

SIEMENS

Unternehmensrichtlinie
für Konzerngesellschaften (in “Drittländern“^{*)}
zum Schutz personenbezogener Daten

^{*)} *Drittländer im Sinn dieser Unternehmensrichtlinie sind alle Staaten, die nicht zu den Staaten gehören, die über ein angemessenes Datenschutzniveau im Sinne von Artikel 25 der EU-Richtlinie Nr. 95/46/EG vom 24.10.1995 (Amtsblatt Nr. L281/31) verfügen.
Diese Staaten mit einem angemessenen Datenschutzniveau umfassen die Mitgliedsstaaten der Europäischen Union (EU), die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) und die durch Feststellung der EU-Kommission anerkannten Staaten;*

Inhaltsverzeichnis

	Seite
1. Ziel und Anwendungsbereich	3
1.1 Verbindlichkeit	3
1.2 Verhältnis zu gesetzlichen Regelungen	3
2. Begriffsbestimmungen	4
3. Grundsätze für die Verarbeitung personenbezogener Daten	5
3.1 Zulässigkeit der Datenverarbeitung	5
3.2 Zweckbestimmung	5
3.3 Transparenz	5
3.4 Datenqualität	6
3.5 Übermittlung von Daten innerhalb des Drittlandes oder in ein anderes Drittland	6
3.6 Besondere Arten personenbezogener Daten	6
3.7 Direktmarketing/Markt- oder Meinungsforschung	7
3.8 Automatisierte Einzelentscheidungen	7
3.9 Datensicherheit	7
3.10 Vertraulichkeit der Datenverarbeitung	7
3.11 Datenverarbeitung im Auftrag	8
4. Rechte des Betroffenen	8
5. Verfahrensfragen	9
5.1 Umsetzung im Unternehmen	9
5.2 Fragen und Beschwerden	9
6. Publizität	9
7. Überwachung der Einhaltung	9

Ziffer 1.1 mitzuteilen sowie die Konzerngesellschaften in EU/EWR-Staaten (s. Fußnote auf Seite 1) zu unterrichten, die bis dahin Daten an sie übermittelt haben, auch wenn diese gesetzlichen Verpflichtungen sich nachträglich ergeben. ZV CPO wird in einem solchen Fall gemeinsam mit der betreffenden Konzerngesellschaft nach einer praktikablen Lösung im Sinne der EU-Datenschutz-Richtlinie suchen und diese im Register gemäß Ziffer 1.1 Abs. 2 dokumentieren.

Die Verantwortung für die grundsätzliche Umsetzung dieser Richtlinie liegt bei der Leitung der einzelnen Konzerngesellschaft im Drittland, die Ausführung im Einzelfall liegt jeweils bei der Stelle innerhalb dieser Konzerngesellschaft, die personenbezogene Daten im Rahmen ihrer Fachaufgabe verarbeitet.

2. Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

- **Auftragnehmer** die natürliche oder juristische Person, die personenbezogene Daten im Auftrag für eine verantwortliche Stelle verarbeitet;
- **Betroffener** jede bestimmte oder bestimmbare natürliche Person, deren Daten verarbeitet werden. Bestimmbar ist eine Person dann, wenn sie direkt oder indirekt identifiziert werden kann, z. B. durch Zuordnung zu einer Kennziffer;
- **Dritter** jede natürliche oder juristische Person, die nicht der verantwortlichen Stelle zuzurechnen ist;
- **Drittland** jeden Staat im Sinne der Fußnote auf Seite 1;
- **Einwilligung** eine ohne Zwang und in Kenntnis der Sachlage erfolgte Willensäußerung, mit der der Betroffene akzeptiert, dass seine personenbezogenen Daten verarbeitet werden*);
- **Konzerngesellschaft** die Siemens Aktiengesellschaft und jede Gesellschaft, bei der der Siemens Aktiengesellschaft direkt oder indirekt die Mehrheit der Stimmrechte zusteht („Verbundene Unternehmen“); diese Unternehmen sind in der jeweils aktuellen Liste der Konzerngesellschaften, derzeit unter <http://www.cf.siemens.de/cft/cft5/> „Aktuell“, „Gesellschaftsübersichten“, mit Nummern 4000 ff. und 5000 ff. sowie Gesellschaftskennzeichen A bis D gekennzeichnet;
- **Kunden und Lieferanten** die natürlichen und juristischen Personen, mit denen eine Geschäftsbeziehung besteht oder geplant ist;
- **Personenbezogene Daten** alle Informationen über einen Betroffenen;

**) Besondere Anforderungen an eine Einwilligung können sich aus dem jeweiligen nationalen Recht ergeben und für die Wirksamkeit der Einwilligung bedeutsam sein.*

- **Übermittlung personenbezogener Daten** oder **Datenübermittlung** die Weitergabe personenbezogener Daten, ihre Verbreitung oder jede Form der Bereitstellung zur Ansicht oder zum Abruf an Dritte;
- **Verantwortliche Stelle** im Verhältnis zu Dritten die juristisch selbstständige Siemens-Konzerngesellschaft, deren Geschäftstätigkeit die Datenverarbeitung veranlasst hat. Unselbstständige Zweigstellen, Niederlassungen und Betriebsstätten sind Teil der Verantwortlichen Stelle;
- **Verarbeitung personenbezogener Daten** oder **Datenverarbeitung** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten - wie etwa das Erheben, Speichern, die Aufbewahrung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung sowie das Sperren, Löschen oder Vernichten.

3. Grundsätze für die Verarbeitung personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten durch Konzerngesellschaften in einem Drittland gelten die folgenden Grundsätze, die von diesen Konzerngesellschaften zu beachten sind.

3.1 Zulässigkeit der Datenverarbeitung

Die Verarbeitung der in Ziffer 1 Abs. 2 genannten personenbezogenen Daten ist nur zulässig, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Betroffene hat eine wirksame Einwilligung erteilt.
- Die Verarbeitung dient der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen.
- Die Verarbeitung ist zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich und es besteht kein Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt.
- Die Verarbeitung wird durch nationale Rechtsvorschriften angeordnet oder erlaubt.

Diese Richtlinie ist in jedem Fall zu beachten.

3.2 Zweckbestimmung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden. Konzerngesellschaften in Drittländern, die sich zur Einhaltung dieser Richtlinie verpflichtet haben, sind verpflichtet, die Zweckbestimmung der von einer Konzerngesellschaft aus einem EU/ EWR-Staat (s. Fußnote auf Seite 1) 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 wenn das jeweilige nationale Recht des Datenexporteurs aus dem EU/ EWR-Staat dies zulässt.

3.3 Transparenz

Betroffene, deren personenbezogene Daten von einer Konzerngesellschaft aus einem EU/ EWR-Staat (s. Fußnote auf Seite 1) übermittelt werden, müssen von der empfangenden Kon-

zerngesellschaft im Drittland (ggf. in Absprache mit dem Datenexporteur) die folgenden Informationen erhalten:

- Identität der verantwortlichen Stelle im Drittland und des Datenexporteurs im EU/EWR-Staat
- Zweckbestimmung der Übermittlung
- andere Informationen, sofern dies aus Billigkeitsgründen erforderlich ist, z.B.
 - Auskunfts-, Berichtigungs- und Löschungsrechte
 - Widerspruchsrecht bei Werbung.

Diese Informationen können unterbleiben, wenn

- dies zum Schutz des Betroffenen oder der Rechte und Pflichten anderer Personen notwendig ist oder
- der Betroffene bereits informiert ist oder
- damit ein unverhältnismäßiger Aufwand verbunden ist oder
- die Daten öffentlich zugänglich sind und eine Information wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

3.4 Datenqualität

Personenbezogene Daten müssen sachlich richtig und – wenn nötig – auf dem neuesten Stand sein. Es sind angemessene Maßnahmen dafür zu treffen, dass nicht zutreffende oder unvollständige Daten berichtigt oder gelöscht werden. Die Datenverarbeitung hat sich an dem Ziel auszurichten, 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 unter Beachtung gesetzlich vorgeschriebener Aufbewahrungspflichten zu löschen.

3.5 Übermittlung von Daten innerhalb des Drittlandes oder in ein anderes Drittland

Die Übermittlung der von einer Konzerngesellschaft aus einem EU/ EWR-Staat (s. Fußnote auf Seite 1) erhaltenen personenbezogenen Daten an eine andere Stelle innerhalb des Drittlandes oder in ein anderes Drittland ist nur zulässig, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Betroffene hat eine wirksame Einwilligung erteilt.
- Die Übermittlung dient der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen.
- Die empfangende Stelle weist ein im Sinne dieser Richtlinie angemessenes Datenschutzniveau auf; sofern es sich um eine Konzerngesellschaft handelt, die sich zur Einhaltung dieser Richtlinie verpflichtet hat, muss das Vorliegen eines angemessenen Datenschutzniveaus nicht geprüft werden.

3.6 Besondere Arten personenbezogener Daten

Die Verarbeitung besonderer Arten personenbezogener Daten, z. B. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, ist grundsätzlich untersagt. Sollte dies erforderlich sein, muss der Betroffene ausdrücklich einwilligen, es sei denn,

- der Betroffene ist nicht in der Lage, seine Einwilligung zu geben (z. B. medizinischer Notfall) oder
- der Betroffene hat die betreffenden Daten öffentlich gemacht oder
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich, wenn kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung überwiegen oder
- die Verarbeitung ist nach dem nationalen Recht gesetzlich geboten (z. B. Erfassung/ Schutz von Minderheiten).

Dies gilt auch, wenn die personenbezogenen Daten im Drittland erhoben werden.

3.7 Direktmarketing/Markt- oder Meinungsforschung

Die Verarbeitung personenbezogener Daten zum Zwecke des Direktmarketings/der Markt- oder Meinungsforschung ist grundsätzlich zulässig, sofern dies mit dem Zweck der ursprünglichen Datenerhebung zu vereinbaren ist und das nationale Recht keine strengeren Regelungen aufstellt (z.B. eine Einwilligung fordert). Jedoch hat der Betroffene das Recht, dieser Verwendung seiner Daten jederzeit zu widersprechen^{*)}. In diesem Fall sind die Daten für diesen Zweck zu sperren.

3.8 Automatisierte Einzelentscheidungen

Werden personenbezogene Daten mit dem Ziel 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 Einzelentscheidung, die der Bewertung einzelner Persönlichkeitsmerkmale (z. B. Kreditwürdigkeit) dient, gestützt, d.h. nicht ausschließlich durch Verwendung von Informationstechnik getroffen werden. Automatisierte Verfahren dürfen grundsätzlich nur als Hilfsmittel für eine solche Entscheidung genutzt werden. Eine Ausnahme gilt nur, wenn die Interessen des Betroffenen durch Informationen über die Logik der Entscheidung und die Möglichkeit zur Stellungnahme gewahrt werden. Für den Fall einer Stellungnahme des Betroffenen ist die verantwortliche Stelle verpflichtet, ihre Entscheidung zu überprüfen.

3.9 Datensicherheit

Die verantwortlichen Stellen haben die zur Gewährleistung der erforderlichen Datensicherheit angemessenen technisch-organisatorischen Maßnahmen zu treffen, die die personenbezogenen Daten gegen unbeabsichtigte oder unrechtmäßige Löschung, Veränderung oder gegen Verlust und gegen unberechtigte Weitergabe oder unberechtigten Zugriff schützen. Die Maßnahmen beziehen sich insbesondere auf Rechner (Server und Arbeitsplatzrechner), Netze bzw. Kommunikationsverbindungen sowie Applikationen und ergeben sich aus der Umsetzung des auch für die Konzerngesellschaften in Drittländern verbindlichen siemens-internen

^{*)} Soweit nationales Recht es vorsieht, ist der Betroffene über sein Widerspruchsrecht und die verantwortliche Stelle zu informieren.

„Regelwerks zur Informationssicherheit“ in der jeweils geltenden Fassung (derzeit im Intranet verfügbar unter <https://cio.siemens.de/de/v4/topics/isec/guide/index.cfm>), das nicht nur die Verarbeitung von Daten über natürliche Personen abdeckt, sondern die gesamte Informationsverarbeitung.

3.10 Vertraulichkeit der Datenverarbeitung

Nur befugte und auf die Einhaltung des Datenschutzes besonders hingewiesene Mitarbeiter dürfen personenbezogene Daten erheben, verarbeiten oder nutzen. Es ist untersagt, solche personenbezogenen Daten für eigene private Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen. Unbefugt in diesem Sinne sind z. B. auch Mitarbeiter, sofern sie die Daten nicht zur Erledigung der ihnen obliegenden Fachaufgaben benötigen.

3.11 Datenverarbeitung im Auftrag

Wenn Konzerngesellschaften im Drittland einen Dritten mit der Verarbeitung personenbezogener Daten beauftragen, gilt zusätzlich folgendes:

- Es ist ein Auftragnehmer auszuwählen, der die für die datenschutzgerechte Verarbeitung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gewährleistet.
- Die Durchführung der Datenverarbeitung im Auftrag muss in einem schriftlich oder anderweitig dokumentierten Vertrag geregelt werden, in dem die Rechte und Pflichten des Auftragnehmers festgelegt werden.
- Der Auftragnehmer ist vertraglich zu verpflichten, die vom Auftraggeber erhaltenen Daten nur im Rahmen des Auftrages und der vom Auftraggeber erteilten Weisungen zu verarbeiten. Verarbeitungen zu eigenen Zwecken oder zu Zwecken Dritter müssen vertraglich ausgeschlossen werden.
- Der Auftraggeber bleibt verantwortlich für die Zulässigkeit der Verarbeitung und ist Ansprechpartner für den Betroffenen (Kunde, Mitarbeiter etc).

4. Rechte des Betroffenen

Der Betroffene hat hinsichtlich seiner personenbezogenen Daten bestimmte unabdingbare Rechte:

- Er kann **Auskunft** (auch schriftlich) über die zu seiner Person gespeicherten Daten verlangen, ebenso über ihre Herkunft und zu welchem Zweck sie gespeichert sind. Bei Übermittlung hat er ein Recht auf Auskunft auch über die Empfänger bzw. die Kategorien von Empfängern.
Ein Recht auf Auskunft besteht nicht, wenn damit die Offenbarung von Geschäftsgeheimnissen verbunden ist.
- Er hat ein Recht auf **Berichtigung**, wenn sich herausstellt, dass seine personenbezogenen Daten unrichtig oder unvollständig sind.
- Er hat ein Recht auf **Sperrung** seiner Daten, wenn sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen lässt.

- Er hat ein Recht auf **Löschung** seiner Daten, wenn die Datenverarbeitung unzulässig war oder die Daten für den Zweck der Datenverarbeitung nicht mehr erforderlich sind. Bestehen gesetzliche Aufbewahrungspflichten, tritt an die Stelle der Löschung die Sperrung der Daten.
- Er hat ein Recht auf **Widerspruch**, wenn seine Daten
 - zu Werbezwecken oder
 - zu Zwecken der Markt- oder Meinungsforschung genutzt werden.
- Darüber hinaus hat er ein **allgemeines Widerspruchsrecht**, das zu berücksichtigen ist, wenn eine Prüfung ergibt, dass ein schutzwürdiges Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle überwiegt.

Der Betroffene kann diese Rechte außergerichtlich kostenfrei und auch gegenüber der übermittelnden Konzerngesellschaft in einem EU/EWR-Staat wahrnehmen.

5. Verfahrensfragen

5.1 Umsetzung im Unternehmen

Die jeweilige Leitung der Konzerngesellschaft im Drittland hat die Umsetzung dieser Richtlinie sicherzustellen, wozu vor allem die entsprechende Unterrichtung der Mitarbeiter gehört. Zu der Unterrichtung zählt auch der Hinweis, dass Verstöße gegen diese Richtlinie strafrechtliche, haftungsrechtliche oder arbeitsrechtliche Konsequenzen nach sich ziehen können. Bei Schulungsbedarf nutzt sie die im Siemens-Intranet weltweit verfügbare Homepage „Datenschutz bei Siemens“ (s. <http://dsb.siemens.de/dspages/>) oder wendet sich an das Referat ZV CPO.

5.2 Fragen und Beschwerden

Die Betroffenen können sich mit Fragen und Beschwerden jederzeit an das Referat ZV CPO bzw. an die gemäß Ziffer 7 örtlich zuständige Person und/oder, soweit vorhanden, an die zuständige Aufsichtsbehörde wenden. Die Konzerngesellschaft im Drittland und ZV CPO sind verpflichtet, bei allen Anfragen der Datenschutz-Aufsichtsbehörde des Staates, in dem die übermittelnde Konzerngesellschaft ihren Sitz hat, mit dieser zu kooperieren und ihre Stellungnahme zu respektieren. Auch die übermittelnde Konzerngesellschaft in einem EU/EWR-Staat (s. Fußnote auf Seite 1) hat das Recht, bei der empfangenden Konzerngesellschaft im Drittland die Datenverarbeitung im Einzelfall zu überprüfen. Sie wird festgestellte Rechte von Betroffenen durchsetzen und Betroffene, die durch die Verletzung der sich aus dieser Richtlinie ergebenden Verpflichtungen einen Schaden erlitten haben, bei der Durchsetzung ihrer Rechte gegenüber der verantwortlichen Konzerngesellschaft im Drittland unterstützen.

6. Publizität

Diese Richtlinie wird den Betroffenen in geeigneter Weise, z. B. über das Internet, zugänglich gemacht.

7. Überwachung der Einhaltung

Neben den Revisionsstellen der Siemens AG und der Konzerngesellschaft im Drittland überwacht die in der Konzerngesellschaft im Drittland für Datenschutz jeweils zuständige Person als Datenschutz-Koordinator die Einhaltung dieser Richtlinie. Dies ist der gemäß CIO-Rundschreiben Nr. 12/2002 vom 08.10.2002 jeweils bestellte Informationssicherheitsbeauftragte („InfoSec Officer“) oder eine andere von der Leitung der Konzerngesellschaft im Drittland bestellte Person. Diese Personen sind von der Leitung und von den jeweiligen Führungskräften zu unterstützen und bei Beschwerden oder Verletzungen der sich aus dieser Richtlinie ergebenden Verpflichtungen zu unterrichten. Die Datenschutz-Koordinatoren schalten in diesen Fällen den Datenschutzbeauftragten der Siemens AG ein, dessen Entscheidungen zur Abhilfe der Datenschutzverletzung von der jeweiligen Leitung der Konzerngesellschaft im Drittland zu respektieren sind.


Alle Mitarbeiter und sonstigen Betroffenen können sich jederzeit mit Fragen, Anregungen und Beschwerden an die Datenschutz-Koordinatoren oder an den Datenschutzbeauftragten der Siemens AG wenden.

Als Ansprechpartner für Problemfälle und Grundsatzfragen und für Unterstützung bei der Umsetzung der Richtlinie stehen der Datenschutzbeauftragte der Siemens AG und sein Referat ZV CPO zur Verfügung.

Kontaktadresse:

Florian Thoma
Siemens AG – ZV CPO
Wittelsbacherplatz 2
D-80333 Munich
Tel.:+49 (0) 89 636-32323
Fax:+49 (0) 89 636-33742
E-mail: datenschutz@siemens.com
Siemens Intranet website: <http://dsb.siemens.de/dspages/>
Internet: <http://www.siemens.com>

SIEMENS

Verpflichtung 
zur Einhaltung der
Unternehmensrichtlinie
für Konzerngesellschaften (in „Drittländern“)
zum Schutz personenbezogener Daten

An
Siemens AG
Referat ZV CPO
D-80312 München
E-Mail: datenschutz@siemens.com

Hiermit bestätigt die u. g. Siemens-Konzerngesellschaft, dass sie die o.g. Unternehmensrichtlinie mit Wirkung vom (Datum: TT.MM.JJ) verbindlich in Kraft gesetzt hat:

(Name und Sitz der Konzerngesellschaft)

(ARE)

Folgende Person ist gemäß Ziffer 5.2 und Ziffer 7 der Richtlinie als Datenschutz-Koordinator für Datenschutz und insbesondere für die Überwachung der Einhaltung der Richtlinie zuständig:

Name, Vorname:

Dienstanschrift:

Tel.-Nr.:

Fax-Nr.:

E-Mail-Adresse:

Der Datenschutz-Koordinator ist auch InfoSec Officer: Ja Nein

Die Siemens-Konzerngesellschaft wird die Umsetzung der Richtlinie sicherstellen und insbesondere die Mitarbeiter gemäß Ziffer 5.1 unterrichten.

(Ort)

(Datum)

(Unterschriften der Leitung der Gesellschaft)

(Namen in Druckschrift)