Diretiva de proteção de dados UE

Mercedes-Benz

Índice

1 Objetivo da diretiva

O Mercedes-Benz Group vê a defesa dos direitos de proteção de dados como parte de sua responsabilidade social.

Em alguns países e regiões, como a União Europeia, o legislador estabeleceu normas para a proteção dos dados das pessoas naturais ("dados pessoais"), exigindo inclusive que tais dados somente possam ser transferidos para outros países se existir um nível adequado de proteção de dados no local de destino.

Esta Diretiva de proteção de dados UE estabelece padrões consistentes e apropriados de proteção de dados intragrupo — tanto para:
- (a) O tratamento de dados pessoais em regiões como a UE/ o Espaço Econômico Europeu (EEE) (doravante denominados coletivamente como "UE/EEE"), bem como
- (b) A transferência transfronteiriça de dados pessoais para empresas do grupo fora da UE/EEE (incluindo seu posterior tratamento).

Para esse fim, esta diretiva estabelece regras obrigatórias para o tratamento de dados pessoais com origem na UE/EEE dentro do Mercedes-Benz Group. Elas dão garantias apropriadas para a proteção de dados pessoais fora da UE/EEE e, assim, compõem as chamadas regras corporativas obrigatórias ("Binding Corporate Rules – BCR") para o Mercedes-Benz Group.

2 Âmbito de aplicação

Esta Diretiva de proteção de dados UE é válida para o Mercedes-Benz Group AG, as empresas controladas do Grupo (doravante designadas empresas do Grupo) e seus funcionários e membros de órgãos gerentes. Para este efeito, o termo 'controlada(s)' significa que o Mercedes-Benz Group AG, direta ou indiretamente, possui autoridade para exigir que esta diretiva seja adotada. Esta autoridade se expressa através da propriedade da maioria dos títulos com direito de voto, da maioria representativa do conselho administrativo ou por contrato.

A diretiva se aplica ao tratamento de dados pessoais por meios total ou parcialmente automáticos e ao tratamento não automático em sistemas de arquivamento, a menos que a legislação nacional amplie a área de aplicação. Na Alemanha, a diretiva também se aplica a todos os dados de funcionários[1] em forma de papel.
A diretiva se aplica ao tratamento de dados pessoais:
- (a) Por empresas do Grupo e suas concessionárias localizadas dentro da UE/EEE ou qualquer outro país onde esta diretiva possa ser aplicada ("empresas sediadas na UE/EEE"),
- (b) Por empresas do Grupo localizadas fora da UE/EEE, na medida em que oferecem bens ou serviços a pessoas naturais dentro da UE/EEE e/ou acompanham o comportamento de pessoas naturais dentro da UE/EEE ("empresas de países terceiros com ofertas para a UE/EEE"); ou
- (c) Por empresas do Grupo localizadas fora da UE/EEE, na medida em que tenham recebido dados pessoais direta ou indiretamente ou divulgado dados pessoais provenientes de empresas às quais a diretiva se aplica em conformidade com a alínea a) ou b) ("empresas de países terceiros que recebem dados da UE/EEE").

[1] **Exclusivamente por motivos de simplificação redacional, quando nos referimos a pessoas naturais nesta diretiva, usamos somente a forma masculina. Os conteúdos abrangem sempre pessoas de todas as identidades de gênero.**

Os tratamentos fora da UE/EEE são referidos, ao longo desta diretiva, como tratamentos em um país terceiro.

As empresas do Grupo que participam no tratamento por empresas de países terceiros, ou a ele estão sujeitas, estão listadas no outro regulamento aplicável "Lista das empresas do Grupo vinculadas à Diretiva de proteção de dados UE".

Esta diretiva pode ser aplicada em países fora da UE/EEE. Nos países onde os dados das pessoas jurídicas têm que ser protegidos tal como os dados pessoais, esta diretiva também deve ser aplicada aos dados de pessoas jurídicas.

3 Caráter jurídico vinculativo dentro do Mercedes-Benz Group

As disposições desta diretiva são obrigatórias para todas as empresas do Grupo que operam dentro de sua área de aplicação. As empresas do Grupo e seus administradores e funcionários são, portanto, responsáveis pelo cumprimento desta diretiva, além dos regulamentos aplicáveis da UE e das leis nacionais de proteção de dados.

As empresas do Grupo não estão autorizadas — sob reserva de exigências legais — a estipular regulamentações divergentes desta diretiva.

4 Relação com as exigências legais

Esta diretiva não substitui os regulamentos da UE e as leis nacionais. Ela complementa as leis nacionais de proteção de dados. Esses regulamentos e leis prevalecem quando o cumprimento desta diretiva resultar em uma violação da legislação nacional. O conteúdo desta diretiva deve ser respeitado mesmo que não exista legislação nacional correspondente.

Se o cumprimento desta diretiva levar a uma violação da legislação nacional ou se a legislação nacional exigir regulamentações divergentes dessa diretiva, isso deve ser comunicado ao encarregado da proteção de dados do Grupo e à organização central de conformidade como parte do monitoramento da legislação de proteção de dados. Em caso de conflitos entre a legislação nacional e esta diretiva, o encarregado da proteção de dados do Grupo e a organização central de conformidade trabalham junto com a respectiva empresa do Grupo para encontrar uma solução prática que atenda à finalidade desta diretiva.

5 Princípios gerais para o tratamento de dados pessoais

5.1 Legalidade

Os dados pessoais devem ser tratados de forma lícita e equitativa. Os dados podem ser tratados somente se e na medida em que exista um fundamento jurídico suficiente para a respectiva operação de tratamento. Isso também se aplica ao tratamento de dados entre as empresas do Grupo. O simples fato de tanto a empresa transmissora quanto a receptora pertencerem ao Mercedes-Benz Group não justifica o tratamento dos dados.

O tratamento de dados pessoais é permitido se existir uma das circunstâncias fatuais permitidas no ponto 5.2 ou 5.3. Também é necessário existir uma dessas circunstâncias fatuais se a finalidade do tratamento dos dados pessoais tiver sido mudada em relação à finalidade inicial.

5.2 Fundamento jurídico para dados de clientes e parceiros

5.2.1 Tratamento de dados para uma relação contratual

Dados pessoais da parte interessada, do cliente ou do parceiro em questão podem ser tratados para fundamentar, realizar e terminar um contrato. Isso abrange também o acompanhamento do cliente ou parceiro, desde que esteja ligado à finalidade do contrato.

Na preparação de um contrato é permitido o tratamento de dados pessoais para a criação de propostas, a preparação de pedidos de compra ou o cumprimento de outras necessidades do interessado para fins de celebração do contrato. É permitido contatar os interessados durante a fase inicial do contrato, utilizando os dados fornecidos por eles. Deverão ser atendidas eventuais limitações mencionadas pelo interessado.

5.2.2 Tratamento de dados para fins publicitários

Se o titular dos dados contatar uma empresa do Grupo com um pedido de informação (por exemplo, solicitação de envio de material informativo sobre um produto), o tratamento de dados é permitido para atender a esse pedido. Ações de fidelização do cliente ou de publicidade requerem outras condições jurídicas. O tratamento de dados pessoais para fins de publicidade ou pesquisa de mercado e opinião é permitido, na medida em que seja conciliável com a finalidade para a qual os dados foram originalmente coletados. O titular dos dados deve ser informado sobre a utilização dos seus dados para fins publicitários. Desde que os dados sejam coletados só para fins de propaganda, a sua indicação é efetuada pelo titular dos dados em caráter opcional. O titular dos dados deve ser informado sobre o caráter opcional da indicação de dados para esse fim. No âmbito da comunicação, deve ser obtido o consentimento do titular dos dados. O titular dos dados pode escolher entre os canais de contato disponíveis, como comunicações eletrônicas e telefone, como parte do processo de consentimento (para consentimento, ver ponto 5.2.3). Se o titular dos dados se opuser à utilização dos seus dados para fins publicitários, uma utilização dos seus dados para essa finalidade será inadmissível e os dados terão que ser restritos ou bloqueados para esse fim. Além disso, deverão ser respeitadas as restrições de alguns países relativas à utilização de dados para fins de propaganda.

5.2.3 Consentimento no tratamento de dados

Um tratamento de dados poderá ser realizado por consentimento do titular dos dados. Antes do consentimento, o titular dos dados deverá ser informado conforme esta diretiva de proteção de dados. Por motivos de comprovação, a declaração de consentimento deverá ser obtida, basicamente, por escrito ou por via eletrônica. Em alguns casos, por exemplo, no aconselhamento telefônico, o consentimento também poderá ser dado verbalmente. O consentimento deverá ser documentado.

5.2.4 tratamento de dados devido à permissão ou obrigação jurídica

O tratamento de dados pessoais também será permitido, se normas jurídicas nacionais exigirem, pressuporem ou autorizarem o tratamento de dados. O tipo e a abrangência do tratamento de dados devem ser necessários para o tratamento juridicamente permitido e devem orientar-se por estas normas jurídicas.

5.2.5 tratamento de dados, devido a interesses legítimos

O tratamento de dados pessoais também pode ocorrer se houver a necessidade de atender um interesse legítimo. Interesses legítimos são geralmente de ordem jurídica (por exemplo, execução de créditos em aberto) ou econômica (por exemplo, evitar interferências contratuais). O tratamento devido a um interesse legítimo não ocorrerá se, em um caso específico, os interesses do titular dos dados na proteção de seus dados se sobrepuserem aos interesses legítimos no tratamento. Devem ser examinados os interesses dignos de proteção para cada tratamento.

5.3 Fundamento jurídico para dados de funcionários

5.3.1 Tratamento de dados para o vínculo empregatício

Para o vínculo empregatício, poderão ser coletados os dados necessários para a celebração, execução e rescisão do contrato de trabalho. Os dados pessoais dos candidatos podem ser tratados com a finalidade de decidir sobre o estabelecimento de um vínculo empregatício. Após uma recusa, os dados do candidato deverão ser eliminados, tendo em conta os respectivos prazos legais, exceto se o candidato tiver consentido que os dados continuem armazenados para um processo de seleção posterior. É necessário um consentimento também para uma utilização dos dados em outros processos de candidatura ou antes do encaminhamento a outras empresas do Grupo. No caso de um vínculo empregatício existente, o tratamento de dados deve estar sempre submetido à finalidade do vínculo, desde que não se aplique uma das seguintes circunstâncias fatuais que permite o tratamento de dados.

Se, no processo inicial da relação de trabalho ou na relação de trabalho existente, for necessário o levantamento de informações adicionais sobre o candidato à vaga junto a terceiros, devem ser consideradas as respectivas exigências legais nacionais. Em caso de dúvida — na medida do permitido — deverá ser obtido o consentimento do titular dos dados.

Deverá existir um dos seguintes fundamentos jurídicos para tratamentos de dados de funcionários, que se encontrem no contexto empregatício, mas que não servem originalmente para estabelecer ou terminar a relação de trabalho (dados de funcionários).

5.3.2 Tratamento de dados devido a permissão ou obrigação jurídica

O tratamento de dados de funcionários também será permitido, se normas jurídicas nacionais exigirem, pressupuserem ou autorizarem o tratamento de dados. O tipo e a abrangência do tratamento de dados devem ser necessários para o tratamento juridicamente permitido e devem orientar-se por essas normas jurídicas. Se houver uma margem de manobra, deverão ser levados em consideração os interesses do funcionário dignos de proteção.

5.3.3 Acordo coletivo para tratamento de dados

Se um tratamento for além da finalidade da execução do contrato, o mesmo será permitido, se tiver sido autorizado por um acordo coletivo. As disposições devem estender-se à finalidade concreta do tratamento pretendido e devem ser estipuladas no âmbito do que é exigido nos regulamentos da UE e nas legislações nacionais.

5.3.4 Consentimento no tratamento de dados

Pode ser realizado um tratamento de dados de funcionários se o titular dos dados tiver dado o seu consentimento. As declarações de consentimento devem ser voluntárias. O não consentimento não deve resultar em desvantagens para os funcionários. Consentimentos involuntários são inválidos. Por motivos de comprovação, a declaração de consentimento deverá ser obtida, basicamente, por escrito ou por via eletrônica. Se as circunstâncias, excepcionalmente, não o permitirem, o consentimento poderá ser concedido verbalmente. Em todo caso, a concessão terá que ser devidamente documentada. Antes do consentimento, o titular dos dados deverá ser informado conforme esta diretiva de proteção de dados.

5.3.5 Tratamento de dados devido a interesse legítimo

O tratamento de dados de funcionários também pode ocorrer se houver a necessidade de atender um interesse legítimo da empresa do Grupo. Interesses legítimos são, geralmente, de ordem jurídica (por exemplo, a reivindicação, o exercício ou a defesa de direitos jurídicos) ou econômica (por exemplo, avaliação de empresas). Antes de cada tratamento deve ser examinado se há interesses dignos de proteção. Os dados pessoais podem ser tratados devido a um interesse legítimo se os interesses do funcionário dignos de proteção não se sobrepuserem ao interesse no tratamento.

Medidas de controle que exijam um tratamento de dados de funcionários além da implementação da relação de trabalho (por ex., controle de desempenho) somente poderão ser tomadas, se existir uma obrigação jurídica ou um motivo fundamentado para tal. Mesmo existindo um motivo fundamentado, deve ser verificada a proporcionalidade da medida de controle. Para esse fim, os interesses legítimos da empresa do Grupo na implementação da medida de controle (por ex., o cumprimento das disposições legais e das regras internas da empresa) devem ser ponderados contra um possível interesse digno de proteção do respectivo funcionário na exclusão da medida. As medidas somente podem ser implementadas se forem apropriadas no caso específico. O interesse legítimo da empresa do Grupo e os eventuais interesses dos funcionários, dignos de proteção, deverão ser constatados e documentados antes de qualquer medida. Além disso, deverão ser considerados outras requisitos legais aplicáveis (por exemplo, direitos por lei de participação do representante dos funcionários e direitos de informação dos titulares dos dados).

5.4 Tratamento de dados dignos de proteção especial

Os dados pessoais que requerem proteção especial somente podem ser tratados se isso for exigido ou permitido por lei. O tratamento de tais dados pela empresa do Grupo pode ser permitido, em particular, se o titular dos dados tiver consentido expressamente o tratamento, se o tratamento for absolutamente necessário para fazer valer, exercer ou defender reivindicações legais contra o titular dos dados ou para poder respeitar direitos e cumprir obrigações ao abrigo da legislação trabalhista ou social.

Se for planejado o tratamento de dados pessoais dignos de proteção especial, o encarregado da proteção de dados do Grupo deverá ser informado antecipadamente.

5.5 Decisões individuais automatizadas (incluindo perfis, se aplicável)

O titular dos dados pode ser submetido a uma decisão exclusivamente automatizada que tenha efeitos legais ou adversos similares somente se isso for necessário para a celebração ou a execução do contrato ou se o titular dos dados tiver consentido. Em casos individuais, essa decisão automatizada pode estar ligada à definição de um perfil, ou seja, ao tratamento de dados pessoais pelos quais são avaliados traços de personalidade individuais (por exemplo, a solvência). Nesse caso, o titular dos dados deve ser informado dos fatos e do resultado de uma decisão individual automatizada e deve ser possibilitada uma análise individual por um responsável pelo tratamento.

5.6 Obrigação de informação/ transparência

O departamento técnico responsável deve informar os titulares dos dados sobre as finalidades e circunstâncias do tratamento de seus dados pessoais de acordo com os artigos 13.º e 14.º do RGPD. Se os dados não se enquadrarem no âmbito de aplicação do RGPD, as informações devem ser fornecidas de acordo com a legislação nacional aplicável. As informações devem ser fornecidas de forma precisa, transparente, compreensível e facilmente acessível e em linguagem clara e simples. As exigências do encarregado da proteção de dados do Grupo e de Data Compliance devem ser observadas. Essas informações devem, em princípio, ser fornecidas no momento da primeira coleta dos dados pessoais. Se a empresa do Grupo obtiver os dados pessoais de terceiros, deverá informar os titulares dos dados dentro de um período de tempo razoável após a obtenção dos dados, a menos que os titulares dos dados:

- Já tenham as informações, ou
- O fornecimento de tais informações se revele impossível, ou
- implique um esforço desproporcional.

5.7 Limitação das finalidades

Os dados pessoais somente podem ser tratados para a finalidade legítima definida antes da coleta dos dados. Alterações posteriores na finalidade do tratamento são permitidas somente na condição de que o tratamento seja compatível com as finalidades para as quais os dados pessoais foram originalmente coletados.

5.8 Minimização de dados

Qualquer tratamento de dados pessoais deve ser limitado ao necessário, tanto quantitativa como qualitativamente, para atingir as finalidades para as quais os dados são tratados legalmente. Isso deve ser levado em consideração já no âmbito da coleta de dados. Sempre que a finalidade o permita e se o esforço for proporcional à finalidade visada, devem ser usados dados anonimizados ou estatísticos.

5.9 Exatidão dos dados

Os dados pessoais armazenados devem estar factualmente corretos e — se necessário — devem ser atualizados. O departamento técnico responsável deve tomar medidas apropriadas para garantir que dados incorretos ou incompletos sejam excluídos, corrigidos, complementados ou atualizados.

5.10 Privacy by Design & Privacy by Default

O princípio da "Privacy by Design" visa assegurar que os departamentos especializados definam estratégias internas de acordo com o estado atual da técnica e tomem medidas para integrar os princípios de proteção de dados na especificação e arquitetura de processos/modelos de negócio, bem como sistemas de TI para tratamento de dados desde o início, na fase de concepção e do design técnico. De acordo com o princípio da "Privacy by Design", os procedimentos e sistemas de tratamento de dados pessoais devem ser concebidos de modo que suas configurações iniciais sejam limitadas ao tratamento de dados necessário para o cumprimento da finalidade (princípio da "Privacy by Default"). Isso inclui o escopo de tratamento, duração do armazenamento e acessibilidade. Outras medidas podem incluir:

- Pseudonimização dos dados pessoais efetuada o mais rápido possível
- Transparência estabelecida com relação às funções e ao tratamento de dados pessoais
- Permitir que o titular dos dados decida sobre o tratamento de dados pessoais
- O operador de processos ou sistemas estar habilitado a criar e melhorar as funções de segurança.

Cada empresa do Grupo deverá implementar e operar medidas técnicas e organizacionais apropriadas durante todo o ciclo de vida de seus processos de tratamento para assegurar que os princípios acima sejam sempre respeitados.

5.11 Exclusão e anonimização

Dados pessoais podem ser conservados somente durante o tempo necessário para a finalidade para a qual esses dados são tratados. Isso significa que dados pessoais devem ser apagados ou anonimizados assim que a finalidade do seu tratamento for cumprida ou anulada de qualquer outro modo, a não ser que continuem existindo obrigações de conservação ou ônus de prova. Os responsáveis pelo tratamento em cada procedimento individual devem assegurar a implementação das rotinas de exclusão e anonimização de seus procedimentos. Cada sistema deve ter uma rotina de exclusão manual ou automatizada. Os pedidos de exclusão ou remoção do dado que pode ser relacionado com a pessoa específica pelos titulares dos dados devem poder ser aplicados tecnicamente nos sistemas. As especificações feitas pelo Mercedes-Benz Group AG para a implementação de rotinas de exclusão (como ferramentas de software, o manual de implementação de requisitos de exclusão, exigências de documentação) devem ser observadas.

5.12 Segurança do tratamento

Os dados pessoais devem ser protegidos contra acesso não autorizado, tratamento ou transmissão ilícita, assim como contra perda involuntária, modificações ou destruição. Antes da introdução de novos procedimentos de tratamento de dados, sobretudo novos sistemas de TI, devem ser definidas e implementadas medidas técnicas e organizacionais para a proteção dos dados pessoais. Essas medidas devem ser baseadas no estado atual da técnica, nos riscos do tratamento e na necessidade de proteger os dados.

Como parte da avaliação de impacto da proteção de dados e do Diretório de Procedimentos, os responsável pelo tratamento devem documentar as medidas técnicas e organizacionais relevantes para a proteção de dados.

Em particular, o departamento técnico responsável deve consultar seu Business Information Security Officer (BISO), seu encarregado de assuntos de segurança (ISO), e sua rede de proteção de dados. As exigências aplicáveis às medidas técnicas e organizacionais para proteger dados pessoais fazem parte da gestão da segurança de informação do Grupo e têm que ser adaptadas continuamente aos desenvolvimentos técnicos e às alterações organizacionais.

5.13 (Re)transferência para fora do Mercedes-Benz Group

A transferência de dados pessoais para destinatários fora das empresas do Grupo ou para destinatários dentro das empresas do Grupo está sujeita às condições de permissibilidade do tratamento de dados pessoais indicadas neste ponto 5. O destinatário dos dados deverá comprometer-se a utilizar os dados apenas para as finalidades determinadas.

Em caso de uma transferência transfronteiriça de dados pessoais (inclusive a autorização de acesso de outro país), devem ser cumpridos os requisitos nacionais relevantes para a transferência de dados pessoais para o exterior. Em particular, os dados pessoais da UE/EEE somente podem ser tratados em um país terceiro fora das empresas do Grupo se o destinatário conseguir provar que possui um nível de proteção de dados que esteja de acordo com esta diretiva. Instrumentos adequados podem ser, por exemplo:

- Acordo sobre as cláusulas contratuais-tipo da UE,
- Participação do destinatário em um sistema de certificação credenciado pela UE para garantir um nível adequado de proteção de dados; ou
- Reconhecimento das regras corporativas obrigatórias do destinatário para estabelecer um nível adequado de proteção de dados pela autoridade de controle da proteção de dados responsável.

As transferências de dados pessoais para uma autoridade somente são permitidas se não forem em massa, desproporcionais ou indiscriminadas e, nesse contexto, não excederem os limites do que é considerado necessário em uma sociedade democrática. Em caso de conflitos entre estas exigências e as das autoridades, o Mercedes-Benz Group AG trabalhará junto com a empresa responsável do Grupo para encontrar uma solução prática que atenda à finalidade desta diretiva (ponto 14.3).

Todas as obrigações estabelecidas neste ponto 5 são favoráveis a terceiros para o titular dos dados.

6 Avaliação de impacto sobre a proteção de dados

Ao introduzir novos processos de tratamento ou modificar substancialmente um processo de tratamento existente antes do tratamento, em particular através do uso de novas tecnologias, as empresas do Grupo devem analisar se tal tratamento apresenta um elevado risco para a privacidade dos titulares dos dados. A natureza, o escopo, o contexto e a finalidade do tratamento de dados devem ser levados em consideração. No âmbito da análise de risco, o departamento técnico responsável realiza uma avaliação dos impactos dos tratamentos planejados sobre a proteção de dados pessoais (avaliação de impacto sobre a proteção de dados). Se existir um elevado risco para os direitos e liberdades dos titulares dos dados após a avaliação de impacto sobre a proteção de dados e a aplicação de medidas de mitigação adequadas, o encarregado da proteção de dados do Grupo deve ser informado para que ele possa consultar a autoridade de controle da proteção de dados responsável. As especificações feitas pela Mercedes-Benz Group AG para a implementação da avaliação de impacto sobre a proteção de dados (tais como ferramentas de software, instruções para a realização da avaliação) devem ser observadas.

7 Documentação dos procedimentos de tratamento de dados

Cada empresa do Grupo deve documentar os procedimentos nos quais os dados pessoais são tratados em um Diretório de Procedimentos. O Diretório de Procedimentos deve ser elaborado por escrito, ou em formato eletrônico, e deve ser colocado à disposição da autoridade de controle da proteção de dados caso esta o solicite. As especificações feitas pela Mercedes-Benz Group AG em relação à documentação (como ferramentas de software, instruções para documentação) devem ser observadas.

8 Tratamento subcontratado

8.1 Aspectos gerais

Um tratamento subcontratado ocorre quando um executante trata dados pessoais em nome de e segundo as indicações do requerente. Nesses casos, um acordo sobre um tratamento subcontratado deve ser celebrado tanto com executantes externos quanto entre empresas do Grupo dentro do Mercedes-Benz Group, de acordo com os requisitos legais relevantes (por exemplo, o modelo "Acordo sobre o tratamento subcontratado"). Nisso, o requerente assume total responsabilidade pelo tratamento correto dos dados.

As disposições do ponto 8.3 também se aplicam aos requerentes externos que não sejam empresas do Grupo.

8.2 Disposições para o requerente

Aquando da subcontratação, devem ser cumpridas as seguintes especificações; o departamento técnico requerente tem que garantir o seu cumprimento:

- O executante deve ser escolhido mediante consideração de sua capacidade para garantir as medidas de proteção técnicas e organizacionais necessárias.
- Devem ser observados os modelos contratuais disponibilizados pelo encarregado da proteção de dados do Grupo.
- A subcontratação deve ser realizada em forma de texto ou em formato eletrônico. Devem estar documentadas as instruções para o tratamento de dados e as competências do requerente e do executante.

Antes do início do tratamento de dados, o requerente deve assegurar por meio de uma verificação adequada que o executante cumpre as obrigações anteriormente referidas. As especificações feitas pelo Mercedes-Benz Group a esse respeito (tais como ferramentas de software, instruções para a realização da avaliação, modelo de contrato) devem ser observadas. Um executante pode documentar o seu cumprimento das exigências de proteção de dados sobretudo através de uma certificação correspondente. As verificações devem ser repetidas regularmente durante o período de contrato, conforme o risco do tratamento dos dados.

8.3 Disposições para executantes intragrupo

O executante está autorizado a tratar dados pessoais só no âmbito das instruções do requerente.

Os executantes podem contratar outras empresas do Grupo ou terceiros ("subfornecedores") para o tratamento de dados pessoais como (sub)contrato próprio somente após o consentimento prévio do requerente. O consentimento somente é concedido quando o executante impõe ao subfornecedor, contratualmente ou de um modo juridicamente vinculativo comparável, as mesmas obrigações de proteção de dados em relação à empresa do Grupo e aos titulares dos dados impostas ao executante de acordo com esta diretiva, bem como medidas de proteção técnicas e organizacionais apropriadas. A forma de consentimento, bem como o dever de informar em caso de mudanças na relação de subcontratação, serão regulamentados no contrato de serviço.

Os executantes são obrigados a prestar assistência adequada ao requerente no cumprimento das disposições de proteção de dados aplicáveis a esse último, em particular fornecendo todas as informações necessárias para demonstrar o cumprimento das mesmas, em particular, o cumprimento:

- dos princípios gerais sobre o tratamento de acordo com o ponto 5,
- dos direitos dos titulares dos dados de acordo com o ponto 10,
- das obrigações de notificação do requerente de acordo com o ponto 12,
- das disposições aplicáveis ao requerente e ao executante de acordo com o ponto 8,
- e do tratamento de pedidos e investigações das autoridades de controle.

Se as normas ou disposições legais aplicáveis exigirem que o executante efetue um tratamento contrariamente às instruções ou se tais disposições legais impedirem o executante de cumprir suas obrigações nos termos desta diretiva ou do acordo sobre o tratamento subcontratado, o executante deverá notificar imediatamente seu requerente, a menos que a respectiva disposição legal proíba tal notificação. Isso se aplica também se o executante não puder cumprir as instruções do requerente por qualquer outro motivo. Nesse caso, o requerente terá o direito de suspender a transferência dos dados e/ou de rescindir o contrato sobre o tratamento subcontratado.

Os executantes são obrigados a informar os requerentes sobre qualquer pedido legalmente vinculante de divulgação de dados pessoais por uma autoridade, a menos que isso seja proibido por outros motivos.

Com o término da prestação do serviço, o executante deve, a critério do requerente, excluir ou devolver todos os dados pessoais fornecidos pelo mesmo.

Os executantes são obrigados a notificar imediatamente seu requerente e — se disponível — o requerente por trás do mesmo de quaisquer reclamações ou aplicações feitas por titulares de dados.

Os requerentes dentro do Grupo também devem obrigar os executantes de fora do Grupo a cumprir as regulamentações acima.

As obrigações específicas do executante em relação ao requerente são favoráveis a terceiros para o titular dos dados.

9 Responsabilidade conjunta

No caso de várias empresas do Grupo determinarem em conjunto os meios e finalidades do tratamento de dados pessoais (se disponível, juntamente com um ou mais terceiros) (entidades corresponsáveis/ Joint Controller), as empresas devem concluir um acordo especificando suas funções e responsabilidades em relação aos titular cujos dados elas tratam. Os modelos contratuais fornecidos pelo encarregado da proteção de dados do Grupo devem ser observados.

10 Direitos aplicáveis aos titulares dos dados

Todos os direitos dos titulares dos dados e obrigações das empresas do Grupo listadas neste ponto 10 são favoráveis a terceiros para os titulares dos dados.

Os pedidos e as reclamações feitas sob este ponto 10 devem ser respondidos no prazo de um mês. Tendo em conta a complexidade e o número de pedidos, esse período de um mês pode ser prorrogado por mais dois meses no máximo, sendo o titular dos dados informado em conformidade.

10.1 Direitos do titular dos dados

Na UE/EEE, um titular dos dados tem os seguintes direitos, conforme estabelecido mais detalhadamente na legislação da UE, contra a respectiva empresa do Grupo responsável ou, se esta última for o executante, contra o requerente:

- O direito de ser informado sobre as circunstâncias do tratamento de seus dados pessoais. As exigências do encarregado da proteção de dados do Grupo em relação a tais informações devem ser observadas.
- O direito de ser informado sobre a forma como seus dados são tratados e sobre seus direitos a esse respeito. Se, de acordo com o respectivo direito trabalhista, estiverem previstos direitos específicos de acesso à documentação do empregador (por exemplo, prontuário do funcionário), estes permanecem inalterados. Mediante solicitação, o titular dos dados receberá uma cópia de seus dados pessoais (se necessário, por uma recompensa apropriada), a menos que os interesses de terceiros sejam dignos de proteção.
- O direito de que os dados pessoais sejam corrigidos ou completados se estiverem imprecisos ou incompletos.
- O direito de ter seus dados excluídos se ele revogar seu consentimento ou se o fundamento jurídico para o tratamento dos dados estiver ausente ou tiver deixado de existir. O mesmo será válido no caso de a finalidade do tratamento de dados ter sido suprimida por vencimento do prazo ou por outros motivos. Devem ser respeitadas as obrigações de arquivamento existentes e os interesses dignos de proteção contrários a um apagamento dos dados.
- O direito de limitação do tratamento de seus dados se ele contestar a exatidão ou se os dados não forem mais necessários à empresa do Grupo, mas o titular dos dados precisar dos dados para usufruir de seus direitos legais. O titular dos dados também pode solicitar que a empresa do Grupo limite o tratamento de seus dados, caso, de outra forma, esta tenha que excluir os dados ou se esta tiver que verificar uma oposição por parte do titular dos dados.
- O direito de obter, em formato digital comumente utilizado, dados pessoais a seu respeito fornecidos com base em um consentimento ou no âmbito de um contrato celebrado ou iniciado com ele, e de transmitir tais dados a terceiros, desde que o tratamento seja realizado com o auxílio de procedimentos automatizados e isso seja tecnicamente viável.
- O direito de se opor ao marketing direto a qualquer momento. Deve ser assegurado o consentimento adequado e a administração de oposições.

- O direito de oposição ao tratamento com o fundamento jurídico de interesses prevalecentes das empresas do Grupo ou de terceiros, se houver fundamentos para isso com base em sua situação pessoal particular. No entanto, o direito de oposição não existe se a empresa do Grupo tiver razões de força maior para o tratamento ou se este servir para reivindicar, exercer ou defender direitos legais. Em caso de uma oposição justificada, os dados devem ser excluídos.

Além disso, o titular dos dados está autorizado a reivindicar os seus direitos também perante a empresa importadora de dados do Grupo em um país terceiro.

10.2 Procedimentos de reclamação

Os titulares dos dados têm o direito de apresentar uma reclamação ao encarregado da proteção de dados do Grupo se considerarem que esta diretiva tenha sido violada. Tais reclamações podem ser enviadas por e-mail.

A empresa do Grupo sediada na UE/EEE agindo como exportadora de dados prestará apoio aos titulares dos dados cujos dados pessoais tenham sido coletados dentro da UE/EEE a determinar os fatos e fazer valer seus direitos sob esta diretiva contra a empresa do Grupo importadora de dados.

Caso o titular dos dados não concorde com a decisão da empresa do Grupo sobre o cumprimento das disposições (ou esteja insatisfeito com seu tratamento), ele pode contestar essa decisão ou conduta, exercendo seus direitos. Para esse fim, ele pode recorrer à autoridade de controle responsável, em particular no país de sua residência habitual, em seu local de trabalho ou no local da suposta violação, ou ainda recorrer aos tribunais (ponto 11.2). Outros direitos e responsabilidades legais permanecem inalterados.

11 Responsabilidade e jurisdição

11.1 Disposições relativas à responsabilidade

A responsabilidade por qualquer violação desta diretiva, cometida por uma empresa de um país terceiro que receba dados da UE/EEE no âmbito de um tratamento de dados de um país terceiro, será assumida pela empresa do Grupo sediada na UE/EEE ("exportador de dados") que transferiu em primeiro os dados pessoais para uma empresa do Grupo sediada em um país terceiro. Essa responsabilidade inclui a obrigação de remediar qualquer situação irregular e de compensar qualquer dano material ou não-material causado por uma violação desta diretiva por empresas do Grupo de países terceiros.

O exportador de dados só estará isento dessa responsabilidade, no todo ou em parte, se provar que a empresa do país terceiro que recebe os dados da UE/EEE não é responsável pelo evento que deu origem ao dano.

11.2 Jurisdição

O titular dos dados pode recorrer aos tribunais na sede onde a entidade responsável ou o requerente está estabelecido ou no local da sua residência habitual.

O titular dos dados que alega uma violação desta diretiva no âmbito de um tratamento de dados em um país terceiro pode fazer valer seus direitos legais tanto contra a empresa importadora de dados quanto contra a empresa exportadora de dados na UE/EEE. Portanto, o titular dos dados pode apresentar a suposta violação e os direitos legais resultantes perante os tribunais e as autoridades de controle, seja na sede da entidade responsável ou no local da sua residência habitual.

As disposições relativas à responsabilidade e jurisdição neste ponto são favoráveis a terceiros para os titulares dos dados.

12 Notificação de incidentes de proteção de dados

Em caso de uma possível violação da segurança de dados ("incidente de proteção de dados"), as empresas do Grupo em questão são obrigadas a investigar, informar e mitigar os danos. Um incidente de proteção de dados é considerado uma violação de dados se ocorrer uma violação da segurança de dados que resulte ilegalmente na exclusão, alteração, divulgação ou uso não autorizado de dados pessoais. Se isso resultar em um risco aos direitos e liberdades de pessoas naturais, os eventos relevantes devem ser comunicados à autoridade de controle responsável, se possível dentro de 72 horas após a empresa do Grupo tomar conhecimento da violação. Além disso, em caso de uma violação de dados que possa representar um elevado risco para seus direitos e liberdades, os titulares dos dados devem ser notificados da respectiva violação. Os executantes, de acordo com o ponto 8.2, são obrigados a comunicar imediatamente os incidentes de proteção de dados a seu requerente.

Se for identificado ou suspeito um incidente de proteção de dados dentro da área de responsabilidade de uma empresa do Grupo, todos os funcionários são obrigados a comunicar imediatamente esse fato no âmbito do processo "Information Security Incident Management". As especificações feitas pelo Mercedes-Benz Group AG a esse respeito (tais como ferramentas de software, instruções para a notificação) devem ser observadas.

Qualquer violação de dados deve ser documentada e a documentação deve ser colocada à disposição da autoridade de controle responsável, caso esta a solicite.

13 Organização de proteção de dados e sanções

13.1 Responsabilidade

Os membros dos órgãos gerentes das empresas do Grupo são responsáveis pelo tratamento de dados em sua área de responsabilidade. Consequentemente, estes comprometem-se a garantir que as exigências legais e as contidas nesta Diretiva de proteção de dados UE serão levadas em consideração (por exemplo, obrigações nacionais de notificação). É tarefa de cada gerente, no âmbito de sua responsabilidade, assegurar o tratamento adequado dos dados em conformidade com a proteção de dados por meio de medidas organizacionais, pessoais e técnicas. Compete aos respectivos funcionários a implementação dessas especificações. O encarregado da proteção de dados do Grupo deve ser imediatamente informado aquando de controles da proteção de dados realizados pelas autoridades.

13.2 Conscientização e treinamento

Os quadros de chefia devem assegurar que seus funcionários recebam e participem do treinamento necessário de proteção de dados, incluindo o conteúdo e a aplicação desta diretiva, na medida em que tenham acesso contínuo ou regular aos dados pessoais ou estejam envolvidos na coleta de dados ou no desenvolvimento de ferramentas para o tratamento de dados pessoais. As exigências do encarregado da proteção de dados do Grupo e de Data Compliance devem ser observadas.

13.3 Organização

O encarregado da proteção de dados do Grupo é internamente independente das instruções relativas ao exercício de suas funções. Ele atua no cumprimento das disposições nacionais e internacionais de proteção de dados. Ele é responsável por esta diretiva e monitora o cumprimento da mesma. Se as empresas do Grupo desejarem participar de um sistema de certificação internacional de regras corporativas obrigatórias sobre a proteção de dados, elas devem coordenar essa participação com o encarregado da proteção de dados do Grupo.

O encarregado da proteção de dados do Grupo é nomeado pelo Conselho Administrativo do Mercedes-Benz Group AG e é apoiado pelo Conselho Administrativo no exercício de suas funções. Geralmente, o encarregado da proteção de dados do Grupo é nomeado pelas as empresas do Grupo obrigadas por lei a nomear um encarregado. O encarregado da proteção de dados do Grupo responde diretamente ao Conselho Administrativo do Mercedes-Benz Group AG e à diretoria de cada empresa do Grupo para a qual o encarregado da proteção de dados do Grupo foi nomeado. Exceções específicas devem ser coordenadas com o encarregado da proteção de dados do Grupo.

No âmbito das obrigações de relatório existentes, o Conselho Fiscal da Mercedes-Benz Group AG deve ser informado sobre o relatório anual do encarregado da proteção de dados do Grupo.

Qualquer titular de dados pode contatar o encarregado da proteção de dados do Grupo a qualquer momento para expressar preocupações, efetuar perguntas, solicitar informações ou fazer reclamações relativas à proteção de dados ou perguntas sobre a segurança de dados. As preocupações e reclamações serão tratadas de forma sigilosa.

Os dados de contato do encarregado da proteção de dados do Grupo são os seguintes:

Mercedes-Benz Group AG, encarregado da proteção de dados do Grupo, HPC E600,
70546 Stuttgart, Alemanha
E-mail: data.protection@mercedes-benz.com
Intranet: https://social.intra.corpintra.net/docs/DOC-71499

O Mercedes-Benz Group também estabeleceu uma organização de conformidade, que é descrita em mais detalhes em regulamentações internas separadas. A organização de conformidade apoia e monitora as empresas do Grupo no que diz respeito ao cumprimento das exigências de proteção de dados. Ela projeta o conteúdo dos treinamentos em proteção de dados e define os critérios para o grupo de participantes.

13.4 Sanções

O tratamento ilegal de dados pessoais ou outras violações das leis de proteção de dados pode estar sujeito a processos regulamentares e criminais em muitos países e também pode dar origem a reclamações por danos. As violações pelas quais os funcionários individuais sejam responsáveis podem ter consequências de ordem trabalhista. As violações desta diretiva serão punidas de acordo com as regulamentações internas.

13.5 Auditoria e controles

O cumprimento desta diretiva e das leis de proteção de dados aplicáveis é avaliado regularmente, com base no risco, no nível de Grupo, pelo menos uma vez por ano. Isso é efetuado através de uma avaliação de risco de conformidade interna, auditorias incluindo tópicos específicos da proteção de dados e outras avaliações. O encarregado da proteção de dados do Grupo tem o direito de solicitar mais avaliações. Os resultados devem ser comunicados ao encarregado da proteção de dados do Grupo, à empresa responsável do Grupo e a seu encarregado da proteção de dados, caso tenha sido nomeado um.

O Conselho Administrativo do Mercedes-Benz Group AG deve ser informado dos resultados no âmbito das obrigações de reportar existentes. A pedido, os resultados dos controles de proteção de dados são disponibilizados à autoridade de controle da proteção de dados responsável. No âmbito das suas atribuições legais, a autoridade de controle da proteção de dados responsável pode submeter qualquer empresa do Grupo a uma auditoria de proteção de dados relativa ao cumprimento das disposições desta diretiva.

14 Alterações a esta diretiva e cooperação com as autoridades

14.1 Responsabilidades em caso de alterações

Essa diretiva pode ser alterada em consulta com o encarregado da proteção de dados do Grupo, no âmbito do procedimento de alteração das diretivas (Diretiva sobre gerenciamento de diretivas, A 1). Quaisquer alterações que tenham um impacto significativo nesta Diretiva de proteção de dados UE, A 17 ou que possam afetar o nível de proteção oferecido (ou seja, alterações de caráter vinculativo) deverão ser comunicadas imediatamente às autoridades competentes de proteção de dados, as quais aprovarão esta diretiva como regras corporativas obrigatórias.

O encarregado da proteção de dados do Grupo é responsável por manter uma lista atualizada de todas as empresas do Grupo que estão vinculadas a essa diretiva (regulamento aplicável "Lista de empresas do Grupo vinculadas à Diretiva de proteção de dados UE"). Com base nesta diretiva, não ocorrerá nenhuma transferência de dados pessoais para uma nova empresa do Grupo até que a nova empresa do Grupo esteja efetivamente vinculada a esta diretiva e atenda às medidas de conformidade adequadas para o cumprimento da mesma.

O titular dos dados tem o direito ao fácil acesso desta diretiva. Por conseguinte, a última versão dessa diretiva será publicada na Internet em https://www.group.mercedes-benz.com sob proteção de dados. Essa especificação é favorável a terceiros para o titular dos dados.

Se forem efetuadas alterações nesta diretiva ou na lista de empresas do Mercedes-Benz Group AG, o encarregado da proteção de dados do Grupo informará a autoridade de controle da sede do Mercedes-Benz Group AG uma vez por ano, explicando de forma breve as razões para a atualização.

14.2 Cooperação com as autoridades

As empresas do Grupo que realizam ou participam de tratamentos em países terceiros são obrigadas a cooperar com a autoridade de controle responsável em caso de problemas, pedidos ou outros procedimentos relacionados com o tratamento de dados pessoais no contexto acima mencionado. Isso inclui a obrigação de aceitar auditorias legítimas por parte das autoridades de controle. Além disso, quaisquer instruções legais das autoridades de controle responsáveis, decorrentes de tratamentos realizados em países terceiros ou de disposições desta diretiva, devem ser cumpridas.

As disposições do ponto 14.2 sobre cooperação com as autoridades são favoráveis a terceiros para os titulares dos dados.

14.3 Monitoramento e relatórios sobre regulamentações de países terceiros

Os responsáveis pelos tratamento em empresas de países terceiros devem informar imediatamente o encarregado da proteção de dados do Grupo se sua empresa tiver motivos razoáveis para acreditar que leis ou outros regulamentos não promulgados pela UE como instituição ou por um de seus Estados-Membros acarretam os seguintes riscos, se as leis ou outros regulamentos:

- Forem susceptíveis de impedir a respectiva empresa de países terceiros ou outra empresa do Grupo de cumprir suas obrigações sob esta diretiva no contexto de operações de tratamento em países terceiros ou
- Puderem ter um efeito adverso significativo sobre os direitos concedidos aos titulares dos dados sob esta diretiva no tratamento em países terceiros. Esse é especialmente o caso quando as autoridades locais exigem uma transferência em massa, desproporcional ou indiscriminada de dados pessoais que exceda os limites do que é considerado necessário em uma sociedade democrática.

O encarregado da proteção de dados do Grupo deverá avaliar o impacto e informar a autoridade de controle da proteção de dados responsável, se existente, se a exigência legal em questão for susceptível de ter um impacto significativo sobre as garantias fornecidas pela diretiva. Esta disposição é favorável a terceiros para o titular dos dados.

Se uma empresa de um país terceiro for obrigada por uma autoridade a não informar a autoridade de controle da proteção de dados sobre a divulgação de dados pessoais, ela deverá fazer todos os possíveis para mitigar ou levantar essa proibição e, dentro desse espaço de manobra, fornecer anualmente, à autoridade de controle da proteção de dados, informações gerais sobre os pedidos recebidos (por exemplo, número de pedidos de divulgação, tipo de dados solicitados e, se possível, autoridade requerente).

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