

Bindende Unternehmensrichtlinie zum Schutz personenbezogener Daten

(Binding Corporate Rules – »BCR«)
Zusammenfassung drittbegünstigender Rechte

© Siemens 2019

siemens.com

1 Zweck der BCR

Der Schutz personenbezogener Daten ist ein wichtiges Anliegen für Siemens. Deshalb betreibt Siemens alle Geschäftstätigkeiten im Einklang mit anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit. Die BCR sind interne Richtlinien, die von Siemens, d.h. der Siemens AG und den weiteren teilnehmenden Konzerngesellschaften, festgelegt wurden, um ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Betroffenen gemäß geltendem Datenschutzrecht, vor allem dem Datenschutzrecht der Mitgliedsstaaten des Europäischen Wirtschaftsraums (»EWR«) zu schaffen.

2 Anwendungsbereich der BCR

Die BCR gelten für die Verarbeitung von personenbezogenen Daten Betroffener durch teilnehmende Gesellschaften mit Sitz

- außerhalb des EWR, wenn die personenbezogenen Daten von einer teilnehmenden Gesellschaft mit Sitz im EWR oder mit Sitz in einem Land, für das die EU-Kommission ein angemessenes Datenschutzniveau anerkannt hat, übermittelt wurden; sowie
- im EWR oder in einem Land, für das die EU-Kommission ein angemessenes Datenschutzniveau anerkannt hat.

3 Materielle Grundsätze für die Verarbeitung personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten durch teilnehmende Gesellschaften im Rahmen dieser BCR gelten die folgenden Grundsätze, die sich insbesondere aus der Datenschutzgrundverordnung (DS-GVO) ableiten:

3.1 Zulässigkeit & Gesetzmäßigkeit der Datenverarbeitung

Die Verarbeitung der personenbezogenen Daten hat gesetzeskonform unter Einhaltung der jeweils geltenden gesetzlichen Bestimmungen sowie unter Beachtung der in diesen BCR niedergelegten Prinzipien zu erfolgen.

Sie ist nur zulässig, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; oder
- Die Datenverarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; oder
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche (im Sinne dieser BCR meint »**Verantwortlicher**«, die juristisch selbstständige Gesellschaft, die über die Zwecke und Mittel der Datenverarbeitung entscheidet; unselbstständige Zweigstellen, Niederlassungen und Betriebsstätten sind Teil des Verantwortlichen) unterliegt; oder
- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; oder
- Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
- Der Verantwortliche muss es der betroffenen Person ermöglichen, auf einfache, schnelle und effiziente Weise jederzeit seine Einwilligung widerrufen zu können.

3.2 Zweckbindung

Personenbezogene Daten dürfen ausschließlich für festgelegte, eindeutige und legitime Zwecke verarbeitet werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

3.3 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Jede teilnehmende Gesellschaft hat personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise zu verarbeiten. Betroffenen Personen, deren personenbezogene Daten von einer teilnehmenden Gesellschaft verarbeitet werden, müssen von der teilnehmenden Gesellschaft (ggf. in Absprache mit der übermittelnden Gesellschaft) gemäß den Artikeln 13 und 14 DS-GVO informiert werden, insbesondere über:

- Identität und Kontaktdaten des Verantwortlichen und der übermittelnden Gesellschaft
- Kategorien von Empfängern oder Identität der empfangenden Stelle
- Zweck der Verarbeitung
- Herkunft der Daten (sofern keine Direkterhebung der personenbezogenen Daten bei der betroffenen Person erfolgt ist)
- Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten der betroffenen Person für Zwecke der Werbung und
- andere Informationen, z.B. über Ansprüche auf Auskunft, Berichtigung und Löschung

3.4 Richtigkeit und Datenminimierung

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Die Datenverarbeitung hat sich am Grundsatz der Datenminimierung auszurichten. Das Ziel ist es nur solche personenbezogenen Daten zu verarbeiten, die dem Zweck angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter oder pseudonymisierter Daten erfolgen, sind nicht datenschutzrelevant, soweit die Daten den Rückschluss auf die betroffene Person nicht mehr ermöglichen.

3.5 Speicherbegrenzung

Personenbezogene Daten, die für die Geschäftszwecke, für die sie ursprünglich erhoben und gespeichert wurden, nicht mehr benötigt werden, sind zu löschen (dabei sind bestehende Aufbewahrungsfristen- und -pflichten zu berücksichtigen).

3.6 Weiterübermittlung von Daten

Die Übermittlung personenbezogener Daten von einer teilnehmenden Gesellschaft an eine nicht teilnehmende Gesellschaft (d.h. eine Gesellschaft, die nicht an die BCR gebunden ist) außerhalb des EWR ist nur unter Beachtung von Kapitel V der DS-GVO (Art. 45 – 49 DS-GVO) zulässig. Das bedeutet, dass die Anforderungen in Kapitel V der DS-GVO vom Verantwortlichen und Auftragsdatenverarbeiter eingehalten werden müssen. Das gilt insbesondere für die Weiterübermittlung personenbezogener Daten von einem Drittland oder von einer internationalen Organisation in einem Drittland an ein anderes Drittland oder an eine andere internationale Organisation im Drittland.

3.7 Besondere Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist grundsätzlich untersagt. Sollte die Verarbeitung besonderer Kategorien personenbezogener Daten erforderlich sein, muss die betroffene Person hierin ausdrücklich einwilligen, es sei denn,

- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben; oder
- die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist; oder
- die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat; oder
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich; oder
- die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich.

Vor der Verarbeitung besonderer Arten personenbezogener Daten ist der zuständige Data Privacy Manager (DPM) der teilnehmenden Gesellschaft zu konsultieren.

3.8 Automatisierte Entscheidungen im Einzelfall

Werden personenbezogene Daten zu dem Zweck verarbeitet, eine automatisierte Einzelentscheidung zu treffen, müssen die berechtigten Interessen der betroffenen Person durch geeignete Maßnahmen gewährleistet werden. Entscheidungen, die für die betroffenen Person negative rechtliche Folgen nach sich ziehen oder erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten, die der Bewertung einzelner Persönlichkeitsmerkmale dient, gestützt werden, d.h. nicht ausschließlich durch Verwendung von Informationstechnik getroffen werden.

3.9 Datensicherheit

Die Verantwortlichen haben zur Gewährleistung der erforderlichen Datensicherheit angemessene technische und organisatorische Maßnahmen zu treffen, die die personenbezogenen Daten gegen unbeabsichtigte oder unrechtmäßige Löschung, unrechtmäßige Verwendung, Veränderung, gegen Verlust, Zerstörung und gegen unberechtigte Weitergabe oder unberechtigten Zugriff schützen. Unter Berücksichtigung des Standes der Technik und bei der Durchführung entstehenden Kosten, sollen solche Maßnahmen ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Besondere Arten personenbezogener Daten sind besonders zu schützen.

Die vorzusehenden Sicherheitsmaßnahmen beziehen sich insbesondere auf Rechner (Server und Arbeitsplatzrechner), Netze bzw. Kommunikationsverbindungen sowie Applikationen.

Zur Sicherstellung eines angemessenen Niveaus technischer und organisatorischer Maßnahmen für den Datenschutz ist die **Siemens Informationssicherheitsrichtlinie** per Rundschreiben konzernweit verbindlich eingeführt.

Zum angemessenen Schutz personenbezogener Daten werden insbesondere Zutrittskontrollen, Zugangskontrollen, Zugriffskontrollen, Weitergabekontrollen, Eingabekontrollen, Auftragskontrollen, Verfügbarkeitskontrollen und Trennungskontrollen eingesetzt.

Alle Arbeitsplatzrechner – inklusive mobiler Geräte (z.B. Laptops) - sind durch komplexe Passwörter geschützt und haben im Regelfall eine Festplattenverschlüsselung. Das Siemens-Intranet verfügt über ein Firewallsystem zum Schutz vor unberechtigtem externem Zugriff auf unternehmensinterne Inhalte. Die Übermittlung personenbezogener Daten innerhalb des unternehmenseigenen Netzwerks erfolgt – soweit aufgrund der Natur und des Verwendungszwecks der personenbezogenen Daten erforderlich – in der Regel verschlüsselt.

3.10 Vertraulichkeit der Datenverarbeitung

Nur befugte und auf die Einhaltung des Datenschutzes besonders hingewiesene Mitarbeiter dürfen personenbezogene Daten verarbeiten. Die Zugriffsberechtigung des jeweiligen Mitarbeiters ist dabei nach Art und Umfang seines spezifischen Tätigkeitsfeldes zu begrenzen. Es ist dem Mitarbeiter untersagt, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen. Unbefugt in diesem Sinne sind z. B. auch andere Mitarbeiter, soweit diese die personenbezogenen Daten nicht zur Erledigung der ihnen obliegenden Fachaufgaben benötigen. Die Vertraulichkeitsverpflichtung besteht über das Ende des Beschäftigungsverhältnisses des betroffenen Mitarbeiters hinaus fort.

3.11 Datenverarbeitung im Auftrag

Wenn eine teilnehmende Gesellschaft eine andere Gesellschaft mit der Verarbeitung personenbezogener Daten im Rahmen dieser BCR beauftragen, sind folgende Maßgaben zu beachten:

- Der Auftragsdatenverarbeiter ist vom Verantwortlichen sorgfältig auszuwählen; es ist ein Auftragsdatenverarbeiter auszuwählen, der die für die datenschutzkonforme Verarbeitung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gewährleisten kann
- Der Verantwortliche hat dafür Sorge zu tragen und sich regelmäßig davon zu überzeugen, dass der Auftragsdatenverarbeiter die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen vollumfänglich einhält
- Die Durchführung der Datenverarbeitung im Auftrag muss in einem Vertrag geregelt werden, in dem die Rechte und Pflichten des Auftragsdatenverarbeiters eindeutig festgelegt werden; dies schließt die Pflicht zur unverzüglichen Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen ein; die Verletzung des Schutzes personenbezogener Daten ist zu dokumentieren (einschließlich der im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Umstände und Tatsachen, der Auswirkungen und der ergriffenen Abhilfemaßnahmen), die Dokumentation ist auf Verlangen der zuständigen Aufsichtsbehörde zugänglich zu machen.
- Der Auftragsdatenverarbeiter ist vertraglich zu verpflichten, die vom Verantwortlichen erhaltenen Daten nur im Rahmen des Auftrages und der vom Verantwortlichen erteilten Weisungen zu verarbeiten. Verarbeitungen zu eigenen Zwecken oder zu Zwecken Dritter müssen vertraglich ausgeschlossen werden und
- der Verantwortliche bleibt für die Zulässigkeit der Verarbeitung verantwortlich und ist weiterhin Ansprechpartner für die betroffene Person.

4 Materielle Rechte betroffener Personen

Die betroffene Person hat hinsichtlich ihrer im Geltungsbereich dieser BCR durch eine teilnehmende Gesellschaft verarbeiteten personenbezogenen Daten die nachfolgend aufgeführten, unabdingbaren Rechte.

- Die betroffene Person kann formfrei **Auskunft** über die zu ihrer Person gespeicherten Daten, deren Herkunft sowie den Zweck der Verarbeitung verlangen. Die betroffene Person kann ferner Auskunft über die Identität des Verantwortlichen sowie – im Falle einer Übermittlung personenbezogener Daten – Auskunft über die Empfänger oder Kategorien von Empfängern verlangen. Das Auskunftsrecht umfasst weiterhin den logischen Aufbau automatisierter Verarbeitungsmaßnahmen, soweit automatisierte Entscheidungen betroffen sind. Soweit nach dem jeweils geltendem Recht vorgesehen, entfällt das Auskunftsrecht der betroffenen Person, wenn damit eine erhebliche Gefährdung der Geschäftszwecke – wie insbesondere die Offenbarung von Geschäftsgeheimnissen – verbunden wäre und das Interesse an der Wahrung der Geschäftsgeheimnisse gegenüber dem Auskunftsinteresse der betroffenen Person überwiegt. Lokal geltende rechtliche Vorschriften können das Auskunftsrecht der betroffenen Person beschränken, wenn dieses innerhalb kurzer Zeit wiederholt ausgeübt wird, es sei denn, die betroffene Person kann einen legitimen Grund für die wiederholte Geltendmachung von Auskunftsansprüchen vorbringen. Die teilnehmende Gesellschaft kann von der betroffenen Person für die Auskunftserteilung eine angemessene Gebühr verlangen, soweit das jeweils anwendbare nationale Recht dies gestattet.
- Die betroffene Person kann Berichtigung ihrer personenbezogenen Daten verlangen, wenn sich herausstellt, dass diese unrichtig oder unvollständig sind.
- Die betroffene Person hat ein Recht auf Einschränkung der Verarbeitung ihrer personenbezogenen Daten, wenn sich deren Richtigkeit nicht feststellen lässt.
- Die betroffene Person hat einen Anspruch auf Löschung ihrer personenbezogenen Daten, wenn die Datenverarbeitung unzulässig war oder in der Zwischenzeit unzulässig geworden ist oder die Daten für den Verarbeitungszweck nicht mehr erforderlich sind. Berechtigte Lösungsansprüche der betroffenen Person sind innerhalb angemessener Frist umzusetzen, soweit keine gesetzlichen Aufbewahrungsfristen oder vertragliche Verpflichtungen einer Löschung entgegenstehen. Beim Bestehen gesetzlicher Aufbewahrungsfristen kann die betroffene Person statt der Löschung eine Einschränkung der Verarbeitung ihrer Daten verlangen. Gleiches gilt, wenn die Löschung der Daten unmöglich wäre.
- Die betroffene Person hat das Recht, der Verarbeitung ihrer personenbezogenen Daten zu Werbezwecken sowie zu Zwecken der Markt- und/oder Meinungsforschung zu widersprechen. Die betroffene Person ist über ihr Widerspruchsrecht zu informieren.
- Die betroffene Person hat ferner ein allgemeines Widerspruchsrecht gegen die Verarbeitung ihrer personenbezogenen Daten, wenn ein schutzwürdiges Interesse der betroffenen Person aufgrund ihrer besonderen persönlichen Situation das berechnete Interesse des Verantwortlichen an einer Verarbeitung der personenbezogenen Daten überwiegt.

Die betroffene Person kann die vorgenannten Rechte gegenüber der jeweiligen teilnehmenden Gesellschaft, dem zuständigen DPM der teilnehmenden Gesellschaft oder aber gegenüber der Globalen Data Privacy Funktion der Siemens AG schriftlich geltend machen. Das berechnete Ersuchen der betroffenen Person ist von der kontaktierten Stelle innerhalb einer angemessenen Frist zu beantworten, und zwar grundsätzlich in Schriftform (Antworten per E-Mail genügen dem Schriftformerfordernis).

5 Verbindlichkeit gegenüber betroffenen Personen

Die in diesem Dokument enthaltenden Regelungen der BCR sind – im Wege der Drittbegünstigung – auch gegenüber betroffenen Personen verbindlich.

Betroffene Personen können – nach ihrer Wahl – die Nichteinhaltung der hierin enthaltenden Regelungen der BCR durch eine teilnehmende Gesellschaft entweder gegenüber der teilnehmenden Gesellschaft oder gegenüber der Siemens AG geltend machen.

Zusätzlich sind betroffene Personen berechtigt, die Einhaltung der vorgenannten drittbegünstigenden Rechte durch eine teilnehmende Gesellschaft durch eine Beschwerde bei der zuständigen Datenschutzaufsicht oder durch die Geltendmachung eines sonstigen Rechtsbehelfs bei den zuständigen Gerichten durchzusetzen. Die betroffenen Personen können dabei Schadensersatz geltend machen.

Betroffene Personen können nach ihrer Wahl eine solche Beschwerde einreichen

- am Gerichtsstand der teilnehmenden Gesellschaft, die die Daten übermittelt hat; oder
- am Gerichtsstand am Hauptsitz der Siemens AG; oder
- bei der zuständigen Datenschutzaufsichtsbehörde und beim zuständigen Gericht der EU-Mitgliedsstaaten.

Im Falle eines Verstoßes gegen die Regelungen der BCR durch eine teilnehmende Gesellschaft mit Sitz außerhalb des EWR sind somit auch Gerichte und Behörden im EWR zuständig. Der betroffenen Person stehen gegenüber der teilnehmenden Gesellschaft, die die Haftung übernommen hat, dieselben Rechte zu, die ihr zustünden, wenn der Verstoß von einer teilnehmenden Gesellschaft mit Sitz in einem EWR-Land begangen worden wäre.

Die vorgenannte Zuständigkeit von Gerichten und Behörden im EWR besteht nicht, wenn der Datenempfänger seinen Sitz zwar in einem Land außerhalb des EWR hat, dieses Land jedoch gemäß Entscheidung der EU Kommission über ein angemessenes Datenschutzniveau verfügt.

Um durchsetzbare drittbegünstigende Rechte der betroffenen Personen auch in den Ländern sicherzustellen, in denen eine Einräumung der drittbegünstigenden Rechte im BCR-Dokument womöglich nicht ausreicht, wird die Siemens AG – soweit erforderlich – entsprechende zusätzliche vertragliche Vereinbarungen mit den betroffenen teilnehmenden Gesellschaften aufsetzen.

6 Beschwerdeverfahren

Jede betroffene Person kann sich jederzeit mit Beschwerden wegen eines Verstoßes gegen die BCR durch eine teilnehmende Gesellschaft sowie mit Fragen an die zuständige Beschwerdestelle bei der Siemens AG (Kontaktangaben finden sich in Ziffer 10) oder den zuständigen DPM der teilnehmenden Gesellschaft wenden. Der Eingang der Beschwerde bei der kontaktierten Stelle ist der betroffenen Person zeitnah zu bestätigen und die Beschwerde innerhalb angemessener Frist unverzüglich – in der Regel innerhalb von einem (1) Monat ab Eingang der Beschwerde– zu bearbeiten; in komplexen Fällen oder in Ausnahmefällen innerhalb von drei (3) Monaten ab Eingang der Beschwerde, mit der Verpflichtung, die betroffene Person entsprechend zu informieren. Im Falle von Verzögerungen, die der teilnehmenden Gesellschaft nicht zurechenbar sind, z.B. in Fällen in denen die betroffene Person erforderliche Informationen nicht rechtzeitig zur Verfügung stellt, darf dieser Zeitraum im jeweils angemessenen Umfang überschritten werden.

Die bei der zuständigen Beschwerdestelle mit der Beschwerdebearbeitung befassten Mitarbeiter verfügen über ein hinreichendes Maß an Unabhängigkeit bei der Wahrnehmung dieser Aufgabe.

Die teilnehmende Gesellschaft und die Siemens AG sind bei Anfragen verpflichtet, mit der Datenschutzaufsicht im jeweiligen Land zu kooperieren und deren Stellungnahme zu respektieren.

7 Kooperation untereinander und mit den Datenschutzaufsichtsbehörden

Siemens AG und die teilnehmenden Gesellschaften werden bei Anfragen und Beschwerden betroffener Personen im Hinblick auf die Nichteinhaltung der BCR vertrauensvoll zusammenarbeiten und einander unterstützen.

Siemens AG und die teilnehmenden Gesellschaften verpflichten sich ferner, im Zusammenhang mit der Umsetzung der BCR vertrauensvoll mit den zuständigen Datenschutzaufsichtsbehörden zusammenzuarbeiten. Sie werden auf BCR-bezogene Anfragen der Datenschutzaufsichtsbehörde innerhalb angemessener Frist und auf angemessene Weise antworten und die Ratschläge und Entscheidungen der zuständigen Datenschutzaufsichtsbehörde im Hinblick auf die Umsetzung der BCR befolgen.

Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft (Art. 36 DS-GVO).

8 Verhältnis der BCR zu lokalen gesetzlichen Regelungen

Die Zulässigkeit der Verarbeitung personenbezogener Daten beurteilt sich anhand des jeweils anwendbaren lokalen Rechts. Soweit das anwendbare lokale Recht einen größeren Schutz personenbezogener Daten vorschreibt als diese BCR, richtet sich die Datenverarbeitung nach dem anwendbaren Recht. Jede teilnehmende Gesellschaft muss selbst prüfen (z. B. durch ihren DPM oder durch die Rechtsabteilung), ob es solche lokalen gesetzlichen Regelungen (z. B. Datenschutzgesetze) gibt und deren Einhaltung sicherstellen. Sofern das anwendbare lokale Recht jeweils einen geringeren Schutz für personenbezogene Daten vorsieht als diese BCR, finden die vorliegenden BCR Anwendung.

Falls sich aus dem anwendbaren lokalen Recht Verpflichtungen ergeben, die im Widerspruch zu den BCR stehen, hat die teilnehmende Gesellschaft unverzüglich die Globale Data Privacy Funktion der Siemens AG zu informieren. Die Globale Data Privacy Funktion der Siemens AG wird den gemeldeten Konflikt dokumentieren.

Die Globale Data Privacy Funktion der Siemens AG wird alle teilnehmenden Gesellschaften, die zuvor Daten an die betreffende teilnehmende Gesellschaft übermittelt haben, über den gemeldeten Widerspruch der BCR mit dem lokalen Recht informieren und ferner die zuständige Datenschutzaufsicht über den Regelkonflikt informieren und gemeinsam mit der Datenschutzaufsicht und der teilnehmenden Gesellschaft nach einer praktikablen Lösung suchen, die den Grundsätzen der DS-GVO möglichst nahekommt.

9 Haftung

Die Siemens AG übernimmt die Haftung für die Nichteinhaltung der BCR durch teilnehmende Gesellschaften mit Sitz außerhalb des EWR. Die Siemens AG verpflichtet sich, die Einhaltung der BCR durch die teilnehmenden Gesellschaften mit Sitz außerhalb des EWR zu überwachen und dafür Sorge zu tragen, dass die teilnehmenden Gesellschaften mit Sitz außerhalb des EWR die erforderlichen Abhilfemaßnahmen ergreifen, um Verstöße gegen die BCR zu beseitigen.

Die Siemens AG verpflichtet sich ferner, im Falle eines nachgewiesenen Verstoßes gegen die BCR und einer hieraus resultierenden Rechtsverletzung einer betroffenen Person Schadensersatz zu leisten.

Die Beweislast trägt die Siemens AG. Die Siemens AG muss nachweisen, dass kein Verstoß gegen die BCR vorliegt oder dass der Verstoß gegen die BCR, mit dem der betroffenen Person ihre Schadensersatzforderung begründet, der teilnehmenden Gesellschaft mit Sitz außerhalb des EWR nicht zuzurechnen ist.

10 Kontakt

Betroffene Personen können sich mit ihren Anliegen an den DPM der betreffenden teilnehmenden Gesellschaft oder an die Globale Data Privacy Funktion der Siemens AG wenden:

Siemens AG
LC CO DP
Otto-Hahn-Ring 6
81739 München

E-Mail: datenschutz@siemens.com

Internet: <http://www.siemens.com/datenschutz>