

# DAIMLER

Protección de datos y privacidad.  
Código de conducta de Daimler

## Nuestro lema:

**Vehículos de primera, servicios de primera, privacidad de primera**

## Nuestros desafíos:

Deseos y exigencias de nuestros clientes

Creciente sensibilidad de nuestros clientes

No existe un marco legal homogéneo que regule la protección de datos

Protección de datos en los procesos de transferencia internacional de datos

Nivel de protección de datos personales adecuado en todo el Grupo

Imagen unificada respecto a nuestra competencia

Un sistema de gestión de protección y de seguridad de datos integrador

## Nuestras soluciones:

Acercamiento global

Nivel de protección de datos adecuado gracias a la autorregulación

La protección de datos supone una ventaja de calidad y respecto a la competencia

Organización de protección de datos interna

Órgano interno para supervisar el cumplimiento de las Directivas sobre protección de datos

Integración de la protección y seguridad de datos en los productos y las prestaciones de servicio

## Estimados empleados:

El cumplimiento de la legislación en materia de protección de datos personales constituye un aspecto importante de la atención debida a nuestros clientes y supone un requisito para la configuración eficiente de nuestros procesos comerciales.

El ámbito universal de operación de la empresa Daimler AG y de las sociedades que forman parte del Grupo exige conocer y cumplir las diferentes exigencias legales vigentes en los distintos países en cuanto a la recogida y el tratamiento convencional o electrónico de datos personales. De modo especial hay que observar las prescripciones legales para el intercambio de informaciones sobre personas entre Sociedades del Grupo con sede en diferentes países. La legislación nacional en numerosos países autoriza la comunicación de datos personales entre Sociedades a escala internacional solamente si en la Sociedad que recibe estas informaciones se puede garantizar un nivel adecuado de protección de los datos.

Con objeto de asegurar el nivel adecuado de protección de datos en todo el Grupo y cumplir así los requerimientos nacionales específicos para la comunicación a nivel internacional de informaciones personales, Daimler AG ha elaborado e implantado el código »Protección de datos y privacidad. Código de conducta de Daimler« para los datos de los clientes y los demás asociados comerciales.

El Encargado de Protección de datos personales del Grupo se encargará de la implementación del código »Protección de datos y privacidad. Código de conducta de Daimler« y del cumplimiento de las normativas legales específicas en los diferentes países. En los Departamentos y en las Sociedades del Grupo en Alemania y en los demás países se han nombrado Coordinadores de protección de datos personales con objeto de garantizar el cumplimiento local de estas tareas y de asistir al Encargado del Grupo. Los coordinadores informan al Encargado de Protección de datos personales del Grupo y reciben de éste instrucciones específicas. El nombre del coordinador responsable en cada Departamento o cada Sociedad se publica en las páginas de Intranet, sección Protección de datos personales.

Tanto los coordinadores locales como yo mismo estamos a su disposición como interlocutores para cualquier consulta relacionada con la implementación del código »Protección de datos y privacidad. Código de conducta de Daimler« en el Grupo.



Dr. Joachim Rieß  
Encargado de Protección de datos del Grupo

# Indice

I. Objeto de este Código de conducta	5
II. Ámbito de aplicación	5
III. Aplicación del Derecho nacional	5
IV. Principios básicos para el tratamiento de datos personales	6
V. Tratamiento de categorías especiales de datos personales	6
VI. Información y consentimiento del interesado	7
VII. Derechos de los interesados	8
VIII. Confidencialidad del tratamiento de los datos	8
IX. Principios básicos de seguridad en el tratamiento de datos	9
X. Datos de marketing / Delegación del tratamiento de datos / Integración de terceros en las secuencias de trabajo	9
XI. Telecomunicación e Internet	10
XII. Recursos judiciales/Sanciones/Responsabilidades	10
XIII. El Encargado de Protección de datos del Grupo	10
Definiciones	12

Las modernas tecnologías de información y comunicación constituyen una herramienta esencial dentro de los procedimientos comerciales y de trabajo de una empresa con ámbito de operación global como Daimler. Una utilización incorrecta o abusiva de esta tecnología puede conllevar una violación de derechos personales. Un objetivo importante en la configuración de la sociedad de la información debe ser garantizar la protección de los derechos personales. Un servicio perfecto a los clientes, objetivo prioritario de nuestra empresa, exige el reconocimiento y la observación de los derechos legítimos de protección de datos de clientes y asociados comerciales. Conscientes de este fin, Daimler AG y las sociedades subsidiarias del Grupo se comprometen a observar el siguiente Código de conducta en todo el mundo.

## I. Objeto de este Código de conducta

El objeto de este código es establecer niveles unificados, adecuados de protección y seguridad de datos, con validez universal para todo el Grupo Daimler, con el fin de satisfacer los requerimientos de la Directiva Europea de protección de datos personales<sup>1</sup> y de otras normativas nacionales en relación con la transferencia internacional de datos. El Código de conducta asegura en todo el Grupo un nivel unificado de protección de datos personales, pero no sustituye a la legitimación requerida para cualquier tratamiento o transferencia de datos. Al mismo tiempo, este Código tiene como fin ayudar e impulsar a los empleados y a los directivos del Grupo a integrar la protección de los datos de nuestros clientes y nuestros asociados comerciales en la configuración de todos los productos y servicios de nuestra empresa. Este Artículo debe interpretarse en conformidad con los demás Artículos de este Código de conducta, en especial con el Artículo III, que regula la aplicabilidad del derecho nacional en cada país.

## II. Ámbito de aplicación

El Código de conducta es una directiva interna del Grupo Daimler y se debe aplicar tanto para el tratamiento de los datos personales de los clientes, de los proveedores, de los asesores y de otros asociados comerciales en la totalidad del Grupo.

## III. Aplicación del Derecho nacional

La licitud de la recogida y el tratamiento de datos personales debe valorarse en función del Derecho nacional y local del país en donde tiene lugar la recogida o el tratamiento de los datos. Esto significa que la licitud del tratamiento de datos personales que hayan sido recogidos en un país no perteneciente a la UE/CEE y que se utilicen fuera de la UE/CEE depende exclusivamente del Derecho nacional y local del país de donde proceden estos datos. Si se transfieren datos desde la UE/CEE o desde países que exigen un nivel adecuado de protección para la transferencia de los datos, la instancia que reciba estos datos tiene que aplicar para el tratamiento de los datos recibidos el derecho nacional vigente en el país de donde proceden estos datos. Esta norma no se aplica a la transferencia de datos dentro de la UE/CEE ni a la transferencia de datos a un país tercero si este país garantiza un nivel adecuado de protección de datos personales, según los criterios definidos en el Artículo 25 de la Directiva de protección de datos personales de la EU y el juicio de la Comisión de las Comunidades Europeas.

Hay que observar en cada caso las obligaciones de notificación vigentes según el Derecho nacional o local de protección de datos. Todas las Sociedades del Grupo Daimler con autonomía jurídica deberán estudiar la vigencia y la amplitud de la obligación de notificación a las autoridades u oficinas de control. En caso de duda, debe consultarse al Encargado de Protección de datos del Grupo.

La recogida o la transferencia de datos personales para el uso en organismos estatales y autoridades se lleva a cabo exclusivamente en conformidad con el Derecho nacional vigente en cada caso.

<sup>1</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación libre de datos

Este Código de conducta contiene solamente las restricciones necesarias para satisfacer los requisitos de la legislación nacional al tráfico internacional de datos personales.

## IV. Principios básicos para el tratamiento de datos personales

1. Durante el tratamiento de los datos deben observarse los derechos personales de los interesados.
2. Los datos personales sólo pueden tratarse si lo permite explícitamente la legislación, o si el interesado ha declarado su consentimiento. Los datos personales pueden tratarse solamente en relación con el fin para el que hayan sido recogidos originariamente, y al que se refiere la licitud legal o el consentimiento del interesado.
3. Los datos personales conservados tienen que ser exactos y deben ser actualizados siempre que sea necesario. Deberán tomarse todas las medidas razonables para que se supriman o se rectifiquen los datos inexactos o incompletos.
4. Sólo deben tener acceso a los datos personales aquellos empleados del Grupo en cuyo ámbito de competencias se encuentre el tratamiento de estos datos; hay que restringir el derecho de acceso a estos datos personales en función del tipo y la extensión del ámbito de trabajo.
5. Una vez que los datos no sean ya necesarios para el objeto comercial para el que fueron recogidos y conservados originariamente, deben borrarse observando en cada caso los plazos de conservación prescritos por la ley.
6. Si un interesado se opone a la utilización de sus datos personales dentro del ámbito de medidas de marketing, no deberán utilizarse sus datos para este objeto.
7. Un objetivo básico que debe observarse en el tratamiento de datos es reducir al mínimo imprescindible la recogida, el procesamiento y la utilización de los datos personales. Hay que hacer uso de las posibilidades existentes de anonimizar y seudonimizar los datos siempre que sea posible y los gastos guarden una relación razonable con el efecto de protección esperado. La evaluación estadística o los estudios basados en datos anonimizados o seudonimizados no se consideran relevantes para la protección de datos personales, siempre que estas informaciones no puedan individualizarse ulteriormente.
8. Las decisiones con efectos jurídicos negativos para el interesado o que constituyan un perjuicio notable para éste no pueden basarse exclusivamente en una evaluación o un tratamiento automatizado de datos personales con objeto de evaluar determinados aspectos de su personalidad, como por ejemplo su solvencia. Como norma general, la tecnología informática puede utilizarse meramente como herramienta auxiliar para una decisión, sin constituir su único fundamento. Si en un caso particular se plantea la necesidad de tomar una decisión automatizada, hay que otorgar al interesado afectado la posibilidad de defender su punto de vista, a no ser que este tipo de decisiones estén expresamente autorizadas por una ley nacional que incluya garantías para la salvaguardia de los intereses legítimos de las personas afectadas.
9. El Departamento de Protección de datos debe tomar parte desde el comienzo en cualquier proyecto de tratamiento de datos del que puedan desprenderse riesgos especiales para los derechos personales de los interesados. Esta norma se aplica especialmente al tratamiento de las categorías especiales de datos personales descritas en el Artículo siguiente.

## V. Tratamiento de categorías especiales de datos personales

Queda prohibido el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos de los interesados, así como el tratamiento de los datos relativos a la salud o a la sexualidad, a no ser que este tratamiento sea lícito en función de una autorización legal o sea necesario por

un requerimiento legal. También se permite el tratamiento de categorías especiales de datos personales para el reconocimiento, ejercicio o defensa de un derecho, también en un procedimiento judicial, si no hay ningún motivo que permita asumir que prevalece el interés del interesado a la prohibición del tratamiento o la utilización de los datos. En todos los demás casos, la licitud requiere el consentimiento explícito del interesado en el tratamiento de estos datos.

## VI. Información y consentimiento del interesado

Los siguientes requerimientos no se refieren a la recogida de datos en los Estados Unidos. En este caso particular se aplica el Derecho nacional o local.

### 1. La relación contractual

Es lícito recoger y procesar datos personales de los interesados sobre la base de una relación contractual o con fines al establecimiento de esta relación. Por este mismo motivo es lícito el tratamiento o la utilización de datos personales para tareas de marketing o para estudios de mercado y de opinión, siempre que esta utilización sea compatible con el objeto para el que se recogieron originariamente los datos. Durante la recogida de los datos, el interesado debe poder apreciar de forma evidente o, en otro caso, hay que informarle de lo siguiente:

- Identidad del responsable del tratamiento
- Los fines del tratamiento de que van a ser objeto los datos
- Terceros o categorías de terceros a los que se vayan a transferir en su caso los datos recogidos.
- Carácter voluntario de la participación en campañas de marketing o en estudios de mercado y de opinión.

Esta transparencia en el tratamiento de los datos debe garantizarse, sea mediante una comunicación individual, sea mediante una información general. Hay que informar al interesado sobre la existencia de derechos de acceso y de rectificación de los datos personales que le conciernen. A más tardar durante la primera utilización de sus datos para medidas de publicidad directa hay que informar al interesado que existe un derecho de oposición contra el tratamiento de estos datos para tareas de marketing directo.

### 2. Relaciones no contractuales

Si no existe una relación contractual o precontractual se requiere el consentimiento del interesado para la recogida y el tratamiento de sus datos personales, a no ser que la licitud de la recogida y el tratamiento de datos sea consecuencia de la aplicación del Derecho nacional. También se requiere un consentimiento explícito si el tratamiento o la utilización de los datos personales supera el ámbito para el que han sido recogidos. Antes de recabar el consentimiento hay que informar al interesado en conformidad con lo estipulado en el Artículo VI, Apartado 1 de este Código de conducta.

Por razones de plausibilidad, la declaración de consentimiento debe recogerse de forma periódica por escrito. Si se trata por ejemplo de una declaración de consentimiento recabada en relación con la celebración de un contrato de compraventa, la cláusula contractual que contiene el consentimiento tiene que destacarse ópticamente. La declaración de consentimiento debe incluir la extensión y el objeto del tratamiento de los datos personales. Bajo circunstancias extraordinarias, por ejemplo, asesoramiento telefónico, puede otorgarse el consentimiento de palabra. Para la configuración de declaraciones de consentimiento por vía electrónica (online) hay que tener en cuenta los estándares de protección de datos y de calidad para aplicaciones de e-business recogidos en <http://cdp.intra.corpintra.net> o las prescripciones vigentes en otro caso.

### 3. Intercambio de datos con terceros externos/adquisición de datos

Como regla general, los datos personales deben recabarse directamente del interesado. Si se encarga a terceros la recogida de datos o si terceros transfieren datos personales, hay que asegurarse de que el interesado está informado, o es informado correspondientemente durante la primera toma de contacto en conformidad con el Artículo VI, Apartado 1 de este Código de conducta.

Las investigaciones sobre la solvencia requieren el consentimiento del interesado. Si se adquieren datos personales a terceros, hay que asegurarse de que estos datos han sido recabados de forma lícita en conformidad con la legislación vigente.

#### 4. Intercambio de datos dentro del Grupo

Si una Sociedad del Grupo con autonomía jurídica transfiere datos personales a otra Sociedad del Grupo, se trata de una transferencia de datos a terceros; por este motivo, también en este caso »interno« tienen que cumplirse los requisitos del Artículo VI, Apartados 1 y 2 de este Código de conducta. Es decir: debe existir una legitimación para el tratamiento de los datos.

Para la transferencia de datos a terceros que no formen parte del Grupo Daimler tienen que cumplirse tanto las condiciones del Artículo VI, Apartado 1 y 2 como los requisitos del Artículo X, Apartado 5 de este Código de conducta.

## VII. Derechos de los interesados

Los interesados pueden dirigir sus consultas y quejas al Coordinador de protección de datos competente, a su interlocutor dentro del Grupo, así como directamente al Encargado de Protección de datos del Grupo. Estas consultas tienen que tramitarse inmediatamente, especialmente si se trata de salvaguardar los derechos especificados a continuación.

1. El interesado puede exigir información sobre los datos personales conservados con relación a su persona, sobre la procedencia de estos datos y sobre el objeto de esta conservación.
2. Si se transfieren datos personales a terceros, hay que informar igualmente acerca de la identidad del destinatario de estos datos o sobre las categorías de los destinatarios.
3. Si se pone de manifiesto durante la tramitación de una consulta en relación con este derecho que los datos personales son inexactos o incompletos, el interesado tiene derecho a exigir que se corrijan estos datos. Si se pone de manifiesto que el objeto del tratamiento de los datos ha prescrito, sea por caducidad temporal, o por otros motivos, o que el tratamiento concreto es ilícito y no se ha constatado la ilicitud durante la comprobación periódica de los datos, hay que borrar los datos, teniendo en cuenta en su caso los plazos legales de conservación.
4. El interesado tiene derecho a oponerse a la utilización de sus datos personales para medidas de publicidad directa o para estudios de mercado o de opinión. Es decir, hay que bloquear los datos conservados para este tipo de medidas.
5. Por lo demás, el interesado tiene un derecho básico de oposición contra el tratamiento de sus datos personales, que hay que tener en cuenta siempre que se constate durante una comprobación que su interés en la protección de sus datos predomina a causa de su situación personal particular sobre el interés de la instancia responsable en el tratamiento de los datos. Este derecho no se aplica si existe una normativa legal que prescriba el tratamiento o la utilización de los datos.

## VIII. Confidencialidad del tratamiento de los datos

Sólo están autorizados a recoger, tratar y utilizar datos personales los empleados autorizados y obligados explícitamente a la observación del secreto profesional. En especial, está prohibido utilizar estos datos para usos privados, comunicarlos a personas no autorizadas o permitir de cualquier otro modo su acceso a terceros. Se consideran también no autorizados según este artículo los compañeros de trabajo, a no ser que exista una situación especial en relación con el ámbito de trabajo o las tareas específicas de estas personas. En Intranet se puede descargar el modelo para una declaración promisorias de confidencialidad de este tipo: <http://cdp.intra.corpintra.net>

La obligación de confidencialidad conserva su validez una vez finalizada la relación laboral con la empresa.



## IX. Principios básicos de seguridad en el tratamiento de datos

Las medidas técnicas y de organización necesarias para garantizar la seguridad de los datos personales afectan a

- los ordenadores (servidores y ordenadores en los puestos de trabajo)
- las redes o líneas de comunicación
- las aplicaciones informáticas.

En relación a los servidores de datos se instalan medidas de seguridad físicas e infraestructurales que comprenden el control de acceso (con distintos niveles de autorización), los sistemas de cierre y las medidas de protección contra incendios. Todos los ordenadores en los puestos de trabajo están protegidos por un sistema de contraseñas.

La red interna de la empresa (Corporate Network) está protegida mediante sistemas Firewall contra el acceso externo por parte de personas no autorizadas y contra el acceso a través de Internet. Antes de enviar datos con relación a personas fuera de la Corporate Network hay que cifrar estos datos. Si no se puede hacer así, hay que justificar esta divergencia ante el Departamento de protección de datos. Con objeto de proteger los datos personales se instala en las bases de datos un sistema escalonado de control y protección de acceso para personas y aplicaciones. Estas medidas técnicas y de organización están integradas en el sistema de gestión de seguridad y protección de datos, en donde se establecen las competencias y responsabilidades.

## X. Datos de marketing/Delegación del tratamiento de datos/Integración de terceros en las secuencias de trabajo

Con frecuencia resulta necesario integrar a terceros externos en determinadas secuencias de trabajo.

Si una Sociedad de nuestro Grupo asume tareas de mandante o de mandatario en el marco de un encargo de este tipo y/o si se acude a terceros para el tratamiento o la utilización de datos personales, hay que tener en cuenta las siguientes indicaciones:

1. Hay que elegir exclusivamente mandatarios o terceros que puedan garantizar el cumplimiento de las exigencias de seguridad y los requerimientos técnicos y de organización necesarios para esta tarea.
2. La ejecución del tratamiento de datos por encargo tiene que regularse en un contrato escrito o reproducible de otro modo. El Encargado de Protección de datos del Grupo puede asumir en caso necesario tareas de asesoramiento y aportar las cláusulas correspondientes para el encargo.
3. El mandante sigue siendo el interlocutor competente para los clientes, proveedores, asesores y otros asociados comerciales que deseen salvaguardar sus derechos de protección de datos.
4. Los terceros externos que reciban encargos de tratamiento de datos o de otro tipo, por ejemplo en el campo del marketing o para la realización de estudios de opinión y de mercado, tienen que comprometerse en un contrato a tratar y utilizar los datos personales que reciban del mandante exclusivamente dentro del marco del encargo de trabajo. Hay que excluir por vía contractual la utilización de estos datos para fines propios o en interés de terceros.
5. En cualquier otra cooperación con terceros que conlleve asimismo la transferencia de datos personales, o durante la que tenga que permitirse el acceso a estos datos, es requisito imprescindible que estos terceros se comprometan a garantizar estándares de protección de datos y de seguridad de datos equivalentes a este Código de conducta.

6. La oposición de los interesados a la utilización de sus datos personales para campañas de marketing o para estudios de mercado y de opinión (véase el Artículo VII, Apartado 4 de este Código de conducta) tienen que observarse igualmente si hay que integrar a terceros en el tratamiento de datos; en caso necesario, hay que extender esta obligación a los terceros implicados, sean internos o externos.

## XI. Telecomunicación e Internet

El tratamiento de datos personales en relación con la telecomunicación con el interesado, incluyendo la comunicación a través de Internet, se rige por el Derecho vigente nacional o local o por las directivas o normativas internas vigentes.

## XII. Recursos judiciales/Sanciones/ Responsabilidades

Las Sociedades de nuestro Grupo, como responsables del tratamiento de datos, están obligadas a garantizar frente a los interesados la observación de los requisitos de protección de datos. Si se aprecia una demanda de formación específica, puede acudir al asesoramiento del Departamento de protección de datos. Los empleados encargados de tratar datos personales tienen que saber que, en numerosos estados, las infracciones de la legislación de protección de datos puede conllevar una persecución por vía penal, así como indemnizaciones por daños y perjuicios. Las transgresiones de determinados empleados conllevan las correspondientes sanciones laborales previstas en el Derecho nacional o local vigente.

Si una Sociedad del Grupo con sede en la UE/CEE transfiere datos personales a una Sociedad del Grupo con sede en un país tercero, el Encargado de Protección de datos del Grupo y la Sociedad que recibe los datos están obligados a cooperar con la autoridad de control del país donde tiene su sede la Sociedad que ha exportado los datos, a responder a todas sus consultas y a respetar las disposiciones de la autoridad de control en relación con el tratamiento de los datos transferidos.

Si un interesado denuncia una transgresión de este Código de conducta por parte de una Sociedad del Grupo con sede en un estado tercero que haya recibido sus datos, la Sociedad del Grupo con sede en la UE/CEE que haya exportado estos datos se compromete a asistir al interesado, cuyos datos hayan sido recogidos en la UE/CEE, tanto en la aclaración de los hechos como en la salvaguardia de sus legítimos derechos frente a la Sociedad del Grupo que ha recibido sus datos en conformidad con el Artículo VII de este Código de conducta. Por lo demás, el interesado puede hacer valer igualmente sus derechos derivados del Artículo VII de este código frente a la Sociedad del Grupo que ha exportado sus datos personales.

## XIII. El Encargado de Protección de datos del Grupo

El Encargado de Protección de datos del Grupo es un órgano interno autónomo que supervisa la observación de las Directivas nacionales e internacionales de protección de datos y del Código de conducta, realizando comprobaciones aleatorias. Los Coordinadores de protección de datos actúan por encargo del Encargado de Protección de datos del Grupo y son responsables de asegurar la protección de datos en los distintos países en conformidad con este Código de conducta y la legislación nacional y local. Las gerencias de las distintas Sociedades del Grupo son responsables del nombramiento de Coordinadores de protección de datos.

Las gerencias de las distintas Sociedades del Grupo están obligadas a asistir al Encargado de Protección de datos del Grupo y a los Coordinadores de protección de datos en el cumplimiento de sus obligaciones. Hay que implicar a tiempo al

Departamento de protección de datos a la hora de evitar o perseguir infracciones en este campo (véase el Artículo IV, Apartado 9 de este Código de conducta).

Si se producen transgresiones y denuncias en relación con las obligaciones derivadas de este Código de conducta, los directivos responsables están obligados a informar lo antes posible al Coordinador de protección de datos responsable o bien al Encargado de Protección de datos del Grupo. Al mismo tiempo, cualquier empleado, cliente o asociado comercial puede dirigirse en todo momento al Encargado de Protección de datos del Grupo o al Coordinador de protección de datos responsable para comunicar sugerencias, tramitar consultas, solicitar información o presentar quejas en relación con la protección de datos personales y la seguridad de estos datos. Los Coordinadores y el Encargado tramitan estas consultas y denuncias de forma confidencial. Si el Coordinador de protección de datos responsable no puede solucionar una reclamación ni subsanar una infracción contra este Código de conducta, está obligado a dirigirse al Encargado del Grupo. Las Gerencias de las Sociedades del Grupo deben respetar las decisiones del Encargado del Grupo en relación con transgresiones de la normativa o las directivas de protección de datos.

El Encargado de Protección de datos del Grupo y sus colaboradores están a disposición en la siguiente dirección:

Daimler AG, Konzernbeauftragter für den Datenschutz, HPC 0624,  
D-70546 Stuttgart, Tel. +49-(0)7 11-17-9 77 27, Fax +49-(0)7 11-17-9 76 99,

e-Mail: joachim.riess@daimler.com

y en Intranet bajo la dirección  
<http://cdp.intra.corpintra.net>.

# Definiciones

- **Interesados** a efectos de este Código de conducta son todas las personas que mantienen o tienen previsto mantener una relación contractual con una Sociedad del Grupo; por lo tanto se incluyen también los llamados Prospects o Potenciales, en la medida en que se recojan y traten los datos personales de estas personas.
- Se consideran **datos personales** toda información sobre una persona física identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse mediante la combinación de una o varias informaciones específicas, incluso con conocimientos adicionales casuales del encargado responsable.
- Se entiende por **tratamiento de datos personales** cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales. Por ejemplo: la recogida, el registro, la organización, la conservación, la elaboración o modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.
- **Una anonimización** de los datos consiste en desligarlos de la identidad de la persona a la que se refieren, de forma duradera y con imposibilidad de que persona alguna pueda restablecer la relación, o que se requiera un coste desproporcionado de tiempo, dinero y mano de obra para restablecer esta relación. Se entiende por seudonimización la sustitución del nombre y otros criterios de identificación por un distintivo, con el fin de evitar la identificación del afectado o bien dificultarla de forma decisiva.
- **Responsable del tratamiento** de datos (instancia responsable) de cara al exterior, esto es, frente a los clientes y otros asociados comerciales del Grupo, es una Sociedad del Grupo Daimler con autonomía jurídica, bajo cuya competencia y actividad comercial se ha tomado la medida de tratamiento de datos. Dentro de esta Sociedad, la estructura administrativa y jerárquica determina los empleados responsables del tratamiento lícito y correcto de datos.
- **Encargado del tratamiento** son aquellas personas físicas o jurídicas, que tratan datos personales (como mandatarios) por cuenta del responsable del tratamiento (mandante). Junto a las empresas de servicios de marketing, estos encargados suelen ser principalmente los explotadores de los centros de cálculo.
- **Tercero** es cualquier persona física o jurídica o autoridad pública distinta y no dependiente **del responsable del tratamiento de datos**. No se consideran por tanto terceros los **encargados del tratamiento**, ni los empleados del responsable, siempre que los datos personales correspondientes queden dentro de su ámbito de responsabilidad.
- **Transferencia** de datos es la comunicación de estos datos a un Tercero que no forma parte del ámbito de responsabilidad del responsable del tratamiento de datos.
- **Consentimiento del interesado** es una manifestación de voluntad, mediante la que el interesado, con conocimiento de causa y sin coacción externa apreciable, consiente de forma explícita el tratamiento de los datos personales que le conciernen.
- **El derecho de oposición (derecho a opt-out)** significa que el interesado puede prohibir la utilización de sus datos para fines de marketing o para estudios de mercado y de opinión.

