DAIMLER

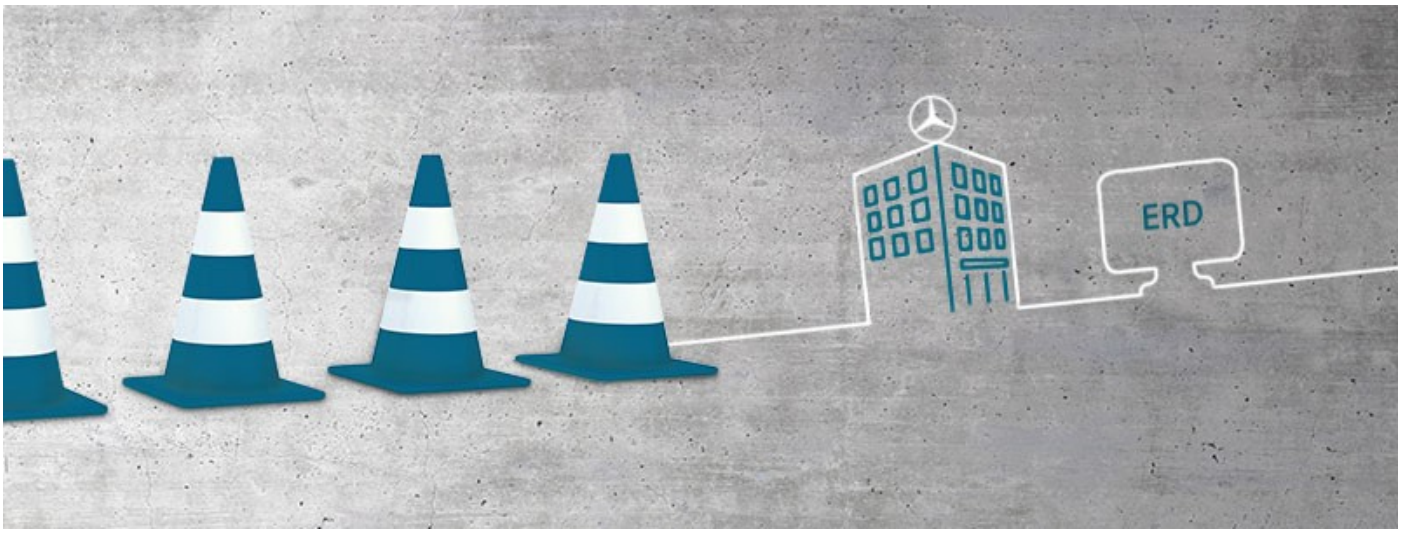
Directriz de protección de datos de la UE A 17.2

Persona de contacto

Andrea Schröder - IL/CDE - Daimler AG (0400)

Responsable de la norma

Sebastian Gress - IL/CD - Daimler AG (0400)



Objeto de la regulación/Resumen

Esta directriz regula el tratamiento de los datos personales de los empleados, clientes y socios de las Empresas del Grupo en el ámbito de aplicación del Reglamento General de Protección de Datos de la UE (RGPD-UE), es decir, las Empresas del Grupo en la UE/Espacio Económico Europeo, así como las Empresas del Grupo fuera de esta área que ofrecen productos o servicios en la UE o tratan datos personales procedentes de la UE. La directriz garantiza en su ámbito de aplicación una norma de protección y seguridad de datos estandarizada y válida a nivel mundial y crea las condiciones marco necesarias para la transferencia global de datos entre las Empresas del Grupo arriba mencionadas. Ya que la directriz también tiene un efecto externo, la última versión de la misma se publicará online en www.daimler.com.

Cambios respecto a la versión anterior

01/22/2020:

- Adaptación de la directriz a las disposiciones del Reglamento General de Protección de Datos de la Unión Europea (RGPD-EU), en vigor desde el 25 de mayo de 2018
- Adaptación del ámbito de aplicación de la directriz en lo que se refiere a «empresas radicadas en la UE», «empresas de terceros países que ofrecen productos o servicios en la UE» y «empresas de terceros países que tratan datos de la UE»
- Propietario de la Directriz actualizado
- Anexos, otras regulaciones aplicables y documentos útiles actualizados

Llamamiento a los empleados afectados

para miembros de órganos directivos de compañías del Grupo

Por favor, ponga en vigor esta directriz de forma inmediata y comuníqueselo a los empleados afectados.

DAIMLER

Directriz de protección de datos de la UE A 17.2

Para directivos de Daimler AG

Por favor, familiarícense con las disposiciones de esta directriz y cúmplanlas.

Para trabajadores de Daimler AG

Por favor, familiarícense con las disposiciones de esta directriz y cúmplanlas.

Para miembros de órganos directivos de compañías del programa Framework Light

Esta es una directriz obligatoria. Su sociedad se encuentra dentro del ámbito de aplicación de esta directriz. Le rogamos que ponga en vigor la directriz sin demora.

Ámbito de aplicación

Esta directriz se aplica a todos los trabajadores y miembros de los órganos directivos de Daimler AG y de todas las compañías controladas por el Grupo.

Período de validez de esta versión

22/01/2020 - 21/01/2025

Última revisión de esta versión

Tema

Integridad y Compliance (Protección de datos)

Aprobación

Renata Jungo Brüngger IL
17/12/2019

Documentación

Publicada en la base de datos unificada de normas corporativas (ERD) en el Portal del empleado de Daimler el 22/01/2020.

Documentos obligatorios

Documento de la directriz

Directriz de protección de datos de la UE: 23 páginas
Anexo 1: Glosario: 3 páginas
Anexo 2: Descripción general de la transmisión de datos a terceros países: 2 páginas

Otras regulaciones aplicables

- Documentación evaluación del impacto de la protección de datos (English)
- Documentación gestión de incidentes: canales de entrada (English)
- Documentación gestión de incidentes: tratamiento dentro de la protección de datos corporativa(English)
- Documentación gestión de incidentes: gestión local y (LCO)/(LCR) (English)
- Documentación gestión de incidentes: empleados (English)
- Documentación derechos de los interesados (English)

DAIMLER

Directriz de protección de datos de la UE A 17.2

- Documentación consentimiento de protección de datos (English)
- Documentación obligación de información (English)
- Documentación concepto de borrado (English)
- Documentación protección de datos por definición y por defecto (English)
- Documentación elaboración de perfiles y toma de decisiones automatizada (English)
- Documentación seguridad del tratamiento (English)
- Documentación clasificación de la confidencialidad de los datos personales (English)
- Documentación obligación de nombrar a un responsable de protección de datos en virtud del RGPD-UE y de notificar a la autoridad de supervisión compete
- Lista de Empresas del Grupo sujetas a la Directriz de protección de datos de la UE (English)

Documentos útiles

- Declaración de privacidad y banner de cookies (English)
- Plantilla de acuerdo de tratamiento en representación de terceros (English)
- Plantilla Compromiso de confidencialidad (English)

Índice

1 Objetivo de esta Directriz

El Grupo Daimler considera que la salvaguarda de los derechos de protección de datos forma parte de su responsabilidad social.

En algunos países y regiones, como la Unión Europea, los legisladores han definido normas para la protección de los datos de las personas físicas («datos personales»), incluido el requisito de que dichos datos solo puedan transferirse a otros países si la legislación local aplicable en el lugar de destino ofrece un nivel adecuado de protección de datos.

Esta Directriz de protección de datos de la UE establece estándares de protección de datos uniformes y adecuados dentro del Grupo para:

- (a) el tratamiento de datos personales en regiones como la UE/el Espacio Económico Europeo (EEE) (en lo sucesivo y colectivamente «**UE**») y
- (b) la transmisión transfronteriza de datos personales a Empresas del Grupo fuera de la UE (incluido el tratamiento posterior de datos en las mismas).

Con este fin, la presente Directriz establece normas vinculantes para el tratamiento de datos personales procedentes de la UE dentro del Grupo Daimler. Estas normas proporcionan garantías adecuadas para la protección de datos personales fuera de la UE para el Grupo Daimler denominadas «**Normas corporativas vinculantes (BCR)**».

2 Alcance

Esta Directriz de protección de datos de la UE se aplica a Daimler AG, a sus Empresas del Grupo controladas (en lo sucesivo **Empresas del Grupo**) y a sus empleados y miembros de los órganos de gestión. «Controladas» en este caso significa que Daimler AG puede obligarlas a adoptar esta directriz directa o indirectamente, en base a su mayoría de voto, representación mayoritaria en los órganos o por acuerdo.

La Directriz se aplica al tratamiento total o parcialmente automatizado de los datos personales, así como al tratamiento manual en sistemas de archivo a menos que la legislación nacional ofrezca un ámbito de aplicación más amplio. La Directriz también se refiere a todos los datos de los empleados[1] en formato impreso en Alemania.

La presente Directriz establece normas corporativas vinculantes y estándar para el tratamiento de datos personales procedentes de la UE para el Grupo Daimler, en lo sucesivo «normas corporativas vinculantes» (BCR, Binding Corporate Rules).

[1] Para facilitar la lectura de esta Directriz, el texto utiliza solo pronombres en su forma masculina para las personas físicas. Las palabras «él», «su» y «lo/a él» pretenden siempre incluir a todos los individuos con independencia de su identidad de género.

La Directriz se aplica al tratamiento de datos personales:

- (a) de Empresas del Grupo y sus filiales establecidas en la UE o en otro país al que pueda extenderse la presente Directriz («empresas radicadas en la UE»),
- (b) de Empresas del Grupo establecidas fuera de la UE, si ofrecen bienes o servicios a personas físicas dentro de la UE y/o supervisan el comportamiento de personas físicas dentro de la UE («empresas de terceros países con ofertas para la UE») o
- (c) de Empresas del Grupo establecidas fuera de la UE, si han recibido datos personales directa o indirectamente de empresas que están sujetas a la Directriz en sus puntos a) o b), o si se les han revelado dichos datos («empresas de terceros países que reciben datos de la UE»).

La directriz se aplica al tratamiento de datos personales de

- empresas radicadas en la UE
- empresas de terceros países con ofertas para la UE
- de empresas de terceros países que reciben datos de la UE

El tratamiento fuera de la UE se denomina también en la presente Directriz como tratamiento en un tercer país.

Las Empresas del Grupo que participan o son objeto de tratamiento por parte de empresas de terceros países se enumeran en la normativa aplicable adicional «Lista de Empresas del Grupo sujetas a la Directriz de protección de datos de la UE».

Esta Directriz puede extenderse a países fuera de la UE. En aquellos países en los que los datos de las personas jurídicas están protegidos de la misma manera que los datos personales, esta Directriz también se aplicará de la misma manera a los datos de las personas jurídicas.

3 Exigibilidad legal dentro del Grupo Daimler

Las normas y disposiciones de esta Directriz son vinculantes para todas las Empresas del Grupo que operan dentro de su ámbito de aplicación. Además de la legislación comunitaria aplicable y de las leyes nacionales de protección de datos, las Empresas del Grupo, así como sus directivos y empleados, son responsables del cumplimiento de esta Directriz.
En la medida en la que los requisitos legales no lo exijan, las Empresas del Grupo no están facultadas para adoptar regulaciones que se aparten de esta Directriz.

4 Relación con los requisitos legales

Esta Directriz no sustituye a la legislación comunitaria ni a las leyes nacionales. Complementa las leyes nacionales en materia de protección de datos. Estas regulaciones y leyes tendrán prioridad si como resultado del cumplimiento de esta Directriz se infringiera la legislación nacional. También debe respetarse el contenido de esta Directriz en ausencia de las leyes nacionales correspondientes.

En caso de que el cumplimiento de esta Directriz implicara que se infringiera la legislación nacional, o en caso de que la legislación nacional

exigiera una regulación que se aparte de esta Directriz, se deberá informar de ello al Director corporativo de protección de datos (Chief Officer Corporate Data Protection) y a la organización central de cumplimiento a efectos de control de la legislación en materia de protección de datos. En caso de conflicto entre las leyes nacionales y esta Directriz, el Director corporativo de protección de datos y la organización central de cumplimiento colaborarán con la empresa responsable del Grupo para encontrar una solución práctica que cumpla con los objetivos de la presente Directriz.

5 Principios generales para el tratamiento de datos personales

5.1 Legalidad

Todo tratamiento de datos personales requiere un fundamento jurídico adecuado.

Los datos personales deben ser tratados de forma lícita y de buena fe. El tratamiento de datos solo podrá llevarse a cabo si y en la medida en que exista un fundamento jurídico suficiente para la actividad de tratamiento. Esto también se aplica al tratamiento de datos entre Empresas del Grupo. El mero hecho de que ambas partes, la Empresa del Grupo que cede los datos y la que los recibe, estén afiliadas al Grupo Daimler no constituye de por sí dicho fundamento jurídico.

El tratamiento de datos personales será lícito si se da una de las siguientes circunstancias para la autorización conforme a los apartados 5.2 o 5.3. Tales circunstancias de permisibilidad también son necesarias si la finalidad del tratamiento de los datos personales ha de modificarse con respecto a la finalidad original.

5.2 Fundamento jurídico de datos de clientes y socios

5.2.1 Tratamiento de datos para una relación contractual

Los datos de clientes y socios pueden tratarse para formalizar, ejecutar y rescindir un contrato y para el proceso de negociación del contrato.

Los datos personales de clientes potenciales, clientes o socios pueden tratarse para formalizar, ejecutar y rescindir un contrato. Esto también incluye los servicios de asesoramiento para el cliente o socio en virtud del contrato si está relacionado con la finalidad del contrato.

Antes del contrato, los datos personales pueden ser tratados para preparar ofertas u órdenes de compra o para cumplir con otras peticiones del cliente potencial relacionadas con la formalización del contrato. Puede contactarse con los clientes potenciales durante el proceso de preparación del contrato tratando la información que estos han proporcionado. Deben cumplirse todas las limitaciones solicitadas por los clientes potenciales.

5.2.2 Tratamiento de datos con fines publicitarios

Si el interesado se pone en contacto con una Empresa del Grupo para solicitar información (por ejemplo, para recibir material informativo sobre un producto), se permite el tratamiento de los datos personales para dar respuesta a esta solicitud. La fidelización de los clientes o las acciones publicitarias están sujetas a otros requisitos legales. Los datos personales pueden ser tratados con fines publicitarios o de investigación de mercado y de opinión, siempre que cumplan con la finalidad para la que fueron recogidos originalmente. El interesado debe ser informado con antelación sobre el uso de sus datos personales con fines publicitarios. Si los datos personales se recogen solo con fines publicitarios, el interesado podrá elegir si desea facilitarlos o no. Se informará al interesado de que el suministro de datos con este fin es voluntario. Como parte del proceso de comunicación, debe obtenerse el consentimiento del interesado. Al dar su consentimiento, el interesado debe poder elegir entre las formas de contacto disponibles, como correo electrónico y teléfono (consentimiento, véase el apartado 5.2.3). Si el interesado se opone a la utilización de sus datos con fines publicitarios, ya no se podrán utilizar a tal efecto y se deberá restringir o bloquear su utilización para estos fines. Deberá respetarse cualquier otra limitación en países específicos con respecto al uso de los datos con fines publicitarios.

Si los datos de los clientes y socios se recopilan únicamente con fines publicitarios, deberá obtenerse el consentimiento del interesado antes de iniciar el tratamiento.

5.2.3 Consentimiento para el tratamiento de datos

Los datos personales pueden ser tratados previo consentimiento del interesado. Antes de dar su consentimiento, el interesado debe ser informado conforme a la presente Directriz de protección de datos de la UE. La declaración de consentimiento debe obtenerse por escrito o electrónicamente a efectos de documentación. En algunas circunstancias, como en las conversaciones telefónicas, también se puede dar el consentimiento verbalmente. La concesión de dicho consentimiento debe documentarse.

5.2.4 Tratamiento de datos en virtud de la autorización u obligación legal

El tratamiento de datos personales también está permitido si la legislación nacional lo solicita, exige o permite. El tipo y el alcance del tratamiento de datos deben ser los necesarios para la actividad de tratamiento autorizada legalmente y deben cumplir las disposiciones legales relevantes.

Los datos de clientes y socios pueden tratarse para cumplir con la legislación nacional.

5.2.5 Tratamiento de datos por interés legítimo

Los datos personales también pueden tratarse si son necesarios para un interés legítimo. Los intereses legítimos son generalmente de naturaleza comercial (por ejemplo, el cobro de créditos pendientes) o legal (por ejemplo, evitar incumplimientos de contrato). El tratamiento no puede basarse en un interés legítimo si, en un caso concreto, los intereses de los interesados sujetos a protección prevalecen sobre los intereses

Los datos de clientes y socios pueden tratarse en base a un interés legítimo, a menos que los intereses del interesado sujetos a protección, sean superiores al interés legítimo del tratamiento.

legítimos del tratamiento. Antes de tratar los datos, es necesario determinar si existen intereses sujetos a protección.

5.3 Fundamento jurídico Datos de empleados

5.3.1 Tratamiento de datos para la relación laboral

En el caso de las relaciones laborales, los datos personales pueden tratarse si es necesario para establecer, desarrollar y rescindir la relación laboral. Los datos personales de los candidatos pueden tratarse para ayudar a decidir si desean formalizar una relación laboral. Si el candidato es rechazado, sus datos deben ser eliminados teniendo en cuenta el período de retención requerido, a menos que el candidato haya aceptado que permanezcan en el archivo para futuros procesos de selección. También es necesario el consentimiento para utilizar los datos en otros procesos de solicitud o antes de compartir la solicitud con otras Empresas del Grupo. En la relación laboral existente, el tratamiento de datos debe estar siempre relacionado con la finalidad de la relación laboral si no se aplica ninguna de las siguientes circunstancias para el tratamiento autorizado de los datos.

Los datos de los empleados pueden tratarse para establecer, desarrollar y rescindir una relación laboral y como parte del proceso de solicitud de empleo.

Si durante el procedimiento de solicitud fuera necesario recopilar información sobre un candidato proveniente de un tercero, deberán tenerse en cuenta los requisitos de las leyes nacionales correspondientes. En caso de duda, en los casos en los que esté permitido, deberá obtenerse el consentimiento del interesado.

Para tratar los datos personales relativos a la relación laboral, pero que no formaban parte originalmente del establecimiento, desarrollo o rescisión de la relación laboral (datos de los empleados), deberá cumplirse el fundamento jurídico que se indica a continuación.

5.3.2 Tratamiento de datos en virtud de la autorización u obligación legal

El tratamiento de los datos de empleados también está permitido si la legislación nacional lo solicita, exige o permite. El tipo y el alcance del tratamiento de datos deben ser los necesarios para la actividad de tratamiento autorizada legalmente y deben cumplir las disposiciones legales relevantes. Si existe cierta flexibilidad legal, se deben tener en cuenta los intereses de protección del empleado.

5.3.3 Convenio colectivo sobre tratamiento de datos

Si una actividad de tratamiento de datos excede los fines del cumplimiento de un contrato, puede seguir siendo lícita si se autoriza a través de un convenio colectivo. Los acuerdos deben abarcar la finalidad específica de la actividad de tratamiento de datos prevista y deben elaborarse dentro de los parámetros de la legislación comunitaria y nacional.

El tratamiento de los datos de empleados puede realizarse si está autorizado por un convenio colectivo.

5.3.4 Consentimiento para el tratamiento de datos

Los datos de los empleados pueden tratarse con el consentimiento del interesado. Las declaraciones de consentimiento deben presentarse voluntariamente. No se pueden imponer sanciones por no ofrecer el consentimiento. El consentimiento involuntario no es válido. La declaración de consentimiento debe obtenerse por escrito o electrónicamente a efectos de documentación. Si, excepcionalmente, las circunstancias no lo permiten, se puede dar el consentimiento verbalmente. En cualquier caso, su concesión debe estar debidamente documentada. Antes de dar su consentimiento, el interesado debe ser informado conforme a la presente Directriz de protección de datos de la UE.

5.3.5 Tratamiento de datos por interés legítimo

Los datos de empleados también pueden tratarse si son necesarios para un interés legítimo de una Empresa del Grupo. Los intereses legítimos son generalmente de naturaleza legal (por ejemplo, la presentación, ejecución o defensa contra reclamaciones legales) o comercial (por ejemplo, la aceleración de los procesos comerciales, la valoración de las empresas). Antes de tratar los datos, se debe determinar si existen intereses sujetos a protección. Los datos personales pueden tratarse en base a un interés legítimo si los intereses sujetos a protección del empleado no prevalecen sobre el interés del tratamiento.

Los datos de empleados pueden tratarse en base a un interés legítimo, a menos que los intereses del interesado sujetos a protección, sean superiores al interés legítimo del tratamiento.

Las medidas de control que requiere el tratamiento de los datos de empleados más allá del desarrollo de la relación laboral (por ejemplo, controles de rendimiento) no pueden tomarse a menos que exista una obligación legal o una razón justificada para ello. Incluso si existe una razón legítima, también debe examinarse la proporcionalidad de la medida de control. A tal fin, deben sopesarse los intereses legítimos de la Empresa del Grupo en la ejecución de la medida de control (por ejemplo, el cumplimiento de las disposiciones legales y de las normas internas de la empresa) con los intereses de protección que pueda tener el empleado afectado por la medida por la exclusión de la misma. Las medidas solo pueden tomarse si son apropiadas para el caso específico. El interés legítimo de la Empresa del Grupo y los intereses sujetos a protección del empleado deben identificarse y documentarse antes de tomar cualquier medida. Además, deberá tenerse en cuenta cualquier requisito adicional previsto en la legislación aplicable (por ejemplo, los derechos de participación de los representantes de los trabajadores y los derechos de los interesados a obtener información).

5.4 Tratamiento de datos altamente sensibles

El tratamiento de datos personales altamente sensibles debe permitirse expresamente o estar prescrito por la legislación nacional. El tratamiento de dichos datos por parte de la Empresa del Grupo podrá permitirse, en particular, si el interesado ha dado su consentimiento expreso, si el tratamiento es necesario para hacer valer, ejercer o defender

Para el tratamiento de datos altamente sensibles se requiere la autorización legal o el consentimiento expreso del interesado.

reclamaciones legales con respecto al interesado o si es necesario para que el responsable del tratamiento pueda cumplir sus derechos y responsabilidades en el ámbito del derecho laboral. Si se planea realizar el tratamiento de datos personales altamente sensibles, se deberá informar previamente al Director corporativo de protección de datos.

5.5 Toma de decisiones individual automatizada (posiblemente incl. elaboración de perfiles)

Los interesados solo podrán ser objeto de una decisión totalmente automatizada que pueda tener un impacto jurídico o similarmente negativo en ellos si es necesario para celebrar o ejecutar un contrato, o si el interesado ha dado su consentimiento. Esta decisión automatizada puede incluir la elaboración de perfiles en algunos casos, es decir, el tratamiento de datos personales que evalúa las características individuales de la personalidad (por ejemplo, la solvencia). En este caso, debe notificarse al interesado la existencia y el resultado de una decisión individual automatizada y se le debe dar la oportunidad de que un responsable del tratamiento lleve a cabo una revisión individual.

Las decisiones individuales automatizadas y la elaboración de perfiles solo se permiten bajo condiciones estrictas.

5.6 Deber de información/Transparencia

El departamento responsable deberá informar a los interesados de las finalidades y circunstancias del tratamiento de sus datos personales de forma concisa, transparente, inteligible, fácilmente accesible y en un lenguaje claro y sencillo. Deben tenerse en cuenta los requisitos del Director corporativo de protección de datos y del Cumplimiento de datos. Esta información deberá facilitarse cada vez que se recopilen por primera vez los datos personales. Si la Empresa del Grupo recibe los datos personales de un tercero, deberá facilitar la información al interesado en un plazo razonable tras la obtención de los datos, salvo que

- el interesado ya disponga de la información o
- sea imposible o
- extremadamente difícil facilitar dicha información.

El interesado debe ser informado de las finalidades y circunstancias del tratamiento de sus datos personales.

5.7 Limitación de la finalidad

Los datos personales solo podrán tratarse para la finalidad legítima definida antes de la recopilación de los datos. Las modificaciones posteriores de la finalidad del tratamiento solo son admisibles con la condición de que el tratamiento sea compatible con los fines para los que se recogieron inicialmente los datos personales.

Los datos personales solo podrán tratarse para la finalidad legítima definida antes de la recopilación de los datos.

5.8 Minimización de datos

Cualquier tratamiento de datos personales debe limitarse, tanto cuantitativa como cualitativamente, a lo que sea necesario para alcanzar los fines para los que se tratan legalmente. Esto debe tenerse en cuenta durante la recopilación inicial de datos. Si la finalidad lo permite, y el

El tratamiento de datos personales debe limitarse a lo que sea necesario para alcanzar la finalidad para la que se tratan legalmente.

esfuerzo es proporcional al objetivo perseguido, se deben utilizar datos anonimizados o estadísticos.

5.9 Exactitud de los datos

Los datos personales almacenados deben ser objetivamente correctos y, si es necesario, estar actualizados. Deben adoptarse las medidas adecuadas para garantizar que los datos incorrectos o incompletos se eliminen, corrijan, completen o actualicen.

5.10 Privacidad mediante el diseño

El principio de «privacidad mediante el diseño» tiene como objetivo garantizar que los departamentos definan estrategias internas de vanguardia y adopten medidas para integrar los principios de protección de datos en las especificaciones y la arquitectura de los modelos, procesos de negocio y sistemas de TI para el tratamiento de datos desde el principio, durante la fase de conceptualización y diseño técnico. Según el principio de «privacidad mediante el diseño», los procedimientos y sistemas para el tratamiento de datos personales deben diseñarse de tal manera que su configuración predeterminada se limite al tratamiento de datos necesario para cumplir la finalidad. Esto incluye el alcance del tratamiento, el período de almacenamiento y la accesibilidad. Otras medidas podrían incluir:

- seudonimización de los datos personales en cuanto sea posible
- garantizar la transparencia de las funciones y del tratamiento de los datos personales
- permitir que los interesados decidan sobre el tratamiento de sus datos personales
- permitir a los operadores de los procedimientos o sistemas diseñar y mejorar las características de seguridad

Los principios de protección de datos deben integrarse en la arquitectura de los modelos de negocio, los procesos y los sistemas de TI.

Todas las Empresas del Grupo implementarán y mantendrán las medidas técnicas y organizativas adecuadas a lo largo de todo el ciclo de vida de sus actividades de tratamiento, con el fin de asegurar en todo momento el cumplimiento de los principios anteriores.

5.11 Borrado y anonimización

Los datos personales solo podrán almacenarse durante el tiempo que sea necesario para la finalidad del tratamiento. Esto significa que los datos personales deberán borrarse o anonimizarse tan pronto como se haya cumplido la finalidad de su tratamiento o caduque, a menos que se sigan aplicando las obligaciones de documentación o retención. Los responsables de los procedimientos individuales deben garantizar la implementación de las rutinas de borrado y anonimización en sus procedimientos. Todos los sistemas deben tener una rutina de borrado manual o automática. Las solicitudes de borrado de los interesados mediante la supresión o eliminación de los identificadores personales deberán poder realizarse técnicamente en los sistemas. Se deben respetar los requisitos que Daimler AG imponga para la ejecución de las

Los datos personales solo podrán almacenarse durante el tiempo que sea necesario para la finalidad del tratamiento.

rutinas de borrado (como las herramientas de software, conceptos de documentación para la implementación del borrado, requisitos de documentación).

5.12 Seguridad del tratamiento

Los datos personales deben estar protegidos contra el acceso no autorizado y el tratamiento o la transferencia ilícitos, así como contra la pérdida accidental, alteración o destrucción. Antes de introducir nuevos métodos de tratamiento de datos, en particular de nuevos sistemas de TI, deberán definirse y aplicarse las medidas técnicas y organizativas necesarias para proteger los datos personales. Estas medidas deben basarse en el estado actual de la técnica, los riesgos del tratamiento y la necesidad de proteger los datos.

Las medidas técnicas y organizativas deben garantizar la seguridad del tratamiento de los datos.

Las medidas técnicas y organizativas pertinentes para la protección de datos deben ser documentadas por el responsable del tratamiento en el contexto de la evaluación de impacto de la protección de datos y del registro de actividades de tratamiento.

En particular, el departamento responsable debe consultar a su Responsable de seguridad de la información empresarial (BISO, Business Information Security Officer), a su responsable de seguridad de la información (ISO, Information Security Officer) y a su Red de protección de datos. Los requisitos de las medidas técnicas y organizativas para la protección de datos personales forman parte de la Gestión de Seguridad de la Información Corporativa y deben adaptarse continuamente según los avances técnicos y los cambios organizativos.

5.13 (Adicional) Transmisión fuera del Grupo Daimler

La transmisión de datos personales a destinatarios fuera o dentro de las Empresas del Grupo está sujeta a los requisitos de autorización para el tratamiento de datos personales incluidos en el presente apartado 5. Se debe obligar al destinatario de los datos a utilizarlos solo para los fines definidos.

En caso de transmisión transfronteriza de los datos personales (incluida la concesión de acceso desde otro país), deberán cumplirse los requisitos nacionales pertinentes para la transferencia de datos personales al extranjero. En particular, los datos personales de la UE solo podrán tratarse fuera de las Empresas del Grupo en un tercer país si el destinatario puede demostrar que dispone de un nivel de protección de datos equivalente al de la presente Directriz. Para ello son adecuadas las siguientes herramientas:

- Acuerdo sobre cláusulas contractuales estándar de la UE,
- Participación del destinatario en un sistema de certificación acreditado por la UE para garantizar un nivel adecuado de protección de datos, o

En caso de transmisión transfronteriza, el destinatario debe demostrar que dispone de un nivel de protección de datos equivalente al de la presente Directriz.

- Reconocimiento de las normas corporativas vinculantes del receptor para crear un nivel adecuado de protección de datos por parte de las autoridades de supervisión responsables.

Las transferencias de datos personales a cualquier autoridad pública no pueden ser masivas, desproporcionadas e indiscriminadas de manera que vayan más allá de lo necesario en una sociedad democrática. En caso de conflicto entre estos y los requisitos de la autoridad pública, Daimler AG trabajará con la Empresa del Grupo responsable para encontrar una solución práctica que cumpla con la finalidad de esta Directriz.

Todas las obligaciones enumeradas en este apartado 5 son derechos de terceros beneficiarios para el interesado.

6 Evaluación de impacto de la protección de datos

Las Empresas del Grupo, al introducir nuevos tratamientos, o en el caso de que se produzca un cambio significativo en un tratamiento existente, en particular mediante el uso de nuevas tecnologías, evaluarán si este tratamiento supone un alto riesgo para la privacidad de los interesados. Debe tenerse en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento de datos. Como parte del análisis de riesgos, el departamento responsable llevará a cabo una evaluación de impacto del tratamiento previsto sobre la protección de los datos personales (evaluación de impacto de la protección de datos). Se deberán respetar las disposiciones establecidas por Daimler AG para realizar dicha evaluación (como herramientas de software, instrucciones sobre la realización de la evaluación).

Una evaluación de impacto de la protección de datos evalúa el tratamiento previsto en materia de protección de datos personales.

7 Documentación de los procedimientos de tratamiento de datos

Cada Empresa del Grupo deberá documentar en un Registro de actividades de tratamiento los procedimientos en los que se procesan datos personales. Se deberán respetar las disposiciones establecidas por Daimler AG para la documentación (como las herramientas de software y las instrucciones sobre la documentación).

Los procedimientos de tratamiento de datos se documentan en un registro de actividades de tratamiento.

8 Tratamiento en representación de terceros

8.1 Generalidades

El tratamiento en representación de terceros significa que un contratista trata los datos personales como proveedor de servicios (encargado del tratamiento) en nombre del responsable del tratamiento y según sus instrucciones. En estos casos, debe celebrarse un acuerdo de tratamiento en representación de terceros tanto con los encargados del tratamiento externos como entre las Empresas del Grupo Daimler. El

El tratamiento en representación de terceros requiere un acuerdo escrito entre el responsable del tratamiento y el encargado del tratamiento.

responsable del tratamiento sigue siendo el responsable único de la correcta realización del tratamiento de los datos.

Las disposiciones del apartado 8.3. también se aplican a los responsables del tratamiento externos que no son Empresas del Grupo.

La exigibilidad de estas disposiciones debe ser garantizada por los encargados del tratamiento internos del Grupo mediante la inclusión de la siguiente regulación en el acuerdo de tratamiento en representación de terceros: La actividad de tratamiento de datos está sujeta a las normas corporativas vinculantes del encargado del tratamiento, que la autoridad de supervisión competente considere suficientes para crear un nivel adecuado de protección de datos según se recoge en la legislación comunitaria. En este sentido, las normas corporativas vinculantes del responsable del tratamiento son vinculantes para el encargado del tratamiento.

8.2 Disposiciones para los responsables del tratamiento

Al emitir el pedido, se deben cumplir los siguientes requisitos, por lo que el departamento que realiza el pedido debe asegurarse de que se cumplan:

- La elección del encargado del tratamiento debe basarse en su capacidad para cumplir con las medidas de protección técnicas y organizativas necesarias.
- Deben cumplirse las normas contractuales de protección de datos del Director corporativo de protección de datos.
- El pedido debe realizarse por escrito o en formato electrónico. Deberán documentarse las instrucciones sobre el tratamiento de datos y las responsabilidades del responsable del tratamiento y del encargado del tratamiento.

Antes de iniciar el tratamiento de datos, el responsable del tratamiento debe confirmar mediante una evaluación adecuada que el encargado del tratamiento cumplirá las obligaciones antes mencionadas. Se deberán respetar las disposiciones establecidas por Daimler AG en esta materia (como herramientas de software, instrucciones sobre la realización de la evaluación, plantillas de contrato). Un encargado del tratamiento puede documentar su cumplimiento de los requisitos de protección de datos, en particular presentando una certificación adecuada. En función del riesgo del tratamiento de datos, se deben repetir las revisiones periódicamente durante la vigencia del contrato.

8.3 Disposición para encargados del tratamiento internos

El encargado del tratamiento puede tratar datos personales únicamente según las instrucciones del responsable del tratamiento.

Los encargados del tratamiento pueden involucrar a otras Empresas del Grupo o a terceros («**subcontratistas**») para que traten los datos

personales en su propio (sub)contrato solo con el consentimiento previo del responsable del tratamiento. Este consentimiento solo se concederá si el encargado del tratamiento somete al subcontratista, contractualmente o por otros medios jurídicamente vinculantes comparables, a las mismas obligaciones de protección de datos a las que está sujeto el encargado del tratamiento en virtud de esta directriz en lo que se refiere a la Empresa del Grupo y a los interesados. También debe obligar al subcontratista a tomar las medidas de protección técnicas y organizativas adecuadas. La forma de consentimiento, así como las obligaciones de información en caso de cambios en la relación de subcontratación, deben establecerse en el contrato de servicios.

Los encargados del tratamiento están obligados a prestar el apoyo adecuado al responsable del tratamiento en el cumplimiento de las disposiciones de protección de datos aplicables a este último, en particular facilitando toda la información necesaria. Esto se refiere, en particular, a la salvaguarda de

- los principios generales para el tratamiento en virtud del apartado 5
- los derechos de los interesados en virtud del apartado 10
- la notificación de incidentes de protección de datos en virtud del apartado 12
- las disposiciones relativas al responsable del tratamiento y a los encargados del tratamiento en virtud del apartado 8
- y el tratamiento de las solicitudes e investigaciones por parte de las autoridades de supervisión.

Si las normas o disposiciones legales aplicables exigen que el encargado del tratamiento realice el tratamiento en contra de las instrucciones del responsable del tratamiento, o si estas disposiciones impiden al encargado del tratamiento cumplir sus obligaciones en virtud de la presente Directriz o del acuerdo sobre el tratamiento en representación de terceros, el encargado del tratamiento informará inmediatamente a su responsable del tratamiento, a menos que la disposición legal en cuestión prohíba dicha notificación. Esto se aplica en consecuencia si el encargado del tratamiento no puede cumplir con las instrucciones de su responsable del tratamiento por otras razones. En tal caso, el responsable del tratamiento tiene derecho a suspender la transmisión de los datos y/o a rescindir el contrato de tratamiento en representación de terceros.

Los encargados del tratamiento están obligados a notificar a sus responsables del tratamiento cualquier solicitud jurídicamente vinculante de divulgación de datos personales por parte de las autoridades públicas, a menos que esté prohibido por otras razones.

A elección del responsable del tratamiento, el encargado del tratamiento deberá borrar o devolver todos los datos personales facilitados por el responsable del tratamiento en el momento de la finalización del servicio.

Los encargados del tratamiento están obligados a informar inmediatamente a su responsable del tratamiento y, en su caso, al cliente del responsable del tratamiento de cualquier reclamación, solicitud o queja de los interesados.

Los responsables del tratamiento internos del Grupo también deben obligar a los encargados del tratamiento externos a cumplir con la regulaciones anteriormente mencionada.

Las obligaciones específicas del encargado del tratamiento frente al responsable del tratamiento son derechos de terceros beneficiarios para el interesado.

9 Responsabilidad conjunta

En el caso de que varias Empresas del Grupo definan conjuntamente los medios y finalidades del tratamiento de los datos personales (junto con uno o varios terceros, en su caso) (corresponsables del tratamiento), las empresas deberán suscribir un acuerdo en el que se estipulen sus deberes y responsabilidades para con el interesado cuyos datos vayan a tratar.
Deben tenerse en cuenta las plantillas de contrato facilitadas por el Director corporativo de protección de datos.

Si los medios y finalidades del tratamiento de los datos son definidos conjuntamente por varias Empresas del Grupo, deberá celebrarse un acuerdo por escrito entre los responsables del tratamiento.

10 Derechos exigibles a los interesados

Todos los derechos de los interesados y obligaciones de las Empresas del Grupo enumeradas en el presente apartado 10 son derechos de terceros beneficiarios del interesado.

Las consultas y reclamaciones presentadas de conformidad con el presente apartado 10 deberán, en general, recibir respuesta en el plazo de un mes; en casos excepcionales justificados, este plazo podrá ampliarse a un máximo de tres meses a partir de la fecha de recepción.

10.1 Derechos de los interesados

Un interesado comunitario goza de los siguientes derechos, tal y como se especifica con más detalle en la legislación de la UE, frente a la Empresa del Grupo responsable o, si la Empresa del Grupo es el encargado del tratamiento, frente al responsable del tratamiento:

- el derecho a ser informado de las circunstancias del tratamiento de sus datos personales. Deben tenerse en cuenta los requisitos del Director corporativo de protección de datos para dicha información.
- el derecho a obtener información sobre el tratamiento de sus datos y sobre los derechos que le corresponden a este respecto. Si existen otros derechos para ver los documentos del empleador (por ejemplo, el archivo de personal) para la relación laboral en virtud de las leyes laborales pertinentes, estos no se verán afectados. Previa solicitud, el interesado puede recibir una copia de sus datos personales (posiblemente por un precio razonable), a menos que los intereses de terceros sujetos a protección lo prohíban.
- el derecho a corregir o complementar los datos personales si son incorrectos o incompletos.
- el derecho a suprimir sus datos personales si retira su consentimiento o si el fundamento jurídico ha dejado de aplicarse. Lo mismo se aplica si la finalidad del tratamiento de datos ha caducado o ha dejado de ser aplicable por otros motivos. Deben respetarse los plazos de retención existentes y los intereses sujetos a protección que prohíben la supresión.
- el derecho a limitar el tratamiento de sus datos si no está de acuerdo con su exactitud o si la Empresa del Grupo ya no necesita los datos mientras que el interesado los necesita para sus reclamaciones legales. El interesado también puede solicitar a la Empresa del Grupo que limite el tratamiento de sus datos en caso de que, de lo contrario, tenga que borrarlos o si está estudiando una objeción por parte del interesado.
- el derecho a recibir los datos personales que le conciernen, que haya facilitado sobre la base de su consentimiento, o en el contexto de un acuerdo celebrado o iniciado con él, en un formato digital de uso común. También tiene derecho a transmitir estos datos a un tercero si los datos se gestionan por medios automatizados y esto es técnicamente viable.
- el derecho a oponerse al marketing directo en cualquier momento. Debe garantizarse un sistema adecuado de gestión de los consentimientos y las objeciones.
- el derecho a oponerse al tratamiento de los datos personales que se realice sobre el fundamento jurídico de los intereses prioritarios de una Empresa del Grupo o de un tercero, por motivos relacionados con su situación personal particular. Sin embargo, este derecho de oposición no se aplica si la Empresa del Grupo tiene razones de peso para el tratamiento o si los datos están siendo tratados para el establecimiento, ejercicio o defensa de

En la UE, los interesados tienen los siguientes derechos:
- Derecho a la información
- Derecho de acceso
- Derecho de rectificación
- Derecho de supresión
- Derecho de limitación
- Derecho de portabilidad de los datos
- Derecho de objeción
- Derecho a presentar reclamaciones ante el Director corporativo de protección de datos o ante la autoridad de supervisión competente
- El derecho a interponer una demanda ante el tribunal competente

reclamaciones legales. Si hay una objeción legítima, los datos deben ser borrados.

Además, el interesado también tiene la facultad de hacer valer sus derechos frente a la Empresa del Grupo que importe los datos en un tercer país.

10.2 Procedimiento de reclamaciones

Los interesados tienen derecho a presentar una reclamación ante el Director corporativo de protección de datos si consideran que se ha infringido esta Directriz. Las reclamaciones de este tipo pueden enviarse por correo electrónico.

La Empresa del Grupo establecida en la UE que exporte los datos ayudará a los interesados cuyos datos personales hayan sido recopilados en la UE a establecer los hechos y a hacer valer sus derechos en virtud de la presente Directriz frente a la Empresa del Grupo que importe los datos.

En caso de que el interesado esté en desacuerdo con la decisión de una Empresa del Grupo sobre el cumplimiento de los requisitos (o no esté satisfecho con su tratamiento), podrá impugnar dicha decisión o conducta mediante el ejercicio de sus derechos. A tal fin, podrá dirigirse a la autoridad de supervisión competente o interponer un recurso ante los tribunales. Otros derechos y responsabilidades legales no se verán afectados.

11 Responsabilidad y jurisdicción

11.1 Disposiciones de responsabilidad

La Empresa del Grupo establecida en la UE («exportador de los datos») que inicialmente transfirió los datos personales a una Empresa del Grupo radicada en un tercer país asumirá la responsabilidad por cada vulneración de esta Directriz por parte de la Empresa del Grupo de dicho tercer país que reciba los datos de la UE para su tratamiento en un tercer país. Esta responsabilidad incluye la obligación de subsanar las situaciones ilícitas, así como la de indemnizar por los daños materiales y no materiales causados por el incumplimiento de esta Directriz por parte de las Empresas del Grupo de terceros países.

El exportador de los datos es el responsable de remediar situaciones ilegales y de compensar los daños causados por el incumplimiento de esta Directriz por parte de una Empresa del Grupo de un tercer país.

El exportador de datos solo quedará exento de toda o parte de esta responsabilidad si puede demostrar que la Empresa del Grupo de un tercer país que recibe datos de la UE no es responsable de la acción que ha provocado el daño.
Si una Empresa del Grupo trata datos personales como encargado del tratamiento para una empresa que no forma parte del Grupo Daimler y dicho tratamiento incluye la transmisión de datos personales a subcontratistas fuera de la UE, la Empresa del Grupo será la responsable, de conformidad con el presente apartado 11, del incumplimiento de la

presente Directriz de protección de datos de la UE y del acuerdo que se celebre en virtud del apartado 8.1. También será responsable de los incumplimientos de su subcontratista respecto de la anterior Directriz de protección de datos de la UE. Asimismo, los interesados afectados tienen derecho a reclamar a la Empresa exportadora del Grupo el reembolso de la totalidad de los daños causados por la Empresa del Grupo y el subcontratista. Esto se aplica especialmente si las reclamaciones de los interesados afectados en virtud del apartado 10 contra el responsable del tratamiento o su sucesor legal no son exigibles porque este último ya no existe o es insolvente.

11.2 Jurisdicción

Cualquier consumidor, que también sea el titular de los datos/interesado, podrá interponer una demanda ante el órgano jurisdiccional competente. El resto de personas solo podrán presentar acciones legales ante los tribunales en la sede del responsable del tratamiento.

Cualquier consumidor, que también sea titular de los datos/interesado y que alegue el incumplimiento de esta Directriz en el contexto del tratamiento de datos en un tercer país, podrá hacer valer sus derechos legales tanto contra la empresa importadora como contra la empresa exportadora de los datos en la UE. Por lo tanto, el consumidor puede presentar la presunta infracción y las consiguientes reclamaciones legales ante los tribunales y las autoridades reguladoras competentes, ya sea en el lugar donde se encuentra el responsable del tratamiento o en su residencia habitual.

Las disposiciones sobre responsabilidad y jurisdicción de este apartado son derechos de terceros beneficiarios para el interesado.

12 Notificación de incidentes de protección de datos

En caso de vulneración potencial de los requisitos de seguridad de datos («incidente de protección de datos»), las Empresas del Grupo implicadas tienen la obligación de investigar, informar y mitigar los daños. Un incidente de protección de datos es una vulneración de los datos personales si existe una vulneración de la seguridad que conlleve la destrucción, alteración, revelación o uso ilegal de los datos personales. Cuando la vulneración de los datos personales pueda suponer un riesgo para los derechos y libertades de las personas físicas, la autoridad de supervisión responsable deberá ser informada en general de dicha vulneración en un plazo de 72 horas a partir de su detección inicial. Además, deberá notificarse a los interesados cualquier vulneración de los datos personales que pueda suponer un riesgo elevado para sus derechos y libertades. Los encargados del tratamiento, tal como se definen en el apartado 8.2, están obligados a comunicar inmediatamente al responsable del tratamiento los incidentes relacionados con la protección de datos.

Las vulneraciones de datos personales que puedan suponer un riesgo elevado para los derechos y libertades de los interesados deberán comunicarse a la autoridad de supervisión competente y a los interesados.

Si se ha identificado o se sospecha que se ha producido un incidente de protección de datos dentro del área de responsabilidad de una Empresa del Grupo, todos los empleados están obligados a comunicarlo inmediatamente de conformidad con el Proceso de gestión de incidentes de seguridad de la información. Deben cumplirse los requisitos estipulados por Daimler AG a este respecto (por ejemplo, herramientas de software, instrucciones para la elaboración de informes).

13 Organización de la protección de datos y sanciones

13.1 Responsabilidades

Los miembros de los órganos de gestión de las Empresas del Grupo son responsables del tratamiento de datos en su área de responsabilidad. Por lo tanto, se les exige que garanticen el cumplimiento de los requisitos legales en materia de protección de datos y los contenidos en la presente Directriz de protección de datos de la UE (por ejemplo, las obligaciones nacionales de información). Dentro de su área de responsabilidad, el personal directivo es responsable de garantizar que las medidas organizativas, de recursos humanos y técnicas estén en establecidas, de manera que cualquier tratamiento de datos se lleve a cabo de acuerdo con los requisitos de protección de datos. El cumplimiento de estos requisitos es responsabilidad de los empleados correspondientes. Si las autoridades públicas realizan controles de protección de datos, se debe informar inmediatamente al Director corporativo de protección de datos.

Los miembros de los órganos de gestión de las Empresas del Grupo son responsables del tratamiento de datos en su área de responsabilidad y deben asegurarse de que sus empleados tengan los conocimientos necesarios en materia de protección de datos.

13.2 Concienciación y formación

La Dirección debe asegurarse de que sus empleados reciban y asistan a la formación necesaria en materia de protección de datos, incluidos el contenido y el tratamiento de esta Directriz, si tienen un acceso constante o frecuente a datos personales. Deben tenerse en cuenta los requisitos del Director corporativo de protección de datos y del Cumplimiento de datos.

13.3 Organización

El Director corporativo de protección de datos es internamente independiente de las instrucciones en lo relativo al desempeño de sus tareas. Deberá garantizar el cumplimiento de las leyes nacionales e internacionales en materia de protección de datos. Es el responsable de esta Directriz y supervisa su cumplimiento. El Director corporativo de protección de datos es nombrado por la junta directiva de Daimler AG. En general, las Empresas del Grupo que están legalmente obligadas a nombrar un director de protección de datos designarán al Director corporativo de protección de datos. Las excepciones específicas deberán ser acordadas con el Director corporativo de protección de datos.

El Director corporativo de protección de datos es internamente independiente de las instrucciones.

Todos los interesados podrán ponerse en contacto con el Director corporativo de protección de datos en cualquier momento para expresar sus inquietudes, formular preguntas, solicitar información o presentar reclamaciones en relación con la protección de datos o la seguridad de los datos. Si así lo solicitan, las inquietudes y reclamaciones serán tratadas de manera confidencial.

La información de contacto del Director corporativo de protección de datos es:
Daimler AG, Chief Officer Corporate Data Protection, HPC E600,
70546 Stuttgart, Alemania
E-mail: data.protection@daimler.com
Intranet: https://social.intra.corpintra.net/docs/DOC-105811
El Grupo Daimler también ha establecido una organización de cumplimiento, que se describe con mayor detalle en regulaciones internas separadas. La organización de cumplimiento da apoyo y supervisa a las Empresas del Grupo en lo relativo al cumplimiento de las leyes de protección de datos. Define el contenido de la formación en materia de protección de datos y establece los criterios para el grupo de participantes.

La organización de cumplimiento:
- da apoyo y supervisa a las Empresas del Grupo en lo relativo al cumplimiento de las leyes de protección de datos
- define el contenido de la formación en materia de protección de datos

13.4 Sanciones

El tratamiento ilícito de datos personales u otros delitos contra la ley de protección de datos puede ser perseguido en muchos países en virtud del derecho penal y la legislación reguladora y también puede dar lugar a reclamaciones de indemnización. Las vulneraciones de las que son responsables los empleados pueden dar lugar a medidas disciplinarias en virtud de la legislación laboral. Las vulneraciones de esta Directriz se sancionarán conforme al regulaciones interno.

El tratamiento ilícito de datos personales puede dar lugar a reclamaciones de indemnización y medidas disciplinarias.

13.5 Auditoría y controles

El cumplimiento de esta Directriz y de las leyes de protección de datos aplicables se revisará periódicamente a nivel del Grupo mediante auditorías de protección de datos y otros controles. Los resultados de estas auditorías deben ser comunicados al Director corporativo de protección de datos, a la Empresa del Grupo responsable y a su responsable de protección de datos, en caso de que haya sido designado. Además, los resultados de esta auditoría deberán facilitarse a responsables del tratamiento externos de conformidad con las disposiciones contractuales del acuerdo sobre el tratamiento en representación de terceros. Asimismo, los responsables del tratamiento externos tienen derecho a realizar auditorías de protección de datos a los encargados internos del tratamiento de datos conforme a las disposiciones contractuales del acuerdo sobre el tratamiento en representación de terceros. Asimismo, las Empresas del Grupo deberán realizar sus propios exámenes y revisiones para determinar el cumplimiento de la presente Directriz, si así lo solicita el Director corporativo de protección de datos.

Se deberá informar el consejo de administración de Daimler AG de los hallazgos significativos como parte de las obligaciones de información existentes. Previa solicitud, los resultados de las revisiones se pondrán a disposición de la autoridad de supervisión competente en materia de protección de datos. La autoridad de supervisión competente en materia de protección de datos puede llevar a cabo sus propias comprobaciones sobre el cumplimiento de las regulaciones de la presente Directriz, al amparo de la legislación nacional.

14 Modificaciones de la presente Directriz y cooperación con las autoridades públicas

14.1 Responsabilidad en caso de modificaciones

Las modificaciones de esta Directriz deben coordinarse con el Director corporativo de protección de datos.

La Directriz solo puede modificarse mediante el procedimiento definido para la modificación de las directrices en coordinación con el Director corporativo de protección de datos. Los cambios que tengan efectos significativos en la Directriz o que afecten al nivel de protección ofrecido por la misma (es decir, cambios en el carácter vinculante) deben ser comunicados sin demora a las autoridades competentes de supervisión de la protección de datos, que emiten la aprobación de esta Directriz como normas corporativas vinculantes.

El Director corporativo de protección de datos es el responsable de mantener una lista actualizada de todas las Empresas del Grupo que están sujetas a esta Directriz (normativa aplicable adicional «Lista de Empresas del Grupo sujetas a la Directriz de protección de datos de la UE»). En el caso de que las Empresas del Grupo traten datos personales por cuenta de otras sociedades ajenas al Grupo, las Empresas del Grupo comunicarán a estas los cambios en la lista. En el caso de que se produzcan cambios en la directriz que afecten a las condiciones de tratamiento, se informará a estas empresas ajenas al Grupo con la suficiente antelación para que puedan oponerse a la modificación o rescindir el contrato con el encargado del tratamiento.

Para los interesados que no pertenezcan al Grupo Daimler, la última versión de esta Directriz se publicará online en https://www.daimler.com. Este requisito es un derecho de terceros beneficiarios para el interesado.

En caso de que se modifique esta Directriz o la lista de Empresas del Grupo afiliadas, el Director corporativo de protección de datos informará una vez al año a la autoridad de supervisión de la sede de Daimler AG.

14.2 Cooperación con las autoridades

Las Empresas del Grupo que lleven a cabo o participen en el tratamiento de datos en terceros países están obligadas a cooperar con las autoridades de supervisión responsables en asuntos relativos a problemas, investigaciones u otros procedimientos relacionados con el tratamiento de datos personales en el contexto mencionado anteriormente. Esto incluye el deber de permitir las auditorías legales de las autoridades de supervisión. Además, deberán cumplirse todas las instrucciones legales de las autoridades de supervisión responsables basadas en los procedimientos de tratamiento en terceros países o las disposiciones de esta Directriz.

La obligación de cooperar con las autoridades incluye:
- permitir las auditorías legales
- cumplir con las instrucciones legales

Si las Empresas del Grupo forman parte de un sistema de certificación internacional de normas corporativas vinculantes sobre protección de datos, deberán garantizar la cooperación con las empresas y organismos de auditoría responsables. La participación en dichos sistemas de certificación debe acordarse con el Director corporativo de protección de datos.

Las disposiciones del apartado 14.2 sobre la cooperación con las autoridades son derechos de terceros beneficiarios para el interesado.

14.3 Supervisión y presentación de informes sobre la normativa de terceros países

Los responsables de las empresas de terceros países deben comunicar inmediatamente al Director corporativo de protección de datos si para su empresa existe una expectativa legítima de que las leyes u otras regulaciones aprobadas por un país o una institución distinta de la UE y sus estados miembros presentan los siguientes riesgos:

- las leyes o regulaciones puedan impedir que la sociedad de un tercer país u otra Empresa del Grupo en cuestión cumpla con sus obligaciones en virtud de la presente Directriz al tratar datos en terceros países, o
- las leyes o regulaciones puedan tener graves efectos adversos sobre los derechos que la presente Directriz otorga a los interesados para el tratamiento de datos en terceros países. Especialmente si la autoridad pública local exige una transferencia de datos masiva, desproporcionada e indiscriminada de manera que vaya más allá de lo necesario en una sociedad democrática.

Los responsables de las empresas de terceros países deben informar al Director corporativo de protección de datos si, debido a la regulación nacional, existen los siguientes riesgos:
- la empresa de un tercer país pudiera no cumplir con sus obligaciones en virtud de esta Directriz
- la regulación nacional tiene graves efectos adversos sobre los derechos que la presente Directriz otorga a los interesados.

El Director corporativo de protección de datos evaluará el impacto e informará a la autoridad competente en materia de protección de datos (si procede) si se espera que el requisito legal correspondiente interfiera de forma significativa con las garantías previstas en esta Directriz. Esta disposición es un derecho de terceros beneficiarios para el interesado.

Si una empresa de un tercer país es obligada por una autoridad pública a abstenerse de notificar a la autoridad de supervisión de la protección de datos la divulgación de datos personales, adoptará todas las medidas adecuadas para atenuar en la medida de lo posible esta prohibición o

derogarla, y facilitará a las autoridades de control competentes información general sobre las solicitudes que haya recibido (por ejemplo, el número de solicitudes de divulgación, el tipo de datos solicitados y, si es posible, el solicitante).

Anonimizados	se refiere a los datos que no permiten que la identidad personal pueda ser rastreada por nadie, o que solo puede ser recreada invirtiendo una cantidad no razonable de tiempo, costes y trabajo.
Clientes potenciales	se refiere a las personas que están interesadas en los productos o servicios de una o más Empresas del Grupo.
Consentimiento	se refiere a una declaración voluntaria y jurídicamente vinculante de que el interesado está de acuerdo con el tratamiento de sus datos. Es emitido expresamente por el interesado antes del inicio del tratamiento de los datos.
Consumidor	se refiere a cualquier persona física que cierra una transacción legal con fines que no sirven fundamentalmente para sus actividades comerciales o de autoempleo.
Convenios colectivos	se refiere a acuerdos de escalas salariales o acuerdos entre las empresas y los representantes de los trabajadores, dentro del alcance permitido por la legislación laboral pertinente.
Datos altamente sensibles	se refiere a los datos sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos, datos genéticos o biométricos, datos de salud, datos sobre la vida u orientación sexual del interesado o datos sobre condenas o delitos penales. En virtud de la legislación nacional, otras categorías de datos pueden considerarse altamente sensibles o el contenido de las categorías de datos puede cumplimentarse de forma diferente.
Datos de empleados	se refiere a los datos personales de los empleados del Grupo Daimler y también a las personas que soliciten empleo, así como a las personas cuyas relaciones laborales hayan concluido si los datos hacen referencia a la relación laboral inactiva.
Datos personales	se refiere a toda información relacionada con una persona identificada o identificable. Se considera que una persona física es «identificable» si puede ser identificada directa o indirectamente, en particular vinculándole un nombre, un número de identificación, datos de localización, un nombre de usuario en línea o una o más características especiales que expresen la identidad física, fisiológica, genética, psicológica, económica, cultural o social de dicha persona física. También puede ser suficiente si la identificación personal se puede hacer combinando información con conocimientos adicionales (incluso hechos que se conocen por casualidad).
Derechos de terceros beneficiarios	son normas que permiten a los interesados hacer valer directamente sus reclamaciones en virtud de la Directriz de protección de datos de la UE contra las Empresas del Grupo que procesan los datos, incluso en el caso de que dichos interesados no tengan una relación jurídica directa con ellos

	y las Empresas del Grupo incumplan sus obligaciones en virtud de la Directriz de protección de datos de la UE.
Encargado del tratamiento	se refiere a una persona física o jurídica que realiza el tratamiento de datos personales en representación del responsable del tratamiento.
Espacio Económico Europeo (EEE)	se refiere al espacio económico asociado con la UE, Noruega, Islandia y Liechtenstein.
Incidente de protección de datos	se refiere a un incidente de seguridad de la información con una posible vulneración de los datos.
Interesado	en virtud de esta Directriz de protección de datos de la UE, se refiere a cualquier persona física cuyos datos sean objeto de tratamiento. En algunos países, las personas jurídicas también pueden ser las personas interesadas.
Medidas proporcionales	se refiere a las medidas que son aptas, necesarias y adecuadas para lograr una finalidad legítima. Las medidas son aptas si se puede lograr la compra legítima con dicha medida, o al menos ser de ayuda. Las medidas son necesarias si no existen medios menores para lograr el mismo éxito con la misma certeza. Las medidas son adecuadas si no resultan excesivamente gravosas o no razonables para el interesado.
Nivel adecuado de protección de datos	siempre se garantiza para la transmisión de datos dentro de la UE/EEE. Aparte de las excepciones definidas en el RGPD-UE, los datos personales solo pueden transmitirse a un país no perteneciente a la UE/EEE si la Comisión de la UE ha reconocido la idoneidad del nivel de protección de datos del tercer país, o si se han aportado otras garantías adecuadas. Con la Directriz de protección de datos de la UE como norma corporativa vinculante, el Grupo Daimler ofrece las garantías adecuadas de este tipo para la transmisión de datos personales de Empresas del Grupo en la UE/EEE a Empresas del Grupo fuera de la UE/EEE.
Normas corporativas vinculantes (BCR)	se aplican al tratamiento de datos personales. Constituyen un marco adecuado para la transmisión de datos personales de Empresas del Grupo radicadas en la UE/EEE a Empresas del Grupo establecidas fuera de la UE/EEE. Solo se aplican dentro del Grupo Daimler. Deben ser jurídicamente vinculantes y de obligado cumplimiento para cada una de las Empresas del Grupo relevantes.
Red de protección de datos	incluye al Director de cumplimiento local (LCO), al Responsable de cumplimiento local (LCR) y a los respectivos multiplicadores.
Registro de actividades de tratamiento	se refiere a un resumen de los procedimientos de un responsable del tratamiento que procesa datos personales.
Responsable del tratamiento	se refiere a cualquier persona física o jurídica que decida por sí sola o con otros las finalidades y métodos de tratamiento de los datos personales.

Seudonimizados	se refiere a los datos que sin utilizar información adicional, ya no pueden atribuirse a un interesado específico, siempre y cuando dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas para garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
Tercer país	se refiere a todos los países fuera de la UE/EEE.
Terceros	se refiere a cualquier persona que realiza el tratamiento de datos personales pero que no es el interesado ni el responsable del tratamiento. Los encargados del tratamiento dentro de la UE/EEE no se consideran terceros en virtud del RGPD-UE porque son asignados por ley por el responsable del tratamiento.
Tratamiento de datos personales	se refiere a cualquier operación, ya sea por medios automatizados o no, como la recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, utilización, divulgación mediante transmisión, difusión o cualquier otra forma de puesta a disposición, alineación o combinación, restricción, supresión o destrucción.
Vulneración de datos personales	se refiere a una vulneración de la seguridad que tiene como resultado la alteración o destrucción ilegal, divulgación o uso no autorizados de los datos personales.

La siguiente lista ofrece una descripción general de las transmisiones de datos a terceros países dentro del Grupo Daimler. Esta lista describe ejemplos de transmisión de datos a terceros países para que las autoridades de supervisión competentes puedan evaluar la conformidad del tratamiento realizado en esos terceros países.

BCR-Responsable del tratamiento

Finalidad del tratamiento de datos	• **Tratamiento con fines de gobernanza y cumplimiento** (cumplimiento con los requisitos legales, directrices de empresa, normas reconocidas y otras disposiciones normativas: comprobaciones de debida diligencia, comprobaciones de listas de sanciones, investigaciones internas de sospechas concretas de vulneraciones de normas, auditorías, hacer valer sus derechos o defenderse frente a reclamaciones legales, procesos de proveedores, gestión de contratos, procesamiento de asuntos financieros y tributarios) • **Atención al cliente y ventas** (tratamiento como parte de la relación contractual, incluida la administración y gestión de datos de clientes, así como para la administración de la empresa, para la retención de clientes y fines promocionales, análisis de utilización de sitios web, aplicaciones y publicidad en internet/correo electrónico, gestión de socios comerciales) • **Estrategia y desarrollo de producto** (desarrollo y mejora de productos y servicios, incluyendo estudios de mercado, análisis de utilización y usuarios, control de productos) • **Defensa de productos** (responsabilidad por productos, defensa de productos, control de productos) • **RR. HH.** (selección de personal, administración y gestión de personal, desarrollo del personal, remuneración, planificación e informes del personal, gestión de viajes) • **TI** (soporte de TI, operaciones de TI/hosting, desarrollo adicional de TI (incluidas pruebas), análisis y asesoría de seguridad de TI, consultoría de TI, gestión de TI, implementación y gestión del archivo, copias de seguridad de datos, gestión de la nube, alojamiento y otros servicios) • Comunicación interna
Categorías de datos personales	• Datos de contacto (p. ej., nombre, dirección, número de teléfono, dirección de correo electrónico) • Datos de empleados (p. ej., número de empleado, departamento/organización, educación, formación, carrera profesional, información sobre conocimientos profesionales y aptitudes personales, datos de salario, datos bancarios, fecha de nacimiento, nacionalidad, género) • Datos de comercio electrónico (p. ej., datos de utilización de sitios web, aplicaciones y direcciones de correo electrónico) • Datos de los vehículos (p. ej., VIN, datos técnicos de unidades de control, información sobre piezas de vehículos) • Datos de contratos (p. ej. datos de contacto, datos de facturación, datos sobre productos y servicios utilizados) • Datos de socios comerciales (datos de contratos, datos de contacto) • Datos de TI (p. ej., dirección IP, registros) • Resultados de diferentes actividades de cumplimiento
Interesados	Empleados, clientes potenciales, clientes, socios, proveedores
Terceros países	potencialmente todas las Empresas del Grupo sujetas a las BCR (normativa aplicable adicional: ”Lista de Empresas del Grupo sujetas a la Directriz de protección de datos de la UE”)

BCR-Encargado del tratamiento

Finalidad del tratamiento de datos	• **TI** (soporte de TI, operaciones de TI/hosting, desarrollo adicional de TI (incluidas pruebas), análisis y asesoría de seguridad de TI, gestión de TI, implementación y gestión del archivo, copias de seguridad de datos) • **Gestión de datos de clientes** (gestión de datos de clientes, administración y análisis con fines promocionales y de ventas, evaluación de datos de utilización y vehículos con fines promocionales y de ventas, análisis de utilización de sitios web, aplicaciones y publicidad en internet/correo electrónico)
Categorías de datos personales	• Datos de contacto (p. ej., nombre, dirección, número de teléfono, dirección de correo electrónico) • Datos de empleados (p. ej., número de empleado, departamento/organización, educación, formación, carrera profesional, información sobre conocimientos profesionales y aptitudes personales, datos de salario, datos bancarios, fecha de nacimiento, nacionalidad, género) • Datos de comercio electrónico (p. ej., datos de utilización de sitios web, aplicaciones y direcciones de correo electrónico) • Datos de los vehículos (p. ej., VIN, datos técnicos de unidades de control, información sobre piezas de vehículos) • Datos de contratos (p. ej. datos de contacto, datos de facturación, datos sobre productos y servicios utilizados) • Datos de TI (p. ej., dirección IP, registros)
Interesados	Empleados, clientes potenciales, clientes, socios, proveedores
Terceros países	potencialmente todas las Empresas del Grupo sujetas a las BCR (normativa aplicable adicional: ”Lista de Empresas del Grupo sujetas a la Directriz de protección de datos de la UE”)