Datenschutzrichtlinie EU

Mercedes-Benz

Inhaltsverzeichnis

1 Ziel der Richtlinie

Die Mercedes-Benz Group sieht die Wahrung von Datenschutzrechten als Teil ihrer sozialen Verantwortung.

In einigen Ländern und Regionen, wie der Europäischen Union, hat der Gesetzgeber Standards für den Schutz der Daten von natürlichen Personen („personenbezogene Daten“) festgelegt, einschließlich der Anforderung, dass diese Daten nur dann in andere Länder übermittelt werden dürfen, wenn am Bestimmungsort ein angemessenes Datenschutzniveau beim Empfänger besteht.

Diese Datenschutzrichtlinie EU legt einheitliche und angemessene konzerninterne Datenschutzstandards fest – sowohl für:

- (a) die Verarbeitung personenbezogener Daten in Regionen wie der EU/dem Europäischen Wirtschaftsraum (EWR) (nachstehend einheitlich als „**EU/EWR**“ bezeichnet) als auch
- (b) die grenzüberschreitende Übermittlung personenbezogener Daten an Konzerngesellschaften außerhalb der EU/EWR (einschließlich deren anschließender dortiger Verarbeitung).

Zu diesem Zweck gibt diese Richtlinie verbindliche Regeln für die Verarbeitung personenbezogener Daten mit EU/EWR-Herkunft innerhalb der Mercedes-Benz Group vor. Sie schaffen angemessene Garantien für den Schutz personenbezogener Daten außerhalb der EU/EWR und bilden somit sogenannte verbindliche Unternehmensregeln („Binding Corporate Rules – BCR“) für die Mercedes-Benz Group.

2 Anwendungsbereich

Diese Datenschutzrichtlinie EU gilt für die Mercedes-Benz Group AG, die von ihr kontrollierten Konzerngesellschaften (im Folgenden **Konzerngesellschaften**) und deren Mitarbeiter und Mitglieder geschäftsführender Organe. Kontrolliert in diesem Sinne bedeutet, dass die Mercedes-Benz Group AG, unmittelbar oder mittelbar, aufgrund des Besitzes der Stimmrechtsmehrheit, einer Mehrheit in der Unternehmensleitung oder einer Vereinbarung verlangen kann, dass diese Richtlinie übernommen wird.

Die Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht-automatisierte Verarbeitung in Dateisystemen, soweit nicht nationales Recht den Geltungsbereich ausdehnt. In Deutschland gilt die Richtlinie auch für sämtliche Mitarbeiterdaten[1] in Papierform.

Die Richtlinie gilt für die Verarbeitung personenbezogener Daten:

- (a) von Konzerngesellschaften und ihren Niederlassungen, die ihren Standort innerhalb der EU/EWR oder eines anderen Landes haben, auf die diese Richtlinie ausgedehnt werden kann, („EU/EWR-ansässige Gesellschaften“),
- (b) von Konzerngesellschaften mit einem Standort außerhalb der EU/EWR, soweit sie Waren oder Dienstleistungen natürlichen Personen innerhalb der EU/EWR anbieten und/oder das Verhalten von natürlichen Personen innerhalb der EU/EWR überwachen („Drittlandsgesellschaften mit Angeboten für die EU/EWR“) oder

[1] In dieser Richtlinie wird allein aus Gründen der sprachlichen Vereinfachung für natürliche Personen lediglich die männliche Form verwendet. Inhaltlich sind stets Personen aller geschlechtlichen Identitäten gemeint.

- (c) von Konzerngesellschaften mit Standort außerhalb der EU/EWR, soweit sie personenbezogene Daten direkt oder indirekt von Gesellschaften, für die die Richtlinie nach a) oder b) gilt, erhalten haben oder ihnen gegenüber offengelegt werden („Drittlandsgesellschaften, die Daten aus der EU/EWR erhalten“).

Verarbeitungen außerhalb der EU/EWR werden im weiteren Verlauf dieser Richtlinie als Verarbeitung in einem Drittland bezeichnet.

Die Konzerngesellschaften, die an der Verarbeitung durch Drittlandsgesellschaften teilnehmen bzw. dieser unterliegen, sind in der Mitgeltenden Regelung "Liste der an die Datenschutzrichtlinie EU gebundenen Konzerngesellschaften" aufgeführt.

Diese Richtlinie kann auf Länder außerhalb der EU/EWR erstreckt werden. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten geschützt werden, gilt diese Richtlinie auch in gleicher Weise für die Daten juristischer Personen.

3 Rechtsverbindlichkeit innerhalb der Mercedes-Benz Group

Die Bestimmungen dieser Richtlinie sind verbindliche Vorschriften für alle Konzerngesellschaften, die in ihrem Anwendungsbereich tätig sind. Die Konzerngesellschaften sowie deren Management und Mitarbeiter sind daher neben den geltenden EU-Vorschriften und nationalen Datenschutzgesetzen für die Einhaltung dieser Richtlinie verantwortlich.

Konzerngesellschaften sind – vorbehaltlich gesetzlicher Anforderungen – nicht berechtigt, von dieser Richtlinie abweichende Regelungen zu treffen.

4 Verhältnis zu gesetzlichen Anforderungen

Diese Richtlinie ersetzt nicht EU-Vorschriften und die nationalen Gesetze. Sie ergänzt die nationalen Datenschutzgesetze. Diese Vorschriften und Gesetze haben Vorrang, wenn die Einhaltung dieser Richtlinie zu einem Verstoß gegen nationales Recht führen würde. Der Inhalt dieser Richtlinie ist auch dann zu beachten, wenn es keine entsprechenden nationalen Gesetze gibt.

Sofern die Einhaltung dieser Richtlinie zu einem Verstoß gegen nationales Recht führen würde oder nach nationalem Recht abweichende Regelungen zu dieser Richtlinie erforderlich sind, ist dies im Rahmen des Datenschutzrechts-Monitorings dem Konzernbeauftragten für den Datenschutz und der zentralen Compliance-Organisation zu melden. Im Falle von Konflikten zwischen nationaler Gesetzgebung und dieser Richtlinie werden der Konzernbeauftragte für den Datenschutz und die zentrale Compliance-Organisation mit der zuständigen Konzerngesellschaft zusammenarbeiten, um eine praktische Lösung zu finden, die dem Zweck dieser Richtlinie entspricht.

5 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

5.1 Rechtmäßigkeit

Personenbezogene Daten müssen auf rechtmäßige Weise nach Treu und Glauben verarbeitet werden. Die Datenverarbeitung darf nur dann und soweit erfolgen, wie eine ausreichende Rechtsgrundlage für den jeweiligen Verarbeitungsvorgang vorhanden ist. Dies gilt auch für die Datenverarbeitung zwischen Konzerngesellschaften. Allein die Tatsache, dass sowohl die übermittelnde als auch die empfangende Gesellschaft zur Mercedes-Benz Group gehören, rechtfertigt die Datenverarbeitung noch nicht.

Die Verarbeitung personenbezogener Daten ist zulässig, wenn einer der Erlaubnistatbestände unter Ziffer 5.2 oder 5.3 vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Verarbeitung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

5.2 Rechtsgrundlage Kunden- und Partnerdaten

5.2.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, Durchführung und Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Kunden oder Partners, sofern dies im Zusammenhang mit dem Vertragszweck steht.

Im Vorfeld eines Vertrages 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 erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten.

5.2.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an eine Konzerngesellschaft (z. B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig. Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, soweit sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist vorab über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene muss über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation soll eine Einwilligung des Betroffenen eingeholt werden. Der Betroffene kann im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie elektronische Mitteilungen und Telefon auswählen (Einwilligung s. Ziffer 5.2.3). Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke eingeschränkt bzw. gesperrt werden. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke sind zu beachten.

5.2.3 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutzrichtlinie EU informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z. B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

5.2.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis oder Pflicht

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.

5.2.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z. B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z. B. Vermeidung von Vertragsstörungen). Eine Verarbeitung aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn im Einzelfall die Interessen des Betroffenen an dem Schutz seiner Daten gegenüber den berechtigten Interessen an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

5.3 Rechtsgrundlage Mitarbeiterdaten

5.3.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlich sind. Für die Entscheidung über die Begründung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Konzerngesellschaften erforderlich. Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsverhältnisses bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist – soweit zulässig – eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Begründung oder Beendigung des Arbeitsverhältnisses dienen (Mitarbeiterdaten), muss eine der nachstehenden Rechtsgrundlagen vorliegen.

5.3.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis oder Pflicht

Die Verarbeitung von Mitarbeiterdaten 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. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

5.3.3 Kollektivvereinbarung für Datenverarbeitungen

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivvereinbarung gestattet wird. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen der Vorgaben der EU-Vorschriften und nationalen Gesetze gestaltbar.

5.3.4 Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Die Nichterteilung einer Einwilligung darf nicht zu Nachteilen für Mitarbeiter führen. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutzrichtlinie EU informiert werden.

5.3.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung von Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der Konzerngesellschaft erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z. B. Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftliche (z. B. Beschleunigung von Betriebsabläufen, Bewertung von Unternehmen). Das Vorliegen schutzwürdiger Interessen ist vor jeder Verarbeitung zu prüfen. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf erfolgen, wenn schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung nicht überwiegen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten über die Durchführung des Arbeitsverhältnisses hinaus (z. B. Leistungskontrolle) erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Dazu müssen die berechtigten Interessen der Konzerngesellschaft an der Durchführung der Kontrollmaßnahme (z. B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) gegen ein mögliches schutzwürdiges Interesse des betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden. Die Maßnahmen dürfen nur durchgeführt werden, wenn sie im konkreten Fall angemessen sind. Das berechtigte Interesse der Konzerngesellschaft und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach geltendem Recht bestehende weitere Anforderungen (z. B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

5.4 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich vorgeschrieben oder erlaubt ist. Eine Verarbeitung solcher Daten durch die Konzerngesellschaft kann insbesondere zulässig sein, wenn der Betroffene ausdrücklich in die Verarbeitung eingewilligt hat, die Verarbeitung zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben bzw. zu verteidigen oder um Rechten und Pflichten aus dem Arbeitsrecht bzw. Sozialrecht entsprechen zu können.

Wird die Verarbeitung besonders schutzwürdiger personenbezogener Daten geplant, ist der Konzernbeauftragte für den Datenschutz im Vorfeld zu informieren.

5.5 Automatisierte Einzelfallentscheidungen (ggf. inklusive Profiling)

Der Betroffene darf nur dann einer ausschließlich automatisierten Entscheidung unterworfen werden, die ihm gegenüber rechtliche oder ähnlich nachteilige Wirkungen hat, wenn dies für den Abschluss oder die Erfüllung des Vertrages erforderlich ist oder der Betroffene eingewilligt hat. Diese automatisierte Entscheidung kann im Einzelfall mit einem Profiling verbunden sein, also einer Verarbeitung personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z. B. Kreditwürdigkeit) bewertet werden. In diesem Fall müssen dem Betroffenen die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und eine individuelle Prüfung durch einen Verantwortlichen ermöglicht werden.

5.6 Informationspflicht/Transparenz

Der verantwortliche Fachbereich muss die Betroffenen über die Zwecke und Umstände der Verarbeitung ihrer personenbezogenen Daten gemäß Artikel 13 und 14 DSGVO informieren. Wenn die Daten nicht in den Anwendungsbereich der DSGVO fallen, erfolgt die Information gemäß dem anwendbaren nationalen Recht. Die Information muss in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache erfolgen. Die Vorgaben des Konzernbeauftragten für den Datenschutz und von Data Compliance sind zu beachten. Diese Information muss grundsätzlich zum Zeitpunkt der ersten Erhebung der personenbezogenen Daten erfolgen. Sofern die Konzerngesellschaft die personenbezogenen Daten von einem Dritten erhält, muss sie die Information in angemessener Frist den Betroffenen nach Erlangung der Daten mitteilen, es sei denn, dass die Betroffenen:

- bereits über die Informationen verfügen oder
- die Erteilung dieser Informationen sich als unmöglich erweist oder
- einen unverhältnismäßigen Aufwand erfordern würde.

5.7 Zweckbindung

Personenbezogene Daten dürfen nur für den legitimen Zweck verarbeitet werden, der vor der Datenerhebung definiert wurde. Nachträgliche Änderungen des Verarbeitungszwecks sind nur zulässig unter der Voraussetzung, dass die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist.

5.8 Datenminimierung

Jede Verarbeitung personenbezogener Daten muss so gestaltet sein, dass sie sowohl quantitativ als auch qualitativ auf das für die Erreichung der Zwecke, für die die Daten rechtmäßig verarbeitet werden, erforderliche Maß beschränkt ist. Dies ist bereits beim Umfang der Datenerhebung zu berücksichtigen. Sofern der Zweck es zulässt und der Aufwand in einem angemessenen Verhältnis zu dem verfolgten Ziel steht, sind anonymisierte oder statistische Daten zu verwenden.

5.9 Richtigkeit der Daten

Die gespeicherten personenbezogenen Daten müssen sachlich richtig und – falls erforderlich – auf dem neuesten Stand sein. Der verantwortliche Fachbereich muss angemessene Maßnahmen treffen, um sicherzustellen, dass unrichtige oder unvollständige Daten gelöscht, korrigiert, ergänzt oder aktualisiert werden.

5.10 Privacy by Design & Privacy by Default

Das Prinzip „Privacy by Design“ zielt darauf ab, dass die Fachbereiche nach dem Stand der Technik interne Strategien festlegen und Maßnahmen ergreifen, um Datenschutzprinzipien von Anfang an in der Phase der Konzeption und des technischen Designs in die Spezifikation und Architektur von Geschäftsmodellen/Prozessen sowie von IT-Systemen der Datenverarbeitung zu integrieren. Nach dem Grundsatz „Privacy by Design“ müssen die Verfahren und Systeme zur Verarbeitung personenbezogener Daten so gestaltet sein, dass ihre initialen Einstellungen auf die für die Erfüllung des Zwecks erforderliche Datenverarbeitung beschränkt sind (Prinzip „Privacy by default“). Dies umfasst den Verarbeitungsumfang, die Speicherdauer und die Zugänglichkeit. Weitere Maßnahmen können darin bestehen, dass:

- personenbezogene Daten so schnell wie möglich pseudonymisiert werden
- Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird
- dem Betroffenen ermöglicht wird, über die Verarbeitung personenbezogener Daten zu entscheiden
- der Betreiber von Verfahren oder Systemen in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.

Jede Konzerngesellschaft führt während des gesamten Lebenszyklus ihrer Verarbeitungsprozesse geeignete technische und organisatorische Maßnahmen ein und betreibt diese, um sicherzustellen, dass die oben genannten Grundsätze jederzeit eingehalten werden.

5.11 Löschung & Anonymisierung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Zweck, für den diese Daten verarbeitet werden, erforderlich ist. Dies bedeutet, dass personenbezogene Daten gelöscht oder anonymisiert werden müssen, sobald der Zweck ihrer Verarbeitung erfüllt ist oder anderweitig erlischt, es sei denn, es bestehen weiterhin Aufbewahrungs- oder Nachweispflichten. Die für die einzelnen Verfahren Verantwortlichen müssen die Umsetzung der Lösch- und Anonymisierungsroutinen für ihre Verfahren sicherstellen. Jedes System muss eine manuelle oder automatisierte Löschroutine haben. Löschverlangen von Betroffenen nach Löschung oder Entfernen des Personenbezugs müssen in den Systemen technisch umsetzbar sein. Vorgaben, die die Mercedes-Benz Group AG zur Umsetzung von Löschroutinen macht (wie Softwaretools, die Handreichung zur Umsetzung von Löschanforderungen, Dokumentationsanforderungen), sind zu beachten.

5.12 Sicherheit der Verarbeitung

Personenbezogene Daten sind vor unbefugtem Zugriff und unrechtmäßiger Verarbeitung oder Weitergabe sowie vor versehentlichem Verlust, Veränderung oder Zerstörung zu schützen.
Vor der Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, müssen technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten definiert und umgesetzt werden. Diese Maßnahmen müssen auf dem Stand der Technik, den Risiken der Verarbeitung und dem Schutzbedarf der Daten beruhen.

Im Rahmen der Datenschutz-Folgenabschätzung und des Verfahrensverzeichnisses sind die für den Datenschutz relevanten technischen und organisatorischen Maßnahmen durch die Verantwortlichen zu dokumentieren.

Insbesondere soll sich der zuständige Fachbereich mit seinem Business Information Security Officer (BISO), seinen Informationssicherheitsbeauftragten (ISO) sowie seinem Datenschutz-Netzwerk beraten. Die Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des konzernweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und organisatorischen Veränderungen angepasst werden.

5.13 (Weiter-)Übermittlung außerhalb der Mercedes-Benz Group

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der Konzerngesellschaften oder an Empfänger innerhalb der Konzerngesellschaften unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter dieser Ziffer 5. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu festgelegten Zwecken zu verwenden.

Im Falle einer grenzüberschreitenden Übermittlung personenbezogener Daten (einschließlich der Gewährung des Zugriffs aus einem anderen Land) müssen die einschlägigen nationalen Anforderungen für die Weitergabe personenbezogener Daten ins Ausland erfüllt sein. Insbesondere dürfen personenbezogene Daten aus der EU/EWR nur dann in einem Drittland außerhalb der Konzerngesellschaften verarbeitet werden, wenn der Empfänger nachweisen kann, dass er über einen Datenschutzstandard verfügt, der dieser Richtlinie entspricht. Geeignete Instrumente können sein:

- Vereinbarung über EU-Standardvertragsklauseln,
- Teilnahme des Empfängers an einem von der EU akkreditierten Zertifizierungssystem zur Gewährleistung eines ausreichenden Datenschutzniveaus oder
- Anerkennung verbindlicher Unternehmensregeln des Empfängers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständige Datenschutzaufsicht.

Übermittlungen personenbezogener Daten an eine Behörde sind nur dann zulässig, wenn sie nicht massenhaft, unverhältnismäßig oder undifferenziert sind und in diesem Zusammenhang die Grenzen dessen, was in einer demokratischen Gesellschaft als erforderlich gilt, nicht übersteigen. Im Falle von Konflikten zwischen diesen und behördlichen Vorgaben wird die Mercedes-Benz Group AG mit der zuständigen Konzerngesellschaft zusammenarbeiten, um eine praktische Lösung zu finden, die dem Zweck dieser Richtlinie entspricht (Ziffer 14.3).

Alle in dieser Ziffer 5 aufgeführten Pflichten sind für den Betroffenen drittbegünstigend.

6 Datenschutz-Folgenabschätzung

Die Konzerngesellschaften analysieren bei der Einführung neuer Verarbeitungsvorgänge oder bei einer wesentlichen Änderung eines bestehenden Verarbeitungsvorganges vor der Verarbeitung, insbesondere durch die Verwendung neuer Technologien, ob diese Verarbeitung ein hohes Risiko für die Privatsphäre der Betroffenen darstellt. Dabei sind Art, Umfang, Kontext und Zweck der Datenverarbeitung zu berücksichtigen. Im Rahmen der Risikoanlayse führt der verantwortliche Fachbereich eine Bewertung der Auswirkungen der geplanten Verarbeitungen auf den Schutz personenbezogener Daten durch (Datenschutz-Folgenabschätzung). Besteht nach Durchführung der Datenschutz-Folgenabschätzung und der Anwendung geeigneter Maßnahmen zur Risikominderung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen, muss der Konzernbeauftragte für den Datenschutz darüber informiert werden, damit er die zuständige Datenschutzaufsichtsbehörde konsultieren kann. Vorgaben, die die Mercedes-Benz Group AG zur Umsetzung der Datenschutz-Folgenabschätzung macht (wie Softwaretools, Anweisungen zu Durchführung der Bewertung), sind zu beachten.

7 Dokumentation von Datenverarbeitungsverfahren

Jede Konzerngesellschaft muss die Verfahren, in denen personenbezogene Daten verarbeitet werden, in einem Verfahrensverzeichnis dokumentieren. Das Verfahrensverezeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann, und der Datenschutzaufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Vorgaben, die die Mercedes-Benz Group AG zur Dokumentation macht (wie Softwaretools, Anweisungen zu Dokumentation), sind zu beachten.

8 Verarbeitung im Auftrag

8.1 Allgemeines

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer als Dienstleister personenbezogene Daten im Namen und nach Weisung des Auftraggebers verarbeitet. In diesen Fällen ist sowohl mit externen Auftragnehmern als auch zwischen Konzerngesellschaften innerhalb der Mercedes-Benz Group eine Vereinbarung über eine Auftragsverarbeitung abzuschließen gemäß den einschlägigen gesetzlichen Anforderungen (z. B. der Vorlage "Vereinbarung über die Auftragsverarbeitung"). Dabei behält der Auftraggeber die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung.

Die Bestimmungen der Ziffer 8.3. finden ebenfalls Anwendung bei externen Auftraggebern, die keine Konzerngesellschaften sind.

8.2 Bestimmungen für Auftraggeber

Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten, wobei der beauftragende Fachbereich die Umsetzung sicherstellen muss:

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
- Die vom Konzernbeauftragten für den Datenschutz bereitgestellten Vertragsstandards müssen beachtet werden.
- Der Auftrag muss schriftlich oder in elektronischer Form erteilt werden. Die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers sind zu dokumentieren.

Der Auftraggeber muss sich vor Beginn der Datenverarbeitung durch geeignete Prüfung vergewissern, dass der Auftragnehmer die vorgenannten Pflichten erfüllt. Vorgaben, die die Mercedes-Benz Group AG hierzu macht (wie Softwaretools, Anweisungen zu Durchführung der Bewertung, Vertragsmuster), sind zu beachten. Ein Auftragnehmer kann seine Einhaltung der Datenschutzanforderungen insbesondere durch eine entsprechende Zertifizierung dokumentieren. Je nach Risiko der Datenverarbeitung müssen Prüfungen während der Vertragslaufzeit regelmäßig wiederholt werden.

8.3 Bestimmungen für konzerninterne Auftragnehmer

Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten.

Auftragnehmer dürfen andere Konzerngesellschaften oder Dritte („**Unterauftragnehmer**“) zur Verarbeitung personenbezogener Daten im eigenen (Unter-)Auftrag nur mit vorherigem Einverständnis des Auftraggebers beauftragen. Das Einverständnis wird nur erteilt, wenn der Auftragnehmer dem Unterauftragnehmer – vertraglich oder vergleichbar rechtlich bindend – die gleichen Datenschutzpflichten auferlegt, die dem Auftragnehmer nach Maßgabe dieser Richtlinie gegenüber der Konzerngesellschaft und den Betroffenen obliegen, sowie angemessene technische und organisatorische Schutzmaßnahmen. Die Form des Einver-ständnisses sowie Informationspflichten bei Änderungen im Unterauftragsverhältnis sind im Dienstleistungsvertrag zu regeln.

Auftragnehmer sind zur angemessenen Unterstützung des Auftraggebers bei der Einhaltung der für letzteren geltenden Datenschutzbestimmungen verpflichtet, insbesondere durch die Bereitstellung aller zum Nachweis hierfür erforderlichen Informationen; dies betrifft insbesondere die Wahrung:

- der allgemeinen Grundsätze für die Verarbeitung nach Ziffer 5
- der Betroffenenrechte nach Ziffer 10
- der Meldepflichten des Auftraggebers nach Ziffer 12
- der Bestimmungen für Auftraggeber und Auftragnehmer nach Ziffer 8
- sowie die Handhabung von Anfragen und Untersuchungen von Aufsichtsbehörden.

Geben anwendbare Normen oder Rechtsbestimmungen dem Auftragnehmer eine weisungswidrige Verarbeitung vor oder hindern diese Rechtsbestimmungen den Auftragnehmer seinen Verpflichtungen aus dieser Richtlinie oder aus der Vereinbarung über die Auftragsverarbeitung nachzukommen, teilt dieser dies unverzüglich seinem Auftraggeber mit, es sei denn die betreffende Rechtsbestimmung untersagt die entsprechende Mitteilung. Dies gilt entsprechend, sollte der Auftragnehmer aus sonstigen Gründen zur Einhaltung der Weisungen seines Auftraggebers außerstande sein. In dem Fall ist der Auftraggeber berechtigt, die Übermittlung der Daten auszusetzen und/oder den Vertrag zur Auftragsverarbeitung zu beenden.

Auftragnehmer sind verpflichtet, Auftraggeber über jegliches rechtlich verbindliche Ersuchen um Offenlegung der personenbezogenen Daten durch eine Behörde in Kenntnis zu setzen, es sei denn dies ist aus anderen Gründen untersagt.

Bei Beendigung der Leistungserbringung müssen Auftragnehmer nach Wahl des Auftraggebers alle von letzterem überlassenen personenbezogenen Daten löschen oder zurückgeben.

Auftragnehmer sind verpflichtet, ihren Auftraggeber und – sofern vorhanden – den hinter diesem stehenden Auftraggeber unverzüglich über geltend gemachte Ansprüche, Anträge oder Beschwerden von Betroffenen zu benachrichtigen.

Konzerninterne Auftraggeber haben gleichfalls konzernfremde Auftragnehmer auf vorstehende Regelungen zu verpflichten.

Die spezifischen Pflichten des Auftragsnehmers gegenüber dem Auftraggeber sind für den Betroffenen drittbegünstigend.

9 Gemeinsame Verantwortung

Für den Fall, dass mehrere Konzerngesellschaften gemeinsam die Mittel und Zwecke der Verarbeitung personenbezogener Daten festlegen (falls vorhanden, zusammen mit einem oder mehreren Dritten) (gemeinsam verantwortliche Stellen/Joint Controller), müssen die Gesellschaften eine Vereinbarung abschließen, in denen ihre Aufgaben und Verantwortlichkeiten gegenüber den Betroffenen, deren Daten sie verarbeiten, festgelegt sind. Dabei sind die vom Konzernbeauftragten für den Datenschutz zur Verfügung gestellten vertraglichen Vorlagen zu beachten.

10 Durchsetzbare Rechte für den Betroffenen

Alle in dieser Ziffer 10 aufgeführten Rechte der Betroffenen und Pflichten der Konzerngesellschaften sind für den Betroffenen drittbegünstigend.

Die nach dieser Ziffer 10 gerichteten Anfragen und Beschwerden müssen innerhalb von einem Monat beantwortet werden. Unter Berücksichtigung der Komplexität und der Anzahl der Anträge kann dieser Zeitraum von einem Monat um höchstens zwei weitere Monate verlängert werden, worüber der Betroffene entsprechend unterrichtet werden muss.

10.1 Rechte des Betroffenen

Ein Betroffener in der EU/EWR hat gegenüber der jeweils verantwortlichen Konzerngesellschaft oder – wenn diese Auftragnehmer ist – gegenüber dem Auftraggeber, folgende Rechte, wie sie in den näheren Einzelheiten des EU-Rechts festgelegt sind:

- das Recht, über die Umstände der Verarbeitung seiner personenbezogenen Daten informiert zu werden. Die Vorgaben des Konzernbeauftragten für den Datenschutz an derartige Informationen sind zu beachten.
- das Recht auf Auskunft darüber, in welcher Art und Weise seine Daten verarbeitet werden und welche Rechte ihm insofern zustehen. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht spezifische Einsichtsrechte in Unterlagen des Arbeitgebers (z. B. Personalakte) vorgesehen sind, so bleiben diese unberührt. Auf Wunsch erhält der Betroffene (ggf. gegen ein angemessenes Entgelt) eine Kopie seiner personenbezogenen Daten, es sei denn schutzwürdige Interessen Dritter stehen dem entgegen.
- das Recht auf Berichtigung oder Ergänzung personenbezogener Daten, sollten diese unrichtig oder unvollständig sein.
- das Recht auf Löschung seiner Daten, wenn er seine Einwilligung widerruft oder die Rechtsgrundlage für die Verarbeitung der Daten fehlt bzw. weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
- das Recht auf Einschränkung der Verarbeitung seiner Daten, wenn er die Richtigkeit bestreitet oder die Daten von der Konzerngesellschaft nicht mehr benötigt werden, aber der Betroffene die Daten für seine Rechtsansprüche braucht. Der Betroffene kann zudem verlangen, dass die Konzerngesellschaft die Verarbeitung seiner Daten einschränkt, wenn sie ansonsten die Daten löschen müsste oder wenn sie einen Widerspruch des Betroffenen prüft.
- das Recht, die ihn betreffenden und von ihm auf Grundlage einer Einwilligung oder im Rahmen eines mit ihm geschlossenen oder angebahnten Vertrages bereitgestellten personenbezogenen Daten in einem gängigen digitalen Format zu erhalten und dieses an einen Dritten zu übermitteln, soweit die Verarbeitung mithilfe automatisierter Verfahren erfolgt und dies technisch machbar ist.

- das Recht, jederzeit dem Direktmarketing zu widersprechen. Ein entsprechendes Einwilligungs- und Widerspruchsmanagement muss sichergestellt werden.
- das Recht, der Verarbeitung auf der Rechtsgrundlage überwiegender Interessen der Konzerngesellschaften oder Dritter zu widersprechen, wenn hierfür Gründe aus seiner besonderen persönlichen Situation vorliegen. Das Widerspruchsrecht besteht allerdings nicht, wenn die Konzerngesellschaft zwingende Gründe für die Verarbeitung hat oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Im Fall eines berechtigten Widerspruchs sind die Daten zu löschen.

Darüber hinaus ist der Betroffene berechtigt, seine Rechte auch gegenüber der datenimportierenden Konzerngesellschaft in einem Drittland geltend zu machen.

10.2 Beschwerdeverfahren

Betroffene sind berechtigt, eine Beschwerde bei dem Konzernbeauftragten für den Datenschutz einzureichen, wenn sie der Ansicht sind, dass gegen diese Richtlinie verstoßen wurde. Solche Beschwerden können per E-Mail eingereicht werden.

Die in der EU/EWR ansässige Konzerngesellschaft, die als Datenexporteur tätig ist, wird Betroffenen, deren personenbezogene Daten innerhalb der EU/EWR erhoben wurden, bei der Feststellung des Sachverhalts und der Geltendmachung ihrer Rechte gemäß dieser Richtlinie gegen die datenimportierende Konzerngesellschaft unterstützen.

Für den Fall, dass der Betroffene mit der Entscheidung der Konzerngesellschaft über die Einhaltung der Vorschriften nicht einverstanden ist (oder aus anderen Gründen mit ihrer Handhabung nicht zufrieden ist), steht es ihm frei, diese Entscheidung oder dieses Verhalten durch Ausübung seiner Rechte anzufechten. Dazu kann er sich an die zuständige Aufsichtsbehörde wenden, insbesondere in dem Land seines gewöhnlichen Aufenthaltsortes, seines Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, oder Klage bei Gericht erheben (Ziffer 11.2). Weitergehende gesetzliche Rechte und Zuständigkeiten bleiben hiervon unberührt.

11 Haftung & Gerichtsstand

11.1 Haftungsbestimmungen

Die Haftung für jeden Verstoß gegen diese Richtlinie, den eine Drittlandsgesellschaft, die Daten aus der EU/EWR erhält, im Rahmen einer Drittlandsverarbeitung begangen hat, wird von der in der EU/EWR ansässigen Konzerngesellschaft („Datenexporteur“) übernommen, die die personenbezogenen Daten zunächst an eine in einem Drittland ansässige Konzerngesellschaft übermittelt hat. Diese Haftung umfasst die Verpflichtung, rechtswidrige Situationen zu beheben sowie materielle und immaterielle Schäden zu ersetzen, die durch einen Verstoß gegen diese Richtlinie durch Konzerngesellschaften aus Drittländern verursacht werden.

Der Datenexporteur ist von dieser Haftung nur dann ganz oder teilweise befreit, wenn er nachweist, dass die Drittlandsgesellschaft, die Daten aus der EU/EWR erhält, für das schadensverursachende Ereignis nicht verantwortlich ist.

11.2 Gerichtsstand

Der Betroffene kann bei den Gerichten am Sitz der verantwortlichen Stelle oder des Auftragnehmers klagen oder an seinem gewöhnlichen Aufenthaltsort.

Der Betroffene, der im Rahmen einer Drittlandsverarbeitung einen Verstoß gegen diese Richtlinie geltend macht, kann seine Rechtsansprüche sowohl gegen die datenimportierende als auch gegen die datenexportierende Gesellschaft in der EU/EWR geltend machen. Daher kann der Betroffene die behauptete Verletzung und die daraus resultierenden Rechtsansprüche vor den zuständigen Gerichten und Aufsichtsbehörden entweder am Sitz der verantwortlichen Stelle oder an seinem gewöhnlichen Aufenthaltsort geltend machen.

Die Bestimmungen zu Haftungs- und Gerichtsstand in dieser Ziffer sind für den Betroffenen drittbegünstigend.

12 Meldung von Datenschutzvorfällen

Im Falle eines potentiellen Verstoßes gegen die Maßgaben zur Datensicherheit („Datenschutzvorfall“) unterliegen die betroffenen Konzerngesellschaften Untersuchungs-, Informations- und Schadensminderungspflichten. Ein Datenschutzvorfall ist dann eine Datenschutzverletzung, wenn eine Verletzung der Datensicherheit vorliegt, die unrechtmäßig zur Löschung, Änderung, unbefugten Offenlegung oder Nutzung personenbezogener Daten führt. Soweit daraus voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen entsteht, müssen entsprechende Ereignisse möglichst innerhalb von 72 Stunden nachdem der Konzerngesellschaft die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde mitgeteilt werden. Zusätzlich müssen die Betroffenen im Falle einer Datenschutzverletzung mit voraussichtlich hohem Risiko für ihre Rechte und Freiheiten über diese Datenschutzverletzung benachrichtigt werden. Auftragnehmer im Sinne der Ziffer 8.2 sind verpflichtet, Datenschutzvorfälle unverzüglich ihrem Auftraggeber zu melden.

Wurde ein Datenschutzvorfall im Verantwortungsbereich einer Konzerngesellschaft festgestellt oder vermutet, ist jeder Mitarbeiter verpflichtet, dies unverzüglich im Rahmen des Information Security Incident Management Prozesses zu melden. Vorgaben, die die Mercedes-Benz Group AG hierzu macht (wie Softwaretools, Anweisungen zu Durchführung der Meldung), sind zu beachten.

Jede Datenschutzverletzung muss dokumentiert werden, und die Dokumentation muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden.

13 Datenschutzorganisation & Sanktionen

13.1 Verantwortung

Die Mitglieder geschäftsführender Organe der Konzerngesellschaften sind verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in dieser Datenschutzrichtlinie EU enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z. B. nationale Meldepflichten). Die Aufgabe einer jeden Führungskraft ist es im Rahmen ihrer Verantwortung, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist der Konzernbeauftragte für den Datenschutz umgehend zu informieren.

13.2 Sensibilisierung & Training

Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter die erforderlichen Datenschutzschulungen, einschließlich des Inhalts und der Handhabung dieser Richtlinie, erhalten und daran teilnehmen, soweit sie ständigen oder regelmäßigen Zugang zu personenbezogenen Daten haben, an der Erhebung von Daten oder an der Entwicklung von Instrumenten zur Verarbeitung personenbezogener Daten beteiligt sind. Die Vorgaben des Konzernbeauftragten für den Datenschutz und von Data Compliance sind zu beachten.

13.3 Organisation

Der Konzernbeauftragte für den Datenschutz ist intern unabhängig von Weisungen hinsichtlich seiner Aufgabenerfüllung. Er wirkt auf die Einhaltung der nationalen und internationalen Datenschutzbestimmungen hin. Er ist für diese Richtlinie verantwortlich und überwacht deren Einhaltung. Wenn Konzerngesellschaften an einem internationalen Zertifizierungssystem für verbindliche Unternehmensregeln zum Datenschutz teilnehmen möchten, müssen sie diese Teilnahme mit dem Konzernbeauftragten für den Datenschutz abstimmen.

Der Konzernbeauftragte für den Datenschutz wird vom Vorstand der Mercedes-Benz Group AG benannt und wird vom Vorstand bei der Erfüllung seiner Aufgaben unterstützt. In der Regel werden Konzerngesellschaften, die gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet sind, den Konzernbeauftragten für den Datenschutz benennen. Der Konzernbeauftragte für den Datenschutz berichtet direkt an den Vorstand der Mercedes-Benz Group AG und an die jeweilige Geschäftsleitung aller Konzerngesellschaften, für die der Konzernbeauftragte für den Datenschutz benannt wurde. Spezifische Ausnahmen sind mit dem Konzernbeauftragten für den Datenschutz abzustimmen.

Der Aufsichtsrat der Mercedes-Benz Group AG ist im Rahmen bestehender Berichtspflichten über den Jahresbericht des Konzernbeauftragten für den Datenschutz zu informieren.

Jeder Betroffene kann sich jederzeit an den Konzernbeauftragten für den Datenschutz wenden, um Bedenken zu äußern, Fragen zu stellen, Informationen anzufordern oder Beschwerden in Bezug auf den Datenschutz oder Fragen der Datensicherheit vorzubringen. Auf Wunsch werden Bedenken und Beschwerden vertraulich behandelt.

Die Kontaktdaten des Konzernbeauftragten für den Datenschutz lauten wie folgt:

Mercedes-Benz Group AG, Konzernbeauftragter für den Datenschutz, HPC E600,
70546 Stuttgart, Germany
Email: data.protection@mercedes-benz.com
Intranet: https://social.intra.corpintra.net/docs/DOC-71499

Die Mercedes-Benz Group hat zudem eine Compliance-Organisation eingerichtet, welche durch gesonderte interne Regelungen näher beschrieben ist. Die Compliance-Organisation unterstützt und überprüft die Konzerngesellschaften in Bezug auf die Einhaltung der datenschutzrechtlichen Vorgaben. Sie konzipiert inhaltlich die Datenschutzschulungen und legt die Kriterien für den Teilnehmerkreis fest.

13.4 Sanktionen

Eine unrechtmäße Verarbeitung personenbezogener Daten oder andere Verstöße gegen die Datenschutzgesetze können in vielen Ländern ordnungs- und strafrechtlich verfolgt werden und auch zu Schadenersatzansprüchen führen. Verstöße, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen. Verstöße gegen diese Richtlinie werden gemäß den internen Regelungen geahndet.

13.5 Auditierung und Kontrollen

Die Einhaltung dieser Richtlinie und der geltenden Datenschutzgesetze wird auf Konzernebene regelmäßig, mindestens einmal jährlich, risikobasiert überprüft. Dies erfolgt mittels einer internen Compliance-Risikobewertung, Audits einschließlich spezifischer Datenschutzthemen und anderer Prüfungen. Der Konzernbeauftragte für den Datenschutz hat das Recht, weitere Prüfungen zu verlangen. Die Ergebnisse sind dem Konzernbeauftragten für den Datenschutz, der verantwortlichen Konzerngesellschaft und ihrem Datenschutzbeauftragten, sofern ein solcher benannt wurde, mitzuteilen.

Der Vorstand der Mercedes-Benz Group AG ist im Rahmen bestehender Berichtspflichten über Ergebnisse zu informieren. Die Ergebnisse der Kontrollen werden der zuständigen Datenschutzaufsichtsbehörde auf Anfrage zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse jede Konzerngesellschaft einem Datenschutzaudit auf Einhaltung der Vorschriften dieser Richtlinie unterziehen.

14 Änderungen dieser Richtlinie und Zusammenarbeit mit Behörden

14.1 Verantwortlichkeiten im Falle von Änderungen

Diese Richtlinie kann in Abstimmung mit dem Konzernbeauftragten für den Datenschutz im Rahmen des definierten Verfahrens zur Änderung der Richtlinien (Richtlinie zum Richtliniemanagement, A 1) geändert werden. Änderungen, die wesentliche Auswirkungen auf diese Datenschutzrichtlinie EU, A 17 haben oder das gewährte Schutzniveau möglicherweise beeinträchtigen (d. h. Änderungen der Verbindlichkeit), sind den zuständigen Datenschutzbehörden unverzüglich zu melden, die die Genehmigung dieser Richtlinie als verbindliche Unternehmensregeln erteilen.

Der Konzernbeauftragte für den Datenschutz ist dafür verantwortlich, eine aktuelle Liste aller Konzerngesellschaften zu führen, die an diese Richtlinie gebunden sind (Mitgeltende Regelung „Liste der an die Datenschutzrichtlinie EU gebundenen Konzerngesellschaften"). Auf der Grundlage dieser Richtlinie erfolgt keine Übermittlung personenbezogener Daten an eine neue Konzerngesellschaft, bis die neue Konzerngesellschaft wirksam an diese Richtlinie gebunden ist und die entsprechenden Compliance Maßnahmen zur Einhaltung der Richtlinie berücksichtigt.

Der Betroffene hat ein Recht auf leichten Zugang zu dieser Richtlinie. Deshalb wird die neueste Version dieser Richtlinie im Internet auf https://www.group.mercedes-benz.com unter Datenschutz veröffentlicht. Diese Vorgabe ist für den Betroffenen drittbegünstigend.

Sofern Änderungen an dieser Richtlinie oder der Liste gebundener Konzerngesellschaften vorgenommen werden, wird die Aufsichtsbehörde der Hauptniederlassung der Mercedes-Benz Group AG einmal pro Jahr hierüber durch den Konzernbeauftragten für den Datenschutz informiert, wobei die Gründe für die Aktualisierung kurz darzulegen sind.

14.2 Zusammenarbeit mit den Behörden

Konzerngesellschaften, die Verarbeitungen in Drittländern durchführen oder sich daran beteiligen, sind verpflichtet, mit der zuständigen Aufsichtsbehörde zusammenzuarbeiten, wenn es um Probleme, Anfragen oder andere Verfahren im Zusammenhang mit der Verarbeitung personenbezogener Daten im oben genannten Zusammenhang geht. Dies beinhaltet die Pflicht, rechtmäßige Audits durch die Aufsichtsbehörden zu akzeptieren. Darüber hinaus sind alle rechtmäßigen Anweisungen der zuständigen Aufsichtsbehörden einzuhalten, die aufgrund von Verarbeitungsprozessen in Drittländern oder von Bestimmungen dieser Richtlinie entstehen.

Die Bestimmungen der Ziffer 14.2 zur Zusammenarbeit mit den Behörden ist für den Betroffenen drittbegünstigend.

14.3 Überwachung und Berichterstattung über die Regelungen von Drittländer

Die Verantwortlichen in Drittlandsgesellschaften müssen den Konzernbeauftragten für den Datenschutz unverzüglich informieren, wenn für ihre Gesellschaft die berechtigte Annahme besteht, dass Gesetze oder andere Vorschriften, die nicht von der EU als Institution oder einem ihrer Mitgliedsstaaten erlassen wurden, folgende Risiken mit sich bringen, wenn die Gesetze oder andere Vorschriften:

- geeignet sind zu verhindern, dass die jeweilige Drittlandsgesellschaft oder eine andere Konzerngesellschaft ihren Verpflichtungen aus dieser Richtlinie im Rahmen von Verarbeitungen in Drittländern nachkommt oder
- erhebliche nachteilige Auswirkungen auf die Rechte haben können, die den Betroffenen im Rahmen dieser Richtlinie bei der Verarbeitung in Drittländern gewährt werden. Dies gilt insbesondere, wenn die lokalen Behörden eine massenhafte, unverhältnismäßige oder undifferenzierte Übermittlung personenbezogener Daten verlangen, die die Grenzen dessen übersteigt, was in einer demokratischen Gesellschaft als erforderlich gilt.

Der Konzernbeauftragte für den Datenschutz bewertet die Auswirkungen und informiert – soweit vorhanden – die zuständige Datenschutzaufsicht, falls die betreffende gesetzliche Anforderung die von der Richtlinie gebotenen Garantien voraussichtlich in erheblichem Maße beeinträchtigt. Diese Bestimmung ist für den Betroffenen drittbegünstigend.

Wird eine Drittlandsgesellschaft von einer Behörde verpflichtet, die Information der Offenlegung von personenbezogenen Daten an die Datenschutzaufsicht zu unterlassen, so unternimmt sie alle angemessenen Anstrengungen, um dieses Verbot so weit wie möglich abzumildern oder aufzuheben und der Datenschutzaufsicht innerhalb dieses Handlungs-spielraums jährlich allgemeine Informationen über die erhaltenen Anfragen zur Verfügung zu stellen (z. B. Anzahl der Anträge um Offenlegung, Art der angefragten Daten, soweit möglich ersuchende Stelle).

Mercedes-Benz Group AG, Mercedesstraße 120, 70327 Stuttgart, Germany, www.group.mercedes-benz.com