(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
5. Januar 2012 (05.01.2012)

(10) Internationale Veröffentlichungsnummer
WO 2012/000751 A1

(51) Internationale Patentklassifikation: *G07C 5/00* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP201 1/059478

(22) Internationales Anmeldedatum: 8. Juni 201 1 (08.06.201 1)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2010 030 794.7 1. Juli 2010 (01 .07.2010) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US):* **BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT** [—/DE]; Petuelring 130, 80809 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nurfür US):* **ZIMMERMANN, Sebastian** [DE/DE]; Görresstraße 17, 80798 München (DE).

(74) Gemeinsamer Vertreter: **BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT;** Patentabteilung AJ-3, 80788 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz V*

(54) Title: METHOD FOR PROCESSING DATA IN ONE OR MORE CONTROL DEVICES OF A VEHICLE, PARTICULARLY OF A MOTOR VEHICLE

(54) Bezeichnung : VERFAHREN ZUM VERARBEITEN VON DATEN IN EINEM ODER MEHREREN STEUERGERÄTEN EINES FAHRZEUGS, INSBESONDERE EINES KRAFTFAHRZEUGS

(57) Abstract: The invention relates to a method for processing data in one or more control devices of a vehicle, particularly of a motor vehicle. According to the invention, a data-protection mode for the control device(s) can be activated by a user of said vehicle. In this data-protection mode, predetermined data to which the control device(s) has/have access during use of the vehicle are prevented from being transmitted out of the vehicle, or transmission thereof is permitted exclusively after entry of a confirmation requested by the vehicle user. Alternatively or additionally in said data-protection mode, predetermined data which were stored in the control device(s) during use of the vehicle are deleted once a predetermined time period has elapsed.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Verarbeiten von Daten in einem oder mehreren Steuergeräten eines Fahrzeugs, insbesondere eines Kraftfahrzeugs. Erfindungsgemäß ist für das oder die Steuergeräte durch einen Benutzer des Fahrzeugs ein Datenschutzmodus aktivierbar. In diesem Datenschutzmodus wird eine Übermittlung von vorbestimmten Daten, auf welche das oder die Steuergeräte während der Fahrzeugnutzung Zugriff haben, aus dem Fahrzeug heraus unterbunden oder ausschließlich nach Eingabe einer beim Benutzer des Fahrzeugs angeforderten Bestätigung zugelassen. Alternativ oder zusätzlich wird in dem Datenschutzmodus eine Löschung von vorbestimmten Daten, welche während der Fahrzeugnutzung in dem oder den Steuergeräten gespeichert werden, nach einer vorbestimmten Zeitspanne durchgeführt.

WO 2012/000751 A1

Verfahren zum Verarbeiten von Daten in einem oder mehreren Steuergeräten eines Fahrzeugs, insbesondere eines Kraftfahrzeugs

Die Erfindung betrifft ein Verfahren zum Verarbeiten von Daten in einem oder mehreren Steuergeräten eines Fahrzeugs, insbesondere eines Kraftfahrzeugs, sowie ein entsprechendes Fahrzeug.

In modernen Fahrzeugen wird heutzutage eine Vielzahl von Daten in entsprechenden Steuergeräten des Fahrzeugs erfasst und abgespeichert. Es ist dabei bekannt, dass diese Daten gegebenenfalls über eine Kommunikationseinrichtung, insbesondere eine Mobilfunkschnittstelle des Fahrzeugs, nach außen an dritte Stellen übertragen werden, z.B. an ein sog. Backend-System, welches diese Daten zu Diagnosezwecken und Servicezwecken bzw. zur Verkehrsdatenerfassung verarbeitet.

In der Druckschrift DE 102 15 887 A 1 ist ein Verfahren zur Erfassung einer Routenhistorie einer von einem Kraftfahrzeug gefahrenen Route beschrieben, wobei während der Fahrt Fahrzustandsdaten gespeichert werden und aus diesen Daten Verkehrsinformationen abgeleitet werden sowie die Fahrzeugpositionen während der Fahrt erfasst werden. Diese Daten werden nach der Beendigung der Fahrt an eine Zentrale übermittelt, welche die Daten weiterverarbeitet, um beispielsweise Stauprognosen für die Zukunft zu treffen.

Im Rahmen der Erfassung und Speicherung von Daten in einem Fahrzeug und deren Übermittlung an externe Stellen ist es problematisch, dass diese Daten schützenswerte personenbezogene oder personenbeziehbare Daten umfassen können, aus denen sich Rückschlüsse auf den Benutzer des Fahrzeugs bzw. dessen Verhalten ziehen lassen. Es besteht somit das Bedürfnis, dass ein Fahrzeugnutzer Einfluss darauf nehmen kann, welche Daten in dem Fahrzeug abgespeichert werden bzw. an Dritte übermittelt werden, um hierdurch einem Datenmissbrauch durch unbefugte Dritte entgegenzuwirken.

Aufgabe der Erfindung ist es deshalb, ein Verfahren zum Verarbeiten von Daten in einem oder mehreren Steuergeräten eines Fahrzeugs anzugeben, bei dem ein Benutzer auf die Verarbeitung der Daten Einfluss nehmen kann und insbesondere die Weitergabe bzw. Speicherung von schützenswerten Daten steuern kann.

Diese Aufgabe wird durch das Verfahren gemäß Patentanspruch 1 bzw. das Fahrzeug gemäß Patentanspruch 14 gelöst. Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen definiert.

Das erfindungsgemäße Verfahren dient zum Verarbeiten von Daten in einem oder mehreren Steuergeräten eines Fahrzeugs, insbesondere eines Kraftfahrzeugs, wie z.B. eines Personenkraftwagens. Dabei ist für das oder die Steuergeräte durch einen Benutzer des Fahrzeugs ein Datenschutzmodus aktivierbar, d.h. ein Benutzer hat über eine geeignete Benutzerschnittstelle bzw. Mensch-Maschine-Schnittstelle die Möglichkeit, diesen Datenschutzmodus im Fahrzeug zu aktivieren. Diese Benutzerschnittstelle ist vorzugsweise eine Schnittstelle im Fahrzeug, insbesondere in der Form einer Kontrolleinheit mit entsprechendem Display. Gegebenenfalls besteht jedoch auch die Möglichkeit, dass die Benutzerschnittstelle eine Schnittstelle außerhalb des Fahrzeugs ist, beispielsweise ein Display auf einem Computer bzw. einem Endgerät, welches mit dem Fahrzeug kommunizieren kann. Auf diese Weise wird die Möglichkeit geschaffen, dass ein Benutzer den Datenschutzmodus auch dann aktivieren kann, wenn er sieh entfernt vom Fahrzeug befindet. Im Folgenden umfasst der Begriff der Benutzerschnittstelle sowohl eine Benutzerschnittstelle im Fahrzeug als auch gegebenenfalls eine entfernt vom Fahrzeug angeordnete Benutzerschnittstelle.

Basierend auf dem erfindungsgemäßen Verfahren wird im Rahmen des aktivierten Datenschutzmodus eine Übermittlung von vorbestimmten Daten, auf weiche das oder die Steuergeräte während der Fahrzeugnutzung durch den Fahrzeugnutzer Zugriff haben, aus dem Fahrzeug heraus unterbunden oder ausschließlich nach Eingabe einer beim Benutzer des Fahrzeugs angeforderten Bestätigung zugelassen, wobei diese Bestätigung wiederum über eine geeignete Benutzerschnittstelle vom Fahrzeugnutzer angefordert werden kann, der über diese Benutzerschnittstelle dann die Bestätigung eingeben kann bzw. verweigern kann. Alternativ bzw. zusätzlich kann der Datenschutzmodus auch derart ausgestaltet sein, dass eine Löschung von vorbestimmten Daten, welche während der Fahrzeugnutzung in dem oder den Steuergeräten gespeichert werden, nach einer vorbestimmten Zeitspanne durchgeführt wird. Der Begriff des Benutzers des Fahrzeugs ist im Sinne der Erfindung weit zu verstehen. Es kann sich z.B. um den Fahrer des Fahrzeugs handeln, jedoch auch um eine andere Person, welche basierend auf einer entsprechenden Autorisierung Zugang zum Fahrzeug bzw. Zugriff auf Steuergeräte des Fahrzeugs hat.

Der Benutzer des Fahrzeugs kann z.B. ein Angestellter einer Mietwagenfirma sein, der den Datenschutzmodus aktivieren kann, um insbesondere die persistente Speicherung von Daten der Fahrzeugmieter im Fahrzeug zu verhindern. Der Datenschutzmodus kann dabei z.B. über eine internetbasierte Schnittstelle zum Fahrzeug aktiviert werden.

Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass einem Fahrzeug nutzer die Möglichkeit gegeben wird, die Übermittlung von Daten an externe Stellen nur unter bestimmten Bedingungen zuzulassen bzw. eine persistente Speicherung von Daten lokal im Fahrzeug zu verhindern. Auf diese Weise kann erreicht werden, dass bestimmte schützenswerte Daten nicht gegen den Willen des Nutzers an unbefugte Dritte gelangen können, wodurch ein Missbrauch solcher Daten verhindert werden kann.

In einer besonders bevorzugten Ausführungsform umfassen die vorbestimmten Daten personenbezogene und/oder personenbeziehbare Daten des Benutzers des Fahrzeugs, wobei der Begriff der personenbezogenen und/oder personenbeziehbaren Daten weit zu verstehen ist und jede Art von Daten umfassen kann, welche mit dem Benutzer in Zusammenhang gebracht werden können. Insbesondere sind solche Daten persönliche Daten des Benutzers, wie z.B. Authentisierungsdaten, persönliche Zertifikate, Passwörter und dergleichen, oder Daten, welche das Verhalten und/oder eine oder mehrere Aktionen des Benutzers während der Benutzung des Fahrzeugs charakterisieren, insbesondere die vom Benutzer zurückgelegte Fahrtroute bzw. Fahrzeugpositionen entlang der Fahrtroute bzw. das Fahrverhalten des Benutzers in der Form von Geschwindigkeits- und/oder Beschleunigungsdaten und dergleichen. Weiterhin können personenbezogene und/oder personenbeziehbare Daten über eine Benutzerschnittstelle eingegebene Daten umfassen und/oder Daten, welche aus einem Endgerät des Benutzers des Fahrzeugs, beispielsweise aus seinem Mobiltelefon, ausgelesen werden, bzw. auch von außerhalb des Fahrzeugs empfangene Daten. Solche Daten betreffen beispielsweise von dem Benutzer eingegebene Navigationsziele, von dem Benutzer gewählte Telefonnummern bzw. vom Benutzer empfangene Telefonanrufe, von dem Benutzer ausgesendete oder empfangene Nachrichten (z.B. SMS oder Emails) oder während der Benutzung des Fahrzeugs in eine Maske eingegebene Informationen, wie Logins, Passwörter und dergleichen.

Die personenbezogenen und/oder personenbeziehbaren Daten können ferner vom Benutzer vorgenommene Einstellungen des Fahrzeugs umfassen, wie z.B. Außenspiegel-

einstellungen, Einstellungen der Sitzposition, der Lenkradposition und dergleichen. Bei Aktivierung des Datenschutzmodus wird insbesondere eine persistente Speicherung dieser Daten verhindert, d.h. die Daten werden nach einer vorbestimmten Zeitspanne, beispielsweise nach der Beendigung einer Fahrt, wieder gelöscht, bzw. die ursprünglichen Positionen werden wieder eingestellt.

In einer weiteren, besonders bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird nach Aktivierung des Datenschutzmodus dennoch unter bestimmten Umständen die Übertragung von Daten aus dem Fahrzeug heraus zugelassen. Insbesondere werden im Falle eines Unfalls und/oder einer Notfallsituation weiterhin die Fahrzeugposition des Fahrzeugs und/oder weitere Fahrzeugdaten aus dem Fahrzeug heraus übermittelt. Diese Daten gelangen dabei an eine dritte Stelle, welche entsprechende Rettungsmaßnahmen einleiten kann. Das Ereignis des Unfalls kann dabei beispielsweise durch das Auslösen von Airbags detektiert werden, und eine Notfallsituation kann beispielsweise dann vorliegen, wenn der Fahrzeugbenutzer eine Notfalltaste im Fahrzeug betätigt, über welche eine Kommunikation mit einem Backend-System aufgenommen wird.

Die oben beschriebene Zeitspanne, nach deren Ablauf die Löschung von vorbestimmten Daten durchgeführt wird, ist in einer Ausgestaltung der Erfindung nicht durch ein explizites Zeitintervall gegeben, sondern an ein Ereignis gekoppelt, insbesondere an die Beendigung einer Benutzung des Fahrzeugs. Die Benutzung eines Fahrzeugs erstreckt sich dabei über die Zeitspanne zwischen der Inbetriebnahme des Fahrzeugs (z.B. detektiert durch das Anschalten der Zündung) bis zum anschließenden Abstellen des Fahrzeugs (z.B. detektiert durch das Abschalten der Zündung). Gegebenenfalls besteht auch die Möglichkeit, dass die vorbestimmte Zeitspanne von dem Benutzer verändert wird und über ein längeres, vorbestimmtes Zeitintervall ausgedehnt wird oder auf ein kürzeres Zeitintervall verkürzt wird.

In einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens wird ein aktivierter Datenschutzmodus automatisch bei Vorliegen von einer oder mehreren Bedingungen deaktiviert, insbesondere am Ende einer Benutzung des Fahrzeugs und/oder bei Erreichen eines im Fahrzeug eingegebenen Routen-Ziels und/oder wenn das Fahrzeug länger als eine vorbestimmte Zeitspanne abgestellt ist.

Gegebenenfalls kann der Fahrzeugnutzer das Ende eines Datenschutzmodus über eine Benutzerschnittstelle spezifizieren. Zum Beispiel kann der Benutzer über die Benutzerschnittstelle festlegen, dass der Datenschutzmodus sofort deaktiviert wird. Alternativ oder zusätzlich kann der Benutzer gegebenenfalls auch den zukünftigen Zeitpunkt der Beendigung des Datenschutzmodus verändern. Insbesondere kann er am Ende der Fahrt den Datenschutzmodus auf die nächste Fahrzeugnutzung verlängern, wenn er sein Fahrzeug z.B. nur temporär abstellt.

In einer weiteren, besonders bevorzugten Ausgestaltung der Erfindung wird über eine Benutzerschnittstelle ein aktivierter Datenschutzmodus, insbesondere in Kombination mit Informationen zu dem Datenschutzmodus, dem Fahrzeugnutzer z.B. visuell oder akustisch angezeigt. Auf diese Weise ist der Benutzer immer über den aktuellen Betriebsmodus der Steuergeräte informiert.

In einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens beinhaltet der Datenschutzmodus eine durch den Benutzer des Fahrzeugs über eine Benutzerschnittstelle aktivierbare Löschfunktion, über welche der Benutzer eine oder mehrere Kategorien von vorbestimmten Daten löschen kann. Insbesondere besteht dabei gegebenenfalls die Möglichkeit, dass alle vorbestimmten Daten, welche im Rahmen des Datenschutzmodus geschützt werden, durch eine einzige Benutzereingabe gelöscht werden. Zum Beispiel kann ein Angestellter einer Mietwagenfirma manuell die Löschfunktion nach der Rückgabe eines vermieteten Fahrzeugs aktivieren.

In einer weiteren Ausführungsform der Erfindung kann der Benutzer über eine Benutzerschnittstelle festlegen, für welche vorbestimmten Daten und insbesondere welche Kategorien von vorbestimmten Daten im aktivierten Datenschutzmodus die Übertragung aus dem Fahrzeug heraus unterbunden oder nur bei Bestätigung zugelassen werden soll und/oder die Löschung nach einer vorbestimmten Zeitspanne durchgeführt werden soll. Der Benutzer kann somit den Datenschutzmodus individuell nach seinen Bedürfnissen konfigurieren.

Die vorbestimmten Daten, welche gemäß dem oben beschriebenen Datenschutzmodus geschützt werden, können Daten sein, welche von beliebigen Steuergeräten im Fahrzeug verarbeitet werden. In einer besonders bevorzugten Ausführungsform werden die vorbe-

stimmten Daten zumindest teilweise in einem oder mehreren Steuergeräten eines Informations- und Unterhaltungssystems im Fahrzeug verarbeitete Daten. Das Informations- und Unterhaltungssystem, welches insbesondere auch unter dem Begriff Infotainment-System bekannt ist, stellt im Fahrzeug Funktionen im Bereich Komfort und Sicherheit bereit und ist eine hinlänglich aus dem Stand der Technik bekannte Einheit.

Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein Fahrzeug, insbesondere ein Kraftfahrzeug, umfassend ein oder mehrere Steuergeräte, wobei für das oder die Steuergeräte durch einen Benutzer des Fahrzeugs ein Datenschutzmodus basierend auf dem erfindungsgemäßen Verfahren und insbesondere basierend auf einer oder mehreren der oben beschriebenen Varianten des erfindungsgemäßen Verfahrens aktivierbar ist.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend anhand der beigefügten Fig. 1 detailliert beschrieben.

Gemäß Fig. 1 wird die Verwendung eines Datenschutzmodus für ein Steuergerät 2 in einem Fahrzeug-Infotainment-System eines Fahrzeugs 1 beschrieben, wobei das Infotainment-System unter anderem die Funktionalitäten der GPS-basierten Fahrzeugnavigation, der Kommunikation des Fahrzeugs mit dem Fahrer und nach außen und der Wiedergabe von Multimediainhalten umfasst. Die Steuereinheit ist dabei vorzugsweise die sog. Haupteinheit (englisch: Head Unit) des Infotainment-Systems. Im normalen Betriebsmodus kann das Fahrzeug über eine entsprechende drahtlose Schnittstelle, wie z.B. eine Mobilfunkschnittstelle, mit einem Backend-System aus einer Mehrzahl von Servern kommunizieren, wobei ein Server dieses Backend-Systems mit Bezugszeichen 3 angedeutet ist und die Kommunikation zwischen Fahrzeug 1 und dem Backend-Server 3 durch den Doppelpfeil P wiedergegeben ist. Das Backend-System, welches in der Regel vom Fahrzeughersteller betrieben wird, kann verschiedene Funktionalitäten übernehmen, beispielsweise kann an das Backend-System die aktuelle Fahrzeugposition bzw. Informationen zum Verkehrsfluss bzw. Routenberechnungsdaten des Navigationssystems des Fahrzeugs übermittelt werden. Diese Daten werden genutzt, um Mehrwertdienste bereitzustellen. Beispielsweise können dem Nutzer Informationen zu der von ihm gefahrenen Route, insbesondere Stauinformationen, bereitgestellt werden. Diese Information kann sich der Fahrzeugnutzer

dann auf einer entsprechenden Mensch-Maschine-Schnittstelle im Fahrzeug anzeigen lassen.

Im Rahmen der Kommunikation des Fahrzeugs mit einem Backend-System ist es problematisch, dass die ausgetauschten Daten oftmals benutzerspezifische Daten sind, welche Rückschlüsse auf die Person des Benutzers bzw. dessen Verhalten bzw. dessen Gewohnheiten ermöglichen. Zwar werden diese Daten zum Schutz vor Missbrauch anonymisiert, jedoch hat ein Fahrzeugnutzer nicht die Möglichkeit, die Übertragung solcher Daten und deren Weiterverarbeitung in einem Backend-System zu verhindern. Mit der im Folgenden beschriebenen Erfindung wird es nunmehr einem Fahrzeugnutzer ermöglicht, die Übertragung von Daten zwischen dem Fahrzeug 1 und dem Backend-System 3 zu kontrollieren. Dies wird durch die Implementierung eines Datenschutzmodus in dem Steuergerät 2 erreicht, wobei dieser Datenschutzmodus durch den Fahrzeugnutzer über eine geeignete Benutzerschnittstelle im Fahrzeug aktiviert werden kann. Gegebenenfalls besteht dabei auch die Möglichkeit, dass ein Benutzer entfernt über sein Endgerät, beispielsweise sein Mobiltelefon, einen solchen Datenschutzmodus basierend auf einer Kommunikation zwischen Mobiltelefon und Fahrzeug aktiviert bzw. deaktiviert. Um einen solchen Datenschutzmodus zu ermöglichen, wird die Software des Steuergeräts 2 geeignet modifiziert, um Übertragungen aus dem Fahrzeug heraus an das Backend-System zu unterbinden bzw. nur unter vorbestimmten Bedingungen zuzulassen.

Die im Rahmen des Datenschutzmodus geschützten Daten, für welche eine Übertragung aus dem Fahrzeug heraus unterbunden bzw. nur eingeschränkt möglich ist, können beliebige Daten sein, welche in irgendeiner Weise einen Bezug zum Benutzer haben. Solche Daten sind insbesondere Informationen, welche den Benutzer bzw. Eigenschaften des Benutzers bzw. das Verhalten bzw. Aktionen des Benutzers spezifizieren. Beispiele von benutzerbezogenen Daten sind die vom Benutzer gefahrene Fahrtstrecke bzw. die aktuelle Fahrzeugposition bzw. persönliche Zertifikate des Benutzers, wie z.B. eine Authentisierung des Benutzers für Email-Abruf, den Aufbau eines VPN-Kanals und dergleichen.

Der Datenschutzmodus im Fahrzeug kann dabei verschieden ausgestaltet sein. Beispielsweise besteht die Möglichkeit, dass jegliche Übertragung von personenbezogenen und/oder personenbeziehbaren Daten aus dem Fahrzeug heraus unterbunden wird bzw.

für bestimmte personenbezogene und/oder personenbeziehbare Daten eine Übertragung aus dem Fahrzeug heraus zugelassen wird und für andere personenbezogene und/oder personenbeziehbare Daten eine Übertragung nach außen heraus nicht zugelassen wird. Ebenso besteht die Möglichkeit, dass eine Übertragung für jede Art von personenbezogenen und/oder personenbeziehbaren Daten bzw. bestimmte personenbezogene und/oder personenbeziehbare Daten dann zugelassen wird, wenn eine vom Steuergerät angeforderte Bestätigung durch den Fahrzeugnutzer in eine entsprechende Benutzerschnittstelle ihm Fahrzeug eingegeben wird. Das heißt, nur nach expliziter Bestätigung einer vorgesehenen Übertragung von Informationen aus dem Fahrzeug heraus wird diese Übertragung auch durchgeführt.

In einer Variante des erfindungsgemäßen Verfahrens sind solche Daten vom Datenschutzmodus ausgenommen, welche bei einem Unfall bzw. einer Notfallsituation an das Backend-System übermittelt werden. Solche Daten umfassen insbesondere die über GPS ermittelte Position des Fahrzeugs, so dass vom Backend-System Rettungsdienste an den Ort des Fahrzeugs geschickt werden können. Ein Unfall kann beispielsweise basierend auf der Detektion des Auslösens von Airbags oder anderen Schutzsystemen im Fahrzeug detektiert werden. Ebenso besteht die Möglichkeit, dass eine Notfallsituation über die Betätigung einer Notfalltaste im Fahrzeug durch den Fahrzeugnutzer ausgelöst wird, woraufhin eine Kommunikation zu dem Backend-System, insbesondere über Mobilfunk, aufgebaut wird, wobei im Rahmen der Kommunikation auch die Fahrzeugposition übermittelt wird.

Der oben beschriebene Datenschutzmodus kann in geeigneter Weise auch auf die lokale Speicherung von benutzerbezogenen Daten im Steuergerät des Fahrzeugs erweitert werden. Gemäß dieser Erweiterung werden vorbestimmte benutzerbezogene Daten nicht persistent im Fahrzeug gespeichert, sondern nach einer vorbestimmten Zeitspanne, insbesondere nach einem sog. Life-Cycle des Fahrzeugs wieder gelöscht. Der Life-Cycle spezifiziert dabei ein Benutzungsintervall des Fahrzeugs, welches insbesondere ab dem Einschalten der Zündung des Fahrzeugs bis zum nächsten Abstellen des Fahrzeugs läuft. Mit dieser Erweiterung wird sichergestellt, dass im Fahrzeug erfasste bzw. über eine entsprechende Benutzerschnittstelle eingegebene Daten im nächsten Life-Cycle nicht mehr zur Verfügung stehen, so dass im Falle, dass im nächsten Life-Cycle ein anderer Benutzer das Fahrzeug fährt, dieser keinen Zugriff auf Informationen betreffend den Vorbenut-

zer hat. Diese Variante der Erfindung kann im Rahmen einer verteilten Nutzung eines Fahrzeugs eingesetzt werden, beispielsweise bei der Verwendung des Fahrzeugs von einer Mietwagenfirma, da in diesem Fall das Fahrzeug von vielen unterschiedlichen Nutzern gefahren wird. Die am Ende eines Life-Cycles aus dem Fahrzeug gelöschten Daten können wiederum beliebige benutzerbezogene Daten sein, beispielsweise von dem Benutzer während seiner Fahrzeugnutzung gewählte Telefonrufnummern, von dem Benutzer empfangene Anrufe, von dem Benutzer vorgenommene Einstellungen am Fahrzeug, wie z.B. die Einstellung der Klimaanlage, der Außenspiegel, der Sitzposition, der Lenkradposition und dergleichen. Die Daten können auch von dem Benutzer über eine Benutzerschnittstelle des Fahrzeugs eingegebene Login oder ausgefüllte Suchmasken umfassen, beispielsweise Suchmasken eines bei der Fahrzeugnutzung verwendeten Webbrowsers. Ebenso können die Daten von dem Benutzer ausgesendete oder im Fahrzeug empfangene Nachrichten, wie z.B. Emails, SMS-Nachrichten und dergleichen, betreffen. Weiterhin könnten diese Daten auch auf Stationstasten gespeicherte Sender, sonstige Einstellungen frei programmierbarer Tasten, Lesezeichen oder sonstige MMI-Einstellungen umfassen. All diese Informationen, welche während der Fahrt temporär gespeichert sind, werden nach dem Ende der Fahrt dann permanent gelöscht.

In einer weiteren Ausgestaltung der Erfindung besteht die Möglichkeit, dass der Datenschutzmodus nach dem Ende einer Fahrt bzw. eines Life-Cycles automatisch beendet wird und beim nächsten Life-Cycle durch den Benutzer wieder explizit aktiviert werden muss. Gegebenenfalls kann der Fahrzeugnutzer dabei am Ende eines Life-Cycles spezifizieren, dass der Datenschutzmodus auf den nächsten Life-Cycle verlängert wird, beispielsweise wenn der Fahrzeugnutzer seine Fahrt nur temporär unterbricht. Ebenso ist es möglich, dass der Fahrzeugnutzer die nach einem Life-Cycle durchgeführte Löschung von lokal im Fahrzeug gespeicherten personenbezogenen und/oder personenbeziehbaren Daten auf den nächsten Life-Cycle hinausschiebt, so dass er noch länger auf die bereits von ihm eingegebenen persönlichen Daten Zugriff hat und diese nicht neu eingeben muss.

Im Rahmen der Erfindung kann die Beendigung des Datenschutzmodus nicht nur an das Ende eines Life-Cycles, sondern auch an beliebige andere Bedingungen geknüpft sein. Beispielsweise kann der Datenschutzmodus erst nach einem längeren Fahrzeugstillstand deaktiviert werden bzw. erst nach Erreichen eines von dem Fahrer des Fahrzeugs spezifi-

zierten Routenziels. In einer weiteren Ausgestaltung des erfindungsgemäßen Datenmodus wird die Aktivierung des Datenschutzmodus auf einer Mensch-Maschine-Schnittstelle im Fahrzeug geeignet angezeigt, beispielsweise über ein aussagekräftiges Icon auf einem Display, wobei gegebenenfalls zusätzliche Informationen zu dem Datenschutzmodus auf der Mensch-Maschine-Schnittstelle wiedergegeben werden, beispielsweise die Information, welche Daten im Rahmen des Datenschutzmodus nicht nach außen übertragen werden bzw. nach Beendigung der Fahrt wieder gelöscht werden.

Gegebenenfalls kann der oben beschriebene Datenschutzmodus um eine Löschfunktion erweitert werden, so dass alle personenbezogenen und/oder personenbeziehbaren Daten nach der Aktivierung der Löschfunktion gelöscht werden, wobei die Löschfunktion durch den Fahrzeug nutzer über eine entsprechende Mensch-Maschine-Schnittstelle aktiviert werden kann. Es können somit z.B. auf einmal alle vom Benutzer während der Fahrt spezifizierten Navigationsziele, seine Anruflisten, seine Musikabspiellisten, die von ihm ausgesendeten bzw. empfangenen Nachrichten, seine Logins, persönliche Zertifikate sowie beliebige andere personenbezogene und/oder personenbeziehbare Daten gelöscht werden.

Das im Vorangegangenen beschriebene erfindungsgemäße Verfahren weist eine Reihe von Vorteilen auf. Insbesondere kann die Verwendung von personenbezogenen und/oder personenbeziehbaren Daten eines Fahrzeugnutzers durch unbefugte Dritte über die Aktivierung eines Datenschutzmodus unterbunden werden. Je nach Anwendungsfall kann dabei der Datenschutzmodus unterschiedlich ausgestaltet sein. Insbesondere kann eine Übertragung von personenbezogenen und/oder personenbeziehbaren Daten aus dem Fahrzeug heraus generell unterbunden werden bzw. nur nach expliziter Bestätigung durch den Benutzer erlaubt werden. Der Datenschutzmodus kann auch auf die Speicherung von personenbezogenen und/oder personenbeziehbaren Daten im Fahrzeug erweitert werden, wobei diese Daten bei aktiviertem Datenschutzmodus nicht persistent im Fahrzeug hinterlegt werden, sondern nach einer vorbestimmten Zeitspanne, insbesondere nach der Beendigung eines Life-Cycles des Fahrzeugs, wieder gelöscht werden. Gegebenenfalls kann der Datenschutzmodus auch derart ausgestaltet sein, dass er nur die persistente Speicherung von personenbezogenen und/oder personenbeziehbaren Daten verhindert und sich nicht auf die Unterbindung der Übertragung von Daten aus dem Fahrzeug heraus bezieht.

Patentansprüche

1. Verfahren zum Verarbeiten von Daten in einem oder mehreren Steuergeräten (2) eines Fahrzeugs (1), insbesondere eines Kraftfahrzeugs,
dadurch gekennzeichnet, dass
für das oder die Steuergeräte (2) durch einen Benutzer des Fahrzeugs (1) ein Datenschutzmodus aktivierbar ist, wobei in dem Datenschutzmodus eine Übermittlung von vorbestimmten Daten, auf weiche das oder die Steuergeräte (2) während der Fahrzeugnutzung (1) Zugriff haben, aus dem Fahrzeug (1) heraus unterbunden wird oder ausschließlich nach Eingabe einer beim Benutzer des Fahrzeugs (1) angeforderten Bestätigung zugelassen wird und/oder wobei in dem Datenschutzmodus eine Löschung von vorbestimmten Daten, welche während der Fahrzeugnutzung (1) in dem oder den Steuergeräten (2) gespeichert werden, nach einer vorbestimmten Zeitspanne durchgeführt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die vorbestimmten Daten personenbezogene und/oder personenbeziehbare Daten des Benutzers des Fahrzeugs (1) umfassen, insbesondere persönliche Daten des Benutzers und/oder Daten, welche das Verhalten und/oder eine oder mehrere Aktionen des Benutzers während der Fahrzeugnutzung (1) charakterisieren.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die personenbezogenen und/oder personenbeziehbaren Daten eine oder mehrere, bei der Fahrt des Fahrzeugs (1) erfasste Fahrzeugpositionen umfassen und/oder eine oder mehrere Informationen, welche die durch den Benutzer des Fahrzeugs (1) zurückgelegte Fahrroute spezifizieren.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, dass die personenbezogenen und/oder personenbeziehbaren Daten über eine Benutzerschnittstelle eingegebene Daten umfassen und/oder Daten, welche aus einem Endgerät des Benutzers des Fahrzeugs (1) ausgelesen werden, und/oder von außerhalb des Fahrzeugs empfangene Daten.

5. Verfahren nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, dass die personenbezogenen und/oder personenbeziehbaren Daten vom Benutzer des Fahrzeugs (1) vorgenommene Einstellungen des Fahrzeugs umfassen.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im Datenschutzmodus im Falle eines Unfalls des Fahrzeugs (1) und/oder einer Notfallsituation weiterhin die Fahrzeugposition des Fahrzeugs (1) und/oder weitere Fahrzeugdaten aus dem Fahrzeug heraus übermittelt werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die vorbestimmte Zeitspanne an ein Ereignis gekoppelt ist, insbesondere an die Beendigung einer Fahrzeugnutzung, wobei die vorbestimmte Zeitspanne von dem Benutzer des Fahrzeugs (1) vorzugsweise verändert werden kann

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass ein aktivierter Datenschutzmodus automatisch bei Vorliegen von einer oder mehreren Bedingungen deaktiviert wird, insbesondere am Ende einer Fahrzeugnutzung (1) und/der bei Erreichen eines im Fahrzeug (1) eingegebenen Routenziels und/oder wenn das Fahrzeug länger als eine vorbestimmte Zeitspanne abgestellt ist.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Benutzer des Fahrzeugs (1) über eine Benutzerschnittstelle das Ende eines aktivierten Datenschutzmodus spezifizieren kann.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass dem Benutzer des Fahrzeugs (1) über eine Benutzerschnittstelle ein aktivierter Datenschutzmodus, insbesondere in Kombination mit Informationen zu dem Datenschutzmodus, angezeigt wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Datenschutzmodus eine durch den Benutzer des Fahrzeugs (1) über eine Benutzerschnittstelle aktivierbare Löschfunktion beinhaltet, über welche der Benutzer eine oder mehrere Kategorien von vorbestimmten Daten löschen kann.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Benutzer des Fahrzeugs (1) über eine Benutzerschnittstelle festlegen kann, für welche vorbestimmten Daten und insbesondere für welche Kategorien von vorbestimmten Daten im aktivierten Datenschutzmodus die Übertragung aus dem Fahrzeug (1) heraus unterbunden oder nur bei Bestätigung zugelassen werden soll und/oder die Löschung nach einer vorbestimmten Zeitspanne durchgeführt werden soll.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die vorbestimmten Daten zumindest teilweise in einem oder mehreren Steuergeräten (2) eines Informations- und Unterhaltungssystems im Fahrzeug (1) verarbeitet werden.

14. Fahrzeug, insbesondere Kraftfahrzeug, umfassend ein oder mehreren Steuergeräte (2), dadurch gekennzeichnet, dass
für das oder die Steuergeräte (2) durch einen Benutzer des Fahrzeugs (1) ein Datenschutzmodus aktivierbar ist, wobei in dem Datenschutzmodus eine Übermittlung von vorbestimmten Daten, auf weiche das oder die Steuergeräte (2) während der Fahrzeugnutzung Zugriff haben, aus dem Fahrzeug (1) heraus unterbunden wird oder ausschließlich nach Eingabe einer beim Benutzer des Fahrzeugs (1) angeforderten Bestätigung zugelassen wird und/oder wobei in dem Datenschutzmodus eine Löschung von vorbestimmten Daten, welche während der Fahrzeugnutzung (1) in dem oder den Steuergeräten (2) gespeichert werden, nach einer vorbestimmten Zeitspanne durchgeführt wird.

15. Fahrzeug nach Anspruch 13, dadurch gekennzeichnet, dass das Fahrzeug derart ausgestaltet ist, dass in dem Fahrzeug ein Verfahren nach einem der Ansprüche 2 bis 13 durchführbar ist.

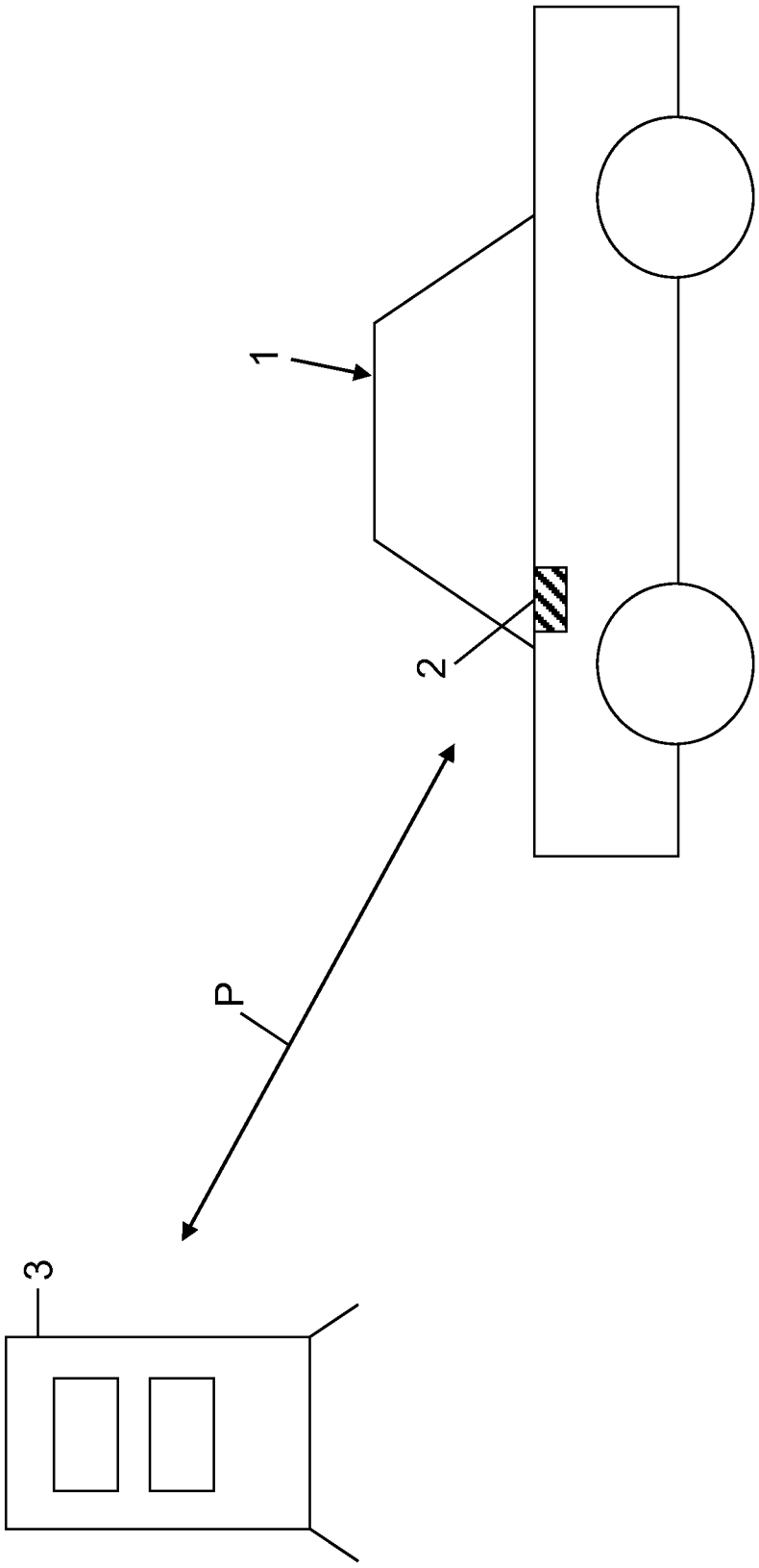

Fig. 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/059478

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C5/00
ADD.

According to International Patent Classification (IPC) orto both national Classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (Classification System followed by Classification Symbols)
G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
X Y	US 2007/263632 Al (SOBUE TSUNEO [JP] ET AL) 15 November 2007 (2007-11-15) abstract Paragraph [0007] - paragraph [0020] Paragraph [0050] - paragraph [0064] -----	1-6, 12-15 7-11
Y	DE 10 2004 026205 Al (MITSUBISHI ELECTRIC CORP [JP]) 5 January 2005 (2005-01-05) abstract paragraph [0009] - paragraph [0010] paragraph [0036] - paragraph [0041] -----	7-11
A	DE 10 2009 045711 Al (CONTINENTAL TEVES AG & CO 0HG [DE]) 22 Apri l 2010 (2010-04-22) abstract paragraph [0023] paragraph [0038] -----	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general State of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" documentwhich maythrow doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but laterthan the priority date claimed

"T" later document published after the international filing date or priority date and not in conflictwith the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such docu¬ ments, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2011	19/08/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Teutl off, Ivo

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/059478

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007263632 A1	15-11-2007	JP 2007264730 A	11-10-2007
DE 102004026205 A1	05-01-2005	CN 1573295 A	02-02-2005
		JP 4270946 B2	03-06-2009
		JP 2004361116 A	24-12-2004
		US 2006190173 A1	24-08-2006
		US 2005004755 A1	06-01-2005
DE 102009045711 A1	22-04-2010	EP 2350979 A1	03-08-2011
		WO 2010043659 A1	22-04-2010

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2011/059478

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G07C5/00
ADD..

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter MindestprUfstoff (Klassifikationssystem und Klassifikationssymbole)
G07C

Recherchierte, aber nicht zum MindestprUfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal , WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y	US 2007/263632 AI (SOBUE TSUNEO [JP] ET AL) 15. November 2007 (2007-11-15) Zusammenfassung Absatz [0007] - Absatz [0020] Absatz [0050] - Absatz [0064] -----	1-6, 12-15 7-11
Y	DE 10 2004 026205 AI (MITSUBISHI ELECTRIC CORP [JP]) 5. Januar 2005 (2005-01-05) Zusammenfassung Absatz [0009] - Absatz [0010] Absatz [0036] - Absatz [0041] -----	7-11
A	DE 10 2009 045711 AI (CONTINENTAL TEVES AG & CO 0HG [DE]) 22. April 2010 (2010-04-22) Zusammenfassung Absatz [0023] Absatz [0038] -----	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. August 2011	19/08/2011
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Teutloff, Ivo

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2011/059478

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2007263632 A1	15-11-2007	JP 2007264730 A	11-10-2007
DE 102004026205 A1	05-01-2005	CN 1573295 A	02-02-2005
		JP 4270946 B2	03-06-2009
		JP 2004361116 A	24-12-2004
		US 2006190173 A1	24-08-2006
		US 2005004755 A1	06-01-2005
DE 102009045711 A1	22-04-2010	EP 2350979 A1	03-08-2011
		WO 2010043659 A1	22-04-2010