporteur in einem Geregelten Zuständigkeitsbereich im Anschluss an diese erste relevante Übermittlung sowie für Weiterübermittlungen und der Rückgriff auf Verstöße gegen die Bestimmungen dieser BCR über die Rechte Dritter, Beschwerden und Haftung (wie in den Artikeln VII, VIII und IX dieser BCR dargelegt) ist auf Datensubjekte mit einem geregelten Zuständigkeitsbereich beschränkt.

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 auf den Philippinen 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 und Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit mit den AXA Gesellschaften ausüben, 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, wie in Anlage 1 zu Anhang 1 oder in der gruppeninternen Vereinbarung aufgeführt.

Jede AXA Gesellschaft oder jedes Unternehmen, das mit AXA Gesellschaften, die ein IGA unterzeichnen, eine gemeinsame wirtschaftliche Tätigkeit ausübt, wird ab dem Datum der Unterzeichnung oder (falls später) ab dem im anwendbaren IGA festgelegten Datum des Inkrafttretens eine 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 jedes andere geeignete Mittel, die BCR für die Arbeitnehmer der AXA oder der BCR-Unternehmen in dem jeweiligen Land verbindlich zu machen.

Nach Maßgabe mit dem geltenden Arbeitsrecht, den eigenen internen Vorschriften und Arbeitsverträgen kann jede der BCR AXA Gesellschaften Disziplinarmaßnahmen gegen jeden seiner eigenen AXA-Mitarbeiter oder Mitarbeiter der BCR-Gesellschaften ergreifen, insbesondere in folgenden Fällen:

- Verstoß gegen dieser BCR durch einen AXA-Mitarbeiter oder Mitarbeiter der BCR-Gesellschaften
- 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 oder Mitarbeitern von BCR-Gesellschaften, Bewerbern, Vertretern, Lieferanten und anderen Dritten erhoben werden.

Zu den Kategorien personenbezogener Daten, die von den BCR AXA Unternehmen verarbeitet werden und die gemäß den geltenden Rechtsvorschriften vor Ort erhoben werden müssen oder können, gehören:

- Daten zu Familienstand/Identität/Identität/Identifikation,
- Das Berufsleben,
- Persönliches Leben,
- Verbindungsdaten,
- Standortdaten,
- Sozialversicherungsnummer,
- Wirtschaftliche und finanzielle Informationen
- Straftaten, Verurteilungen, Sicherheitsmaßnahmen,
- Philosophische, politische, religiöse, gewerkschaftliche, sexuelle Lebensdaten, Gesundheitsdaten, rassische Herkunft,
- Biometrische Daten,
- Genetische Daten,
- Tod von Personen,
- Würdigung der sozialen Schwierigkeiten der Menschen,
- Daten zur Krankenversicherung

Die BCR decken sowohl automatisierte als auch manuelle Arten der Verarbeitung ab.

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 des Datenschutzes erfolgen wird:

- Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in transparenter Weise sowie unter Wahrung des Auskunftsrechts der betroffenen Person erhoben werden, es sei denn, diese Informationen sind aufgrund gesetzlicher Ausnahmen nicht erforderlich und sie dürfen nur verarbeitet werden, wenn die Betroffene Person ihre Einwilligung gegeben hat oder wenn die Verarbeitung anderweitig durch anwendbares Recht erlaubt ist.

- 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, dass für die durch die Verarbeitung und die Art der zu schützenden Daten dargestellten Risiken angemessen ist.

- Sowohl zum Zeitpunkt der Festlegung der Mittel der Verarbeitung, als auch zum Zeitpunkt der Verarbeitung selbst müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Grundsätze des Datenschutzes wirksam umzusetzen und die erforderlichen Schutzmaßnahmen von vornherein in die Verarbeitung zu integrieren, um die Anforderungen der europäischen Verordnung zu erfüllen und die Rechte der betroffenen Personen zu schützen.

- Geeignete technische und organisatorische Maßnahmen müssen umgesetzt werden, um sicherzustellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, die für jeden spezifischen Zweck der Verarbeitung erforderlich sind.

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

- Personenbezogene Daten, die erhoben werden, müssen so gering wie möglich gehalten werden, d.h. sie müssen angemessen und relevant sein und sich auf das beschränken,

was in Bezug auf den Zweck bzw. die Zwecke, für die sie erhoben und/oder weiterverarbeitet werden, tatsächlich erforderlich ist.

- Personenbezogene Daten dürfen nicht länger aufbewahrt werden, als es für den Zweck/die Zwecke, für den/die sie erhoben wurden, erforderlich ist, es sei denn, anwendbare Gesetze schreiben etwas anderes vor. Weitere Informationen zu den relevanten Datenaufbewahrungsfristen finden Sie in der in jedem BCR AXA Unternehmen geltenden Datenaufbewahrungspolitik

- Es müssen Verfahren eingeführt werden, die eine rasche Beantwortung von Anfragen der betroffenen Personen gewährleisten, um sicherzustellen, dass sie ihre Rechte auf Zugang, Berichtigung, Löschung ihrer Personenbezogenen Daten sowie ihr Recht auf Einschränkung und Widerspruch gegen die Verarbeitung (sofern das anwendbare Recht nichts anderes vorsieht) ordnungsgemäß ausüben können und um die Einwilligung zurückzuziehen, wenn sich die Verarbeitung auf diese Rechtsgrundlage stützt.

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

- das Datensubjekt seine Einwilligung gegeben 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 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 personenbezogener Daten ausschließlich auf der automatisierten Verarbeitung von Daten, einschließlich der Erstellung von Profilen, beruht und rechtliche Folgen für die Betroffene Person hat oder sie erheblich beeinträchtigt, haben die betroffenen Personen das Recht, einer solchen Entscheidung nicht unterworfen zu werden, es sei denn, eine solche Verarbeitung erfolgt:

- im Rahmen des Abschlusses oder der Erfüllung eines Vertrags erforderlich ist, vorausgesetzt, dem Antrag der betroffenen Person auf Abschluss oder Erfüllung des Vertrags wurde stattgegeben oder es gibt geeignete Maßnahmen zur Wahrung ihrer berechtigten Interessen, wie beispielsweise Regelungen, die es ihr ermöglichen, ihren Standpunkt zu vertreten und die Entscheidung anzufechten; oder

- durch ein Gesetz zugelassen ist, das auch Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht; oder

- basiert auf der ausdrücklichen Zustimmung der betroffenen Person, vorausgesetzt, es gibt geeignete Maßnahmen zur Wahrung seiner legitimen Interessen, z.B. Vorkehrungen, die es ihm erlauben, menschliches Eingreifen zu erwirken, seinen Standpunkt zu äußern und die Entscheidung anzufechten.

Jeder für die Verarbeitung Verantwortliche führt Aufzeichnungen über alle Kategorien von Verarbeitungsaktivitäten, die mit personenbezogenen Daten von EWR-Datensubjekten durchgeführt werden und stellt diese Aufzeichnungen der koordinierenden Datenschutzbehörde und allen anderen zuständigen Datenschutzbehörden auf Anfrage zur Verfügung.

Jeder für die Verarbeitung Verantwortliche führt Datenschutzfolgenabschätzungen durch, wenn dies für Verarbeitungsvorgänge erforderlich ist, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten von EWR-Datensubjekten führen. Wenn eine Datenschutzfolgenabschätzung darauf hinweist, dass die Verarbeitung zu einem hohen Risiko führen würde, wenn das Unternehmen BCR AXA keine Maßnahmen zur Risikominimierung ergreift, sollte die koordinierende Datenschutzbehörde oder jede andere relevante Datenschutzbehörde konsultiert werden.

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, das Sexualleben der Betroffenen Person, genetische Daten, biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen 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 spezieller Datenkategorien ist verboten, es sei denn

1. die Betroffene Person hat ausdrücklich in die Verarbeitung dieser besonderen Datenkategorien eingewilligt, und diese Einwilligung wird gemäß den anwendbaren Gesetzen und Vorschriften als gültig betrachtet; oder

2. die Verarbeitung ist für die Erfüllung der Pflichten und spezifischen Rechte des für die Verarbeitung Verantwortlichen oder der betroffenen Person auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit und des Sozialschutzes erforderlich, soweit sie nach geltendem Recht, das angemessene Garantien vorsieht, zulässig ist; oder

3. die Verarbeitung ist notwendig, um die lebenswichtigen Interessen der betroffenen Person oder einer anderen Person zu schützen, wenn die Betroffene Person physisch oder rechtlich nicht in der Lage ist, ihre Einwilligung zu geben; oder

4. die Verarbeitung erfolgt im Rahmen rechtmäßiger Tätigkeiten mit angemessenen Garantien durch eine Stiftung, eines Verbandes oder eine andere nicht gemeinnützigen Organisation mit politischer, philosophischer, religiöser oder gewerkschaftlicher Zielsetzung und unter der Bedingung, dass sich die Verarbeitung

ausschließlich auf die Mitglieder der Einrichtung oder auf Personen bezieht, die im Zusammenhang mit dem/den Zweck(en) regelmäßige Kontakte mit ihr haben und dass die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder

5. die Verarbeitung bezieht sich auf besondere Kategorien von Daten, die von der betroffenen Person erkennbar veröffentlicht wurden; oder

6. die Verarbeitung besonderer Datenkategorien ist für die Erhebung, Geltendmachung oder Abwehr von gesetzlichen Ansprüchen erforderlich; oder

7. die Verarbeitung ist aus Gründen eines wichtigen öffentlichen Interesses auf der Grundlage von Rechtsvorschriften der Union oder der Mitgliedstaaten erforderlich, die in einem angemessenen Verhältnis zum verfolgten Ziel stehen, den wesentlichen Inhalt des Rechts auf Datenschutz wahren und geeignete und spezifische Maßnahmen zur Wahrung der Grundrechte und der Interessen der betroffenen Person vorsehen; oder

8. die Verarbeitung der besonderen Datenkategorien ist erforderlich für die Zwecke der präventiven Medizin, für die Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, für die medizinische Diagnose, für die Bereitstellung von Gesundheits- oder Sozialfürsorge oder - behandlung oder für die Verwaltung von Gesundheits- oder Sozialfürsorgesystemen und - diensten auf der Grundlage des Rechts der Union oder der Mitgliedstaaten oder aufgrund eines Vertrags mit einem Angehörigen der Gesundheitsberufe und unter Einhaltung der Bedingungen und Garantien und wo diese Daten verarbeitet werden:
   - durch einen Berufsangehörigen, der zur Verschwiegenheit verpflichtet ist, oder
   - durch eine andere Person, die ebenfalls einer äquivalenten Geheimhaltungspflicht unterliegt; oder

9. die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit auf der Grundlage der Rechtsvorschriften der Union oder der Mitgliedstaaten erforderlich, die geeignete und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsehen;

10. die Verarbeitung ist für Archivierungszwecke im öffentlichen Interesse, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke im Einklang mit einer auf dem Recht der Union oder der Mitgliedstaaten beruhenden Europäischen Verordnung erforderlich, die in einem angemessenen Verhältnis zum verfolgten Zweck steht, das Wesen des Rechts auf Datenschutz achtet und geeignete und spezifische Maßnahmen zur Wahrung der Grundrechte und des Interesses der betroffenen Person vorsieht.

11. Die Verarbeitung ist ansonsten nach dem geltenden Recht des Landes, in dem der Datenexporteur sitzt, zulässig.

3. Unterbeauftragungen von Verarbeitern

Wird die Verarbeitung durch ein Subunternehmen im Namen eines Datenimporteurs durchgeführt, muss dieser die vorherige schriftliche Genehmigung des Datenexporteurs einholen, ein Subunternehmen auswählen, das ausreichende Garantien für die Durchführung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen bietet, um sicherzustellen, dass die Verarbeitung im Einklang mit den BCR durchgeführt wird und der Datenimporteur muss sicherstellen, dass das Subunternehmen diese Maßnahmen einhält. Der Datenimporteur, der das Subunternehmen auswählt, muss sicherstellen, dass das Subunternehmen diesen technischen Sicherheitsmaßnahmen und organisatorischen Maßnahmen schriftlich zustimmt, indem es einen Vertrag in Übereinstimmung mit der Europäischen Verordnung ausführt, der insbesondere festlegt, dass das Subunternehmen nur auf Anweisung des Datenimporteurs handelt.

4. Datenübermittlungen

1. Datentransfers innerhalb der AXA Gruppe und Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit mit AXA Unternehmen ausüben

Personenbezogene Daten dürfen nicht an einen Datenimporteur mit Sitz in einem Land außerhalb des EWR (oder im Falle von Exporten aus einer anderen geregelten Zuständigkeitsbereich, dieser geregelte Zuständigkeitsbereich) übertragen werden, bis der Datenexporteur festgestellt hat, dass der Datenimporteur gebunden ist an:

- diese BCR, oder,

- andere Maßnahmen, welche die Übermittlung von Personendaten nach anwendbarem Recht 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 und Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit mit AXA Unternehmen ausüben

In Bezug auf jede Übermittlung an eine dritte Gesellschaft außerhalb des EWR (im Falle des Exports aus dem EWR und sonst außerhalb des 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).

5. Datenschutzverletzung

Im Falle einer Datenschutzverletzung von personenbezogenen Daten von Betroffenen mit geeignetem Zuständigkeitsbereich melden die betroffenen BCR AXA-Gesellschaften die Datenverletzung unverzüglich dem/den Datenschutzbeauftragten der betroffenen BCR AXA Gesellschaft und wenn mehr als 1 000 Betroffene mit geeignetem Zuständigkeitsbereich betroffen sind, auch dem Gruppendatenschutzbeauftragten.

Die BCR AXA-Unternehmen, die als für die Verarbeitung Verantwortliche an einer Datenverletzung beteiligt sind, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person des geregelten Zuständigkeitsbereich führt, müssen die betroffene Person des geregelten Zuständigkeitsbereichs ebenfalls direkt benachrichtigen.

Jede Benachrichtigung über eine Datenverletzung ist zu dokumentieren und muss mindestens Folgendes umfassen:

- die Fakten im Zusammenhang mit der Datenverletzung,
- die wahrscheinlichen Folgen der Datenverletzung,
- die Abhilfemaßnahmen, die ergriffen wurden, um die Datenverletzung zu beheben, einschließlich, wenn angemessen, Maßnahmen zur Milderung ihrer möglichen nachteiligen Auswirkungen.

Diese Dokumentation wird der zuständigen Datenschutzbehörde und allen anderen einschlägigen Datenschutzbehörden auf Anfrage zur Verfügung gestellt.

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,

12. 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;
13. Informationen über gespeicherte Personenbezogene Daten anzufordern, einschließlich Informationen in Bezug darauf, wie Personenbezogene Daten erhoben wurden;
14. die Liste der Empfänger oder Kategorien der Empfänger, an die ihre Personenbezogenen Daten übermittelt werden;
15. Auskünfte zum Zweck der Erhebung der Personenbezogenen Daten sowie der Übermittlung einzuholen;
16. die Berichtigung ihrer Persönlichen Daten ohne unangemessene Verzögerung zu erhalten, wenn diese ungenau sind;
17. der Verarbeitung ihrer Personenbezogenen Daten aus zwingenden, legitimen Gründen bezüglich ihrer spezifischen Situation zu widersprechen, wenn nicht durch das anwendbare Recht anders vorgesehen;
18. die Löschung ihrer personenbezogenen Daten ohne unangemessene Verzögerung zu verlangen, wenn dies rechtlich möglich ist und aus den in der Europäischen Verordnung genannten Gründen;
19. die Einschränkung der Verarbeitung in Übereinstimmung mit der Europäischen Verordnung zu erwirken
20. alle anderen Informationen zu erhalten, die nach anwendbaren lokalen Recht erforderlich sind,
21. Ihre persönlichen Daten, die sie dem BCR AXA Unternehmen zur Verfügung gestellt haben, in einem geeigneten Format zu erhalten und diese Daten einem anderen Datenverantwortlichen zu transferieren, ohne dass ein BCR AXA Unternehmen eingreift

(nur im Falle der Verarbeitung aufgrund eines Vertrags oder der vorherigen Überlassung der Daten durch die betroffene Person durch Einwilligung)

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

Die BCR AXA Unternehmen verpflichten sich zur Durchführung von Schulungsprogrammen über den Schutz personenbezogener Daten für AXA-Mitarbeiter oder Mitarbeiter von BCR-Unternehmen, die an der Verarbeitung personenbezogener Daten beteiligt sind sowie zur Entwicklung von Instrumenten zur Verarbeitung personenbezogener Daten im Hinblick auf die in diesen BCR enthaltenen Grundsätze.

Die allgemeinen Grundsätze für Schulung und Sensibilisierung werden zentral ausgearbeitet und praktische Beispiele ausgetauscht, während die endgültige Entwicklung und Durchführung der Schulungs- und Sensibilisierungssitzungen (E-Learning, Face-to-Face...) von jedem BCR AXA Unternehmen in Übereinstimmung mit dem anwendbaren Recht und Prozessen durchgeführt wird.

Jedes BCR AXA Unternehmen legt fest, wie es die Kontrolle des Niveaus der erfolgreich abgeschlossenen Schulung durchführt. Darüber hinaus bestimmt jedes BCR AXA Unternehmen die Intervalle der Auffrischungsschulungen, die Schulung über den Schutz personenbezogener Daten neu eingestellter AXA-Mitarbeiter oder Mitarbeiter von BCR-Unternehmen im Rahmen ihrer Einführungsveranstaltung bei Eintritt in ein BCR AXA Gesellschaften sowie die Schulung, die sich speziell an AXA-Mitarbeiter oder Mitarbeiter von BCR-Gesellschaften richtet, die sich intensiver mit kritischen Aspekten personenbezogener Daten befassen.

2. BCR-Führung

Der **AXA BCR-Steuerungsausschuss:**

- Genehmigt den Geltungsbereich
- Genehmigt Ansätze
- Genehmigt Dokumente
- Schlichtet potenzielle Ressourcen, Konflikte

Die Führungsstruktur kann einer Weiterentwicklung und Veränderung unterliegen, z.B. als Folge möglicher künftiger gesetzlicher/behördlicher oder struktureller Veränderungen innerhalb der AXA-Gruppe. Derartige künftige Änderungen werden vom **AXA BCR- Steuerungsausschuss** beschlossen, der speziell für die BCR zuständig ist und sich aus Vertretern der Konzernleitung und Datenschutzbeauftragten ausgewählter BCR AXA-Gesellschaften wie GDPO, Datenschutzbeauftragten und einigen Vertretern/DPOs von BCR AXA-Gesellschaften zusammensetzt.

Bevor Änderungen beschlossen werden, haben alle BCR AXA Gesellschaften die Möglichkeit, im Rahmen eines Konsultationsprozesses ihren Beitrag zu den Änderungen zu leisten. Im Falle von Konflikten wird der BCR-Steuerungsausschuss zusammen mit dem betreffenden BCR-AXA-Gesellschaften sein Bestes tun, um diesen Konflikt zu lösen, um sicherzustellen, dass das betreffende BCR AXA Unternehmen weiterhin unter die BCR fällt.

Die BCR AXA Unternehmen erklären sich damit einverstanden, dass die BCR-Governance-Struktur den Entscheidungen des **BCR- Steuerungsausschuss von AXA** unterliegt und dass sie alle

Entwicklungen und Änderungen, die aufgrund von Entscheidungen dieses Ausschusses in diese Struktur eingebracht werden, einhalten werden (vorbehaltlich des oben beschriebenen vorherigen Konsultationsprozesses und möglicher rechtlicher und regulatorischer Einschränkungen).

Die BCR AXA Gesellschaften stimmen zu, dass nicht substanzielle Änderungen in einer Entscheidung des **AXA BCR Steuerungsausschuss** angenommen werden können, ohne dass eine Konsultation mit einem der BCR AXA Gesellschaften erforderlich ist.

Der GDPO ist für die Überwachung der Umsetzung der BCR durch ein Netzwerk von DPOs verantwortlich.

In Zukunft können BCR AXA-Hubs eingerichtet werden, um die Umsetzung der BCR in Zusammenarbeit mit dem GDPO zu unterstützen, z. B. durch Überwachung der Einhaltung und Befolgung der BCR durch die BCR AXA-Gesellschaften innerhalb ihres Geltungsbereichs.

Jedes BCR AXA-Unternehmen wird einen DSB ernennen, der für die Koordinierung mit dem GDPO und für die Gewährleistung der Einhaltung der BCR durch die BCR AXA Gesellschaften verantwortlich ist. Zu diesem Zweck kann der DSB von der Holdinggesellschaft einer konsolidierten Untergruppe (z. B. AXA Frankreich, AXA Großbritannien, AXA Deutschland) zum DSB einiger oder aller ihrer konsolidierten Tochtergesellschaften bestellt werden.

Der behördliche Datenschutzbeauftragte als zweite Verteidigungslinie unterstützt die Unternehmensleitung und das Management durch die Entwicklung und Umsetzung von Verfahren, Schutzmaßnahmen und Kontrollen, die darauf abzielen, die Erfüllung lokaler Anforderungen und die Übereinstimmung mit diesen BCR zu gewährleisten, insbesondere in Bezug auf

- Grundsätze der Verarbeitung
- Aktionen zur BCR-Implementierung
- Rechte von Drittbegünstigten
- Beschwerden
- Gegenseitige Hilfe und Zusammenarbeit mit Datenschutzbehörden.

Die GDPO wird für den Wissenstransfer zwischen den BCR AXA Gesellschaften sorgen, um sowohl Verbesserungen der lokalen Datenschutzprogramme zu ermöglichen als auch - wo angebracht - einen konsistenten Ansatz für die Datenschutzziele der Gruppe zu fördern und gleichzeitig die notwendigen lokalen Unterschiede aufgrund gesetzlicher oder anderer lokaler Anforderungen zu berücksichtigen.

Die GDPO kann in Zusammenarbeit mit Group IT, Compliance, Audit oder anderen die Schulungs-, Überwachungs- und Berichterstattungsanforderungen innerhalb der AXA-Gruppe weiterentwickeln, um eine angemessene Einhaltung der BCR zu gewährleisten. Diese Berichterstattung wird die lokalen Anforderungen nicht ersetzen, wenn die lokalen Rechtsfragen zusätzliche Maßnahmen erfordern.

Gegebenenfalls können regionale Datenschutzbeauftragte ernannt ("RDPO") und das Datenschutz-Governance-Modell für die Region nachgebildet werden. Der RDPO hat die Aufgabe, die BCR innerhalb der BCR AXA Gesellschaften in der Region zu fördern und koordiniert zwischen den DPOs in der Region und dem GDPO.

3. Verantwortlichkeiten für die BCR und das BCR-Compliance-Check-Programm

In Bezug auf die vorliegenden BCR gilt generell Folgendes.

Die Geschäftsleitung und die Unternehmensleitung sind als erste Verteidigungslinie dafür verantwortlich, dass die Verarbeitung personenbezogener Daten im Einklang mit den BCR erfolgt.

Die Datenschutzbeauftragte des AXA-Konzerns ist die zweite Verteidigungslinie. Die zweite Verteidigungslinie berät die Geschäftsleitung und die Geschäftsleitung in Bezug auf die BCR und die damit verbundenen Kontrollanforderungen. Sie führen jährlich das BCR-Kontrollprogramm zur Einhaltung der BCR durch. Das Programm zur Überprüfung der Einhaltung der BCR ist in Anhang 2 ausführlich beschrieben, die Abdeckung ist im Fragebogen zur Einhaltung der BCR detailliert aufgeführt.

Die Interne Revision, die die dritte Verteidigungslinie darstellt, bietet unabhängige Sicherheit über die Wirksamkeit der BCR. Die dritte Linie verifiziert die Wirksamkeit der zweiten und ersten Linie innerhalb des normalen fünf-Jahres-Zyklus der internen Revision.

Externe Audits und Audits der Datenschutzbehörden bieten zusätzliche unabhängige Sicherheit für die Wirksamkeit der BCR.

Das BCR-Compliance-Check-Programm deckt alle wesentlichen Aspekte der BCR ab, einschließlich der Methoden, die sicherstellen, dass Korrekturmaßnahmen ergriffen werden. Das Ergebnis des BCR-Compliance-Checkprogramms und relevante Prüfberichte - intern, extern und von Datenschutzbehörden - werden dem GDPO und dem DSB jedes betroffenen BCR AXA Unternehmens sowie jährlich dem Group Audit Committee mitgeteilt.

Die Ergebnisse des BCR-Compliance-Check-Programms und relevante Audit-Berichte - intern, extern und von Datenschutzbehörden - werden in einer Form aufbewahrt, dass Datenschutzbehörden mit Sitz im EWR darauf zugreifen können, wenn sie von ihrem unten dargelegten Audit-Recht Gebrauch machen.

Jeder Datenexporteur gestattet der örtlichen Datenschutzbehörde, die betreffenden BCR AXA Gesellschaften zu prüfen, damit die Datenschutzbehörde die Informationen erhalten kann, die erforderlich sind, um die Einhaltung der BCR durch die BCR AXA Gesellschaften nachzuweisen. Jede dieser Prüfungen unterliegt dem gleichen Umfang und den gleichen Bedingungen, wie wenn die örtliche Datenschutzbehörde den Datenexporteur nach dem Datenschutzgesetz des geregelten Zuständigkeitsbereiches der Datenschutzbehörde prüft. Jede dieser Prüfungen ist nicht erforderlich, soweit ein solcher Antrag gegen anwendbares Recht oder geltende Vorschriften verstößt und BCR AXA Gesellschaften auf keine Einreden und/oder Rechte verzichten, die den BCR-AXA-Gesellschaften zur Verfügung stehen.

Eine BCR-AXA-Gesellschaft ist nicht verpflichtet, auf Anfragen des DPA hin etwas offenzulegen, das nicht die Einhaltung der BCR betrifft und ist nicht verpflichtet, privilegierte oder vertrauliche Informationen Dritter offenzulegen, es sei denn, die betreffenden Dritten gestatten dies und ist nicht verpflichtet, die eigenen wirtschaftlich sensiblen Informationen der AXA offenzulegen, es sei denn, es ist unmöglich, die Elemente, die die Einhaltung der BCR betreffen, von denen zu trennen, die die eigenen wirtschaftlich sensiblen Informationen der AXA enthalten.

4. BCR-Zugang zu und Offenlegung von Daten, die dem geregelten Zuständigkeitsbereich unterliegen

Die Unterrichtung von Subjekten, die keinen Zugang zur Intranet-Website der AXA haben, wie z.B. Kunden, gleichgestellte Personen (Antragsteller, Unfallopfer und andere Begünstigte einer Versicherungspolice, die diese nicht abgeschlossen haben), Stellenbewerber und Lieferanten über die BCR erfolgt durch die Veröffentlichung der öffentlichen Fassung der BCR auf der öffentlichen Internet-Website der AXA.

Die Information von Personen, die Zugang zur Intranet-Website von AXA haben, wie z.B. AXA-Mitarbeiter und ihnen gleichgestellte Personen (Agenten, Vertreter...), über die BCR erfolgt durch die Veröffentlichung der öffentlich zugänglichen Fassung der BCR auf der Intranet-Website von AXA.

Weitere fakultative Möglichkeiten der Information von Kunden, Anbietern, AXA-Mitarbeitern und Mitarbeitern von BCR-Gesellschaften in jeder BCR AXA Gesellschaft können sein: die Bereitstellung von Informationen an Kunden in einem Schreiben/einer Mitteilung zu verschiedenen Themen, die Bereitstellung von Informationen an Kunden durch eine Agentur - z.B. durch den Zugang von Agenten zum Intranet - und die Bereitstellung von Informationen an AXA-Mitarbeiter und Mitarbeiter von BCR-Gesellschaften durch Betriebsräte oder andere zuständige Arbeitnehmervertretungen. In vielen Fällen ist es nicht möglich (da übermäßig schwierig und kostspielig), einen dedizierten Brief an alle Kunden zu senden, wie z.B. Geschädigte, Unfallopfer oder Begünstigte von Policen, die nicht versichert sind oder diese nicht abonniert haben.

ARTIKEL VII - RECHTE DRITTER BEGÜNSTIGTER

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:

- an den Datenschutzbeauftragten,
- die zuständige Datenschutzbehörde, bei der es sich entweder um die Datenschutzbehörde in der geregelten Gerichtsbarkeit des Ortes handelt, an dem er zum Zeitpunkt der Erhebung der

personenbezogenen Daten, die Gegenstand der Beschwerde sind, seinen gewöhnlichen Aufenthalt hatte, oder um den Ort des mutmaßlichen Verstoßes, und

- die zuständigen Gerichtsbarkeiten eines EWR-Landes nach Wahl der betroffenen Person: Die Betroffene Person kann wählen, ob sie vor den Gerichten des EWR-Landes, in dem der Datenexporteur eine Niederlassung hat, oder vor den Gerichten des EWR-Landes, in dem die Betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten, die Gegenstand der Beschwerde sind, ihren gewöhnlichen Aufenthalt hatte, auftreten möchte.

Zur Vermeidung von Zweifeln wird davon ausgegangen, dass die Betroffene Person, wenn die Antworten des Datenschutzbeauftragten nicht zufriedenstellend sind, das Recht hat, eine Beschwerde bei der zuständigen Datenschutzbehörde und/oder den zuständigen Gerichten des Landes gemäß obigem Absatz einzureichen.

Jede BCR AXA Gesellschaft wird auf seiner Internet-Website über praktische Hilfsmittel verfügen, die es den Betroffenen unter den geregelten Zuständigkeitsbereich ermöglichen, ihre Beschwerden einzureichen, darunter mindestens eines der unten aufgeführten:

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

Sofern es sich nicht als besonders schwierig erweist, die für die Durchführung der Untersuchung erforderlichen Informationen zu finden, müssen Beschwerden innerhalb eines (1) Monats nach dem Datum der Einreichung der Beschwerde untersucht werden. Im Falle besonderer Schwierigkeiten und unter Berücksichtigung der Komplexität und der Anzahl der Anträge kann diese Frist von einem (1) Monat um höchstens zwei (2) weitere Monate verlängert werden; in diesem Fall werden die Betroffenen von Daten der geregelten Gerichtsbarkeit entsprechend informiert.

ARTIKEL IX - HAFTUNG

1. Allgemeiner Standpunkt

Jede BCR AXA Gesellschaft trägt die alleinige Verantwortung für die Verstöße gegen die BCR, die in seinen Verantwortungsbereich fallen, gegenüber anderen BCR AXA Gesellschaften, den jeweils zuständigen Datenschutzbehörden und den betroffenen Rechtssubjekten, soweit dies im Rahmen der anwendbaren Gesetze und Vorschriften vorgesehen ist.

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 den anwendbaren Gesetzen und Vorschriften und vorbehaltlich von Artikel IX(2) und IX(3) vorgesehen, haftet jeder EWR-Datenexporteur, wenn die personenbezogenen Daten der betroffenen Person im EWR von einem EWR-Datenexporteur stammen, individuell für jeden Schaden, den eine Betroffene Person im EWR aufgrund eines Verstoßes gegen die BCR erleidet, den sie selbst oder ein Datenimporteur begangen hat, der die personenbezogenen Daten aus dem EWR im Rahmen einer relevanten Übermittlung oder Weiterübermittlung, die von dem verbundenen EWR-Datenexporteur stammen, erhalten 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 in Fällen, in denen ein Datenimporteur als für die Verarbeitung Verantwortlicher handelt, und legen die einzigen Umstände dar, unter denen ein Anspruch von einem Betroffenen, der einer geregelten Gerichtsbarkeit unterliegt, gegen einen solchen Datenimporteur geltend gemacht 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, wenn der Datenimporteur ein Verarbeiter 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 DEN DATENSCHUTZBEHÖRDEN

1. Zusammenarbeit mit den 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:

- indem sie das erforderliche Personal für den Dialog mit den Datenschutzbehörden zur Verfügung stellen,
- durch aktive Überprüfung und Berücksichtigung aller von den Datenschutzbehörden getroffenen Entscheidungen und der Ansichten des Europäischen Datenschutzrates in Bezug auf die BCR,
- indem sie alle wesentlichen Änderungen der BCR ihren jeweiligen Datenschutzbehörden mitteilen,
- durch Beantwortung von Informationsanfragen oder Beschwerden der Datenschutzbehörden
- durch Anwendung einschlägiger Empfehlungen oder Ratschläge ihrer zuständigen Datenschutzbehörden in Bezug auf die Einhaltung der BCR durch die AXA-Gesellschaften der BCR.

Die BCR AXA-Gesellschaften verpflichten sich, sich an eine formelle Entscheidung der zuständigen Datenschutzbehörde bezüglich der Auslegung und Anwendung dieser BCR zu halten, soweit dies mit dem geltenden Recht oder den geltenden Vorschriften vereinbar ist und ohne auf Einreden und/oder Rechtsmittel des für die Verarbeitung Verantwortlichen zu verzichten.

2. Verhältnis zwischen dem anwendbaren 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.

3. Antrag auf Offenlegung von Strafverfolgungsbehörden

Wenn eine BCR AXA-Gesellschaft von einer Strafverfolgungsbehörde oder einer staatlichen Sicherheitsbehörde einen rechtsverbindlichen Antrag auf Offenlegung personenbezogener Daten erhält, der sich wahrscheinlich nachteilig auf die in den BCR gebotenen Garantien auswirkt, wird die zuständige Datenschutzbehörde vom DSB oder der GDPO informiert, es sei denn, dies ist nach den geltenden örtlichen Gesetzen verboten. Die Information der Datenschutzbehörde muss Informationen über die angeforderten Daten, die ersuchende Stelle und die Rechtsgrundlage für die Offenlegung enthalten.

In Fällen, in denen die Benachrichtigung über Auskunftsersuchen nach den anwendbaren lokalen Gesetzen verboten ist, wird sich die ersuchte BCR AXA Gesellschaft nach besten Kräften bemühen, dieses Verbot aufzuheben. Wenn das Verbot trotz aller Bemühungen nicht aufgehoben werden kann, muss die ersuchte BCR AXA Gesellschaft der zuständigen Datenschutzbehörde jährlich allgemeine Informationen über die bei ihm eingegangenen Anfragen zur Verfügung stellen.

In jedem Fall muss die Weitergabe personenbezogener Daten durch eine BCR AXA Gesellschaft an eine Behörde den in Artikel IV aufgeführten Verarbeitungsgrundsätzen entsprechen und darf nicht massiv, unverhältnismäßig und unterschiedslos in einer Weise erfolgen, die über das in einer demokratischen Gesellschaft erforderliche Maß hinausgehen würde.

4. Lokale Gesetze und Geschäftspraktiken, die die Einhaltung der BCR beeinflussen

Der Datenimporteur und der Datenexporteur garantieren, dass sie keinen Grund zu der Annahme haben, dass die im Bestimmungsdrittland für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Gesetze und Praktiken, einschließlich etwaiger Anforderungen an die Offenlegung personenbezogener Daten oder Maßnahmen zur Genehmigung des Zugangs von Behörden, den Datenimporteur daran hindern, seinen Verpflichtungen aus diesen BCR nachzukommen. Dabei wird davon ausgegangen, dass Gesetze und Praktiken, die den Kern der Grundrechte und -freiheiten achten und nicht über das hinausgehen, was 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, nicht im Widerspruch zu diesen BCR stehen.

Der Datenimporteur und der Datenexporteur erklären, dass sie bei der Abgabe der Garantie gemäß Artikel X (4) insbesondere Folgendes gebührend berücksichtigt haben:

- die besonderen Umstände der jeweiligen Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der Beteiligten und der verwendeten Übermittlungskanäle; die beabsichtigten Weiterübermittlungen; die Art des Empfängers; den Zweck der Verarbeitung; die Kategorien und das Format der übermittelten personenbezogenen Daten; den Wirtschaftssektor, in dem die relevante Übermittlung stattfindet; den Speicherort der übermittelten Daten;
- die Gesetze und Gepflogenheiten des Bestimmungsdrittlandes - einschließlich derjenigen, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang solcher Behörden gestatten -, die im Lichte der besonderen Umstände der relevanten Übermittlung, sowie die geltenden Einschränkungen und Sicherheiten;
- alle relevanten vertraglichen, technischen oder organisatorischen Sicherheiten, die eingesetzt wurden, um die Sicherheiten unter diesen BCR zu ergänzen, einschließlich der Maßnahmen, die während der Übermittlung und zur Verarbeitung der personenbezogenen Daten im Bestimmungsland angewendet werden.

Der Datenimporteur sichert zu, dass er sich bei der Beurteilung nach Artikel X (4) Unterabsatz 2 seine besten Bemühungen gemacht hat, dem Datenexporteur relevanten Informationen zur Verfügung zu stellen, und stimmt zu, weiterhin mit dem Datenexporteur zusammenzuarbeiten, um die Einhaltung dieser BCR zu gewährleisten.

Der Datenimporteur und der Datenexporteur vereinbaren, die Bewertung gemäß Artikel X Absatz 4 Unterabsatz 2 zu dokumentieren und sie der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung zu stellen.

Der Datenimporteur verpflichtet sich, den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach der Zustimmung zu diesen BCR und während der Laufzeit der BCR Grund zu der Annahme hat, dass er Gesetzen oder Praktiken unterworfen ist oder unterworfen wurde, die nicht im Einklang mit den Anforderungen des Artikels X Absatz 4 stehen, einschließlich einer Änderung der Gesetze des Drittlandes oder einer Maßnahme (z. B. einer Aufforderung zur Offenlegung), die auf eine Anwendung dieser Gesetze in der Praxis hinweist, die nicht im Einklang mit den Anforderungen des Artikels X Absatz 4 steht. Wo der Datenimporteur als auch der Datenexporteur Auftragsverarbeiter sind, leitet der Datenexporteur die Meldung an den Daten-Controller weiter.

Nach einer Meldung gemäß Artikel X Absatz 4 Unterabsatz 1 oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Verpflichtungen aus diesen BCR nicht mehr nachkommen kann, identifiziert der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit) fest, die vom Datenexporteur und/oder Datenimporteur zu ergreifen sind, um der Situation zu begegnen, und wo sowohl der Datenimporteur als auch der Datenexporteur Auftragsverarbeiter sind, gegebenenfalls in Abstimmung mit dem Daten-Controller. Der Datenexporteur setzt die betreffende Übermittlung aus, wenn er der Ansicht ist, dass keine angemessenen Garantien für diese betreffende Übermittlung gewährleistet werden können, oder wenn er vom daten-Controller, wenn der Datenimporteur und der Datenexporteur beide Auftragsverarbeiter sind, oder von der zuständigen Datenschutzbehörde dazu angewiesen wird. In diesem Fall soll der Datenexporteur berechtigt sein, die betreffende Übermittlung auszusetzen, sofern sie die Verarbeitung personenbezogener Daten im Rahmen dieser BCR betrifft, und er soll it dem Datenimporteur erörtern, wie die geeigneten Garantien für die betreffende Übermittlung festgelegt und implementiert werden können.

ARTIKEL XI - DATUM DES INKRAFTTRETENS UND LAUFZEIT

Die BCR treten am 15. Januar 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 - Gerichtsbarkeit

1. **Rechtswahl**
   Diese BCR (einschließlich aller BCR-Vereinbarungen) unterliegen französischem Recht und sind gemäß diesem auszulegen.

2. **Streitigkeiten zwischen dem Datenimporteur und dem Datenexporteur**

   Alle Streitigkeiten, die zwischen dem Datenimporteur und dem Datenexporteur im Rahmen dieser BCR-Vereinbarung entstehen, werden von der zuständigen Gerichtsbarkeit des Landes des Datenexporteurs beigelegt, es sei denn, örtliche Gesetze sehen etwas anderes vor.

3. **Sonstige Streitigkeiten zwischen BCR AXA Unternehmen**

   Alle sonstigen Streitigkeiten, die zwischen den BCR AXA-Gesellschaften im Rahmen der BCR (einschließlich aller BCR-Vereinbarungen) entstehen, werden von den zuständigen Gerichten in Paris entschieden, sofern nicht eine zwingende Vorschrift des anwendbaren Rechts etwas anderes vorsieht.

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

Die GDPO sorgt für eine regelmäßige Überprüfung und Aktualisierung der BCR, beispielsweise infolge größerer Veränderungen in der Unternehmensstruktur und im aufsichtsrechtlichen Umfeld.

Alle BCR AXA-Unternehmen erkennen dies ausdrücklich an und stimmen dem zu:

- Wesentliche Änderungen dieser BCR, die die Verpflichtungen der BCR-AXA-Gesellschaften erheblich erhöhen, können in einer Entscheidung des BCR-Steuerungsausschusses der AXA nach einmonatiger (1) E-Mail-Konsultation der BCR-AXA-Gesellschaften über die der GDPO bekannten E-Mails der DSB angenommen werden; und

- Nicht wesentliche Änderungen dieser BCR, bei denen es sich um alle anderen Änderungen handelt, können in einer Entscheidung des AXA BCR-Steuerungsausschusses angenommen werden, ohne dass eine Konsultation mit einem der BCR AXA-Gesellschaften erforderlich ist.

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: Programm zur Überprüfung der Einhaltung

Anhang 3: Unternehmensvereinbarung