DAIMLER

# Directriz de protección de datos.

# Prólogo

**Estimados señores:**

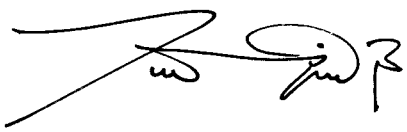
En consonancia con la era digital, ofrecemos al cliente la posibilidad de permanecer siempre comunicado en línea, también en su vehículo. A tal efecto es imprescindible registrar y procesar datos. Uno de nuestros principios de alcance general, vigente tanto en el vehículo como en el taller o el concesionario, consiste en garantizar un alto grado de protección y seguridad de la información en todas las situaciones que requieran el almacenamiento y la transmisión de datos. Un principio que aplicamos por igual para todas las informaciones, independientemente de las personas a las que atañan: clientes, interesados, socios y empleados. Porque protegiendo los datos protegemos a la persona.

Queremos que Daimler no sólo sea sinónimo de vehículos seguros, sino que además marque pautas en materia de protección de datos. En calidad de empresa de proyección internacional, consideramos que es nuestro deber atenernos a las distintas prescripciones legales vigentes en los diferentes países en relación con la recogida y el procesamiento de datos personales. Nuestra máxima prioridad en este contexto es asegurar un estándar homogéneo vigente a nivel internacional para el tratamiento de datos de carácter personal. Porque salvaguardar la esfera privada y los derechos relacionados con la personalidad de cada individuo aporta, a nuestro modo de ver, la base necesaria para unas relaciones comerciales de confianza.

En la directriz de protección de datos del Grupo hemos establecido reglas severas para el procesamiento de datos personales de clientes, personas interesadas, socios y empleados. Esta directriz corresponde a las exigencias de la Normativa Europea de Protección de Datos, y asegura el cumplimiento de los principios de las leyes nacionales e internacionales de protección de datos vigentes en todo el mundo. De este modo definidos para nuestra empresa un estándar de protección y seguridad de datos vigente en todo el mundo y reglamentamos el intercambio de información entre las sociedades que componen nuestro Grupo. Nuestro canon engloba siete principios fundamentales de protección de datos, entre los que cuentan la transparencia, la reducción al mínimo de los datos recogidos y la seguridad de esta información.

Nuestros directivos y todos los empleados tienen la obligación de atenerse a la directriz de protección de datos del Grupo y de observar las leyes aplicables en esta materia. Como encargado de protección de datos del Grupo, soy responsable del cumplimiento de las prescripciones legales y de los principios de protección de datos de Daimler en todo el mundo.

Mi equipo y yo responderemos con mucho gusto cualquier pregunta que deseen dirigirnos en relación con la protección y la seguridad de datos en Daimler.



Joachim Rieß
Encargado de Protección de Datos del Grupo

# Índice

# I. Objetivo de la directriz de protección de datos

Como expresión de su responsabilidad social, el Grupo Daimler se compromete al cumplimiento de la legislación internacional de protección de datos de carácter personal. Esta directriz de protección de datos es válida para el Grupo Daimler en todo el mundo y se basa en principios generales reconocidos en todo el mundo sobre la protección de datos de carácter personal. La protección de datos es una de las bases de una relación comercial de confianza y de la reputación del Grupo Daimler como patrono atractivo.
La directriz de protección de datos crea una de las condiciones marco necesarias para un intercambio global de datos[1] entre las Sociedades del Grupo. La directriz garantiza el nivel adecuado de protección de datos[2] de carácter personal exigido por la Directiva Europea de Protección de datos y por diversas leyes nacionales para el intercambio internacional de datos en los países en donde no existe todavía una protección legal adecuada para los datos de carácter personal[3].

# II. Ámbito de aplicación y modificación de la directriz de protección de datos

Esta directriz de protección de datos tiene validez para todas las empresas del Grupo Daimler, esto es, para Daimler AG y todas las sociedades del Grupo dependientes de Daimler, así como para todas las empresas asociadas y sus empleados. Se considera sociedad dependiente según esta directriz a cualquier sociedad en la que Daimler AG pueda exigir el cumplimiento de esta directriz de protección de datos de forma inmediata o mediata, por poseer mayoría de votos en el capital social, por contar con una mayoría en la dirección de la empresa o por razón de un acuerdo. La directriz de protección de datos se aplica a cualquier tratamiento de datos de carácter personal[4]. En aquellos países en los que los datos de personas jurídicas gocen de la misma protección que los datos de carácter personal, se aplica esta directriz de protección de datos también y del mismo modo a los datos de personas jurídicas. Los datos anonimizados[5], por ejemplo, para evaluaciones o estudios estadísticos, no están contemplados en esta directriz de protección de datos.

Las sociedades individuales del Grupo no están autorizadas a adoptar disposiciones que difieran de esta directriz de protección de datos. Es posible crear directrices adicionales sobre protección de datos previa coordinación con el Encargado de Protección de datos del Grupo si así lo requiere la legislación nacional. Sólo pueden introducirse modificaciones en esta directriz de protección de datos previa coordinación con el Encargado de Protección de datos del Grupo, dentro del procedimiento establecido a este fin para modificación de directrices. Los cambios se comunicarán sin retardo a las empresas del Grupo Daimler dentro del procedimiento previsto para modificación de directrices. Si se trata de cambios con repercusiones considerables sobre el cumplimiento de la directriz de protección de datos, se comunicarán anualmente a las autoridades estatales de protección de datos responsables de la autorización de esta directriz como regulación interna vinculante de protección de datos.

La versión actual de la directriz de protección de datos puede descargarse de los avisos sobre protección de datos de carácter personal en la página de Internet de Daimler AG, www.daimler.com

1 Ver el apartado XV.
2 Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de estos datos.
La directiva puede descargarse de http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm#richtlinie
3 Ver el apartado XV.
4 Ver el apartado XV.
5 Ver el apartado XV.

# III. Aplicación del Derecho nacional

Esta directriz de protección de datos contiene los principios de protección de datos aceptados comúnmente en todo el mundo, sin pretender reemplazar al Derecho nacional vigente. La directriz complementa el derecho nacional aplicable. Se aplicará el Derecho nacional vigente en cada caso siempre que existan divergencias preceptivas con respecto a esta directriz de protección de datos, o si contiene exigencias más estrictas. Se observará el contenido de esta directriz de protección de datos también en el caso de que no exista un Derecho nacional vigente. Se observarán en cada caso las obligaciones de notificación del tratamiento de datos vigentes según el Derecho nacional o local.

Todas las empresas del Grupo Daimler son responsables del cumplimiento de esta directriz de protección de datos y de las obligaciones legales. Si tiene motivos para suponer que existen obligaciones legales que contradicen las obligaciones derivadas de esta directriz de protección de datos, la empresa del Grupo afectada informará sin demora al Encargado de Protección de datos del Grupo. En caso de colisión entre una prescripción legal nacional y la directriz de protección de datos, Daimler AG buscará junto con la empresa del Grupo afectada una solución viable de conformidad con los objetivos de la directriz.

# IV. Principios básicos para el tratamiento de datos de carácter personal

**1. Honradez y legitimidad**
Durante el tratamiento de los datos de carácter personal deben observarse los derechos de la personalidad de los interesados[6]. Los datos de carácter personal deben recogerse y tratarse con honradez y de forma legítima.

**2. Uso para fines específicos**
Los datos de carácter personal pueden tratarse solamente en relación con el fin para el que hayan sido recogidos originariamente. La modificación posterior del fin específico es posible sólo bajo determinadas condiciones y requiere una justificación.

**3. Transparencia**
El interesado tiene que ser informado sobre el uso de sus datos. Como norma general, los datos de carácter personal se recogen siempre directamente de los interesados. Siempre que se recogen datos de carácter personal, el interesado tiene que estar en condiciones de reconocer personalmente los siguientes aspectos, o ser informado sobre los mismos:

- La identidad de la instancia responsable que recoge los datos[7]
- El fin del tratamiento de los datos
- Terceros[8] o categorías de terceros a los que se transfieren en su caso los datos

[6] Ver el apartado XV.
[7] Ver el apartado XV.
[8] Ver el apartado XV.

**4. Evitar y reducir la recogida y el tratamiento de datos**
Antes de proceder al tratamiento de datos de carácter personal debe estudiarse si este tratamiento es necesario, y en qué medida resulta necesario, para lograr el fin previsto. Siempre que sea posible para lograr el fin previsto, y que los costes sean razonables en relación con el fin previsto, se utilizarán datos anonimizados o estadísticos.

No está permitido memorizar datos de carácter personal a título preventivo para posibles usos en el futuro, a no ser que lo exija o lo permita así el Derecho nacional.

**5. Borrado**
Se borrarán los datos de carácter personal que no sean necesarios una vez transcurridos los plazos de conservación prescritos por la ley[9]. Si, en un caso individual, existen indicios de una necesidad de protección o de interés histórico de estos datos, se prolongará el plazo de almacenamiento de estos datos hasta que se haya aclarado la necesidad legal de protección, o hasta que el Archivo del Grupo haya valorado la relevancia histórica de los datos para su inclusión en el archivo.

**6. Exactitud y actualidad de los datos**
Los datos de carácter personal conservados tienen que ser exactos y completos y deben ser actualizados siempre que sea necesario. Deberán tomarse todas las medidas razonables para que se supriman, se rectifiquen, se completen o se actualicen los datos inexactos, incompletos u obsoletos.

**7. Confidencialidad y seguridad de datos**
Los datos de carácter personal están sujetos a una obligación de confidencialidad. Es decir, se tratarán de forma confidencial en el trato personal y se protegerán con medidas organizativas y técnicas adecuadas contra el acceso por parte de personas no autorizadas, el tratamiento ilegal o la transferencia ilícita a terceros, así como contra la pérdida casual, la modificación o la destrucción.

# V. Licitud del tratamiento de datos

Es lícito recoger, procesar y utilizar datos de carácter personal solamente si se cumple uno de los supuestos de licitud descritos en lo que sigue. Debe darse asimismo uno de los supuestos de licitud si desea modificarse el objetivo de la recogida, el tratamiento y el uso de los datos de carácter personal con relación al objetivo original.

[9] Ver el apartado XV.

# 1. Datos de clientes y de socios

### 1.1 Tratamiento de datos para una relación contractual

Los datos de carácter personal del interesado, el cliente o el socio pueden tratarse para la preparación, para la realización y para la cancelación de un contrato. Esto incluye también la atención del socio contractual, siempre que esté en relación con el objeto del contrato.
Antes de la conclusión de un contrato —es decir, en la fase de negociación del contrato— está permitido el tratamiento de datos de carácter personal para elaborar ofertas, para preparar solicitudes de compra o para cumplir otros deseos del interesado con el fin de llegar a la conclusión del contrato. Está permitido ponerse en contacto con los interesados durante la fase de negociación, utilizando los datos que han comunicado. Deberán tenerse en cuenta en su caso las restricciones mencionadas por el interesado. Para llevar a cabo medidas de publicidad más allá de las acciones mencionadas tienen que cumplirse los requisitos mencionados bajo V.1.2.

### 1.2 Tratamiento de datos para fines publicitarios

Si el interesado se dirige a una empresa del Grupo Daimler solicitando información (por ejemplo, petición de envío de material informativo sobre un producto), está permitido el tratamiento de sus datos para cumplir este deseo.

Las medidas publicitarias y de fidelización de los clientes requieren el cumplimiento de otros requisitos legales. El tratamiento de datos de carácter personal para fines publicitarios o de estudios de mercado y de opinión está permitido si este tratamiento es compatible con el fin para el que se recogieron los datos en su momento. Se informará a los afectados acerca del uso de sus datos para tareas de publicidad. Si se recogen datos exclusivamente para medidas publicitarias, la comunicación de los mismos por parte del afectado es siempre voluntaria. Se informará al afectado acerca del carácter voluntario de la comunicación de los datos para este fin. Dentro del marco de las medidas de comunicación con el interesado debe solicitarse el consentimiento[10] del interesado para el tratamiento de sus datos con fines publicitarios. En el marco del consentimiento, el interesado debe poder elegir entre los canales de contacto disponibles, como correo postal, correo electrónico y teléfono (Consentimiento, ver V.1.3).
Si el interesado rechaza el uso de sus datos con fines publicitarios, no está permitido seguir utilizando sus datos para este fin y se bloquearán de forma correspondiente. Se tendrán además en cuenta las restricciones vigentes en algunos países acerca del uso de datos para fines publicitarios.

### 1.3 Consentimiento con el tratamiento de datos

Es posible llevar a cabo el tratamiento de datos si el interesado ha otorgado su consentimiento.
Antes de solicitar su consentimiento, se informará al interesado en conformidad con el apartado IV.3 de esta Directriz sobre protección de datos. Por razones de plausibilidad, la declaración de consentimiento debe recogerse siempre por escrito o por vía electrónica. Bajo determinadas condiciones, como por ejemplo el asesoramiento telefónico, puede otorgarse el consentimiento de palabra. Se documentará el consentimiento otorgado.

### 1.4 Tratamiento de datos por razón de permiso legal

El tratamiento de datos de carácter personal es también lícito si existen disposiciones legales que exijan, presupongan o autoricen este tratamiento. El tipo y la extensión del tratamiento de datos tienen que ser necesarios para el tratamiento autorizado por la legislación, y tienen que realizarse de acuerdo con estas disposiciones.

[10] Ver el apartado XV.

### 1.5 Tratamiento de datos por razón de un interés legítimo

También pueden tratarse datos de carácter personal si resulta necesario para salvaguardar un interés legítimo del Grupo Daimler. En general, los intereses legítimos pueden ser de tipo legal (por ejemplo, realizar títulos pendientes) o económico (por ejemplo, evitar perturbaciones del contrato). No está permitido el tratamiento de datos de carácter personal por razón de un interés legítimo si existen en algún caso particular indicios de que la protección de los intereses legítimos del interesado predomina sobre el interés de la instancia responsable en el tratamiento de los datos. Se examinará la legitimidad de estos intereses antes de cada tratamiento de datos.

### 1.6 Tratamiento de datos sujetos a una protección especial

Los datos de carácter personal sujetos a una protección especial[11] pueden tratarse solamente si resulta obligatorio por ley, o si el interesado ha otorgado su consentimiento expreso.
Por lo demás, también puede estar permitido el tratamiento de estos datos si ello es necesario para que la instancia responsable pueda ejercer sus derechos, reclamarlos o defenderlos frente al interesado. Si existe la intención de tratar datos sujetos a una protección especial, se informará con antelación al Encargado de Protección de datos del Grupo.

### 1.7 Decisiones individuales automatizadas

El tratamiento automatizado de datos de carácter personal con objeto de evaluar determinados aspectos de su personalidad, como por ejemplo su solvencia, no debe constituir el único fundamento de una decisión con consecuencias legales negativas o perjuicios considerables para el interesado. Se comunicará al interesado el hecho y el resultado de una decisión individual automatizada, y se le otorgará la posibilidad de defender su punto de vista. A fin de impedir decisiones equivocadas, deben garantizarse un control y una comprobación de la plausibilidad por parte de un empleado.

### 1.8 Datos de usuarios e Internet

Siempre que se recogen, se tratan o se usan datos de carácter personal en páginas web o en Apps debe informarse a los interesados sobre este aspecto en avisos sobre la protección de datos y, en su caso, sobre cookies. Los avisos sobre la protección de datos y sobre cookies deben integrarse de modo que estén disponibles continuamente, y que el interesado pueda reconocerlos con facilidad y acceder a ellos de forma inmediata.

Si se elaboran perfiles de usuario para el análisis del comportamiento de los visitantes de páginas web o usuarios de Apps (tracking), se informará a los interesados sobre este aspecto en cada caso en los avisos sobre protección de datos. Solamente está permitido el tracking con relación a personas determinadas si lo permite la legislación nacional o si el interesado ha otorgado su consentimiento. Si se lleva a cabo el tracking bajo seudónimo, debe otorgarse al interesado una posibilidad de contradicción en los avisos de protección de datos (Opt-out).

Si se ofrece la posibilidad de acceder a datos de carácter personal en un área restringida (sujeta a registro) de páginas web o Apps, se configurarán la identificación y autentificación del interesado de tal manera que se logre un nivel adecuado de protección de este acceso.

[11] Ver el apartado XV.

# 2. Datos de empleados

**2.1 Tratamiento de datos para la relación laboral**
Es lícito tratar datos de carácter personal sobre la base de una relación laboral si esto es necesario para la conclusión, el cumplimiento y la terminación del contrato laboral.
Es lícito recoger y tratar datos de carácter personal de los candidatos con el fin de preparar una relación laboral. Si se rechaza una solicitud de empleo, se borrarán los datos del candidato, teniendo en cuenta los plazos legales establecidos para los comprobantes, a no ser que el candidato haya consentido en la memorización de los datos para un proceso de selección posterior. También se requiere un consentimiento para el uso de los datos en otros procesos de selección de personal, o para la entrega de la solicitud a otras sociedades del Grupo.

Si existe una relación laboral, el tratamiento de datos tiene que estar siempre relacionado con el contrato laboral, a no ser que se cumpla uno de los supuestos especificados a continuación que autorizan el tratamiento de datos.

Si resulta necesario en el proceso de candidatura o dentro del marco de una relación laboral recoger información adicional de terceros sobre el candidato, se tendrán en cuenta las exigencias legales nacionales a esta transferencia de datos. En caso de duda se debe solicitar el consentimiento del interesado.

El tratamiento de datos de carácter personal de los empleados relacionados con una relación laboral con fines diferentes del cumplimiento del contrato laboral requiere para su licitud una legitimación legal. Ejemplos de esta legitimación pueden ser exigencias de la legislación, estipulaciones del convenio colectivo con el consejo de empresa, el consentimiento del empleado o también legítimos intereses de la empresa.

**2.2 Tratamiento de datos por razón de permiso legal**
El tratamiento de datos de carácter personal de los empleados es también lícito si existen disposiciones legales que exijan, presupongan o autoricen este tratamiento. El tipo y la extensión del tratamiento de datos tienen que ser necesarios para el tratamiento autorizado por la legislación, y tienen que realizarse de acuerdo con estas disposiciones. Si la legislación prevé un cierto margen en la legitimidad del tratamiento de datos, se observarán los intereses legítimos del empleado.

**2.3 Disposiciones colectivas para el tratamiento de datos**
El tratamiento de datos de carácter personal que trascienda el fin inicial de realización del contrato es legítimo también si está autorizado por una regulación colectiva. Se consideran regulaciones colectivas los convenios colectivos o los acuerdos entre el empresario y el consejo de empresa dentro de las posibilidades previstas en el Derecho laboral aplicable. Las regulaciones tienen que guardar relación con el fin concreto del tratamiento de datos deseado, y pueden configurarse dentro del marco del Derecho nacional de protección de datos.

**2.4 Consentimiento con el tratamiento de datos**
Los datos de los empleados pueden tratarse si el interesado ha declarado su consentimiento. Las declaraciones de consentimiento tienen que ser voluntarias. Un consentimiento no voluntario se considera inválido. Por razones de plausibilidad, la declaración de consentimiento debe recogerse siempre por escrito o por vía electrónica. Si las circunstancias no permiten proceder así en un caso excepcional, el consentimiento puede otorgarse también de palabra. Se documentará siempre el consentimiento otorgado. Puede asumirse que existe consentimiento en la comunicación voluntaria consciente de datos si la legislación nacional no prescribe un consentimiento explícito. Antes de solicitar su consentimiento, se informará al interesado en conformidad con el apartado IV.3 de esta Directriz sobre protección de datos.

### 2.5 Tratamiento de datos por razón de un interés legítimo

También pueden tratarse datos de carácter personal de los empleados si resulta necesario para salvaguardar un interés legítimo del Grupo Daimler. En general, los intereses legítimos pueden ser de tipo legal (por ejemplo, el ejercicio, la reivindicación o la defensa de títulos legales) o de tipo económico (por ejemplo, la valoración de empresas).

No está permitido el tratamiento de datos de carácter personal por razón de un interés legítimo si existen en algún caso particular indicios de que la protección de los intereses legítimos del empleado predomina sobre el interés de la instancia responsable en el tratamiento de los datos. Se examinarán los intereses legítimos antes de cada tratamiento de datos.

Sólo está permitido realizar medidas de control que requieran el tratamiento de datos de carácter personal de los empleados si existe una obligación legal para ello, o si hay motivos justificados. También se examinará que la medida de control es razonable si existe un interés legítimo. Se ponderarán los intereses legítimos de la empresa en la realización de la medida de control (por ejemplo, el cumplimiento de exigencias legales o reglas internas de la empresa), frente al posible interés legítimo del empleado afectado a la supresión de la medida, y solamente se realizará si resulta razonable. Antes de realizar cada medida de este tipo se estudiarán y documentarán el interés legítimo de la empresa y los posibles intereses legítimos de los empleados. Además, puede ser necesario cumplir otras exigencias del Derecho nacional (por ejemplo, derechos de cogestión del Comité de empresa y derechos de información de los afectados).

### 2.6 Tratamiento de datos sujetos a una protección especial

Los datos de carácter personal sometidos a una especial protección pueden tratarse solamente si se cumplen determinados requisitos. Se consideran datos sometidos a una especial protección los datos de carácter personal que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos de los interesados, así como los datos relativos a la salud o a la sexualidad. El Derecho nacional puede considerar datos sujetos a una protección especial a otras categorías de datos, o puede establecer categorías de datos diferentes. Del mismo modo, es frecuente que los datos relacionados con delitos penales sólo puedan tratarse bajo determinadas condiciones, especificadas en el Derecho nacional.

El tratamiento de estos datos tiene que estar autorizado expresamente o prescrito por el Derecho nacional. Por lo demás, también puede estar permitido el tratamiento de datos de carácter personal si este tratamiento es necesario para que la instancia responsable pueda ejercer sus derechos y cumplir sus obligaciones en el campo del derecho laboral. El empleado puede consentir expresamente a título voluntario en el tratamiento de los datos.

Si existe la intención de tratar datos sujetos a una protección especial, se informará con antelación al Encargado de Protección de datos del Grupo.

### 2.7 Decisiones automatizadas

En caso de que, dentro del marco de la relación laboral, se realice un tratamiento automatizado de datos de carácter personal de los empleados con objeto de evaluar determinados aspectos de su personalidad (por ejemplo para la selección de personal o para la evaluación de perfiles de aptitudes), el tratamiento automatizado no debe constituir el único fundamento de una decisión con consecuencias negativas o perjuicios considerables para el empleado afectado. A fin de impedir decisiones equivocadas, en las decisiones automatizadas debe incluirse una valoración del contenido por parte de una persona física, que constituya el fundamento para la decisión. Además, se comunicarán al empleado afectado el hecho y el resultado de una decisión individual automatizada, y se le otorgará la posibilidad de defender su punto de vista.

### 2.8 Telecomunicación e Internet

Los sistemas telefónicos, las direcciones de e-mail, la Intranet y el Internet, así como las redes sociales internas, se ponen a disposición en primera línea en el marco de las tareas profesionales asignadas por la empresa. Son medios de trabajo y recursos de la empresa. Pueden utilizarse en el marco de la legislación vigente en cada caso y de las normas internas de la empresa. Si se autoriza el uso para fines particulares, se deberán observar la legislación sobre el secreto de las comunicaciones y el derecho de telecomunicación nacional vigentes.

No se lleva a cabo una supervisión general de la comunicación telefónica y por e-mail, ni del uso de la Intranet o del Internet. Como medida de protección frente a ataques a la infraestructura informática o a usuarios individuales pueden implementarse medidas de protección en los accesos a la red de Daimler que bloquean contenidos perjudiciales para la técnica o que analizan patrones de ataques. Por motivos de seguridad, pueden realizarse protocolos de duración limitada sobre el uso de los sistemas telefónicos, de las direcciones de e-mail, de la Intranet y del Internet, así como de las redes sociales internas. Solamente podrán realizarse evaluaciones con relación a personas de estos datos si existe una sospecha justificada de infracción contra las leyes o contra las normas del Grupo Daimler. Solamente podrán realizar estos controles los departamentos encargados de la investigación, con cumplimiento del principio de la proporcionalidad. Se observarán las leyes nacionales vigentes y las regulaciones internas del Grupo.

# VI. Transferencia de datos de carácter personal

La transferencia de datos de carácter personal a destinatarios fuera del Grupo Daimler o a destinatarios dentro del Grupo Daimler está sometida a los requisitos de legitimidad para el tratamiento de datos de carácter personal descritos en el apartado V. El destinatario de los datos debe comprometerse a utilizarlos exclusivamente para los fines definidos.

En caso de transferencia de datos a un destinatario fuera del Grupo Daimler con sede en un estado tercero[12], el destinatario debe garantizar un nivel de protección de datos adecuado a los términos de esta directriz. Este requisito no se aplica si la transferencia de datos se realiza por razón de una obligación legal. Esta obligación legal puede resultar de la legislación del país en el que tiene su sede la sociedad del Grupo que transfiere los datos, o si la legislación del país donde tiene su sede la sociedad del Grupo reconoce el fin de la transmisión de datos perseguido con la obligación legal de un estado tercero.

En caso de transferencia de datos de terceros a empresas del Grupo Daimler, debe asegurarse que los datos pueden utilizarse legítimamente para el uso previsto.

Si se transfieren datos de carácter personal de una sociedad del Grupo con sede en el Espacio Económico Europeo a una sociedad del Grupo con sede fuera del Espacio Económico Europeo[13] (estado tercero), la sociedad que importa los datos está obligada a cooperar en todas las consultas del organismo de control responsable de la sociedad que exporta los datos y a observar las disposiciones de este organismo de control en relación con los datos transferidos. Esto mismo se aplica a la transferencia de datos por sociedades del Grupo de otros estados. Si toman parte en un sistema internacional de certificación para regulaciones empresariales vinculantes para la protección de datos, deben asegurar la cooperación contemplada en este sistema con los órganos y autoridades de control. La participación en un sistema de certificación de este tipo se coordinará con el Encargado de Protección de datos del Grupo.

[12] Ver el apartado XV.
[13] Ver el apartado XV.

Si un interesado denuncia una transgresión de esta Directriz sobre protección de datos por parte de la sociedad del Grupo con sede en un estado tercero que ha importado los datos, la sociedad del Grupo con sede en el Espacio Económico Europeo que ha exportado los datos está obligada a asistir al interesado afectado, cuyos datos han sido recogidos en el Espacio Económico Europeo, tanto en la aclaración de los hechos como en el ejercicio de sus derechos de acuerdo con esta directriz de protección de datos frente a la sociedad del Grupo que ha importado los datos. Por lo demás, el interesado tiene también derecho a reclamar sus derechos frente a la sociedad del Grupo que ha exportado los datos. Si se denuncia una transgresión, la sociedad que ha exportado los datos deberá demostrar al interesado que la sociedad del Grupo que ha importado los datos en un estado tercero no ha cometido una infracción contra esta directriz en el tratamiento de los datos recibidos.

En caso de una transferencia de datos de carácter personal de una sociedad del Grupo con sede en el Espacio Económico Europeo a una sociedad del Grupo con sede en un estado tercero, la instancia que transfiere los datos asume frente al interesado cuyos datos personales han sido recogidos en el Espacio Económico Europeo, la responsabilidad por transgresiones de la sociedad del Grupo con sede en un estado tercero contra esta Directriz sobre protección de datos, como si el autor de la transgresión hubiera sido la instancia que ha transferido los datos. Se considera competente el tribunal local de la instancia que ha exportado los datos.

# VII. Tratamiento de datos por encargo

Existe un supuesto de tratamiento de datos por encargo si se asigna a un contratista el tratamiento de datos de carácter personal, sin traspasar por ello la responsabilidad por el proceso comercial correspondiente. En estos casos debe tomarse un acuerdo de tratamiento de datos por encargo, tanto con el contratista externo como entre las empresas dentro del Grupo Daimler. La empresa que otorga el encargo conserva la plena responsabilidad por la realización correcta del tratamiento de los datos. El contratista está autorizado a tratar los datos de carácter personal solamente en el marco de las instrucciones del contratante. A la hora de otorgar el pedido deben observarse las siguientes prescripciones; el departamento que otorga el encargo debe asegurar su cumplimiento.

1. Seleccionar el contratista según su idoneidad para garantizar las medidas de protección técnicas y administrativas necesarias.
2. El encargo debe otorgarse de forma textual. En este encargo deben documentarse las instrucciones para el tratamiento de datos y las responsabilidad del contratante y del contratista.
3. Se tendrán en cuenta los contratos estándar puestos a disposición por el Encargado de Protección de datos del Grupo.
4. Antes del comienzo del tratamiento de los datos, el contratante debe convencerse del cumplimiento de las obligaciones por parte del contratista. El contratista puede documentar el cumplimiento de las exigencias de seguridad de datos, especialmente, mediante la presentación de un certificado idóneo. En función del riesgo del tratamiento de datos, puede ser necesario repetir el control de forma periódica durante la duración del contrato.

5. Si se encarga el tratamiento de los datos a una empresa del extranjero, deberán cumplirse las exigencias nacionales aplicables para la transferencia de datos de carácter personal a empresas en el extranjero. En especial, solamente puede encargarse el tratamiento de datos de carácter personal del Espacio Económico Europeo a un tercer estado si el contratista puede documentar un nivel de protección de datos equiparable a esta directriz sobre la protección de datos. Pueden ser instrumentos idóneos:
   a. Un acuerdo de las cláusulas del contrato estándar de la UE para el tratamiento de datos por encargo en estados terceros con el contratista y, en su caso, con los subcontratistas.
   b. La participación del contratista en un sistema de certificación reconocido por la UE para crear un nivel razonable de protección de datos.
   c. El reconocimiento por parte de los órganos de control estatales responsables de reglas vinculantes de la empresa del contratista para crear un nivel adecuado de protección da datos.

# VIII. Derechos del interesado

Todos los interesados pueden hacer valer los derechos especificados a continuación. La instancia responsable debe tramitar inmediatamente la reclamación de derechos, y los interesados no deben ser discriminados de ninguna manera por hacer valer sus derechos.

1. El interesado puede exigir información acerca de los datos de carácter personal memorizados sobre su persona, acerca de su procedencia y acerca del uso previsto. Si el Derecho laboral vigente prevé derechos más amplios de inspección de la documentación del empleador (por ejemplo, expediente personal), esta directriz no afecta a estos derechos.
2. Si se transfieren a terceros datos de carácter personal, se comunicará también la identidad del receptor o las categorías de receptores.
3. Si los datos de carácter personal son incorrectos, o incompletos, el interesado puede exigir su corrección o su complemento.
4. El interesado puede oponerse al tratamiento de sus datos personales con objeto de publicidad, o dentro del marco de estudios de mercado y de opinión. En ese caso se bloquearán los datos para impedir que se utilicen para este fin.
5. El interesado tiene derecho a exigir que se borren sus datos si falta o ha caducado el fundamento jurídico para el tratamiento de los datos. Lo mismo se aplica en el caso de que haya prescrito el motivo del tratamiento de datos, sea por el tiempo transcurrido o por otros motivos. Se tendrán en cuenta los plazos de conservación obligatoria de determinados documentos y los derechos legítimos que se opongan al borrado.
6. El interesado tiene un derecho básico de oposición contra el tratamiento de sus datos personales, que se tendrá en cuenta siempre que se constate que su interés en la protección de sus datos de carácter personal predomina a causa de su situación personal particular sobre el interés en el tratamiento de los datos. Este derecho no se aplica si existe una normativa legal que prescriba el tratamiento de los datos.

Por lo demás, cada interesado puede hacer valer los derechos otorgados a terceros en las cifras III. apartado 2, IV., V., VI., IX., X, y XIV. apartado. 3 si una empresa que se ha comprometido a la observación de la directriz de protección de datos no observa sus prescripciones y lesiona los derechos del interesado.

# IX. Confidencialidad en el tratamiento de datos

Los datos de carácter personal están sujetos a confidencialidad. Se prohíbe a los empleados la recogida, el tratamiento y el uso de datos sin autorización. Se considera ilícito cualquier tratamiento de datos realizado por un empleado sin que constituya su cometido de acuerdo con su trabajo y sin estar autorizado para ello. Se aplica el principio de necesidad imperiosa. Se asegurará que los empleados sólo tienen acceso a datos de carácter personal cuando sea necesario y en el marco de la necesidad para sus tareas específicas. Esto exige una asignación y división precisa de roles y competencias, así como su implementación y actualización en el marco de conceptos de autorización.

Los empleados no pueden utilizar datos de carácter personal para usos particulares o económicos, entregarlos a terceros no autorizados o permitir a terceros el acceso de otro modo. Los superiores informarán a sus empleados al comienzo de una relación laboral acerca de la obligación de observar la confidencialidad de los datos. Esta obligación persiste después de finalizar la relación laboral.

# X. Seguridad del tratamiento de datos

Los datos de carácter personal deben protegerse en todo momento contra un acceso no autorizado, el tratamiento o comunicación ilícito y su pérdida, modificación o destrucción. Esta obligación se extiende tanto al tratamiento de los datos por vía electrónica como en forma impresa. Antes de la introducción de nuevos procedimientos de tratamiento de datos, especialmente nuevos sistemas informáticos, se definirán e implementarán medidas técnicas y administrativas idóneas para la protección de los datos de carácter personal. Estas medidas se orientarán por el estado de la técnica, los riesgos derivados del tratamiento de los datos y la demanda de protección de los datos (determinada siguiendo el proceso de clasificación de la información). El área responsable puede solicitar asesoramiento de su Encargado de seguridad de la información (ISO) y del Coordinador de protección de datos. Las medidas técnicas-administrativas para protección de datos de carácter personal forman parte de una gestión integrada de seguridad de la información en el Grupo, y se adaptan de forma continuada teniendo en cuenta el desarrollo técnico y las modificaciones en la organización.

# XI. Control de la protección de datos

El cumplimiento de las directrices sobre protección de datos y de las leyes vigentes de protección de datos se controla por medio de auditorías periódicas y otros controles. La realización es responsabilidad del Encargado de Protección de datos del Grupo, los Coordinadores de protección de datos y otros departamentos de la empresa con derechos de control o auditores externos encargados. Los resultados de los controles de la protección de datos se comunican al Encargado de Protección de datos del Grupo. Se informará al Consejo de vigilancia de Daimler AG sobre resultados relevantes en el marco de las obligaciones de información correspondientes. Los resultados de los controles de la protección de datos se pondrán a disposición de las autoridades competentes sobre protección de datos si éstas lo solicitan. Las autoridades competentes sobre protección de datos pueden realizar también controles propios del cumplimiento de esta norma de acuerdo con las autorizaciones contempladas en la legislación.

# XII. Transgresiones de la protección de datos

Todos los empleados deben informar sin demora a sus superiores, a su Coordinador de protección de datos o al Encargado de Protección de datos del Grupo acerca de infracciones contra la directriz de protección de datos o contra otras normas para la protección de datos de carácter personal (Transgresiones de la protección de datos[14]). El directivo responsable del área o la unidad corporativa está obligado a informar sin demora sobre cualquier transgresión de la protección de datos al Coordinador de protección de datos responsable o al Encargado de Protección de datos del Grupo.

Si se dan casos de
- entrega ilícita de datos de carácter personal a terceros,
- acceso no autorizado de terceros a datos de carácter personal, o
- pérdida de datos de carácter personal

se realizarán sin demora las comunicaciones previstas dentro de la empresa (Information Security Incident Management, 'Gestión de incidentes contra la seguridad de la información'), a fin de poder cumplir las obligaciones legales de información de este tipo de transgresiones.

# XIII. Responsabilidades y sanciones

Las juntas directivas y los órganos directivos de las Sociedades del Grupo son responsables del tratamiento de datos en su ámbito de responsabilidad. Por tanto, están obligados a asegurar que se cumplen los requerimientos de protección de datos exigidos por la ley y los recogidos en la directriz de protección de datos (por ejemplo, obligaciones nacionales de información). Es una tarea de gestión de los directivos asegurar mediante medidas técnicas, personales y de organización el tratamiento correcto de los datos, teniendo en cuenta las exigencias de protección de datos. El cumplimiento de estas prescripciones es responsabilidad de los empleados competentes. Si una autoridad estatal desea realizar un control de la protección de datos, se informará sin demora al Encargado de Protección de datos del Grupo.
Las gerencias de las Sociedades y los órganos de dirección de las plantas nombrarán un Coordinador de protección de datos, y lo darán a conocer al Encargado de Protección de datos del Grupo. Desde el punto de vista organizativo, previo acuerdo con el Encargado de Protección de datos del Grupo, es posible que un Coordinador de protección de datos asuma esta tarea para varias Sociedades o para varias plantas. Los Coordinadores de protección de datos son las personas de contacto locales para los asuntos de protección de datos. Los Coordinadores pueden realizar controles, y darán a conocer a los empleados el contenido de la Directriz sobre protección de datos. Las gerencias de las Sociedades están obligadas a asistir al Encargado de Protección de datos del Grupo y a los Coordinadores de protección de datos en su actividad.
Los responsables técnicos de los procesos comerciales y los proyectos tienen que informar a tiempo a los Coordinadores de protección de datos sobre nuevos procesos de tratamiento de datos de carácter personal. Si está previsto el tratamiento de datos con riesgos especiales para los derechos personales de los afectados, deberá solicitarse la participación del Encargado de Protección de datos del Grupo antes de dar comienzo al tratamiento. Esto se refiere especialmente a datos de carácter personal que requieran especial protección. Los directivos asegurarán que sus empleados reciben instrucción adecuada sobre la protección de datos. En muchos países, el tratamiento abusivo de datos de carácter personal y otras transgresiones similares contra las leyes de protección de datos es causa de persecución penal, y puede conducir a la obligación de pago de daños y perjuicios. Se podrán aplicar sanciones laborales a los empleados responsables de transgresiones.

[14] Ver el apartado XV.

# XIV. El Encargado de Protección de datos del Grupo

El Encargado de Protección de datos del Grupo es un órgano interno autónomo que vela por la observación de las prescripciones nacionales e internacionales de protección de datos. Es responsable de las directrices relacionadas con la protección de datos, y supervisa su cumplimiento. El Encargado de Protección de datos del Grupo es nombrado por la Junta directiva de Daimler AG. Las sociedades del Grupo obligadas a ello designan asimismo al Encargado del Grupo como su encargado legal de protección de datos. Las excepciones específicas a esta regla deben acordarse con el Encargado de Protección de datos del Grupo.
Los Coordinadores de protección de datos informan con diligencia al Encargado de Protección de datos del Grupo sobre riesgos para la protección de datos.
Cualquier interesado 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 de carácter personal y la seguridad de estos datos. Si lo desea el interesado, 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 esta Directriz sobre protección de datos, está obligado a dirigirse al Encargado de Protección de datos del Grupo. Las Gerencias de las Sociedades del Grupo deben tomar en consideración las decisiones del Encargado del Grupo en relación con transgresiones de la normativa de protección de datos. Se comunicarán siempre también al Encargado de Protección de datos del Grupo las consultas de autoridades.

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 0518, D-70546 Stuttgart
E-mail: mbox_datenschutz@daimler.com
En Intranet bajo http://intra.corpintra.net/cdp

# XV. Definiciones

- La Comisión de la UE reconoce un nivel adecuado de protección de datos en estados terceros solamente si se protege esencialmente el ámbito básico de la intimidad, tal como se entiende en el consenso de los estados miembros de la UE. La Comisión de la UE tiene en cuenta en sus decisiones todas las circunstancias relevantes para una transferencia de datos o para una categoría de transferencia de datos. Esto incluye una valoración del Derecho nacional y de las normas profesionales y las medidas de seguridad vigentes.
- Se considera que los datos están anonimizados si es imposible de forma duradera que cualquier persona pueda restablecer su relación con una persona, o bien si la relación con una persona sólo puede restablecerse con un coste desproporcionado de tiempo, dinero y mano de obra.
- Se consideran datos sujetos a una protección especial los datos de carácter personal que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos de los interesados, así como los datos relativos a la salud o a la sexualidad. El Derecho nacional puede considerar datos sujetos a una protección especial a otras categorías de datos, o puede establecer categorías de datos diferentes. Del mismo modo, es frecuente que los datos relacionados con delitos penales sólo puedan tratarse bajo determinadas condiciones, especificadas en el Derecho nacional.

- Interesado de acuerdo con los términos de esta directriz de protección de datos es cualquier persona física cuyos datos son sometidos a tratamiento. En algunos países, pueden ser también interesados las personas jurídicas.
- Transgresiones de la protección de datos son todos los hechos que permitan una sospecha justificada de que se han averiguado, recogido, modificado, copiado, transmitido o utilizado de forma ilegítima datos de carácter personal. Esto puede referirse a acciones de terceros o de los empleados.
- Tercero es cualquier persona o instancia con excepción del interesado y de la instancia responsable del tratamiento de los datos. Tampoco son terceros dentro de la UE según la legislación de protección de datos las empresas externas encargadas del tratamiento de los datos, que se consideran asignadas por ley a la instancia responsable.
- Estados terceros son, según la directiva sobre protección de datos, todos los estados que no pertenecen a la Unión Europea/Espacio Económico Europeo. Se exceptúan de esta consideración los estados con un nivel de protección de datos aceptable, reconocido por la Comisión de la UE.
- Consentimiento es una manifestación de voluntad voluntaria y vinculante, por la que el interesado consiente en el tratamiento de datos.
- Se considera necesario el tratamiento de datos de carácter personal si el objeto admisible o el interés legítimo no pueden alcanzarse sin los datos de carácter personal correspondientes, o sólo con un gasto desproporcionado de dinero o mano de obra.
- El Espacio Económico Europeo (EWR) es un entorno económico asociado con la UE, que incluye Noruega, Islandia y Liechtenstein.
- Se consideran datos de carácter personal todas las informaciones que guardan relación con una persona física determinada o identificable. Se considera identificable una persona, por ejemplo, si es posible establecer la relación de los datos con su persona mediante la combinación de una o varias informaciones, incluso con conocimientos adicionales poseídos de forma casual.
- Se da transferencia de datos cuando la instancia responsable da a conocer datos protegidos a terceros.
- Tratamiento de datos de carácter personal es cualquier operación de recogida, registro, organización, conservación, modificación, consulta, utilización, entrega, transmisión o difusión, aplicada a datos de carácter personal, así como su combinación, cotejo o interconexión, con o sin ayuda de procedimientos automatizados. Esto incluye también la destrucción, el borrado y el bloqueo de datos y soportes de datos.
- Instancia responsable es la Sociedad con autonomía jurídica propia dentro del Grupo Daimler que ha tomado la medida de tratamiento de datos dentro de sus actividades comerciales.

Daimler AG
Mercedesstr. 137
70327 Stuttgart
Germany
www.daimler.com