SIEMENS

Bindende Unternehmensrichtlinie (Binding Corporate Rules) Zusammenfassung drittbegünstigender Rechte

Dieses Dokument enthält in Ziffer 3 – 9 alle Regelungen der „Binding Corporate Rules („BCR“) für Siemens – Konzerngesellschaften und beitretende Gesellschaften zum Schutz personenbezogener Daten“, die gegenüber betroffenen Personen („**Betroffene**“) drittbegünstigende Wirkung entfalten.

1. Zweck der BCR

Der Schutz personenbezogener Daten ist ein wichtiges Anliegen für Siemens. Deshalb betreibt Siemens alle Aktivitäten in Übereinstimmung mit anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit. Die BCR sind interne Richtlinien, die von Siemens, d.h. der Siemens AG und 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 EU-Datenschutzrichtlinie 95/46/EG und der Madrid-Resolution vom 5.November 2009 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:

- Der Betroffene hat freiwillig und eindeutig eine wirksame Einwilligung erteilt; oder
- Die Datenverarbeitung dient der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen; oder
- Die Verarbeitung ist zur Wahrung berechtigter Interessen der verantwortlichen Stelle (im Sinne dieser BCR ist „**verantwortliche Stelle**“, die juristisch selbstständige Gesellschaft, die über die Zwecke und Mittel der Datenverarbeitung entscheidet; unselbstständige Zweigstellen, Niederlassungen und Betriebsstätten sind Teil der verantwortlichen Stelle) erforderlich und es besteht kein Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt; oder
- Die Verarbeitung wird durch für die verantwortliche Stelle geltende nationale Rechtsvorschriften angeordnet oder erlaubt; oder
- Die Verarbeitung ist für die Einhaltung rechtlicher Verpflichtungen, denen die verantwortliche Stelle unterliegt, erforderlich; oder

- Die Verarbeitung ist ausnahmsweise nötig, um das Leben, die Gesundheit oder die Sicherheit des Betroffenen zu schützen.

Die verantwortliche Stelle muss es dem Betroffenen ermöglichen, auf einfache, schnelle und effiziente Weise jederzeit seine Einwilligung widerrufen zu können.

3.2 Zweckbestimmung

Personenbezogene Daten dürfen ausschließlich für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden. In keinem Fall dürfen personenbezogene Daten auf eine Weise verarbeitet werden, die mit den legitimen Zwecken, für die die personenbezogenen Daten erhoben wurden, nicht vereinbar ist. Teilnehmende Gesellschaften sind verpflichtet, die ursprüngliche Zweckbestimmung der von einer anderen teilnehmenden Gesellschaft an sie übermittelten Daten bei der Speicherung und weiteren Verarbeitung und Nutzung dieser Daten zu beachten; Zweckänderungen sind nur mit Einwilligung des Betroffenen zulässig oder soweit das jeweilige nationale Recht der übermittelnden teilnehmenden Gesellschaft dies zulässt.

3.3 Transparenz

Jede teilnehmende Gesellschaft hat personenbezogene Daten auf transparente Art und Weise zu verarbeiten. Betroffene, deren personenbezogene Daten von einer teilnehmenden Gesellschaft verarbeitet werden, müssen von der teilnehmenden Gesellschaft (ggf. in Absprache mit der übermittelnden Gesellschaft) über Folgendes informiert werden:

- Identität der verantwortlichen Stelle und der übermittelnden Gesellschaft;
- Kategorien von Empfängern oder Identität der empfangenden Stelle;
- Zweck der Verarbeitung;
- Herkunft der Daten (sofern keine Direkterhebung der personenbezogenen Daten beim Betroffenen erfolgt ist);
- Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten des Betroffenen für Zwecke der Werbung; und
- andere Informationen, sofern dies aus Billigkeitsgründen erforderlich ist, z.B.
- über Ansprüche auf Auskunft, Berichtigung und Löschung.

Soweit die personenbezogenen Daten nicht direkt beim Betroffenen erhoben wurden, kann die Information ausnahmsweise unterbleiben, wenn dies zum Schutz des Betroffenen oder der Rechte anderer Personen notwendig ist, der Betroffene bereits informiert wurde oder damit ein unverhältnismäßiger Aufwand verbunden wäre.

3.4 Datenqualität und Datensparsamkeit

Personenbezogene Daten müssen sachlich richtig sein und – wenn nötig – auf den neuesten Stand gebracht werden. Es sind angemessene Maßnahmen dafür zu treffen, dass nicht zutreffende oder unvollständige Daten berichtigt oder gelöscht werden.

Die Datenverarbeitung hat sich am Grundsatz der Datensparsamkeit auszurichten. Das Ziel ist es nur die erforderlichen personenbezogenen Daten – d. h. so wenig personenbezogene Daten wie möglich – zu erheben, zu verarbeiten oder zu nutzen. 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 den Betroffenen nicht mehr ermöglichen.

Personenbezogene Daten, die für die Geschäftszwecke, für die sie ursprünglich erhoben und gespeichert wurden, nicht mehr benötigt werden, sind zu löschen. Im Falle gesetzlicher Aufbewahrungsfristen sind die Daten anstelle der Löschung zu sperren.

3.5 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 folgenden Voraussetzungen zulässig:

- Die empfangende Stelle verfügt über einen im Sinne des Art. 25 der EU-Datenschutzrichtlinie 95/46/EG angemessenen Schutz für die personenbezogenen Daten, z.B. durch Abschluss eines EU- Standardvertrages (Standardvertragsklauseln für Auftragsverarbeiter 2010/87/EU bzw. Standardvertragsklauseln zwischen für die Datenverarbeitung Verantwortlichen 2001/497/EG oder 2004/915/EG) oder durch Abschluss anderer geeigneter vertraglicher Vereinbarungen zwischen der übermittelnden und der empfangenden Stelle; oder
- Die Übermittlung ist nach einer der in Art. 26 der EU-Datenschutzrichtlinie 95/46/EG angeführten Ausnahmen zulässig;
- Soweit die empfangende Stelle Auftragsdatenverarbeiter ist, müssen zusätzlich die Voraussetzungen der Art. 16 und 17 der EU-Datenschutzrichtlinie 95/46/EG erfüllt werden.

3.6 Besondere Arten personenbezogener Daten

Die Verarbeitung besonderer Arten personenbezogener Daten, also von Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, ist grundsätzlich untersagt.

Sollte die Verarbeitung besonderer Arten personenbezogener Daten erforderlich sein, muss der Betroffene hierin ausdrücklich einwilligen, es sei denn,

- der Betroffene ist nicht in der Lage, seine Einwilligung zu geben (z. B. medizinischer Notfall) und die Verarbeitung ist zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen Person erforderlich; oder
- die Verarbeitung ist erforderlich im Zusammenhang mit medizinischer Diagnostik, Gesundheitsvorsorge oder der Behandlung oder der Verwaltung von Gesundheitsdiensten; wobei die Datenverarbeitung durch medizinisches Personal erfolgt, das dem Berufsgeheimnis unterworfen ist oder durch sonstiges, einer entsprechenden Geheimhaltungspflicht unterworfenes Personal; oder
- der Betroffene hat die jeweiligen Daten bereits selbst öffentlich gemacht; oder
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich, wenn kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung überwiegen; oder
- die Verarbeitung ist nach dem anwendbaren nationalen Recht ausdrücklich gesetzlich erlaubt (z. B. zum Zweck der Erfassung bzw. des Schutzes von Minderheiten) und bei der Verarbeitung der Daten werden zusätzliche Garantien im Sinne der EU-Datenschutzrichtlinie 95/46/EG, wie insbesondere angemessene Sicherheitsmaßnahmen für diese Daten, ergriffen.

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

3.7 Automatisierte Einzelentscheidungen

Werden personenbezogene Daten zu dem Zweck verarbeitet, eine automatisierte Einzelentscheidung zu treffen, müssen die berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet werden. Entscheidungen, die für den Betroffenen negative rechtliche Folgen nach sich ziehen oder ihn 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. Eine Ausnahme gilt nur, wenn die Entscheidung

- im Rahmen des Abschlusses oder der Erfüllung eines Vertrags ergeht und dem Ersuchen des Betroffenen auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung seines berechtigten Interessen durch geeignete Maßnahmen – beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen – garantiert wird; oder

- durch eine Rechtsvorschrift zugelassen ist, die Garantien zur Wahrung der berechtigten Interessen des Betroffenen festlegt.

3.8 Datensicherheit

Die verantwortlichen Stellen 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 hat Siemens das konzerninterne Regelwerk zur Informationssicherheit 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 passwortgeschützt. 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.

3.9 Vertraulichkeit der Datenverarbeitung

Nur befugte und auf die Einhaltung des Datenschutzes besonders hingewiesene Mitarbeiter dürfen personenbezogene Daten erheben, verarbeiten oder nutzen. 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.

3.10 Datenverarbeitung im Auftrag

Wenn eine teilnehmende Gesellschaft eine andere Gesellschaft („**Auftragsdatenverarbeiter**“) mit der Verarbeitung personenbezogener Daten im Rahmen dieser BCR beauftragt, sind folgende Maßgaben zu beachten:

- Der Auftragsdatenverarbeiter ist von der verantwortlichen Stelle sorgfältig auszuwählen; es ist ein Auftragsdatenverarbeiter auszuwählen, der die für die datenschutzkonforme Verarbeitung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gewährleisten kann;
- Die verantwortliche Stelle 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 schriftlich oder anderweitig dokumentierten Vertrag geregelt werden, in dem die Rechte und Pflichten des Auftragsdatenverarbeiters eindeutig festgelegt werden;
- Der Auftragsdatenverarbeiter ist vertraglich zu verpflichten, die von der verantwortlichen Stelle erhaltenen Daten nur im Rahmen des Auftrages und der von der verantwortlichen Stelle erteilten Weisungen zu verarbeiten; Verarbeitungen zu eigenen Zwecken oder zu Zwecken Dritter müssen vertraglich ausgeschlossen werden; und

- Die verantwortliche Stelle bleibt für die Zulässigkeit der Verarbeitung verantwortlich und ist weiterhin Ansprechpartner für den Betroffenen.

4. Materielle Rechte des Betroffenen

Der Betroffene hat hinsichtlich seiner im Geltungsbereich dieser BCR durch eine teilnehmende Gesellschaft verarbeiteten personenbezogenen Daten die nachfolgend aufgeführten, unabdingbaren Rechte.

- Der Betroffene kann formfrei **Auskunft** über die zu seiner Person gespeicherten Daten, deren Herkunft sowie den Zweck der Verarbeitung verlangen. Der Betroffene kann ferner Auskunft über die Identität der verantwortlichen Stelle 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 des Betroffenen, 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 des Betroffenen überwiegt. Lokal geltende rechtliche Vorschriften können das Auskunftsrecht des Betroffenen beschränken, wenn dieses innerhalb kurzer Zeit wiederholt ausgeübt wird, es sei denn, der Betroffene kann eine legitimen Grund für die wiederholte Geltendmachung von Auskunftsansprüchen vorbringen. Die teilnehmende Gesellschaft kann vom Betroffenen für die Auskunftserteilung eine angemessene Gebühr verlangen, soweit das jeweils anwendbare nationale Recht dies gestattet.
- Der Betroffene kann **Berichtigung** seiner personenbezogenen Daten verlangen, wenn sich herausstellt, dass diese unrichtig oder unvollständig sind.
- Der Betroffene hat ein Recht auf **Sperrung** seiner personenbezogenen Daten, wenn sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen lässt.
- Der Betroffene hat einen Anspruch auf **Löschung** seiner 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 Löschungsansprüche des Betroffenen sind innerhalb angemessener Frist umzusetzen, soweit keine gesetzlichen Aufbewahrungsfristen oder vertragliche Verpflichtungen einer Löschung entgegenstehen. Beim Bestehen gesetzlicher Aufbewahrungsfristen kann der Betroffene statt der Löschung eine Sperrung seiner Daten verlangen. Gleiches gilt, wenn die Löschung der Daten unmöglich wäre.
- Der Betroffene hat das Recht, der Verarbeitung seiner personenbezogenen Daten zu Werbezwecken sowie zu Zwecken der Markt- und/oder Meinungsforschung zu **widersprechen**. Der Betroffene ist über sein Widerspruchsrecht zu informieren.
- Der Betroffene hat ferner ein **allgemeines Widerspruchsrecht** gegen die Verarbeitung seiner personenbezogenen Daten, wenn ein schutzwürdiges Interesse des Betroffenen aufgrund seiner besonderen persönlichen Situation das berechtigte Interesse der verantwortlichen Stelle an einer Verarbeitung der personenbezogenen Daten überwiegt.

Der Betroffene kann die vorgenannten Rechte gegenüber der jeweiligen teilnehmenden Gesellschaft, dem zuständigen Data Privacy Officer (DPO) einer solchen teilnehmenden Gesellschaft oder aber gegenüber der Globalen Data Privacy Funktion (LC CO DP) schriftlich geltend machen. Das berechtigte Ersuchen des Betroffenen 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

Die in Ziffer 3 – 9 dieses Dokuments enthaltenden Regelungen der BCR sind – im Wege der Drittbegünstigung – auch gegenüber Betroffenen verbindlich.

Betroffene 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 (LC CO DP) geltend machen.

Zusätzlich sind die Betroffenen 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 können dabei Schadensersatz geltend machen.

Die Betroffenen 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.

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. Dem Betroffenen stehen gegenüber der teilnehmenden Gesellschaft, die die Haftung übernommen hat, dieselben Rechte zu, die ihm 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 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. Eine Verpflichtung auf die drittbegünstigenden Rechte, die sicherstellt, dass die Betroffenen die jeweils erforderlichen Rechte geltend machen können, ist in der Verpflichtungserklärung enthalten, die die Konzerngesellschaften als Zeichen ihrer Akzeptanz und Umsetzung der BCR unterschreiben. Gleiches gilt für den Beitrittsvertrag, den die beitretenden Gesellschaften mit der Siemens AG abschließen.

6. Beschwerdeverfahren

Jeder Betroffene 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 (LC CO DP; Kontaktangaben vgl. Ziffer 10) oder den lokalen Ansprechpartner für Datenschutzfragen (regelmäßig der Data Privacy Officer (DPO)) der teilnehmenden Gesellschaft wenden. Der Eingang der Beschwerde bei der kontaktierten Stelle ist dem Betroffenen zeitnah zu bestätigen und die Beschwerde innerhalb angemessener Frist – in der Regel innerhalb von drei (3) Monaten ab Eingang der Beschwerde – zu bearbeiten. Im Falle von Verzögerungen, die der teilnehmenden Gesellschaft nicht zurechenbar sind, z.B. in Fällen in denen der Betroffene 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 LC CO DP 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 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.

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 Data Privacy Officer (DPO) 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 LC C DP zu informieren. LC C DP wird den gemeldeten Konflikt dokumentieren.

LC C DP 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. LC C DP wird 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 EU-Datenschutzrichtlinie 95/46/EG 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 eines Betroffenen 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 Betroffene seine Schadensersatzforderung begründet, der teilnehmenden Gesellschaft mit Sitz außerhalb des EWR nicht zuzurechnen ist.

10. Kontakt

Betroffene können sich mit ihren Anliegen an den Data Privacy Officer (DPO) der betreffenden teilnehmenden Gesellschaft oder an die globale Data Privacy Funktion der Siemens AG wenden:

Siemens AG

LC CO DP

St.-Martin-Str. 76

D-81541 München

E-Mail: datenschutz@siemens.com

Internet: http://www.siemens.com