Directriz de protección de datos de la UE

Mercedes-Benz

Índice

1 Objetivo de esta directriz

El Mercedes-Benz Group considera el respeto de los derechos de protección de datos como 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 del destinatario ofrece un nivel adecuado de protección de datos.

Esta Directriz de protección de datos de la UE establece normas internas de protección de datos unitarias y adecuadas, tanto para el:
- (a) tratamiento de datos personales en regiones como la UE/el Espacio Económico Europeo (EEE) (en lo sucesivo denominados conjuntamente «UE/EEE»), como para
- (b) la transmisión internacional de datos personales a compañías del Grupo fuera de la UE/EEE (incluyendo el posterior tratamiento en ellas).

Con este fin, esta directriz define regulaciones vinculantes para el tratamiento de datos personales con origen en la UE/EEE dentro del Mercedes-Benz Group. Estas regulaciones establecen garantías adecuadas para la protección de los datos personales fuera la UE/EEE y constituyen por tanto normas empresariales vinculantes («Binding Corporate Rules – BCR») para el Mercedes-Benz Group.

2 Ámbito de aplicación

La presente Directriz de protección de datos de la UE se aplica al Mercedes-Benz Group AG, a las compañías controladas por el Grupo (denominadas en lo que sigue compañías del Grupo), a sus empleados y a los miembros de sus órganos directivos. Se considera compañía controlada según esta directriz a cualquier sociedad en la que Mercedes-Benz Group AG pueda exigir el cumplimiento de esta directriz 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 se aplica al tratamiento de los datos personales total o parcialmente automatizado, así como al tratamiento manual en sistemas de archivo a menos que la legislación nacional ofrezca un ámbito de aplicación más amplio. En Alemania, la directriz se aplica también a todos los datos de los empleados[1] en formato impreso.
La directriz se aplica al tratamiento de datos personales:
- (a) de compañías del Grupo y sus sucursales con sede dentro de la UE/EEE o en otro país al que esta directriz pueda extenderse («sociedades establecidas en la UE/EEE»),
- (b) de compañías del Grupo establecidas fuera de la UE/EEE, si ofrecen bienes o servicios a personas físicas dentro de la UE/EEE y/o supervisan el comportamiento de personas físicas dentro de la UE/EEE («empresas de terceros países con ofertas para la UE/EEE»), o
- (c) de compañías del Grupo con sede fuera de la UE/EEE que hayan recibido a la que se les hayan facilitado datos personales directa o indirectamente por parte de sociedades a las que se aplique la directriz según el punto a) o b) («sociedades en países terceros que reciben datos de la UE/EEE»).

[1] En aras de la simplificación lingüística, en esta directriz se utiliza únicamente la forma masculina para referirse a personas físicas. No obstante, el contenido se refiere en todo momento a personas de cualquier identidad de género.

En el resto de esta directriz, los tratamientos fuera de la UE/EEE se denominarán tratamientos en un país tercero.

Las compañías del Grupo que participan o son objeto de tratamiento por parte de empresas de países terceros se enumeran en las Otras Regulaciones Aplicables, normativa «Lista de compañías del Grupo sujetas a la Directriz de protección de datos de la UE».

Esta directriz puede ampliarse a países fuera de la UE/EEE. En aquellos países en los que los datos de personas jurídicas gocen de la misma protección que los datos personales, se aplica esta directriz también y del mismo modo a los datos de personas jurídicas.

3 Validez jurídica dentro del Mercedes-Benz Group

Las normas y disposiciones de esta directriz son vinculantes para todas las compañías 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 compañías 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 compañías 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 el caso de que el cumplimiento de esta directriz implicara una infracción de la legislación nacional, o en el caso de que la legislación nacional exigiera una regulación que se aparte de esta directriz, se deberá informar de ello al encargado de protección de datos del Grupo y a la organización central de Compliance a efectos de control de la legislación en materia de protección de datos. Si existen conflictos entre las leyes nacionales y esta directriz, el encargado de protección de datos del Grupo y la organización central de Compliance colaborarán con la compañía del Grupo responsable 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

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 compañías del Grupo. El mero hecho de que ambas partes, la compañía del Grupo que cede los datos y la que los recibe, estén afiliadas al Mercedes-Benz Group 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 personales de clientes potenciales, clientes o socios pueden tratarse para formalizar, ejecutar y rescindir un contrato. Esto incluye también los servicios de asesoramiento para el cliente o socio en virtud del contrato, si están relacionados 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. 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.

5.2.2 Tratamiento de datos para fines publicitarios

Si el interesado se pone en contacto con una compañía del Grupo para solicitar información (por ejemplo, para recibir material informativo sobre un producto), está permitido el tratamiento de los datos personales para dar respuesta a esta solicitud. Las medidas publicitarias y de fidelización del cliente requieren el cumplimiento de otros requisitos legales. El tratamiento de datos personales 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. El interesado debe ser informado con antelación sobre el uso de sus datos personales con fines publicitarios. Si se recogen datos exclusivamente para medidas publicitarias, la comunicación de los mismos por parte del interesado es siempre voluntaria. 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. Se tendrán además en cuenta las restricciones vigentes en algunos países acerca del uso de datos para fines publicitarios.

5.2.3 Consentimiento del tratamiento de datos

Es posible llevar a cabo el tratamiento de datos si el interesado ha otorgado su consentimiento. Antes de dar su consentimiento, el interesado debe ser informado conforme a la presente Directriz de protección de datos de la UE. 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.

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

5.2.5 Tratamiento de datos por razón de un interés legítimo

El tratamiento de datos personales también puede realizarse si es 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 legítimos del tratamiento. Se examinará la legitimidad de estos intereses antes de cada tratamiento de datos.

5.3 Fundamento jurídico de datos de empleados

5.3.1 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 de la relación laboral. Los datos personales de los candidatos pueden tratarse para ayudar a decidir si desean formalizar 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. 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.

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, 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 datos 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.

5.3.3 Convenio colectivo para el 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. Las regulaciones 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.

5.3.4 Consentimiento del 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. No se pueden imponer sanciones al empleado por no otorgar el consentimiento. 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. 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 razón de un interés legítimo

Los datos de empleados también pueden tratarse si son necesarios para un interés legítimo de una compañía 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 por razón de un interés legítimo si los intereses sujetos a protección del empleado no prevalecen sobre el interés 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 compañía 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. Antes de realizar cada medida de este tipo se estudiarán y documentarán el interés legítimo de la compañía del Grupo y los posibles intereses legítimos de los empleados. Además, puede ser necesario cumplir otras exigencias del Derecho vigente (por ejemplo, derechos de cogestión del Comité de empresa y derechos de información de los afectados).

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 compañía 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 reclamaciones legales frente al interesado o si es necesario para que el responsable del tratamiento pueda cumplir sus derechos y responsabilidades en el ámbito del derecho laboral o social.

Si se planea realizar el tratamiento de datos personales altamente sensibles, se deberá informar previamente al encargado de protección de datos del Grupo.

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 negativo jurídico o similar en ellos si es necesario para celebrar o ejecutar un contrato, o si el interesado ha dado su consentimiento. Esta decisión automatizada puede incluir en algunos casos la elaboración de perfiles, 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.

5.6 Deber de información/transparencia

El área especializada responsable deberá informar a los interesados sobre la finalidad y las circunstancias del tratamiento de datos personales según los artículos 13 y 14 del RGPD. Si los datos no están comprendidos en el ámbito del RGPD, la información se proporciona de conformidad con la legislación nacional aplicable. La información deberá proporcionarse de forma precisa, transparente, compresible y accesible, así como en un lenguaje claro y sencillo. Deberán tenerse en cuenta las prescripciones del responsable de protección de datos y Data Compliance del Grupo. Esta información deberá facilitarse cada vez que se recopilen por primera vez los datos personales. Si la compañía 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.

5.7 Uso para fines específicos

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.

5.8 Minimización de datos

Cualquier tratamiento de datos personales debe limitarse, tanto cuantitativa como cualitativamente, a la extensión necesaria para alcanzar los fines para los que se tratan los datos lícitamente. Esto debe tenerse en cuenta durante la recopilación inicial de datos. Si la finalidad lo permite, y el 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. El área especializada responsable debe adoptar las medidas adecuadas para garantizar que los datos incorrectos o incompletos se eliminen, corrijan, completen o actualicen.

5.10 Privacy by Design y Privacy by Default

El principio de «Privacy by Design» (privacidad desde el diseño) tiene el objetivo de asegurar que las áreas especializadas definan estrategias internas de acuerdo con el estado de la técnica y tomen medidas para integrar los principios de protección de datos en la especificación y estructuración de modelos/procesos empresariales y de sistemas informáticos de tratamiento de datos desde su inicio en la fase de concepción y diseño técnico. Según el principio de «Privacy by Design», los procedimientos y sistemas para el tratamiento de datos personales deben estar diseñados de manera que su configuración inicial esté limitada al tratamiento de datos necesario para el cumplimiento de la finalidad (principio de «Privacy by Default», privacidad por defecto). 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.

Todas las compañías 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 se deben eliminar o anonimizar cuando se haya cumplido la finalidad de su tratamiento o cuando esta deje de existir, a menos que sigan existiendo obligaciones de conservación o justificación. 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 Mercedes-Benz Group AG imponga para la ejecución de las rutinas de borrado (entre otros, las herramientas de software, conceptos de documentación para la implementación del borrado, requisitos de documentación).

5.12 Seguridad del tratamiento de datos

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 informáticos—, 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 pertinentes para la protección de datos deben ser documentadas por el responsable del tratamiento en el contexto de la evaluación de impacto relativa a la protección de datos y del registro de actividades de tratamiento.

En particular, el área especializada responsable debe consultar a su Responsable de seguridad de 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 Transmisión de los datos fuera del Mercedes-Benz Group

La transmisión de datos personales a destinatarios fuera o dentro de las compañías del Grupo está sujeta a los requisitos de autorización para el tratamiento de datos personales incluidos en el presente apartado 5. El destinatario de los datos debe comprometerse a utilizarlos exclusivamente para los fines definidos.

En caso de transmisión internacional de datos personales (incluyendo la concesión de acceso desde otro país), deberán cumplirse los requisitos nacionales aplicables para la transmisión de datos personales al extranjero. En particular, solo se podrán tratar datos personales procedentes de la UE/EEE en un país tercero fuera de las compañías del Grupo si el destinatario puede demostrar que cuenta con una normativa de protección de datos que cumpla esta directriz. Pueden ser instrumentos aptos:

- Acuerdo a través de cláusulas contractuales tipo de la UE,
- participación del destinatario en un sistema de certificación acreditado por la UE para garantizar un nivel de protección de datos suficiente o
- aprobación por parte de la autoridad supervisora de protección de datos responsable de las normas empresariales vinculantes del destinatario para la consecución de un nivel de protección de datos adecuado por parte.

La transmisión de datos personales a una autoridad solo está permitida si no son masivas, desproporcionadas ni indiscriminadas y, en este contexto, no sobrepasen los límites de lo que se considera necesario en una sociedad democrática. En caso de existir conflictos entre estas prescripciones y las prescripciones legales, Mercedes-Benz Group AG colaborará con la compañía del Grupo responsable para alcanzar una solución práctica que cumpla la finalidad de esta directriz (punto 14.3).

De todas las obligaciones mencionadas en este punto 5 se derivan derechos propios para el interesado.

6 Evaluación de impacto relativa a la protección de datos

Para la introducción de nuevos procedimientos de tratamiento o si se produce un cambio significativo en un proceso de tratamiento existente, las compañías del Grupo analizan antes, especialmente mediante el uso de nuevas tecnologías, si dicho tratamiento representa un riesgo elevado para la privacidad de los interesados. Para ello, deben tenerse en cuenta el tipo, la magnitud, el contexto y la finalidad del tratamiento de datos. Como parte del análisis de riesgos, el área especializada responsable lleva a cabo una evaluación la repercusión de los tratamientos previstos sobre la protección de los datos personales (evaluación del impacto relativa a la protección de datos). Si tras la realización de la evaluación del impacto relativa a la protección de datos y la aplicación de medidas adecuadas para minimizar los riesgos, existe un riesgo elevado para los derechos y libertades de los interesados, se deberá informar al encargado de protección de datos del Grupo para que este consulte a la autoridad competente sobre protección de datos. Deberán tenerse en cuenta todas las prescripciones de Mercedes-Benz Group AG para la implementación de la evaluación de impacto relativa a la protección de datos (por ejemplo, herramientas de software, instrucciones para la realización de la evaluación).

7 Documentación de los procesos de tratamiento de datos

Todas las compañías del Grupo deberán documentar los procesos en los que se tratan datos personales en un directorio de procesos. El directorio de procesos deberá realizarse por escrito —en formato electrónico, si así se desea— y deberá ponerse a disposición de la autoridad competente sobre protección de datos si esta así lo solicita. Deberán tenerse en cuenta las prescripciones de Mercedes-Benz Group AG para la documentación (por ejemplo, herramientas de software, instrucciones para la documentación).

8 Tratamiento de datos por encargo

8.1 Generalidades

El tratamiento de datos por encargo se produce cuando un contratista trata datos personales en calidad de proveedor de servicios en favor del contratante y en su nombre. En estos casos, deberá celebrarse, tanto con el contratista externo como entre las compañías del Mercedes-Benz Group, un acuerdo que regule el tratamiento de datos por encargo de acuerdo con los requisitos legales aplicables (por ejemplo, el escrito modelo «Acuerdo para el tratamiento de datos por encargo»). A este respecto, la empresa contratante asume la responsabilidad total sobre la correcta realización del tratamiento de datos.

Las disposiciones del punto 8.3. son también de aplicación para empresas contratantes externas que no constituyan compañías del Grupo.

8.2 Disposiciones para el contratante

Al otorgar el encargo, se deben cumplir los requisitos especificados a continuación, y el área especializada que realiza el encargo debe asegurarse de que se cumplan:

- Seleccionar el contratista según su idoneidad para garantizar las medidas de protección técnicas y administrativas necesarias.
- Se tendrán en cuenta los contratos estándar puestos a disposición por el Encargado de Protección de datos del Grupo.
- El encargo debe comunicarse por escrito o en formato electrónico. Deberán documentarse las instrucciones para el tratamiento de datos y las responsabilidades del contratante y del contratista.

Antes del comienzo del tratamiento de datos, el contratante debe realizar las comprobaciones necesarias para cerciorarse de que el contratista cumple las obligaciones anteriormente mencionadas. Para ello deberán tenerse en cuenta las prescripciones de Mercedes-Benz Group AG a este respecto (por ejemplo, herramientas de software, instrucciones para llevar a cabo la valoración, contratos modelo). Un contratista 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, deberán repetirse las comprobaciones regularmente durante el periodo contractual.

8.3 Disposiciones para contratistas internos

El contratista está autorizado a tratar los datos personales solamente en el marco de las instrucciones del contratante.

Los encargados del tratamiento solo pueden involucrar a otras compañías del Grupo o a terceros («subcontratistas») para que traten los datos personales por virtud de un (sub)contrato propio si cuentan con el consentimiento previo del contratante. Este consentimiento solo se concederá si el contratista 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 contratista en virtud de esta directriz en lo que se refiere a la compañía del Grupo y a los interesados, y si se toman 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 contratistas están obligados a prestar el apoyo adecuado al contratante 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
- las obligaciones de notificación por parte del contratante en virtud del apartado 12
- las disposiciones relativas al contratante y al contratista en virtud del apartado 8
- y el tratamiento de las solicitudes e investigaciones por parte de las autoridades de control.

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

Los contratistas están obligados a notificar a los contratantes 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 contratante, el contratista deberá borrar o devolver todos los datos personales facilitados por el contratante en el momento de la finalización del servicio.

Los contratistas están obligados a informar inmediatamente a su contratante —así como, en su caso, al contratante de éste— de cualquier reclamación, solicitud o queja de los interesados.

Los contratantes internos del Grupo deben obligar asimismo a los contratistas externos a cumplir con las regulaciones anteriormente mencionadas.

Las obligaciones específicas del contratista frente al contratante fundamentan derechos propios para el interesado.

9 Responsabilidad conjunta

En el caso de que varias compañías 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/Joint Controller), las empresas deberán suscribir un acuerdo en el que se estipulen sus deberes y responsabilidades frente a los interesados cuyos datos vayan a tratar. Deben tenerse en cuenta las plantillas de contrato facilitadas por el encargado de protección de datos del Grupo.

10 Derecho ejecutable para los interesados

El interesado se considera tercer beneficiario de todos los derechos mencionados en este punto 10 y las obligaciones de las compañías del Grupo.

Las consultas y reclamaciones presentadas de acuerdo con este punto 10 deberán responderse en un plazo de un mes. Teniendo en cuenta la complejidad y el número de solicitudes, este periodo de un mes puede prolongarse como máximo otros dos meses, para lo que deberá informarse al interesado en consecuencia.

10.1 Derechos del interesado

Los interesados en la UE/EEE tienen los siguientes derechos, tal y como se establecen en mayor detalle en la legislación europea, frente a la compañía del Grupo responsable o, si se trata de un contratista, frente al contratista:

- el derecho a ser informado de las circunstancias del tratamiento de sus datos personales. Deben tenerse en cuenta las prescripciones del encargado de protección de datos del Grupo acerca de dichas informaciones.
- el derecho a obtener información sobre el tratamiento de sus datos y sobre los derechos que le corresponden a este respecto. Si el Derecho laboral vigente prevé derechos específicos de inspección de la documentación del empleador (por ejemplo, expediente personal), esta directriz no afecta a estos derechos. Previa solicitud, el interesado puede recibir una copia de sus datos personales (eventualmente, 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 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.
- el derecho a la limitación del tratamiento de sus datos si no está de acuerdo con su exactitud o si la compañía del Grupo ya no necesita los datos, mientras que el interesado los necesita para poder ejercer sus reclamaciones legales. El interesado también puede solicitar a la compañía 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 y que haya facilitado sobre la base de su consentimiento —o en el marco de un acuerdo celebrado o iniciado con él— en un formato digital de uso común, así como 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 compañía 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 compañía del Grupo tiene razones de peso para el tratamiento o si los datos están siendo tratados para la ejecución, el ejercicio o la defensa de derechos legales. Si hay una objeción legítima, los datos se deben eliminar.

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

10.2 Procedimiento de reclamación

Los interesados tienen derecho a presentar una reclamación la encargado de protección de datos del Grupo si considera que se ha infringido esta directriz. Las reclamaciones pueden presentarse por correo electrónico.

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

En caso de que el interesado no esté de acuerdo con la decisión de la compañía del Grupo en cuanto al cumplimiento de las prescripciones (o si no está satisfecho con sus actuaciones por otros motivos), es libre de impugnar dicha decisión o comportamiento por medio del ejercicio de sus derechos. Para ello, puede ponerse en contacto con la autoridad de control responsable, concretamente en su país de residencia habitual, de trabajo o en el que tuvo lugar la presunta infracción, o iniciar una acción judicial (apartado 11.2). Esto no afecta al resto de sus derechos y responsabilidades legales.

11 Responsabilidad y jurisdicción

11.1 Disposiciones de responsabilidad

La compañía del Grupo con sede en la UE/EEE («exportador de los datos») que transfirió inicialmente los datos personales a una compañía del Grupo con sede en un país tercero asumirá la responsabilidad por cada vulneración de esta directriz por parte de la compañía del Grupo de dicho tercer país que reciba los datos de la UE/EEE para su tratamiento en un país tercero. 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 compañías del Grupo de países terceros.

La exportadora de datos solo estará total o parcialmente exenta de esta responsabilidad si demuestra que la compañía del país tercero que recibe datos de la UE/EEE no es responsable del evento que ha provocado los daños.

11.2 Jurisdicción

El interesado puede presentar reclamaciones ante los tribunales de la sede de la entidad responsable o del contratista, o en su lugar de residencia habitual.

El interesado que alegue una infracción de esta directriz en el marco del tratamiento en un país tercero puede hacer valer sus derechos legales tanto contra la sociedad importadora de datos como contra la sociedad exportadora en la UE/EEE. Por tanto, el interesado puede denunciar la presunta infracción y presentar las reclamaciones legales resultantes ante los tribunales y autoridades de control responsables tanto en la sede de la entidad responsable como en su lugar de residencia habitual.

El interesado se considera tercer beneficiario de las disposiciones relativas a la responsabilidad y la jurisdicción establecidas en este punto.

12 Comunicación de incidentes relativos a la protección de datos

En caso de una posible infracción de los requisitos vigentes en cuanto a seguridad de los datos («incidente relativo a la protección de datos»), las compañías del Grupo afectadas están sujetas a obligaciones de investigación, información y mitigación de daños. Un incidente relativo a la protección de datos constituye una transgresión de la legislación de protección de datos si se produce una vulneración de la seguridad de los datos que derive de forma ilegal en la eliminación, modificación, divulgación no autorizada o utilización de datos personales. En la medida en que esto pueda resultar en un riesgo para los derechos y libertades de personas físicas, los hechos acaecidos deberán comunicarse a las autoridades de control competentes en un plazo máximo de 72 horas desde que la compañía del Grupo tenga conocimiento de la infracción. Asimismo, los interesados cuyos derechos y libertades se sometan probablemente en un riesgo elevado a causa de una transgresión de la legislación de protección de datos deberán ser informados sobre dicha infracción. Los contratistas en el sentido del punto 8.2 tienen la obligación de comunicar inmediatamente los incidentes de protección de datos a su empresa contratante.

Si se detecta o se sospecha la existencia de un incidente relativo a la protección de datos en el ámbito de responsabilidad de una compañía del Grupo, todos los empleados estarán obligados a comunicarlo sin demora en el marco del proceso de Information Security Incident Management. Para ello deberán tenerse en cuenta las prescripciones de Mercedes-Benz Group AG a este respecto (por ejemplo, herramientas de software, instrucciones para llevar a cabo la comunicación).

Todas las transgresiones de la legislación de protección de datos deben documentarse; la documentación deberá ponerse a disposición de la autoridad de control si así lo solicita.

13 Organización de protección de datos y sanciones

13.1 Responsabilidad

Los miembros de los órganos directivos de las compañías 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 del contenido en la presente directriz de protección de datos de la UE (por ejemplo, las obligaciones nacionales de información). Dentro de su área de responsabilidad, cada directivo es responsable de garantizar que se hayan establecido las medidas organizativas, de recursos humanos y técnicas adecuadas, 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 una autoridad estatal desea realizar un control de la protección de datos, se informará sin demora al Encargado de Protección de datos del Grupo.

13.2 Sensibilización y formación

Los directivos deberán asegurarse de que sus empleados reciban y participen en las formaciones necesarias en materia de protección de datos, incluyendo el contenido y el manejo de esta directriz en caso de que tengan acceso continuado o regular a datos personales o realicen tareas de recopilación de datos o de desarrollo de instrumentos para el tratamiento de datos personales. Deberán tenerse en cuenta las prescripciones del responsable de protección de datos y Data Compliance del Grupo.

13.3 Organización

El encargado de protección de datos del Grupo es independiente a nivel interno de las instrucciones en cuanto al desempeño de sus tareas. Vela por el cumplimiento de las disposiciones nacionales e internacionales en materia de protección de datos. Es responsable de esta directriz y supervisa su cumplimiento. Si las compañías del Grupo desean participar en un sistema de certificación internacional para Normas Empresariales Vinculantes sobre protección de datos, deberán coordinar dicha participación con el encargado de protección de datos del Grupo.

El encargado de protección de datos del Grupo es designado por la Junta Directiva de Mercedes-Benz Group AG y recibe la asistencia de esta en el desempeño de sus tareas. Por lo general, las compañías del Grupo que tengan la obligación legal de designar a un encargado de protección de datos nombrarán al encargado de protección de datos del Grupo. El encargado de protección de datos del Grupo informa directamente a la Junta Directiva de Mercedes-Benz Group AG y al departamento de dirección de todas las compañías del Grupo para las que haya sido designado el encargado de protección de datos del Grupo. Las excepciones específicas a esta regla deben acordarse con el Encargado de Protección de datos del Grupo.

En el marco de las obligaciones de información existentes, se informará al Consejo de Administración de Mercedes-Benz Group AG por medio del informe anual del encargado de protección de datos del Grupo.

Todos los interesados podrán ponerse en contacto con el encargado de protección de datos del Grupo 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 encargado de protección de datos del Grupo es:

Mercedes-Benz Group AG, Encargado de Protección de datos del Grupo, HPC E600,
70546 Stuttgart, Germany
E-mail: data.protection@mercedes-benz.com
Intranet: https://social.intra.corpintra.net/docs/DOC-71499

El Mercedes-Benz Group ha creado además una organización de Compliance, descrita en regulaciones internas específicas. La organización de Compliance da apoyo y supervisa a las compañías 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.

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 a las regulaciones internas.

13.5 Auditorías y controles

El cumplimiento de esta directriz y de las leyes vigentes sobre protección de datos se comprueba en función de los riesgos al nivel del Grupo de forma regular, al menos una vez al año. Para ello, se lleva a cabo una evaluación de riesgos interna en materia de Compliance, así como auditorías que incluyen temas específicos de protección de datos y otras comprobaciones. El encargado de protección de datos del Grupo tiene derecho a solicitar más comprobaciones. Los resultados deberán ponerse en conocimiento del encargado de protección de datos del Grupo, de la compañía del Grupo responsable y de su encargado de protección de datos correspondiente, si cuenta con uno.

En el marco de las obligaciones de información existentes se informará a la Junta Directiva de Mercedes-Benz Group AG sobre los resultados. Los resultados de los controles deberán ponerse a disposición de la autoridad competente sobre protección de datos responsables si así lo solicitan. De acuerdo con autorizaciones contempladas en la legislación estatal, la autoridad competente sobre protección de datos puede someter a todas las compañías del Grupo a una auditoría sobre protección de datos para comprobar el cumplimiento de esta directriz.

14 Modificaciones de esta directriz y colaboración con las autoridades

14.1 Responsabilidades en caso de modificaciones

Esta directriz puede modificarse previa coordinación con el encargado de protección de datos del Grupo y de acuerdo con el procedimiento definido para la modificación de directrices (Directriz sobre gestión de directrices, A 1). Las modificaciones que repercutan de forma significativa en esta directriz de protección de datos de la UE, A 17 o que puedan afectar al nivel de protección de otorga (es decir, modificaciones en cuanto a la obligación) se deberán comunicar inmediatamente a las autoridades competentes sobre protección de datos que aprobaron esta directriz como Normas Empresariales Vinculantes.

El encargado de protección de datos del Grupo es responsable de elaborar una lista actualizada de todas las compañías del Grupo que están sujetas a esta directriz (ordenador de registro de datos «Lista de compañías del Grupo sujetas a la Directriz de protección de datos de la UE»). Sobre la base de esta directriz, no se transmiten datos personales a una nueva compañía del Grupo hasta que dicha nueva compañía esté sujeta de forma efectiva a esta directriz y se tengan en cuenta las medidas correspondientes de Compliance para el cumplimiento de la directriz.

El interesado tiene derecho a un fácil acceso a esta directriz. Por ese motivo, la versión más reciente de esta directriz se publica en Internet, en la página https://www.group.mercedes-benz.com, apartado Protección de datos. El interesado se considera tercer beneficiario de esta disposición.

Si se realizan modificaciones en esta directriz o en la lista de compañías del Grupo sujetas a ella, el encargado de protección de datos del Grupo deberá informar a la autoridad de control de la sede principal de Mercedes-Benz Group AG una vez al año, exponiendo brevemente los motivos de la actualización.

14.2 Colaboración con las autoridades

Las compañías del Grupo que realicen tratamiento de datos en países terceros o participen en él tienen la obligación de colaborar con la autoridad de control competente en caso de que surjan problemas, consultas u otros procedimientos relacionados con el tratamiento de datos personales en el contexto anteriormente mencionado. Esto incluye la obligación de aceptar auditorías legales por parte de las autoridades de control. Asimismo, deben cumplirse las instrucciones legales de las autoridades de control responsables que surjan de los procesos de tratamiento en países terceros o de las disposiciones de esta directriz.

El interesado se considera tercer beneficiario de las disposiciones del apartado 14.2 para la colaboración con las autoridades.

14.3 Supervisión y presentación de informes sobre las regulaciones de países terceros

Los responsables de las empresas de terceros países deben comunicar inmediatamente al encargado de protección de datos del Grupo si consideran por razones justificadas que las leyes u otras regulaciones aprobadas por un país o una institución distinta de la UE y sus estados miembros puedan presentar los riesgos expuestos a continuación, si las leyes y regulaciones:

- puedan impedir que la sociedad de un tercer país u otra compañía del Grupo en cuestión cumpla con sus obligaciones en virtud de la presente directriz al tratar datos en terceros países, o
- puedan tener graves efectos adversos sobre los derechos que la presente directriz otorga a los interesados para el tratamiento de datos en países terceros. En especial, si las autoridades públicas locales exigen una transmisión de datos personales masiva, desproporcionada e indiscriminada de manera que vaya más allá de lo necesario en una sociedad democrática.

El encargado de protección de datos del Grupo evaluará el impacto e informará a la autoridad competente en materia de protección de datos (si procede) si se espera que los requisitos legales correspondientes interfieran de forma significativa en las garantías previstas en esta directriz. Esta disposición es un derecho de terceros beneficiarios para el interesado.

Si una compañía de un país tercero se ve obligada por una autoridad a abstenerse de facilitar datos personales a la autoridad de control de protección de datos, realizará todos los esfuerzos razonables para aminorar o anular dicha prohibición en la medida de lo posible y de proporcionar anualmente a la autoridad de control de protección de datos información general sobre las consultas recibidas (por ejemplo, número de solicitudes de divulgación, tipo de datos solicitados y entidad solicitante cuando sea posible) dentro de este margen de maniobra.

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