DAIMLER

Diretiva de proteção de dados.

Prefácio

Prezadas Senhoras e Senhores,

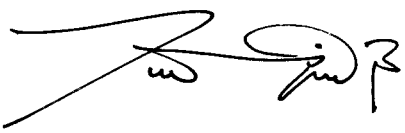
Na era digital em que vivemos, nós oferecemos a nossos clientes a possibilidade de estar “always on” mesmo em seu automóvel. Para tal, é necessário coletar e processar dados. Apesar disso, nós desenvolvemos nossas ações com base em um único princípio, comum a todos os aspetos de nossa atividade, dos veículos propriamente ditos à oficina e ao revendedor: seja onde for que os dados são salvos e enviados, o sistema deve garantir um nível máximo de proteção e segurança de dados. Isso se aplica aos dados de clientes, potenciais interessados e parceiros comerciais, mas também aos dados de nossos colaboradores. Porque a proteção de dados significa proteger a pessoa.

Nossa meta é que a Daimler não seja somente sinônimo de automóveis seguros, mas que também defina padrões no âmbito da proteção de dados. Por esse motivo, enquanto empresa global, nós acreditamos ser nosso dever cumprir os diferentes requisitos legais existentes em todo o mundo relacionados à coleta e ao processamento de dados pessoais. Assim, a nossa prioridade máxima é garantir uma norma relacionada ao tratamento de dados pessoais uniforme e válida em todo o mundo. Isso porque respeitar os direitos de personalidade e a esfera privada de cada indivíduo é, para nós, a base de toda a relação comercial baseada na confiança.

Em nossa diretriz corporativa relacionada à proteção de dados, a Daimler estabeleceu requisitos muito exigentes para o processamento de dados pessoais de clientes, potenciais interessados, parceiros comerciais e colaboradores. Essa diretriz corresponde às exigências da diretiva europeia sobre a proteção de dados pessoais e assegura o cumprimento dos princípios legais nacionais e internacionais relacionados à proteção de dados e aplicáveis em todo o mundo. Desse modo, estamos estabelecendo em nossa empresa uma norma de proteção e segurança de dados válida em todo o mundo e, simultaneamente, regulamentando a troca de dados entre as sociedades do grupo. Nesse sentido, definimos como referência sete princípios da proteção de dados – entre os quais se encontram a transparência, a economia de dados e a segurança de dados.

É dever de nossos executivos e colaboradores respeitar essa diretriz corporativa relacionada à proteção de dados e cumprir as respetivas legislações sobre a proteção de dados. Enquanto Delegado do Grupo responsável pela proteção de dados, eu sou responsável pela observância das regulamentações e princípios legais relacionados à proteção de dados dentro da Daimler.

Meus colaboradores e eu estamos à sua disposição para qualquer dúvida relacionada à proteção e à segurança de dados na Daimler.



Dr. Joachim Rieß
Delegado do Grupo responsável pela proteção de dados

Índice

I. Finalidade da diretiva de proteção de dados

No âmbito da sua responsabilidade social, o Grupo Daimler compromete-se a cumprir a nível internacional os direitos de proteção de dados. Esta diretiva aplica-se a todo o Grupo Daimler mundialmente e está alinhada aos princípios básicos sobre a proteção de dados, aceitos de forma global. A preservação da proteção de dados constitui a base para as relações de negócios, caracterizadas pela confiança, e a reputação do Grupo Daimler como um empregador atrativo.

A diretiva de proteção de dados assegura uma das condições básicas necessárias para um intercâmbio mundial de dados[1] entre as sociedades pertencentes ao Grupo. Ela assegura o nível de proteção de dados adequado exigido pela diretiva de proteção de dados europeia[2] e pelas legislações nacionais para um intercâmbio de dados transnacional também nos países nos quais ainda não exista por lei um nível de proteção de dados[3] adequado.

II. Âmbito de aplicação e alteração da diretiva de proteção de dados

Esta diretiva de proteção de dados aplica-se a todas as empresas do Grupo Daimler, ou seja, à Daimler AG e a todas as empresas controladas do Grupo, bem como empresas associadas e os respectivos colaboradores. Para este efeito, o termo ‚controlada' significa que a Daimler AG, direta ou indiretamente, possui autoridade para exigir que esta diretiva seja adotada. Esta autoridade expressa-se através da propriedade da maioria dos títulos com direito de voto, da maioria representativa do conselho administrativo ou por contrato. A diretiva de proteção de dados abrange todos os processamentos de dados de pessoas[4]. Nos países em que dados de pessoas jurídicas têm que ser protegidos tal como os dados pessoais, esta diretiva de proteção de dados deve ser aplicada também para dados de pessoas jurídicas. Dados anonimizados[5], como, por exemplo, para análises ou pesquisas estatísticas, não são abrangidos por esta diretiva de proteção de dados.

As empresas do Grupo não estão autorizadas a estipular regulamentações divergentes desta diretiva de proteção de dados. Podem ser criadas outras diretivas sobre proteção de dados em coordenação com o delegado de assuntos de proteção de dados do Grupo, desde que isto seja exigido pela legislação nacional. Uma alteração desta diretiva só poderá ser efetuada mediante aprovação do delegado responsável pela proteção de dados, no procedimento previsto para a respectiva alteração de diretivas. As alterações são comunicadas imediatamente às empresas do Grupo Daimler no processo previsto para alteração de diretivas. Alterações que afetem substancialmente o cumprimento da diretiva de proteção de dados devem ser comunicadas anualmente às autoridades de proteção de dados que aprovam esta diretiva como regulamentos internos obrigatórios sobre a proteção de dados.

A versão mais atual da diretiva de proteção de dados pode ser acessada em informações sobre proteção de dados, no site da internet da Daimler AG, www.daimler.com.

1 Vide XV.
2 Diretiva 95/46/CE do Parlamento Europeu e do Conselho para a proteção de pessoas físicas no processamento de dados pessoais e a livre circulação de dados;
pode ser consultada em http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm#richtlinie
3 Vide XV.
4 Vide XV.
5 Vide XV.

III. Validade do direito de cada país

Esta diretiva de proteção de dados contém os princípios de proteção de dados mundialmente aceitos, sem que o direito de cada país seja substituído. Esta complementa a legislação de proteção de dados nacional que por sua vez, tem prioridade, caso a legislação exija disposições divergentes desta diretiva de proteção de dados ou imponha exigências mais rigorosas. Os conteúdos desta diretiva de proteção de dados também deverão ser observados, se não existir uma legislação nacional adequada. Deve ser cumprido o dever de comunicação e informação existente de acordo com o direito para proteção de dados nacional.

Cada empresa do Grupo Daimler é responsável pelo cumprimento desta diretiva de proteção de dados e das imposições legais. Se houver motivo para supor que as imposições legais estejam em contradição com as obrigações decorrentes desta diretiva de proteção de dados, a empresa afetada deve informar imediatamente o delegado responsável por assuntos de proteção de dados. No caso de uma colisão das disposições legais nacionais com as da diretiva de proteção de dados, a Daimler AG juntamente com a respectiva empresa do Grupo irá procurar uma solução prática que atenda a finalidade da diretiva de proteção de dados.

IV. Princípios para o processamento de dados pessoais

1. Equidade e legalidade
No processamento de dados pessoais deverão ser preservados os direitos da personalidade do envolvido[6]. Os dados pessoais devem ser levantados e processados de modo justo e correto.

2. Vinculação
O processamento de dados pessoais só deve servir às finalidades para as quais foi determinado antes do levantamento dos dados. Alterações posteriores das finalidades só serão possíveis com restrições e devem ser justificadas.

3. Transparência
O envolvido deve ser informado sobre o modo como os seus dados são tratados. O levantamento dos dados pessoais deve ser efetuado, basicamente, junto ao próprio envolvido. No levantamento de dados, o envolvido deverá, pelo menos, poder reconhecer ou ser informado adequadamente sobre o seguinte:

- Identidade do departamento responsável[7]
- Finalidade do processamento de dados
- Terceiros[8] ou categorias de terceiros aos quais os dados serão, eventualmente, transmitidos

[6] Vide XV.
[7] Vide XV.
[8] Vide XV.

4. Evitando e economizando dados
Antes do processamento dos dados pessoais deverá ser verificado, se e até que ponto estes são necessários para atingir a finalidade desejada com o processamento. Deverão ser utilizados dados anonimizados ou estatísticos, se isto for possível para atingir a finalidade ou se o esforço se encontrar em uma relação adequada com a finalidade pretendida.
Os dados pessoais não deverão ser guardados para eventuais finalidades futuras, exceto se tal for estipulado ou permitido pela legislação do país.

5. Apagamento
Devem ser apagados dados pessoais que não sejam mais necessários[9] depois da prescrição do período de conservação de dados especificado por lei ou previsto pelo processo de negócios. Se, em casos excepcionais, existir a necessidade de proteger interesses ou se os dados tiverem uma importância histórica, estes devem ser conservados por mais tempo até que os interesses dignos de proteção possam ser esclarecidos legalmente ou os arquivos do Grupo possam ter avaliado os dados quanto ao seu arquivamento para fins históricos.

6. Exatidão dos fatos, atualidade dos dados
Dados pessoais devem ser guardados de forma correta, integral e, se necessário, na versão atual. Deverão ser tomadas as medidas necessárias para assegurar que dados incorretos, incompletos ou desatualizados sejam eliminados, corrigidos, completados ou atualizados.

7. Confidencialidade e segurança dos dados
Dados pessoais estão submetidos ao segredo de dados. Estes têm que ser tratados de forma sigilosa. Através de medidas técnico-organizacionais adequadas, estes devem ser protegidos contra acesso não autorizado, processamento ou encaminhamento indevidos, bem como contra destruição, perda, alteração ou perda inadvertidas.

V. Admissibilidade do processamento de dados

O levantamento, o processamento e a utilização de dados pessoais são admissíveis, se existir uma das circunstâncias fatuais abaixo. Uma destas circunstâncias fatuais é necessária se a finalidade para o levantamento, processamento e a utilização de dados pessoais tiver sido mudada em relação à finalidade inicial.

[9] Vide XV.

1. Dados de clientes e parceiros

1.1 Processamento de dados para uma relação contratual

Dados pessoais do interessado, do cliente ou do parceiro afetado podem ser processados para fundamentar, realizar e terminar um contrato. Isto abrange também o acompanhamento do parceiro contratual, desde que esteja ligado à finalidade do contrato.
Na preparação de um contrato, ou seja, na sua fase inicial, é permitido o processamento de dados pessoais para a criação de propostas, a preparação de solicitações de compra ou o cumprimento de outras necessidades do interessado direcionadas para uma conclusão do contrato. É permitido contactar os interessados durante a fase inicial do contrato, utilizando os dados fornecidos por eles. Deverão ser consideradas atendidas eventuais restrições mencionadas pelo interessado. Para medidas de propaganda que vão mais além, deverão ser observadas as condições indicadas em VI.1.2.

1.2 Processamento de dados para fins publicitários

Se o envolvido contactar uma empresa do Grupo Daimler com um pedido de informação (por exemplo, solicitação de envio de material informativo sobre um produto), o processamento de dados será permitido para atender este pedido.

Medidas de vinculação do cliente ou de propaganda requerem outras condições jurídicas. O processamento de dados pessoais para fins de publicidade ou pesquisa de mercado e opinião é permitido, desde que seja conciliável com a finalidade para a qual os dados foram originalmente levantados. O envolvido deve ser informado sobre a utilização dos seus dados para fins de propaganda. Desde que os dados sejam levantados só para fins de propaganda, a sua indicação é efetuada pelo envolvido em caráter opcional. O envolvido deve ser informado sobre o caráter opcional da indicação de dados para este fim. No âmbito da comunicação com o envolvido, deverá ser solicitado o seu consentimento[10] para o processamento dos seus dados para fins de propaganda. No âmbito do consentimento, o envolvido deverá poder escolher entre os canais de contato disponíveis, como correios, correio eletrônico e telefone (consentimento, vide V.1.3).

Se o envolvido se opuser à utilização dos seus dados para fins de propaganda, uma utilização dos seus dados para esta finalidade será inadmissível e os dados terão que ser bloqueados para este fim. Além disso, deverão ser respeitadas as restrições de alguns países relativas à utilização de dados para fins de propaganda.

1.3 Consentimento no processamento de dados

Um processamento de dados poderá ser realizado por consentimento do envolvido. Antes do consentimento, o envolvido deverá ser informado conforme IV.3. desta 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.

1.4 Processamento de dados, devido a permissão legal

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

[10] Vide XV.

1.5 Processamento de dados, devido a interesses legítimos

O processamento de dados pessoais também pode ocorrer se houver a necessidade de atender um interesse legítimo do Grupo Daimler. Interesses legítimos são geralmente de ordem jurídica (por exemplo, execução de créditos em aberto) ou econômica (por exemplo, evitar interferências contratuais). Não deverá ser efetuado um processamento de dados pessoais, devido a um interesse legítimo, se, em casos individuais, existir evidências que os interesses do envolvido, dignos de proteção, se sobrepõem ao interesse do processamento. Devem ser examinados os interesses dignos de proteção para cada processamento.

1.6 Processamento de dados dignos de proteção especial

O processamento de dados pessoais dignos de especial[11] só pode ser efetuado se necessário por lei ou mediante o consentimento expresso do envolvido.
O processamento destes dados será também permitido se for forçosamente necessário para reivindicar, exercer ou defender direitos legais perante o envolvido. Se for planejado o processamento de dados dignos de proteção especial, o delegado do Grupo responsável pela proteção de dados deverá ser informado antecipadamente.

1.7 Decisões individuais automatizadas

Processamentos de dados pessoais automatizados através dos quais são analisadas características individuais de personalidade (por exemplo, credibilidade) não devem ser a única base de exclusão para decisões com consequências jurídicas negativas ou graves prejuízos para o envolvido. O envolvido deverá ser informado dos fatos e do resultado de uma decisão individual automatizada e deverá ter a oportunidade para se manifestar. A fim de evitar decisões incorretas, um colaborador deverá efetuar um controle e uma verificação de plausibilidade.

1.8 Dados de usuários e Internet

Se forem levantados, processados e utilizados dados pessoais em páginas web ou em apps, os envolvidos devem ser informados sobre as observações relativas à proteção de dados e, se for o caso, sobre as observações de cookies. As instruções de proteção de dados e de cookies devem ser integradas de modo que os envolvidos possam identificá-las com facilidade, acessá-las diretamente e de modo que estas estejam disponíveis constantemente.

Se forem criados perfis de usuários (rastreamento) para avaliação do comportamento de utilização de páginas web e apps, os envolvidos devem ser informados de qualquer forma a respeito nas instruções de proteção de dados. Um rastreamento pessoal só pode ocorrer, se for permitido pela legislação nacional ou o envolvido tiver consentido. Se o rastreamento for realizado sob um pseudônimo, deverá ser concedida ao envolvido a oportunidade de contestação (opt-out) nas instruções de proteção de dados.

Se nas páginas web ou em apps for permitido o acesso a dados pessoais numa área de cadastro, a identificação e autenticidade dos envolvidos devem ser realizadas de modo a assegurar uma proteção adequada para o respectivo acesso.

[11] Vide XV.

2. Dados de colaboradores

2.1 Processamento de dados para o vínculo empregatício
Para o vínculo empregatício, poderão ser levantados os dados necessários para a celebração, execução e rescisão do contrato de trabalho.
Os dados pessoais de candidatos a vagas poderão ser processados para o início 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.

Numa relação de trabalho existente, o processamento de dados deve estar sempre submetido à finalidade do contrato de trabalho, desde que não se aplique uma das seguintes circunstâncias fatuais de autorização para o processamento 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, deverá ser obtido o consentimento do candidato.

Deverá existir uma legitimação jurídica para processamentos de dados de colaboradores, que se encontrem no contexto empregatício, mas que não servem originalmente para o cumprimento do contrato de trabalho. Estas podem ser imposições legais, regulamentações coletivas com representantes dos trabalhadores, um consentimento do colaborador ou interesses legítimos da empresa.

2.2 Processamento de dados, devido a permissão legal
O processamento de dados pessoais de colaboradores também será permitido, se normas jurídicas nacionais exigirem, pressuporem ou autorizarem o processamento de dados. O tipo e a abrangência do processamento de dados devem ser necessários para o processamento juridicamente permitido e devem orientar-se por estas normas jurídicas. Se houver uma margem de manobra, deverão ser levados em consideração os interesses do colaborador dignos de proteção.

2.3 Regulamentações coletivas para processamentos de dados
Se um processamento for além da finalidade da execução do contrato, o mesmo será permitido, se tiver sido autorizado por uma regulamentação coletiva. Regulamentações coletivas são acordos salariais ou acordos entre empregador e os representantes dos trabalhadores no âmbito das possibilidades da respectiva legislação trabalhista. As regulamentações devem estender-se à finalidade concreta do processamento pretendido e devem ser estipuladas no âmbito do direito da proteção de dados de cada país.

2.4 Consentimento no processamento de dados
Pode ser realizado um processamento de dados de colaboradores devido a um consentimento do envolvido. As declarações de consentimento deverão ser voluntárias. Consentimentos involuntários não têm efeitos. 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. No caso de uma indicação de dados voluntária informada pelo envolvido, é possível aceitar um consentimento se a legislação nacional não exigir um consentimento explícito. Antes do consentimento, o envolvido deverá ser informado conforme IV.3. desta diretiva de proteção de dados.

2.5 Processamento de dados, devido a interesses legítimos

O processamento de dados pessoais de colaboradores também pode ser efetuado se houver a necessidade de atender um interesse legítimo do Grupo Daimler. Interesses legítimos são, geralmente, de ordem jurídica (por exemplo, a reivindicação, o exercício ou a defesa de exigências jurídicas) ou econômica (por exemplo, avaliação de empresas).

Não deverá ser efetuado um processamento de dados pessoais, devido a um interesse legítimo, se em casos individuais existir evidências de que os interesses do colaborador, dignos de proteção, se sobrepõem ao interesse do processamento. Para cada processamento deve ser examinado se há interesses dignos de proteção.

Medidas de controle que exijam um processamento de dados pessoais só poderão ser tomadas, se existir uma obrigação jurídica ou um motivo fundamentado para tal. Mesmo existindo um motivo justificado, a proporcionalidade da medida de controle deve ser verificada. Os interesses legítimos da empresa na realização da medida de controle (por exemplo, cumprimento das disposições jurídicas e regulamentos internos da empresa) devem ser ponderados em relação a um possível interesse de proteção do colaborador afetado pela medida na exclusão da medida e só poderão ser realizados se forem adequados. O interesse legítimo da empresa e os eventuais interesses dos trabalhadores, dignos de proteção, deverão ser constatados e documentados antes de qualquer medida. Além disso, deverão ser consideradas outras exigências existentes, de acordo com o direito nacional (por exemplo, direito de voto do representante do colaborador e direitos de informação dos envolvidos).

2.6 Processamento de dados dignos de proteção especial

Dados pessoais dignos de proteção especial só deverão ser processados sob determinadas condições. Dados com proteção especial são dados relativos à raça ou etnia, a posições políticas, convicção religiosa ou filosófica, filiações de sindicatos ou à saúde ou vida sexual do envolvido. A legislação do país pode classificar outras categorias de dados como com necessidade de proteção especial ou o conteúdo das categorias de dados pode divergir. Da mesma forma, os dados relacionados a delitos só poderão ser processados sob condições especiais determinadas pela legislação do país.

O processamento deverá ser explicitamente permitido ou estipulado, por parte da legislação nacional. Um processamento também poderá ser permitido, se o mesmo for necessário, para que o departamento responsável possa atender os direitos e as obrigações no âmbito do direito trabalhista. O colaborador também pode consentir no processamento de forma expressa e voluntária.

Se for planejado o processamento de dados com proteção especial, o delegado do Grupo responsável pela proteção de dados deverá ser informado antecipadamente.

2.7 Decisões automatizadas

Se, no âmbito da relação de trabalho, dados pessoais forem processados de forma automatizada, avaliados por meio de características individuais da personalidade (por exemplo, no âmbito da seleção de pessoal ou na avaliação de perfis de capacidades), um processamento automatizado deste tipo não poderá ser a única base para decisões com consequências negativas ou grandes prejuízos para os colaboradores afetados. No sentido de evitar decisões erradas, deve estar garantido no processo automatizado que uma pessoa física possa realizar uma avaliação do conteúdo do assunto e que esta avaliação seja então a base para a decisão. Além disso, o colaborador em questão deverá ser informado dos fatos e do resultado de uma decisão individual automatizada e deverá ter a possibilidade para se manifestar.

2.8 Telecomunicação e internet

Sistemas telefônicos, endereços eletrônicos, intranet e internet e redes sociais internas são disponibilizados pela empresa em primeira instância no exercício de suas tarefas. Estes são equipamentos de trabalho e recursos empresariais. Podem ser utilizados de acordo com as disposições legais vigentes e as diretivas corporativas internas. No caso de uma utilização autorizada para fins particulares, devem ser respeitados o segredo das telecomunicações e a legislação relativa à telecomunicação nacional, contanto que estes sejam aplicáveis.

Não é realizado um controle geral da comunicação telefônica e por e-mail ou da utilização da intranet e internet. Para combater ataques à estrutura de TI ou a alguns usuários, podem ser implementadas medidas de proteção nas articulações na rede da Daimler que bloqueiem conteúdos tecnicamente danosos ou que analisem os modelos de ataques. Por razões de segurança, a utilização de sistemas telefônicos, de endereços eletrônicos, da intranet e internet e de redes sociais internas é protocolada por um período limitado. Avaliações destes dados pessoais só podem ser efetuadas mediante uma suspeita concreta fundamentada de violação da legislação ou das diretivas corporativas do Grupo Daimler. Estes controles só podem ser processados pelas áreas investigadoras e aplicando-se o princípio da proporcionalidade. As respectivas legislações nacionais também devem ser cumpridas, tal como os regulamentos corporativos existentes a este respeito.

VI. Transmissão de dados pessoais

Uma transmissão de dados pessoais para destinatários fora do Grupo Daimler ou destinatários dentro do Grupo Daimler rege-se pelas condições de admissibilidade do processamento de dados pessoais no tópico V. O destinatário dos dados deverá comprometer-se a utilizar os dados apenas para as finalidades determinadas.

Se for feita uma transmissão dos dados a um destinatário fora do Grupo Daimler que se encontre em um país terceiro[12], este terá que garantir um nível de proteção de dados semelhante ao desta diretiva de proteção de dados. Isto não aplica-se se a transmissão ocorrer devido a uma imposição legal. Uma imposição legal deste tipo pode ocorrer em virtude da legislação do país em que a sociedade do Grupo, que transmite os dados, tenha a sua sede ou a legislação do país sede da sociedade reconhece a finalidade da transmissão de dados relacionada com a imposição legal de um país terceiro.

No caso de uma transmissão de dados de terceiros às empresas do Grupo Daimler, deve estar garantido que os dados poderão ser utilizados para as finalidades previstas.

Se uma empresa do Grupo com sede no Espaço Econômico Europeu transmitir dados pessoais a uma empresa do Grupo com sede fora Espaço Econômico Europeu[13] (país terceiro), a empresa que importa os dados compromete-se a colaborar com a autoridade fiscalizadora em todas as questões relacionadas com a empresa que exporta os dados e a observar as constatações da autoridade fiscalizadora ligadas aos dados transmitidos. O mesmo aplica-se a transmissões de dados realizadas por empresas do Grupo provenientes de outros países. Se estas fizerem parte de um sistema de certificação internacional de regulamentos empresariais obrigatórios sobre a proteção de dados, elas terão que garantir a cooperação prevista lá com as respectivas entidades de inspeção e autoridades. A participação em sistemas de certificação deste tipo deve ser coordenada com o delegado do Grupo responsável pela proteção de dados.

[12] Vide XV.
[13] Vide XV.

No caso de uma violação alegada por parte de um envolvido, contra esta diretiva de proteção de dados, por uma empresa do Grupo importadora de dados, com sede em um país terceiro, a empresa do Grupo exportadora de dados com sede no Espaço Econômico Europeu, compromete-se a apoiar o envolvido cujos dados tenham sido levantados no Espaço Econômico Europeu, tanto no esclarecimento dos fatos, quanto a garantir a imposição dos seus direitos nos termos desta diretiva, perante a empresa do Grupo importadora dos dados. Além disso, o envolvido está autorizado a reivindicar os seus direitos também perante a empresa exportadora de dados do Grupo. No caso de uma violação alegada, a empresa exportadora dos dados terá que comprovar perante o envolvido que uma violação desta diretiva de proteção de dados não é imputável à empresa do Grupo, importadora dos dados em um país terceiro, aquando do processamento posterior dos dados recebidos.

No caso de uma transmissão de dados pessoais de uma empresa do Grupo com sede no Espaço Econômico Europeu a uma empresa do Grupo com sede em um país terceiro, o departamento responsável pela transmissão dos dados tem a obrigação jurídica perante o envolvido, cujos dados foram levantados no Espaço Económico Europeu, de atuar como se o departamento responsável pela transmissão de dados tivesse cometido a violação. A competência jurisdicional é o tribunal responsável na sede do responsável pela exportação dos dados.

VII. Processamento de dados por solicitação

É considerado um processamento de dados por solicitação quando um prestador de serviços fica encarregado do processamento de dados pessoais sem que lhe seja transferida a responsabilidade pelo respectivo processo de negócios. Nestes casos, deve ser celebrado um contrato sobre um processamento de dados por solicitação tanto com prestadores de serviços externos quanto entre empresas do Grupo Daimler. A empresa solicitante arca inteiramente com a responsabilidade pelo processamento correto dos dados. O prestador de serviços está autorizado a processar dados pessoais só no âmbito das instruções do solicitante. Aquando da solicitação, devem ser cumpridas as seguintes especificações; a área solicitante tem que garantir o seu cumprimento.

1. O prestador de serviços deve ser escolhido, considerando-se a sua capacitação para a garantia das medidas de proteção técnico-organizacionais necessárias.
2. A atribuição da solicitação deve ser realizada em forma de texto. Neste devem estar documentadas as instruções para o processamento de dados e as competências do solicitante e do prestador de serviços.
3. Devem ser observados os modelos contratuais disponibilizados pelo delegado responsável pela proteção de dados do Grupo.
4. Antes do início do processamento de dados, o solicitante deve se convencer do cumprimento das obrigações do prestador de serviços. Um prestador de serviços pode comprovar o cumprimento das exigências relativas à segurança de dados, sobretudo, apresentando um certificado adequado. Dependendo do risco do processamento de dados, se for o caso, deve ser repetido regularmente um controle durante o período de vigência do contrato.

5. No caso de um processamento de dados transfronteiras, devem ser cumpridas as respectivas exigências nacionais relativas ao encaminhamento de dados pessoais para o exterior. Principalmente o processamento de dados pessoais, provenientes do Espaço Económico Europeu, só pode ser realizado em um país terceiro se o prestador de serviços comprovar um nível de proteção de dados correspondente ao desta diretiva de proteção de dados. Instrumentos adequados podem ser, por exemplo:
   a. Acordo das cláusulas de contratos modelos da UE sobre o processamento de pedidos em países terceiros com o prestador de serviços e possíveis empresas subcontratadas.
   b. Participação do prestador de serviços em um sistema de certificação reconhecido pela UE para a criação de um nível de proteção de dados adequado.
   c. Reconhecimento por parte das respectivas autoridades fiscalizadoras da proteção de dados dos regulamentos empresariais obrigatórios do prestador de serviços para a criação de um nível de proteção de dados adequado.

VIII. Direitos do envolvido

Todo envolvido tem os seguintes direitos. A reivindicação destes deve ser realizada prontamente pela área responsável e não deve causar nenhum prejuízo ao envolvido.

1. O envolvido poderá exigir informação sobre quais os dados pessoais e de que origem estão guardados a seu respeito e para que finalidade. Se, de acordo com o respectivo direito trabalhista, estiverem previstos direitos mais abrangentes de conferir a documentação do empregador (por exemplo, prontuário do colaborador), estes permanecem inalterados.
2. No caso de transmissões de dados pessoais a terceiros, deverá ser prestada informação sobre a identidade do destinatário ou sobre as categorias de destinatários.
3. Se os dados pessoais estiverem incorretos ou incompletos, o envolvido tem o direito de exigir a correção ou o complemento dos mesmos.
4. O envolvido tem o direito de se opor à utilização dos seus dados pessoais para fins de propaganda ou de pesquisa de opinião e de mercado. Os dados deverão ser bloqueados para estas finalidades.
5. O envolvido tem o direito de exigir a eliminação dos seus dados, se faltar a base jurídica para o processamento dos dados ou se a mesma tiver sido suprimida. O mesmo será válido no caso de a finalidade do processamento de dados tiver sido suprimida por decurso do prazo ou por outros motivos. Devem ser respeitadas as obrigações de arquivamento existentes e os interesses dignos de proteção contrários a uma eliminação dos dados.
6. O envolvido possui o direito fundamental de protesto contra o processamento dos seus dados, que deverá ser respeitado, se o seu interesse a ser protegido se sobrepor ao interesse no processamento dos dados, devido a uma situação pessoal especial. Isto não é válido, se uma norma jurídica obrigar à execução do processamento.

Além disso, todo envolvido pode reivindicar os direitos concedidos nos tópicos III. parág. 2, IV., V., VI., IX., X, e XIV. parág. 3 na qualidade de beneficiário terceiro, caso uma empresa que se compromete com o cumprimento da diretiva de proteção de dados não tenha respeitado as suas especificações, violando os direitos do envolvido.

IX. Confidencialidade do processamento

Dados pessoais gozam da proteção do segredo de dados. É proibido aos colaboradores levantar, processar ou utilizar os dados indevidamente. Indevido é todo o processamento que um colaborador executar sem ser encarregado no âmbito do cumprimento das suas tarefas e sem estar autorizado a tal. Aplica-se o princípio need-to-know: Colaboradores só podem ter acesso a dados pessoais se e contanto que estes sejam necessários para a realização da respectiva tarefa. No âmbito dos conceitos de autorização, isso requer a divisão e separação cuidadosas das funções e responsabilidades e da respectiva aplicação e atualização.

Colaboradores não têm a permissão de utilizar dados pessoais para fins particulares ou económicos, transmiti-los a pessoas não autorizadas ou permitir-lhes o acesso de uma outra forma. Chefes têm que instruir seus colaboradores no começo da relação de trabalho sobre a obrigação de preservar o segredo de dados. Esta obrigação permanece válida também depois do encerramento da relação de trabalho.

X. Segurança do processamento

Dados pessoais devem ser protegidos constantemente contra um acesso não autorizado, um processamento ou uma divulgação indevida, bem como contra perda, falsificação ou destruição. Isto aplica-se independentemente se o processamento de dados é realizado de forma eletrônica ou em papel. Antes da introdução de novos sistemas de processamento de dados, sobretudo novos sistemas de TI, devem ser definidas e implementadas medidas técnico-organizacionais de proteção de dados pessoais. Estas medidas devem reger-se pelo avanço tecnológico, pelos riscos que um processamento comporta e pela necessidade de proteção dos dados (apurada pelo processo de classificação de informação). A área responsável deve consultar especialmente o seu delegado em assuntos de segurança (ISO) e o coordenador de proteção de dados. As medidas tecnico-organizacionais de proteção de dados pessoais fazem parte da gestão de segurança de informação do Grupo e têm que ser adaptadas continuamente aos desenvolvimentos tecnológicos e às alterações organizacionais.

XI. Controle da proteção de dados

O cumprimento das diretivas e das leis vigentes da proteção de dados é verificado, regularmente, por meio de auditorias e de outros controles. A realização cabe ao delegado do Grupo e aos coordenadores responsáveis por assuntos de proteção de dados, às outras áreas da empresa e inspetores externos munidos de direitos de auditoria. Devem ser comunicados ao delegado do Grupo os resultados dos controles de proteção de dados. No âmbito das obrigações de reportar, o conselho fiscal da Daimler AG deve ser informado sobre os resultados mais importantes. A pedido, os resultados dos controles de proteção de dados podem ser disponibilizados à respectiva autoridade fiscalizadora. No âmbito das suas atribuições legais, a autoridade fiscal competente também pode realizar controles próprios relativos ao cumprimento das disposições desta diretiva.

XII. Incidentes de segurança de dados

Todo colaborador deve comunicar imediatamente ao seu chefe, ao coordenador de assunto de proteção de dados ou ao delegado responsável pela proteção de dados casos de violações desta diretiva de proteção de dados ou de outras disposições relativas à proteção de dados pessoais (incidentes de segurança de dados[14]). O chefe, responsável pela função ou pela unidade, compromete-se a comunicar imediatamente o delegado do Grupo ou o coordenador da proteção de dados sobre incidentes de segurança de dados.

Em casos de
- transmissão indevida de dados pessoais a terceiros,
- acesso indevido de terceiros a dados pessoais, ou
- perda de dados pessoais

os comunicados previstos (Information Security Incident Management) devem ser efetuados imediatamente na empresa para que possam ser cumpridas as obrigações legais de notificação de incidentes de segurança de dados.

XIII. Responsabilidades e sanções

As presidências e diretorias das sociedades do Grupo são responsáveis pelo processamento de dados no seu âmbito de responsabilidade. Consequentemente, estes comprometem-se a garantir que as exigências legais e as contidas na diretiva de proteção de dados serão levadas em consideração (por exemplo, obrigações nacionais de notificação). Consiste em uma tarefa administrativa das diretorias executivas a garantia de um processamento de dados correto, visando a proteção de dados através de medidas organizacionais, pessoais e técnicas. Compete ao respectivo colaborador a implementação destas disposições. O delegado em assuntos de proteção de dados deve ser imediatamente informado aquando de controles da proteção de dados realizados pelas autoridades.
As respectivas presidências e as diretorias das fábricas têm que indicar um coordenador para a proteção de dados ao delegado do Grupo. Em termos organizacionais, esta tarefa também poderá ser efetuada, em acordo com o delegado do Grupo para a proteção de dados, por um coordenador para a proteção de dados de várias sociedades ou fábricas. Os coordenadores da proteção de dados são parceiros de contato no local para a proteção de dados. Eles podem efetuar controles e têm que familiarizar os colaboradores com os conteúdos da diretiva de proteção de dados. As presidências são obrigadas a apoiar, nas suas funções, os delegados do Grupo para a proteção de dados e os respectivos coordenadores.

Os técnicos responsáveis por processos de negócios e projetos são obrigados a informar a tempo os coordenadores da proteção de dados sobre novos processamentos de dados pessoais. No caso de serem necessários processamentos de dados, dos quais poderão resultar riscos para os direitos da personalidade dos envolvidos, o delegado do Grupo deverá ser incluído antes do processamento dos dados. Isto aplica-se particularmente a dados pessoais com proteção especial.
Os quadros executivos têm que garantir que os seus colaboradores sejam treinados na proporção necessária sobre a proteção de dados.
Um processamento abusivo dos dados pessoais e outras violações contra o direito da proteção de dados também são punidos legalmente em vários países e podem dar origem a ações de indenização. Infrações para as quais colaboradores são responsáveis individualmente, podem ter consequências de ordem trabalhista.

[14] Vide XV.

XIV. O delegado do Grupo responsável pela proteção dos dados

O delegado do Grupo responsável pela proteção de dados, como órgão interno instrutivo independente, atua no cumprimento das disposições nacionais e internacionais para a proteção de dados. Ele é responsável pelas diretivas de proteção de dados e fiscaliza o seu cumprimento. O delegado do Grupo para a proteção de dados é nomeado pelo conselho de administração da Daimler AG. As empresas do Grupo com nomeação obrigatória também nomeiam o delegado do Grupo como responsável legal pela proteção de dados. Exceções específicas devem ser coordenadas com o delegado do Grupo responsável pela proteção de dados.

Os coordenadores informam, em tempo hábil, o delegado do Grupo sobre os riscos da proteção de dados.

Além disso, todo envolvido poderá dirigir-se ao delegado do Grupo ou a um coordenador responsável pela proteção de dados, dando-lhes sugestões, pedindo informações ou prestando queixas referentes a questões relacionadas com a proteção e segurança de dados. Os pedidos de informação e queixas serão tratados de forma sigilosa.

Se o coordenador responsável pela proteção de dados não puder solucionar ou não puder eliminar uma violação contra esta diretiva de proteção de dados, ele terá que pedir a intervenção do delegado do Grupo. As decisões do delegado do Grupo para solucionar a violação da proteção de dados deverão ser respeitadas pelas respectivas presidências. Consultas de autoridades de fiscalização devem sempre ser levadas ao conhecimento do delegado responsável pela proteção de dados.

O delegado do Grupo e os seus colaboradores podem ser contactados do seguinte modo:
Daimler AG, Konzernbeauftragter für den Datenschutz,
HPC 0518, D-70546 Stuttgart
E-Mail: mbox_datenschutz@daimler.com
Na Intranet em http://intra.corpintra.net/cdp

XV. Definições

» Um nível de proteção de dados adequado de países terceiros será reconhecido pela Comissão UE se o elemento fundamental da privacidade, tal como é entendido nos países membros da UE estiver integralmente protegido.
Na sua decisão, a comissão da UE considera todas as circunstâncias que desempenham um papel importante na transmissão de dados ou numa categoria de transmissões de dados.
Isto engloba a avaliação da legislação do país bem como das normas profissionais e medidas de segurança vigentes.

» Dados são anonimizados quando definitivamente ninguém conseguir mais associá-los a uma pessoa ou se a associação a uma pessoa só for possível mediante um grande esforço desproporcionado de tempo, custos e mão de obra.

» Dados que gozam de proteção especial são dados relativos a origem racial e étnica, sobre opiniões políticas, convicções religiosas e filosóficas, sobre filiação em sindicatos ou sobre a saúde ou a vida sexual do envolvido.
A legislação nacional pode classificar outras categorias de dados como dignos de proteção especialou o conteúdo das categorias de dados pode ser diferente. Da mesma forma, dados relacionados com delitos só podem ser processados sob condições especiais impostas pela legislação nacional.

- Envolvido nos termos desta diretiva de proteção de dados é qualquer pessoa física cujos dados são processados. Em alguns países, os envolvidos também podem ser pessoas jurídicas.
- Incidentes de segurança de dados são todos os acontecimentos, dos quais têm-se uma suspeita justificada que os dados pessoais tenham sido espionados, levantados, alterados, copiados, transmitidos ou utilizados indevidamente. Isto pode estar relacionado tanto com ações de terceiros quanto com ações de colaboradores.
- Terceiro é todo aquele exceto o envolvido e o departamento responsável pelo processamento de dados. Na UE processadores de dados por solicitação não são considerados terceiros nos termos da legislação de proteção de dados, dado que perante a lei estes estão subordinados ao departamento responsável.
- Países terceiros nos termos desta diretiva de proteção de dados são todos os países fora da União Europeia/EEE. Exceto os países cujo nível de proteção de dados tenha sidoreconhecido pela Comissão da UE como adequado.
- Consentimento é uma declaração voluntária, de vínculo legal que autoriza um processamento de dados.
- Necessário é o processamento de dados pessoais, quando a finalidade admissível ou o interesse legítimo não pode ser atingido ou pode ser atingido com um esforço fora do normal sem os respectivos dados pessoais.
- O Espaço Econômico Europeu (EEE) é um espaço econômico associado à UE, ao qual pertencem a Noruega, Islândia e Liechtenstein.
- Dados pessoais são todas as informações sobre uma determinada pessoa física ou uma pessoa física determinável.
  Determinável é uma pessoa, por exemplo, quando através de uma combinação de informações, mesmo com conhecimentos adicionais casuais for possível associar à pessoa.
- Transmissão é toda divulgação de dados protegidos a terceiros por parte de um departamento responsável.
- Processamento de dados pessoais é considerado todo procedimento executado com ou sem ajuda de processos automatizados e que serve para o levantamento, armazenagem, organização, arquivamento, alteração, consulta, utilização, encaminhamento, transmissão, divulgação ou combinação e comparação de dados.
  Também estão abrangidos a destruição, eliminação e bloqueio de dados e de suportes de dados
- Departamento responsável é a sociedade juridicamente autônoma do Grupo Daimler, cuja atividade de negócio solicita a medida de processamento.

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