DAIMLER

Konzernrichtlinien.
Datenschutz für Kunden- und Partnerdaten.

Vorwort

Sehr geehrte Damen und Herren,
liebe Mitarbeiterinnen und Mitarbeiter,

Datenschutz beim Umgang mit den Daten unserer Interessenten und Kunden stellt heute angesichts der weitgehenden elektronischen Abwicklung der Vertriebsprozesse, des Internets und zunehmender gesetzlicher Regelungen erhöhte Anforderungen, denen wir gerecht werden wollen.

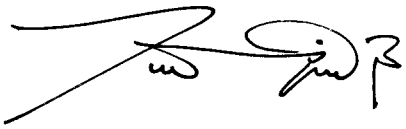
Als global tätiges Unternehmen stehen die Daimler AG und ihre Tochterunternehmen vor der Aufgabe, den weltweit sehr unterschiedlichen rechtlichen Anforderungen an die Erhebung und Verarbeitung personenbezogener Daten zu entsprechen. Wir möchten unseren Kunden und Geschäftspartnern weltweit einen hohen, einheitlichen Standard im Umgang mit ihren personenbezogenen Daten bieten. Ein sorgsamer Umgang mit diesen Daten entspricht der Erwartung unserer Kunden und Geschäftspartner und ist die Basis für eine vertrauensvolle Geschäftsbeziehung.

Diese Konzernrichtlinie gibt einen weltweiten Standard für den Umgang mit den persönlichen Daten unserer Interessenten, Kunden und Geschäftspartner in den Konzernunternehmen vor, der auf den gesetzlichen Anforderungen und auf global anerkannten Datenschutzprinzipien beruht.

Bei einem grenzüberschreitenden Austausch von personenbezogenen Daten zwischen den einzelnen konzernangehörigen Gesellschaften sind besondere rechtliche Erfordernisse zu beachten. Eine grenzüberschreitende Übermittlung personenbezogener Daten ist vielfach nur dann erlaubt, wenn der Datenempfänger ein angemessenes Datenschutzniveau gewährleistet. Dieses angemessene Datenschutzniveau wird durch die Konzernrichtlinie „Datenschutz für Kunden- und Partnerdaten“ sowie „Datenschutz für Personaldaten“ hergestellt.

Die Umsetzung der aus den Datenschutzrichtlinien folgenden Verpflichtungen und die Einhaltung der nationalen Datenschutzgesetze wird durch die Führungskräfte und Mitarbeiter im Unternehmen sichergestellt.

Der Konzernbeauftragte für den Datenschutz hat dafür Sorge zu tragen, dass die Umsetzung der Datenschutzrichtlinien und Gesetze erfolgt. Meine Mitarbeiter und ich stehen Ihnen als Ansprechpartner bei Fragen zum Datenschutz gerne zur Verfügung.



Dr. Joachim Rieß
Konzernbeauftragter für den Datenschutz

Inhalt

I. Ziel der Datenschutzrichtlinie

Die Daten der Kunden und Partner sind ein wichtiger Wettbewerbsfaktor und tragen in großem Umfang zur Wertschöpfung des Daimler-Konzerns bei. Diese Daten sind gegen Gefährdungen eines unzulässigen Zugriffs zu schützen. Neben diesem technischen Schutz erwarten die Kunden und Partner aber auch generell einen sorgsamen Umgang mit ihren Daten. Ohne eine vertrauensvolle Beziehung zu den Kunden und Partnern sind dauerhafte Geschäftsbeziehungen nicht realisierbar. Daimler hat diese Herausforderung erkannt und bekennt sich im Rahmen seiner gesellschaftlichen Verantwortung auch zu seiner Verantwortung im Umgang mit den Daten. Daimler gibt sich mit dieser Richtlinie einen, auf global akzeptierten Grundprinzipien basierenden, einheitlichen und global gültigen Datenschutz- und Datensicherheitsstandard für die Verarbeitung personenbezogener Daten von Kunden und Partnern. Die Richtlinie unterstützt die Wettbewerbsfähigkeit des Konzerns und stellt eine Basis für eine dauerhafte und vertrauensvolle Geschäftsbeziehung dar.

Die Richtlinie schafft auch eine der notwendigen Rahmenbedingungen für einen globalen Datenaustausch zwischen den Konzerngesellschaften, da sie das von der Europäischen Datenschutzrichtlinie[1] und weiteren nationalen Gesetzen verlangte adäquate Datenschutzniveau für den grenzüberschreitenden Datenverkehr auch in solche Länder gewährleistet, in denen bisher noch kein angemessenes Datenschutzrecht besteht.

II. Definitionen

» Ein **angemessenes Datenschutzniveau** von Drittstaaten wird von der EU Kommission dann anerkannt, wenn der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schließt die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Standesregeln und Sicherheitsmaßnahmen ein.

» **Anonymisiert** sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

» **Besonders schutzbedürftige Daten** sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzbedürftig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

» **Betroffener** im Sinne dieser Richtlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.

[1] RL 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy law/index_de.htm#richtlinie

- **Dritter** ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Ebenfalls nicht Dritte sind Auftragsverarbeiter, die gesetzlich der verantwortlichen Stelle zugeordnet sind.

- **Drittstaaten** im Sinne der Richtlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.

- **Einwilligung** ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

- **Erforderlich** ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.

- Der **EWR** ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.

- **Personenbezogene Daten** sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.

- **Übermittlung** ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

- **Verarbeitung personenbezogener Daten** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

- **Verantwortliche Stelle** ist diejenige juristisch selbständige Gesellschaft des Daimler-Konzerns, deren Geschäftsaktivität die jeweilige Verarbeitungsmaßnahme veranlasst.

III. Geltungsbereich und Änderung der Richtlinie

Diese Konzernrichtlinie gilt für alle Unternehmen des Daimler-Konzerns, d.h. für die Daimler AG und alle von ihr abhängigen Konzerngesellschaften sowie verbundenen Unternehmen und deren Mitarbeiter. Abhängig in diesem Sinne bedeutet, dass die Daimler AG, unmittelbar oder mittelbar, auf Grund des Besitzes der Stimmrechtsmehrheit, einer Mehrheit in der Unternehmensleitung oder einer Vereinbarung verlangen kann, dass diese Richtlinie übernommen wird. Die Konzernrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten von Kunden und Partnern. Dies schließt auch die Daten von Interessenten, Lieferanten und Aktionären ein. Diese Richtlinie gilt auch für Daten juristischer Personen, soweit das jeweilige staatliche Recht juristische Personen in den Schutzbereich des Datenschutzrechts einbezieht.

Die einzelnen Konzerngesellschaften sind nicht berechtigt, von dieser Richtlinie abweichende Regelungen zu treffen. Eine Änderung dieser Richtlinie findet ausschließlich durch den Konzernbeauftragten für den Datenschutz innerhalb des für die Änderung von Richtlinien vorgegebenen Verfahrens statt.

Die konzernangehörigen Gesellschaften haben die Bestimmungen dieser Richtlinie in der jeweils gültigen Fassung zu befolgen. Nur für den Fall, dass damit eine Verschlechterung der Position des Betroffenen verbunden sein sollte, gilt diejenige Fassung, die zum Zeitpunkt der Verarbeitung seiner Daten galt.

Für den Fall des Außerkrafttretens ohne eine Neuregelung sind die konzernangehörigen Gesellschaften in Bezug auf die bis zu diesem Zeitpunkt verarbeiteten Daten an die zuletzt geltende Fassung dieser Richtlinie gebunden.

IV. Geltung staatlichen Rechts

Diese Datenschutzrichtlinie beinhaltet die weltweit akzeptierten Datenschutzprinzipien, ohne dass bestehendes staatliches Recht ersetzt wird. Sie gilt immer, soweit sie nicht im Widerspruch zum jeweiligen staatlichen Recht steht; darüber hinaus ist das staatliche Recht anzuwenden, sofern dieses weitergehende Anforderungen stellt. Das jeweilige staatliche Recht ist zu beachten, wenn es zwingende Abweichungen von dieser Datenschutzrichtlinie enthält oder darüber hinausgeht. Die Inhalte dieser Datenschutzrichtlinie sind auch dann zu beachten, wenn es kein entsprechendes staatliches Recht gibt.

Für den Fall von Datenübermittlungen aus der Europäischen Union/EWR oder aus Staaten, die für Datenübermittlungen in andere Länder einen angemessenen Datenschutzstandard fordern, haben die datenimportierenden Stellen bei der Verarbeitung der übermittelten personenbezogenen Daten das jeweilige nationale Recht des Staates anzuwenden, aus dem die Daten übermittelt wurden. Dies gilt nicht für Datenübermittlungen innerhalb der Europäischen Union/EWR oder für Datenübermittlungen in Länder außerhalb der Europäischen Union/EWR, deren Datenschutzniveau von der Europäischen Kommission als angemessen beurteilt wurde.

Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen müssen beachtet werden. Jede juristisch selbständige Gesellschaft des Daimler-Konzerns hat zu überprüfen, ob und in welchem Umfang eine solche Meldepflicht besteht. In Zweifelsfällen kann der Konzernbeauftragte für den Datenschutz zu Rate gezogen werden.

V. Grundsätze für die Verarbeitung personenbezogener Daten

1. Fairness und Rechtmäßigkeit
Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Daten müssen fair und auf rechtmäßige Weise verarbeitet werden.

2. Zweckbindung
Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich. Diese können aufgrund vertraglicher Vereinbarungen mit dem Betroffenen, einer Einwilligung des Betroffenen oder aufgrund staatlichen Rechts stattfinden.

3. Transparenz
Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene folgendes erkennen können oder entsprechend informiert werden über:

» Die Identität der verantwortlichen Stelle
» Den Zweck der Datenverarbeitung
» Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

Der Betroffene sollte über die Freiwilligkeit der Angabe von Daten für Zwecke des Marketings unterrichtet werden.

In Konzernstandards werden Vorgaben zu erforderlichen Informationen über den Umgang mit den Daten des Betroffenen gemacht.

Neben den Vorgaben in Konzernstandards können aufgrund staatlichen Rechts zusätzliche oder abweichende Anforderungen an den Inhalt und Umfang der Informationen bestehen. Dies können zum Beispiel Vorgaben zu Informationen über ein Widerspruchsrecht des Betroffenen gegen Kontakte zu Marketing- und Werbezwecken sein.

4. Datensparsamkeit
Vor einer Verarbeitung personenbezogener Daten muss geprüft werden ob und in welchem Umfang diese notwendig ist, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter Daten erfolgen, sind nicht von dieser Richtlinie erfasst.

Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben.

Daten, die nicht mehr benötigt werden, sollen unter Beachtung bestehender Aufbewahrungspflichten gelöscht werden.

5. Sachliche Richtigkeit, Datenaktualität
Personenbezogene Daten sind richtig und auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende oder unvollständige Daten gelöscht, berichtigt oder ergänzt werden.

6. Besonders schutzbedürftige Daten
Besonders schutzbedürftige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden.

Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein; oder die Verarbeitung ist notwendig, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Der Betroffene kann auch ausdrücklich in die Verarbeitung einwilligen.

7. Need-To-Know Prinzip
Vor dem Hintergrund der immer flexibleren Arbeitsorganisation ist darauf zu achten, dass Mitarbeiter Zugang zu personenbezogenen Daten nur nach dem Need-To-Know Prinzip erhalten. Das Need-To-Know Prinzip bedeutet, dass Mitarbeiter nur nach Art und Umfang ihrer jeweiligen Aufgaben Zugang zu personenbezogenen Daten erhalten dürfen. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten und deren Umsetzung.

8. Automatisierte Einzelentscheidungen
Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, müssen besondere Voraussetzungen erfüllen. Sie dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden. Dem Betroffenen muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden. Strengere Vorgaben aufgrund staatlichen Rechts für automatisierte Einzelentscheidungen sind zu beachten.

VI. Zulässigkeit der Datenverarbeitung

1. Datenverarbeitung für eine vertragliche Beziehung
Personenbezogene Daten des Betroffenen dürfen zur Durchführung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners nach Abschluss des Vertrages, sofern dies im Zusammenhang mit dem Vertragszweck steht. Kundenbindungs- oder Werbemaßnahmen sind davon nicht umfasst.

Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten (z.B. Probefahrt) erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten. Für darüber hinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter VI.2. beachtet werden.

2. Datenverarbeitung zu Werbezwecken
Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Im Rahmen der Kommunikation mit dem Betroffenen sollte eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. (s. VI.3.).

Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen des Daimler-Konzerns (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens unabhängig von dem Vorliegen einer Einwilligung immer zulässig.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke sind zu beachten. Solche können insbesondere für Werbung per E-Mail, Telefon und Telefax bestehen.

3. Einwilligung in die Datenverarbeitung
Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Ebenso kann eine Änderung des Verarbeitungszweckes auf Basis einer Einwilligung des Betroffenen erfolgen. Vor der Einwilligung muss der Betroffene gemäß V.3. dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen regelmäßig schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden. Besondere Anforderungen an die Einwilligungserklärung aufgrund staatlichen Rechts sind einzuhalten.

4. Datenverarbeitung aufgrund gesetzlicher Erlaubnis
Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

5. Datenverarbeitung aufgrund berechtigten Interesses
Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der verantwortlichen Stelle oder einer dritten Stelle erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftlich (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Diese sind für jede Verarbeitung zu prüfen.

VII. Übermittlung personenbezogener Daten

Für einige Geschäftsprozesse ist es notwendig, dass personenbezogene Daten von Kunden oder Partnern an Dritte übermittelt werden. Wenn dies nicht aufgrund einer rechtlichen Verpflichtung erfolgt, muss jeweils geprüft werden, ob ein schutzwürdiges Interesse des Betroffenen entgegensteht. Für eine Übermittlung personenbezogener Daten an eine Stelle außerhalb des Daimler-Konzerns müssen die Voraussetzungen des Abschnitts VI. erfüllt werden. Befindet sich der Empfänger in einem Drittstaat, muss er ein zu dieser Richtlinie adäquates Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Weitergabe aufgrund einer gesetzlichen oder einer anderen zulässigen rechtlichen Verpflichtung erfolgt. Der Empfänger muss vertraglich darauf verpflichtet werden, die Daten nur zu den festgelegten Zwecken zu nutzen.

Eine Übermittlung an staatliche Einrichtungen oder Behörden erfolgt soweit erforderlich aufgrund jeweils einschlägiger Rechtsvorschriften.

Im Falle einer Datenübermittlung von Dritten an Unternehmen des Daimler-Konzerns muss sichergestellt sein, dass die Daten im Rahmen des jeweils geltenden Rechts rechtmäßig erhoben wurden und für die vorgesehene Verarbeitungsmöglichkeiten verwendet werden dürfen.

VIII. Datenübermittlungen innerhalb des Konzerns

Gibt eine rechtlich selbständige Konzerngesellschaft personenbezogene Daten an eine andere Konzerngesellschaft weiter, handelt es sich rechtlich um eine Übermittlung an Dritte. Für eine solche Übermittlung müssen die Voraussetzungen des Abschnitts VI. gegeben sein.

Werden personenbezogene Daten von einer Konzerngesellschaft mit Sitz in der Europäischen Untion/EWR an eine Konzerngesellschaft mit Sitz in einem Drittstaat übermittelt, so ist der Konzernbeauftragte für den Datenschutz und die datenimportierende Gesellschaft verpflichtet, bei allen Anfragen der zuständigen Aufsichtsbehörde, in dem die datenexportierende Stelle ihren Sitz hat, mit dieser zu kooperieren und die Feststellungen der Aufsichtsbehörde im Hinblick auf die Verarbeitung der übermittelten Daten zu beachten.

Im Fall eines von einem Betroffenen behaupteten Verstoßes gegen diese Datenschutzrichtlinie durch eine datenimportierende Konzerngesellschaft mit Sitz in einem Drittstaat verpflichtet sich die datenexportierende Konzerngesellschaft mit Sitz in der Europäischen Union/EWR, den Betroffenen, dessen Daten in der Europäischen Union/EWR erhoben worden sind, sowohl bei der Sachverhaltsaufklärung zu unterstützen als auch die Durchsetzung seiner Rechte nach Abschnitt XI. dieser Datenschutzrichtlinie gegenüber der datenimportierenden Konzerngesellschaft sicherzustellen. Darüber hinaus ist der Betroffene berechtigt, seine Rechte aus Abschnitt XI. auch gegenüber der datenexportierenden Konzerngesellschaft geltend zu machen.

Im Fall einer Übermittlung personenbezogener Daten von einer Konzerngesellschaft mit Sitz in der Europäischen Union/EWR an eine Konzerngesellschaft mit Sitz in einem Drittstaat hat die datenübermittelnde Stelle den Betroffenen, dessen personenbezogene Daten in der Europäischen Union/EWR erhoben worden sind, für Verstöße der Konzerngesellschaft mit Sitz in einem Drittstaat gegen diese Datenschutzrichtlinie haftungsrechtlich so zu stellen, als hätte die datenübermittelnde Stelle den Verstoß begangen.

Gerichtsstand ist das zuständige Gericht am Sitz der datenexportierenden Stelle.

IX. Datenverarbeitung im Auftrag

Bei einer Datenverarbeitung im Auftrag wird ein Dienstleister mit der Durchführung der Datenverarbeitung beauftragt, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. Im Falle einer Weitergabe personenbezogener Daten im Rahmen einer Datenverarbeitung im Auftrag bleibt der Auftraggeber die für die Verarbeitung verantwortliche Stelle. Sämtliche Rechte der Betroffenen sind ihm gegenüber geltend zu machen. Darüber hinaus sind bei der Auftragserteilung folgende Maßgaben zu befolgen:

1. Bei der Auswahl des Auftragnehmers ist sicherzustellen, dass er die für die Verarbeitung notwendigen technischen und organisatorischen Anforderungen und Sicherheitsmaßnahmen gewährleisten kann. Bei der Auswahl sind die Kriterien des Konzernbeauftragten für den Datenschutz zu beachten.

2. Die Durchführung der Auftragsdatenverarbeitung muss in einem schriftlichen Vertrag geregelt werden, in dem die Anforderungen zum Datenschutz und zur Informationssicherheit vereinbart sind. Insbesondere muss festgelegt werden, dass der Auftragnehmer die Daten ausschließlich nach den Weisungen des Auftraggebers verarbeiten darf.

3. Bei der Vertragsgestaltung müssen die Konzernrichtlinien beachtet werden.

4. Bei der Beauftragung von Dienstleistern außerhalb der Europäischen Union/EWR mit der Verarbeitung von personenbezogenen Daten aus der Europäischen Union/EWR muss seitens des Dienstleisters ein dieser Richtlinie entsprechendes adäquates Datenschutzniveau garantiert werden, soweit der Dienstleister die Daten in einem Drittstaat verarbeiten will. Vergleichbare Regelungen in anderen nationalen Datenschutzgesetzen müssen in gleicher Weise beachtet werden. Zusätzlich sind bei der Beauftragung von Dienstleistern außerhalb der Europäischen Union/EWR die Voraussetzungen von Abschnitt VII. zu erfüllen.

X. Telekommunikation und Internet

Die Verarbeitung personenbezogener Daten, die bei der Telekommunikation mit dem Betroffenen einschließlich der Internet-Kommunikation anfallen, richtet sich nach den lokal jeweils geltenden Arbeitsanweisungen bzw. nach dem jeweils geltenden Recht.

Konzernstandards zur Umsetzung rechtlicher Vorgaben bei der Gestaltung von Webseiten sind einzuhalten.

XI. Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind.

2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

4. Der Betroffene ist berechtigt die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten müssen beachtet werden.

5. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Direktwerbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse der verantwortlichen Stelle überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

XII. Vertraulichkeit der Verarbeitung

Personenbezogene Daten von Kunden und Partnern werden vertraulich behandelt; eine unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein.

Insbesondere ist es untersagt, personenbezogene Daten für eigene private oder wirtschaftliche Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen.

XIII. Sicherheit der Verarbeitung

Zur Gewährleistung der Datensicherheit sind geeignete technische und organisatorische Maßnahmen implementiert, die auch den Schutz personenbezogener Daten gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung sicherstellen. Sie beziehen sich auf die Sicherheit schutzwürdiger Daten sowohl bei elektronischen Verarbeitungen als auch in Papierform.

Diese technisch-organisatorischen Maßnahmen sind Teil eines integrierten Informationssicherheitsmanagements und werden kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst.

XIV. Verantwortlichkeiten und Sanktionen

Die Vorstände und Geschäftsführungen der Konzerngesellschaften sind als jeweilige Verantwortliche für die Datenverarbeitung verpflichtet sicherzustellen, dass die gesetzlichen und die in den Datenschutzrichtlinien formulierten Anforderungen des Datenschutzes beachtet werden. Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes in ihrem Verantwortungsbereich sicherzustellen. Die Einhaltung der Datenschutzrichtlinien und der geltenden Datenschutzgesetze wird durch regelmäßige Datenschutzaudits überprüft.

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich gemacht werden können, ziehen grundsätzlich arbeitsrechtliche Sanktionen entsprechend dem jeweils geltenden nationalen Recht nach sich (siehe Richtlinie zu Disziplinarmaßnahmen).

XV. Der Konzernbeauftragte für den Datenschutz

Der Konzernbeauftragte für den Datenschutz als internes fachlich weisungsunabhängiges Organ überwacht die Einhaltung der nationalen und internationalen Datenschutzvorschriften. Er ist verantwortlich für die Richtlinien auf dem Gebiet des Datenschutzes und überwacht deren Einhaltung. Er führt Datenschutz-Kontrollen und -Audits durch. Der Konzernbeauftragte für den Datenschutz wird vom Vorstand der Daimler AG bestellt.

Die jeweiligen Geschäftsführungen und Werkleitungen müssen dem Konzernbeauftragten für den Datenschutz einen Datenschutzkoordinator benennen. Organisatorisch kann diese Aufgabe in Abstimmung mit dem Konzernbeauftragten für den Datenschutz auch von einem Datenschutzkoordinator für mehrere Gesellschaften oder Werke wahrgenommen werden. Die Datenschutzkoordinatoren sind vor Ort Ansprechpartner für den Datenschutz. Sie können Kontrollen durchführen und haben die Inhalte der Datenschutzrichtlinien den Mitarbeitern bekannt zu machen. Die jeweiligen Geschäftsführungen sind verpflichtet, den Konzernbeauftragten für den Datenschutz und die Datenschutzkoordinatoren in ihrer Tätigkeit zu unterstützen.

Die Fachbereiche müssen die Datenschutzkoordinatoren über neue Verarbeitungen personenbezogener Daten informieren. Die Datenschutzkoordinatoren unterrichten den Konzernbeauftragten für den Datenschutz frühzeitig über Datenschutzrisiken. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Konzernbeauftragte für den Datenschutz schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzbedürftige personenbezogene Daten.

Die Fachbereiche sorgen dafür, dass ihre Mitarbeiter im erforderlichen Umfang im Umgang mit personenbezogenen Daten geschult werden. Der Konzernbeauftragte für den Datenschutz stellt ein webbasiertes Schulungstool zur Verfügung.

Bei Datenschutzverletzungen und Beschwerden sind die verantwortlichen Führungskräfte verpflichtet, umgehend entweder den zuständigen Datenschutzkoordinator oder den Konzernbeauftragten für den Datenschutz selbst zu unterrichten. Daneben kann sich jeder Betroffene jederzeit mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Konzernbeauftragten für den Datenschutz wenden. Die Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt. Die Entscheidungen des Konzernbeauftragten für den Datenschutz zur Abhilfe der Datenschutzverletzung sind durch die jeweiligen Geschäftsführungen zu respektieren.

Der Konzernbeauftragte und seine Mitarbeiter können wie folgt erreicht werden:

Daimler AG
Konzernbeauftragter für den Datenschutz
HPC 0518
D-70546 Stuttgart
E-Mail: mbox_datenschutz@daimler.com
Im Intranet unter http://intra.corpintra.net/cdp

Daimler AG
Stuttgart, Germany
www.daimler.com
www.daimler.mobi