DHL GROUP

POLÍTICA DE PRIVACIDADE DE DADOS

Global Data Protection
Version: 2.2 July 2023

PÚBLICO

Sumário

PREAMBULO

1. O uso de tecnologias modernas de informação e comunicação e a rede global de fluxos de informação são fundamentais para os processos de negócios do Grupo DHL. Em particular, as estruturas organizacionais complexas e o desafio de poder executar as aplicações necessárias 24 horas por dia requerem uma infraestrutura de TI internacional em que os dados pessoais são processados em todo o Grupo DHL. Com isso em mente, a proteção dos dados pessoais de clientes, funcionários, acionistas e parceiros de negócios é uma preocupação global essencial de todas as empresas dentro do Grupo DHL.

2. O objetivo da Política de Privacidade de Dados do Grupo DHL é estabelecer um padrão global, adequado e padronizado de proteção e segurança de dados para todo o Grupo DHL. Em particular, o objetivo é garantir a adesão aos requisitos legais para o tráfego de dados transfronteiriços, bem como garantir proteção adequada para os titulares dos dados no processamento interno e interempresarial de dados pessoais. A Política de Privacidade de Dados do Grupo DHL, portanto, contribui e faz parte das medidas de responsabilidade pela proteção de dados tomadas pelo Grupo DHL.

3. As empresas do Grupo DHL estão cientes que, na visão de seus clientes, são vistas como uma única unidade em diversas áreas e, portanto, comprometem-se em compartilhar a responsabilidade pela implementação da Política de Privacidade do Grupo DHL manuseando os dados pessoais de modo confiável e seguro a fim de contribuir com o sucesso comercial do Grupo.

I. ESCOPO

1. Área de aplicação

(1) A Política de Privacidade de Dados do Grupo DHL aplica-se ao processamento de dados pessoais de pessoas físicas, em particular os dados de clientes, colaboradores, acionistas e parceiros de negócio com o objetivo de criar um nível adequado de proteção para transferência de dados pessoais das empresas do Grupo localizados na União Européia para empresas do Grupo localizados em países sem um nível adequado de proteção. A natureza dos dados processados, bem como os propósitos de processamento, depende do relacionamento que um titular de dados individual pode ter com uma ou mais empresas do Grupo DHL. A informação em questão está principalmente conectada, por exemplo, ao gerenciamento de relações de trabalho, cobrindo uma ampla gama de possíveis aspectos, desde o início do trabalho até possíveis oportunidades de carreira e desenvolvimento, bem como gestão de relacionamento com o cliente, que pode incluir uma variação de serviços ao cliente[1].

(2) A Política de Privacidade de Dados do Grupo DHL não se aplica a transferências de dados cobertas pelas derrogações previstas no Artigo 49 sec. 1º do Regulamento Geral de Proteção de Dados (GDPR), por exemplo, quando um titular de dados deu se consentimento ou quando a transferência é necessária para execução de um contrato. Além disso, a Política de Privacidade de Dados do Grupo DHL não se aplica a análises estatísticas ou estudos realizados com base em dados anonimizados ou pseudonimizados e que não permitam conclusões sobre os titulares de dados.

2. Efeito vinculativo legal

(1) A Política de Privacidade de Dados do Grupo DHL dentro do Grupo DHL entrou em vigor após a autorização do Conselho de Administração do Grupo e após a publicação.

(2) A Política de Privacidade de Dados do Grupo DHL torna-se vinculativa para as empresas individuais do Grupo assim que a administração das empresas em questão se compromete a cumprir as regulamentações em uma Declaração de Adesão.

(3) O efeito vinculativo terminará com a revogação da Política de Privacidade de Dados do Grupo DHL ou se a empresa respectiva se retirar do Grupo. Em relação aos dados transferidos até este momento, as empresas do Grupo em questão estão sujeitas à obrigação de observar as disposições, contidas na Política de Privacidade de Dados do Grupo DHL, sobre o manuseio de dados pessoais. Quaisquer transferências de dados futuras e/ou para empresas do Grupo só

[1] O Grupo DHL é construído sobre dois pilares sólidos: um negócio de logística internacional integrado e um sólido negócio de correio. O Grupo DHL, composto por 870 empresas do Grupo e uma força de trabalho de cerca de 500.000 em mais de 220 países e territórios, fornece serviços de transporte para cartas, encomendas, mercadorias e informações. As atividades de negócios que podem ter impacto na natureza e no propósito das transferências de dados são descritas em detalhes no relatório anual. A empresa matriz do Grupo é a Deutsche Post AG, que, juntamente com a sede, está localizada em Bonn (Alemanha).

podem ocorrer se outras salvaguardas adequadas, conforme estipulado pelo Artigo 46 do GDPR, forem apresentadas.

3. Relação com regulamentos legais

(1) Os princípios da Política de Privacidade de Dados do Grupo DHL não substituem a legitimação necessária, sob a lei caso aplicável, para o processamento de dados pessoais, mas garantem a conformidade com requisitos específicos sob a GDPR no contexto de transferência de dados transfronteiriças para países terceiros. Dessa forma, qualquer regulação nacional (que seja mais rigorosa) prevalece sobre os requisitos estipulados nessa Política de Privacidade de Dados.

(2) Dentro da área de aplicação da GDPR, a permissibilidade do processamento de dados pode ainda ser regida pelas respectivas leis nacionais onde permitido pela GDPR. Isso pode ser aplicável também às transferências de dados transfronteiriças realizadas dentro dessa área. Quando os dados são processados entre fronteiras em nome do controlador, as leis aplicáveis ao local do controlador deverão ser autoritativas ao processador.

(3) A admissibilidade do processamento de dados em relação à transferência de dados à países terceiros e todas as transferências de dados transfronteiriças devem ser regidas pelas leis do país onde o exportador dos dados tem sua sede registrada.

(4) A admissibilidade do processamento e transferência de dados pessoais que não foram processados dentro do escopo da GDPR deve ser regida pelas leis do país relevante ao processamento.

(5) Cada empresa do Grupo é responsável por verificar a admissibilidade do processamento de dados, incluindo quaisquer requisitos existentes para notificar as autoridades supervisoras nacionais ou escritórios de inspeção, de acordo com as leis nacionais e locais relevantes. Em caso de dúvida, o Oficial de Proteção de Dados (DPO) relevante ou o Consultor de Proteção de Dados pode ser consultado para aconselhamento.

(6) As obrigações e regulamentos aplicáveis às empresas individuais do Grupo que se relacionam ao processamento e uso de dados pessoais, que vão além dos seguintes princípios e contêm requisitos adicionais para o processamento e uso de dados pessoais, não serão afetados pela Política de Privacidade de Dados do Grupo DHL. No entanto, as empresas concordam que as leis aplicáveis às empresas individuais não os impedirão de cumprir suas obrigações conforme estipulado na Política de Privacidade de Dados do Grupo DHL.

7) A coleta de dados pessoais e/ou sua transferência para escritórios estaduais só ocorrerá de acordo com as regulamentações nacionais relevantes.

(8) A Política de Privacidade de Dados do Grupo DHL está sujeita à lei alemã em todos os outros aspectos.

II. PRINCÍPIOS

1. Transparência de processamento de dados

(1) Titulares de dados devem ser adequadamente informados de como seus dados são utilizados. Isso inclui a publicação da Política de Privacidade de Dados no Smart Connect bem como o sumário da política no website corporativo externo.

(2) O dever de informar contém os seguintes detalhes:

- O nome da entidade legal (empresa do Grupo) responsável pelo processamento dos dados e suas informações de contato (controlador).
- As informações de contato do oficial de proteção de dados, onde aplicável.
- O propósito e escopo do processamento dos dados.
- As bases legais para o processamento de dados.
- Os legítimos interesses, quando aplicável.
- Os destinatários ou categorias de destinatários dos dados pessoais.
- Quando aplicável, o fato de que o controlador pretende transferir dados pessoais para um país terceiro ou organização internacional e a existência ou ausência de uma decisão de adequação pela Comissão, referência às salvaguardas apropriadas ou adequadas e os meios para obter uma cópia delas ou onde elas foram disponibilizadas.
- O período na qual esses dados serão armazenados, caso isso não seja possível, o critério usado para determinar esse período.
- A existência do direito de solicitar ao controlador acesso e retificação ou eliminação de dados pessoais, restrição de processamento referente ao titular dos dados ou de se opor ao processamento, bem como o direito à portabilidade dos dados.
- A existência de um direito de objeção onde o processamento de dados é baseado em legítimo interesse.
- Quando o processamento é baseado no consentimento, a existência do direito de retirar o consentimento a qualquer momento, sem afetar a legalidade do processamento baseado no consentimento antes de sua retirada.
- O direito de apresentar uma reclamação a uma autoridade supervisora.
- Se a provisão de dados pessoais é um requisito estatutário ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular dos dados é obrigado a fornecer os dados pessoais e as possíveis consequências de não fornecer tais dados.

- A existência de tomada de decisão automatizada, incluindo a criação de perfis e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como a importância e as consequências previstas desse processamento para o titular dos dados.

- Quando os dados pessoais não foram obtidos do titular dos dados, as categorias de dados pessoais em questão e de qual fonte os dados pessoais se originam, e se aplicável, se vieram de fontes publicamente acessíveis.

- Quando se pretende processar os dados pessoais para um propósito diferente daquele para o qual os dados pessoais foram coletados, o titular dos dados deve ser informado antes desse processamento adicional sobre esse outro propósito.

- Direitos do titular dos dados (veja a seção 5).

(3) A informação pode ser omitida se:

- O titular dos dados já foi informado.

- Onde os dados pessoais não tenham sido obtidos do titular dos dados, a disponibilização de tais informações se mostra impossível ou implicaria em uma despesa desproporcional,

- A obtenção ou divulgação é expressamente estabelecida por lei da União ou do Estado-Membro a que o controlador está sujeito e que prevê medidas adequadas para proteger os interesses legítimos do titular dos dados, ou

- Os dados pessoais devem permanecer confidenciais sujeitos a uma obrigação de sigilo profissional regulada por lei da União ou do Estado-Membro, incluindo uma obrigação estatutária de sigilo.

(4) As informações devem estar disponíveis para o titular dos dados na primeira vez que os dados são coletados. Quando os dados pessoais não foram obtidos do titular dos dados, as informações devem ser fornecidas no prazo máximo de um mês após a obtenção dos dados pessoais, levando em consideração as circunstâncias específicas. Se os dados pessoais forem usados para comunicação com o titular dos dados, o controlador deverá fornecer as informações no momento da primeira comunicação com esse titular dos dados e se for prevista uma divulgação para outro destinatário, o controlador deverá fornecer as informações no momento em que os dados pessoais forem divulgados pela primeira vez.

2. Requisitos gerais de admissibilidade para o tratamento de dados pessoais

2.1. Princípios

Os dados pessoais devem ser processados de forma legal e justa, com base em permissão ou consentimento legal. Os dados devem ser factualmente corretos e – se aplicável – atualizados. Devem ser tomadas medidas adequadas para garantir que os dados irrelevantes ou incompletos sejam retificados ou eliminados. Os dados deverão ser apagados assim que não forem mais necessários à finalidade – para a qual foram originalmente coletados e armazenados – observadas as obrigações legais de armazenamento.

2.2. Minimização de dados / Evitar o uso de dados

O processamento de dados deve seguir o objetivo de processar apenas os dados pessoais necessários. Levando em conta o propósito pretendido para o uso de dados pessoais, os dados devem ser apropriados e relevantes e não devem ultrapassar o escopo necessário (minimização de dados). Os dados pessoais só podem ser processados dentro de uma aplicação específica se isso for necessário (evitar o uso de dados).

2.3. Anonimização / Pseudonimização

Quando possível e financeiramente viável, devem ser utilizados métodos de anonimização ou pseudonimização. Ambos os métodos devem ser realizados de tal forma que a identidade real do titular dos dados não possa ser reidentificada ou só possa ser reidentificada novamente com um esforço desproporcional.

2.4. Limitação de Propósito

Os dados pessoais só podem ser coletados e processados para fins específicos, explícitos e legítimos. Eles só podem ser usados para o propósito para o qual foram originalmente coletados. Mudanças no propósito só são admissíveis com o consentimento do titular dos dados se permitido pela lei nacional do exportador de dados ou onde o processamento para outro propósito é compatível com o propósito para o qual os dados pessoais foram inicialmente coletados.

2.5. Consentimento

(1) O consentimento do titular dos dados deve ser obtido no máximo até a data em que o processamento dos dados pessoais começa.

(2) O consentimento deve ser dado livremente, especificamente e com base informada como uma indicação inequívoca, que mostra claramente a extensão do consentimento e as possíveis consequências de reter o consentimento ao titular dos dados. A formulação da declaração de consentimento deve ser suficientemente clara e informar o titular dos dados sobre seu direito de revogar seu consentimento a qualquer momento no futuro.

(3) O consentimento deve ser obtido de uma maneira adequada às circunstâncias (por escrito ou eletronicamente, de forma verificável). Em exceções, pode ser dado verbalmente se o fato do consentimento e as circunstâncias particulares que permitem o consentimento verbal forem documentados suficientemente. Se o consentimento for dado por escrito junto com outras declarações, ele deve ser claramente destacado.

2.6. Proibição de Vinculação

O uso de serviços ou o recebimento de produtos e/ou serviços não deve ser feito dependente do titular dos dados dar o seu consentimento para o uso de seus dados para fins que não sejam o estabelecimento e a execução do contrato. Isso só se aplica se o uso de serviços comparáveis ou a aquisição ou uso de produtos comparáveis não for razoavelmente possível ou não for possível de todo para o titular dos dados.

2.7. Tratamento de dados em nome de um controlador

(1) Se uma empresa do Grupo processa dados pessoais em nome de outra empresa do Grupo, as obrigações do contratante, como um processador de dados comissionado, devem ser referidas no contrato entre o controlador e o processador atendendo aos requisitos do Artigo 28 do GDPR, além dos serviços a serem fornecidos por escrito ou em outra forma equivalente (Acordo Controlador-Processador). Em particular, o controlador deve obrigar o processador a processar os dados pessoais exclusivamente de acordo com suas instruções e a tomar as medidas técnicas e organizacionais necessárias para proteger os dados.

(2) Sem a autorização prévia do controlador, o processador não pode usar os dados pessoais, que foram passados para ele, para seus próprios fins ou de terceiros. As regulamentações acima devem ser acordadas pelo menos na mesma extensão com qualquer sub-processador contratado pelo processador. O processador e qualquer sub-processador devem ser selecionados de acordo com sua capacidade de atender aos requisitos acima.

(3) Se acordos forem concluídos com processadores e/ou sub-processadores em países sem um padrão adequado de proteção de dados e que não estejam sob o escopo desta Política de Privacidade de Dados da DPDHL, devem ser obtidas garantias adequadas conforme estipulado pelo Artigo 46 do GDPR em relação à privacidade e aos direitos e liberdades fundamentais dos indivíduos e no que diz respeito ao exercício dos direitos correspondentes.

2.8. Transferência adicional à terceiros

(1) Quando o importador de dados transfere dados pessoais para outras partes que têm sua sede em outro país ou se envolve na transferência transfronteiriça de dados pessoais, o importador de dados deve garantir que esses dados sejam processados de forma legal. Assim, antes da transferência adicional, devem ser acordadas com o destinatário medidas adequadas de proteção e segurança de dados que proporcionem salvaguardas adequadas conforme estipulado pelo Artigo 46 do GDPR. Essas medidas também se aplicarão no caso de qualquer transferência posterior adicional.

(2) Se dados pessoais que foram processados no âmbito do GDPR forem transferidos para entidades legais que não estão sujeitas à Política de Privacidade de Dados do Grupo DHL ou para terceiros em terceiros países (transferência posterior para não-signatários) sem um nível adequado de proteção, devem ser deduzidas salvaguardas adequadas conforme estipulado pelo Artigo 46 do GDPR. Independentemente do acima exposto, os dados pessoais só podem ser transferidos no âmbito do GDPR ou no âmbito das regulamentações nacionais aprovadas com base no GDPR.

(3) A disposição acima não se aplicará se houver regulamentações nacionais, particularmente por razões de segurança nacional, defesa, segurança pública ou prevenção, constatação e repressão de atos criminosos, que expressamente preveem a transferência de dados pessoais por essas razões.

2.9. Responsabilidade

(1) Cada entidade do Grupo DPDHL deve garantir e ser capaz de demonstrar conformidade com os requisitos aplicáveis sob esta Política.

(2) Em particular e quando aplicável, o controlador deve implementar medidas técnicas e organizacionais adequadas, que são projetadas para implementar princípios de proteção de dados, de maneira eficaz e para integrar as salvaguardas necessárias no processamento, a fim de cumprir os requisitos do GDPR e proteger os direitos dos titulares dos dados (Princípio da proteção de dados por design).

(3) Quando aplicável, o controlador deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica do processamento sejam processados (Princípio da proteção de dados por padrão).

3. Casos especiais de tratamento de dados

3.1. Categorias especiais de dados pessoais

(1) O processamento de categorias especiais de dados pessoais é proibido, a menos que o processamento desses dados seja necessário e o titular dos dados consinta explicitamente com isso. Além disso, dados pessoais especiais só podem ser processados dentro do âmbito das exceções especificadas no GDPR ou dentro do âmbito das regulamentações de exceção nacionais aprovadas com base no GDPR.

(2) Antes de tal processamento começar, o Oficial de Proteção de Dados (Data Protection Officer/Coordenador de Proteção de Dados) da empresa em questão deve ser envolvido de acordo com as regulamentações internas da empresa.

3.2. Decisões automatizadas em casos individuais

(1) Decisões que avaliam os aspectos individuais de uma pessoa, e que podem acarretar consequências legais para, ou afetar consideravelmente o titular dos dados, não podem ser baseadas unicamente no processamento automatizado, a menos que isso seja necessário para a celebração ou execução de um contrato entre o titular dos dados e um controlador de dados, seja autorizado pela União ou pelo Estado-Membro ou seja baseado no consentimento explícito do titular dos dados.

(2) Se, em casos individuais, for justificado fazer decisões automatizadas posteriormente, o titular dos dados deve ser informado sobre o resultado da decisão automatizada e deve ser permitido comentar sobre isso dentro de um período adequado. Seus comentários devem ser levados em conta de maneira apropriada antes que uma decisão final seja tomada.

(3) No caso de decisões automatizadas baseadas em categorias especiais de dados pessoais, estas são permitidas apenas se baseadas no consentimento do titular dos dados ou com base na lei da União ou do Estado-Membro.

3.3. Marketing Direto

É geralmente permitido processar dados pessoais para fins de marketing direto / pesquisa de mercado ou de opinião, a menos que a lei nacional ou acordos específicos sobre sigilo / confidencialidade estipulem regulamentos mais rigorosos (por exemplo, necessidade de consentimento). O titular dos dados tem o direito de se opor ao processamento de seus dados para este fim e deve ser informado separadamente sobre isso conforme a seção 1. Se o titular dos dados se opuser, os dados devem ser restringidos e não devem ser processados para este propósito.

4. Qualidade dos dados/segurança dos dados

4.1. Confidencialidade do processamento de dados

Apenas funcionários autorizados especialmente comprometidos com a observância da proteção de dados podem processar dados pessoais. É proibido para um funcionário processar esses dados pessoais para seus próprios fins (privados), transferi-los para partes não autorizadas ou torná-los acessíveis a eles de qualquer outra maneira. Neste contexto, "não autorizado" pode incluir colegas ou funcionários se eles não precisarem dos dados para seu campo de trabalho ou tarefas especializadas.

4.2. Princípios de segurança de dados (medidas técnicas e organizacionais)

(1) Se dados pessoais forem processados, levando em consideração os riscos apresentados pelo processamento, devem ser tomadas medidas técnicas e organizacionais adequadas para proteger os processos da empresa e os sistemas de TI, a fim de proteger os dados pessoais contra destruição acidental ou ilegal, perda, alteração, divulgação não autorizada de, ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados.

(2) Essas medidas incluem:

- Negar a entrada de pessoas não autorizadas em instalações de processamento de dados onde dados pessoais são processados ou utilizados (controle de entrada),

- Impedir que pessoas não autorizadas possam usar sistemas de processamento de dados (controle de uso),

- Garantir que os usuários autorizados de um sistema de processamento de dados só possam acessar dados dentro do escopo de seus direitos de acesso, e que dados pessoais não possam ser lidos, copiados, alterados ou removidos sem autorização, seja durante o processamento ou uso ou quando armazenados (controle de acesso),

- Garantir que dados pessoais não possam ser lidos, copiados, alterados ou removidos sem autorização durante a transferência eletrônica de dados ou no processo de transmissão ou armazenamento em mídias de dados, e que seja possível revisar e estabelecer onde a transmissão de dados pessoais é suportada por instalações de transferência de dados (controle de transferência),

- Garantir que pode ser revisado e estabelecido retrospectivamente se, e por quem, dados pessoais foram inseridos, alterados ou removidos de sistemas de processamento de dados (controle de entrada),

- Garantir que os dados pessoais processados em nome do controlador só possam ser processados de acordo com as instruções do controlador (controle de trabalho),

- Garantir que os dados pessoais estão protegidos contra destruição acidental ou perda (controle de disponibilidade),

- Garantir que os itens de dados coletados para diferentes propósitos sejam processados separadamente (exigência de separação).

- Fornecer a possibilidade de pseudonimização e criptografia de dados pessoais.

- Fornecer a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de processamento, incluindo a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais.

- Fornecer um processo para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento

4.3. Arquivamento de dados

Ao arquivar dados, os princípios do processamento de dados, especialmente no que se refere à minimização de dados e à evitação de dados, devem ser respeitados. O arquivamento de dados pessoais sem o consentimento expresso do titular dos dados é proibido, a menos que seja necessário devido a necessidades operacionais com base em motivos legais. A Seção 2.1 se aplica com relação à obrigação de exclusão.

5. Direitos do titular de dados

5.1. Obrigações Gerais

(1) O controlador deve tomar medidas apropriadas para fornecer informações e comunicação relacionadas ao processamento ao titular dos dados de forma concisa, transparente, compreensível e facilmente acessível. As informações devem ser fornecidas por escrito, ou por outros meios, conforme apropriado.

(2) O controlador deve fornecer informações ou ação tomada em um pedido sob a seção 5.2 ao titular dos dados sem demora indevida e em qualquer caso dentro de um mês após o recebimento do pedido. Quando necessário e com informações do titular dos dados, esse período pode ser prorrogado por mais dois meses

5.2. Direito de acesso

(1) Cada titular dos dados pode exigir confirmação de que os dados pessoais que lhe dizem respeito estão sendo processados e, nesse caso, acesso a esses dados e informações (incluindo informações escritas) sobre os dados armazenados sobre ele/ela, incluindo sua origem, o propósito do armazenamento dos dados, os destinatários aos quais foi divulgado e, quando possível, o período previsto para o qual os dados serão armazenados ou os critérios para determinar esse período. Além disso, o titular dos dados terá acesso a informações sobre se existe tomada de decisão automatizada, incluindo criação de perfis, se for o caso, sobre a lógica

envolvida e o significado e as consequências previstas de tal processamento. O titular dos dados também terá o direito de ser informado sobre salvaguardas apropriadas relacionadas à transferência de dados pessoais para um terceiro país, quando aplicável.

(2) O controlador deve fornecer uma cópia dos dados pessoais em processamento. Para quaisquer cópias adicionais solicitadas pelo titular dos dados, o controlador pode impor uma taxa razoável para a emissão de tais informações com base em custos administrativos.

5.3. Correção, restrição, exclusão, direito de ser esquecido e portabilidade de dados

(1) O titular dos dados tem o direito de exigir a correção se os dados armazenados sobre ele/ela estiverem incompletos e/ou incorretos.

(2) O titular dos dados terá o direito de obter do controlador a restrição de processamento sob as razões do Artigo 18 (1) GDPR quando a precisão dos dados for contestada, o titular dos dados solicitar a restrição de dados não mais necessários pelo controlador ou quando o processamento for ilegal ou quando o titular dos dados tiver se oposto ao processamento de acordo com a seção 5.4.

(3) Além disso, ele/ela tem o direito de exigir a exclusão de seus dados se o processamento de dados foi inadmissível ou os dados não são mais necessários para processamento de dados ou se qualquer outro motivo mencionado no Artigo 17 (1) GDPR for aplicável. Quando o controlador tornou os dados pessoais públicos, o controlador, levando em consideração a tecnologia disponível e os custos de implementação, deve tomar medidas razoáveis para informar os controladores que estão processando os dados pessoais que o titular dos dados solicitou a exclusão de tais controladores de quaisquer links para, ou cópia ou replicação de, esses dados pessoais (direito de ser esquecido). As obrigações acima não se aplicam quando o processamento é necessário para cumprir obrigações legais por lei da União ou do Estado membro que exige processamento

(4) O titular dos dados terá o direito de receber os dados pessoais que lhe dizem respeito, que ele/ela forneceu a um controlador nas condições do Artigo 20 da GDPR em um formato estruturado, comumente usado e legível por máquina (portabilidade de dados).

5.4. Oposição

(1) O titular dos dados pode se opor à empresa responsável por usar seus dados por motivos relacionados à sua situação particular a qualquer momento para processar dados pessoais que lhe dizem respeito, que se baseiam no interesse público, interesse de autoridade oficial investida no controlador ou com base em interesses legítimos perseguidos pelo controlador ou por um terceiro. A menos que o controlador demonstre motivos legítimos convincentes para o processamento que superam os interesses do titular dos dados ou para o estabelecimento, exercício ou defesa de reivindicações legais, o controlador não processará mais os dados.

(2) Quando os dados pessoais são processados para fins de marketing direto, o titular dos dados terá o direito de se opor a qualquer momento ao processamento, que inclui a criação de

perfis na medida em que está relacionado a tal marketing direto. No caso de oposição pelo titular dos dados, os dados pessoais não serão mais processados para fins de marketing direto.

5.5. Proibição de discriminação

Os titulares dos dados não devem ser discriminados de forma alguma se exercerem seus direitos.

5.6. Afirmação

(1) O titular dos dados pode a qualquer momento entrar em contato com o Oficial de Proteção de Dados da empresa responsável e/ou a empresa com perguntas e/ou reclamações sobre o uso de seus dados pessoais ou com perguntas sobre a Política de Privacidade de Dados do Grupo DHL.

(2) Neste contexto, “responsável” denota todas as empresas com as quais o titular dos dados tem uma relação contratual ou nas quais seus dados pessoais são processados. A circunstância deve ser esclarecida em cooperação com as empresas ou divisões envolvidas sem demora culposa. O Oficial de Proteção de Dados da empresa abordada coordenará toda a correspondência relevante com o titular dos dados.

(3) Não obstante o acima exposto, o titular dos dados também tem o direito de apresentar uma reclamação a uma autoridade supervisora e/ou tomar medidas legais.

5.7. Cópia da Política de Privacidade de Dados do Grupo DHL

O Encarregado de Proteção de Dados Corporativos disponibilizará, mediante solicitação, uma cópia da Política de Privacidade de Dados do Grupo DHL.

III. GESTÃO DE PROTEÇÃO DE DADOS

1. Encarregado Corporativo de Proteção de Dados

(1) O Encarregado Corporativo de Proteção de Dados coordena a cooperação e o acordo sobre todas as questões relativas à Política de Privacidade de Dados do Grupo DHL. Em particular, o Encarregado Corporativo de Proteção de Dados é um representante para partes externas e autoridades nacionais/internacionais de supervisão de proteção de dados em todas as questões relativas ao conteúdo da Política de Privacidade de Dados do Grupo DHL. A independência e a liberdade para dar instruções dos Oficiais de Proteção de Dados nomeados com base nas regulamentações nacionais relevantes permanecerão inalteradas por isso.

(2) O Encarregado Corporativo de Proteção de Dados monitora a implementação da Política de Privacidade de Dados do Grupo DHL com base em auditorias, bem como outros instrumentos apropriados, e reporta à Diretoria do Grupo. A pedido, o Encarregado Corporativo de Proteção de Dados fornecerá à Autoridade de Proteção de Dados o relatório de auditoria relevante. Uma Autoridade de Proteção de Dados relevante pode pedir ao Encarregado Corporativo de Proteção de Dados para conduzir ou deixar realizar - de acordo com as regulamentações aplicáveis - uma auditoria em uma empresa do Grupo para verificar a conformidade com a Política de Privacidade de Dados do Grupo DHL. A empresa do grupo em questão deve aceitar tal auditoria e ajustar aspectos identificados de melhorias.

(3) As empresas do Grupo são obrigadas a informar o Encarregado Corporativo de Proteção de Dados se e quando aderem ou se retiram da Política de Privacidade de Dados do Grupo DHL. Anualmente, e a pedido, o Encarregado Corporativo de Proteção de Dados fornecerá à Autoridade de Proteção de Dados a lista de empresas do Grupo que aderiram.

(4) O Encarregado Corporativo de Proteção de Dados também é responsável por atualizar a Política de Privacidade de Dados do Grupo DHL. No caso de quaisquer alterações, ele/ela deve informar as Empresas do Grupo das alterações por meio do Oficial de Proteção de Dados em questão e deve obter o consentimento das Empresas do Grupo para emendas que não sejam obrigatórias por lei ou que não sejam puramente de natureza editorial. O Encarregado Corporativo de Proteção de Dados notificará emendas significativas à Autoridade Líder de Proteção de Dados, que é o Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Comissário Federal para a Proteção de Dados e Liberdade de Informação da Alemanha).

2. Comitê Diretor de Proteção de Dados/Privacidade

Para implementar a Política de Privacidade de Dados do Grupo DHL e para alcançar a integração contínua de Proteção de Dados/Privacidade nos processos de negócios, foi estabelecido um Comitê Diretor de Proteção de Dados composto por representantes das divisões de negócios. Em particular, o Comitê Diretor de Proteção de Dados apoiará o Encarregado Corporativo de Proteção de Dados para estabelecer e manter um Gerenciamento de Proteção de Dados em todo o grupo.

3. Oficiais de Proteção de Dados e Consultores de Proteção de Dados

(1) Para cada empresa do Grupo, deve ser nomeado um Oficial de Proteção de Dados independente (Encarregado de Proteção de Dados / Coordenador de Proteção de Dados). O Oficial de Proteção de Dados é responsável pela implementação de normas e regulamentos.

(2) Para garantir a conformidade com a Política de Privacidade de Dados do Grupo DHL, os Oficiais de Proteção de Dados devem, em particular, ser envolvidos em um estágio inicial no desenvolvimento e design de novos e alterados processos operacionais, produtos/serviços e medidas de marketing. Para permitir que estas tarefas sejam realizadas, as empresas do Grupo devem informar o Oficial de Proteção de Dados relevante sobre quaisquer desenvolvimentos relevantes.

(3) Consultores de Proteção de Dados com experiência jurídica apoiarão os Oficiais de Proteção de Dados no cumprimento de suas tarefas. Em particular, no que diz respeito a questões regulatórias, os Oficiais de Proteção de Dados devem buscar o conselho dos Consultores de Proteção de Dados.

(4) Se não houver restrições legais, o Oficial de Proteção de Dados responsável deve estar autorizado a auditar todos os métodos de processamento localmente que envolvam o uso de dados pessoais. Para este fim, eles podem - na medida em que existam - usar quaisquer métodos em todo o Grupo, por exemplo, auditorias conjuntas de proteção de dados. Um programa de auditoria especial referente à Política de Privacidade de Dados do Grupo DHL será desenvolvido e deve ser conduzido pelas empresas do Grupo relevantes. A pedido, o Oficial de Proteção de Dados deve fornecer ao Encarregado Corporativo de Proteção de Dados um relatório de auditoria.

(5) Os funcionários das empresas do Grupo devem ser adequadamente treinados sobre as regulamentações de proteção de dados e a aplicação da Política de Privacidade de Dados do Grupo DHL.

4. Conformidade

(1) As empresas do Grupo devem garantir que as disposições nacionais de proteção de dados aplicáveis e a Política de Privacidade de Dados do Grupo DHL sejam cumpridas.

(2) O Oficial de Proteção de Dados da empresa em questão deve ser informado de violações (ou suspeita de violações) das disposições de proteção de dados e da Política de Privacidade de Dados do Grupo DHL sem demora.

(3) Em incidentes que são relevantes para mais de uma empresa do Grupo, o Oficial de Proteção de Dados também deve informar o Encarregado Corporativo de Proteção de Dados e o Consultor de Proteção de Dados competente. Eles também devem informar o Encarregado Corporativo de Proteção de Dados se as leis aplicáveis a uma empresa do Grupo mudarem substancialmente de uma maneira desvantajosa e como isso afeta a proteção de dados ou a adesão à Política de Privacidade de Dados do Grupo DHL.

(4) Os Oficiais e Consultores de Proteção de Dados concordarão mutuamente com suas atividades sob a Política de Privacidade de Dados do Grupo DHL, darão apoio uns aos outros e usarão sinergias. Juntos, eles fazem parte da Rede de Proteção de Dados do Grupo DHL.

5. Cooperação com autoridades de supervisão

(1) As empresas do Grupo devem garantir que respondem aos pedidos de uma Autoridade de Proteção de Dados dentro de um prazo razoável e em uma extensão razoável. De acordo com a legislação nacional aplicável, eles devem cumprir o conselho de uma Autoridade de Proteção de Dados.

(2) O Consultor de Proteção de Dados competente deve ser envolvido no tratamento desses pedidos.

IV. RESPONSABILIDADE

1. Transferência de dados para um controlador

(1) O exportador de dados e o importador de dados serão cada um individualmente responsáveis perante os titulares de dados por danos materiais e não materiais que causem por qualquer violação dos direitos de terceiros sob a Política de Privacidade de Dados do Grupo DHL. A responsabilidade do exportador de dados sob a lei nacional de proteção de dados aplicável permanece inalterada.

(2) O exportador de dados e o importador de dados serão responsáveis um perante o outro por danos que causem por qualquer violação da Política de Privacidade de Dados do Grupo DHL. A responsabilidade entre o exportador de dados e o importador de dados é limitada ao dano real sofrido. Para evitar dúvidas, as partes concordam que podem ser isentas desta responsabilidade se provarem que nenhuma delas é responsável pela violação dessas disposições.

(3) Danos punitivos são especificamente excluídos.

(4) O exportador de dados e o importador de dados autorizam os titulares de dados a fazer cumprir as cláusulas estipuladas na seção 3 contra o importador de dados ou o exportador de dados como um beneficiário terceiro, por qualquer de suas respectivas violações de suas obrigações contratuais, no que diz respeito aos seus dados pessoais. A jurisdição para este fim é no país de estabelecimento do exportador de dados ou jurisdição de residência habitual do titular dos dados.

(5) Em casos envolvendo alegações de violação pelo importador de dados, o titular dos dados deve primeiro solicitar ao exportador de dados que tome medidas adequadas para fazer cumprir seus direitos contra o importador de dados; se o exportador de dados não tomar tais medidas dentro de um período razoável (que em circunstâncias normais seria de um mês), o titular dos dados pode então fazer cumprir seus direitos contra o importador de dados diretamente.

(6) Um titular de dados tem o direito de proceder diretamente contra um exportador de dados que não tenha feito esforços razoáveis para determinar que o importador de dados é capaz de cumprir suas obrigações legais sob a Política de Privacidade de Dados do Grupo DHL (o exportador de dados terá o ônus de provar que fez esforços razoáveis).

2. Transferência de dados para um processador e/ou sub-processador

(1) Qualquer titular de dados, que tenha sofrido danos como resultado de qualquer violação das obrigações referidas na seção 3 pelo exportador de dados, o importador de dados ou o sub-processador, tem direito a receber do exportador de dados a compensação pelos danos sofridos.

(2) Se um titular de dados não puder apresentar uma reivindicação de compensação de acordo com o parágrafo 1 contra o exportador de dados, decorrente de uma violação pelo importador de dados ou seu sub-processador de qualquer uma de suas obrigações referidas na seção 3, porque o exportador de dados desapareceu de fato ou deixou de existir em termos legais ou tornou-se insolvente, o importador de dados autoriza o titular de dados a apresentar uma reivindicação contra ele como se fosse o exportador de dados, a menos que qualquer entidade sucessora tenha assumido todas as obrigações legais do exportador de dados por contrato ou por operação de lei, caso em que o titular dos dados pode fazer cumprir seus direitos contra essa entidade.

O importador de dados não pode confiar em uma violação por um sub-processador de suas obrigações para evitar suas próprias responsabilidades.

(3) Se um titular de dados não puder apresentar uma reivindicação contra o exportador de dados ou o importador de dados referido nos parágrafos 1 e 2, decorrente de uma violação pelo sub-processador de qualquer uma de suas obrigações referidas na seção 3 ou capítulo II seção 2.7 porque tanto o exportador de dados quanto o importador de dados desapareceram de fato ou deixaram de existir em termos legais ou tornaram-se insolventes, o sub-processador autoriza o titular de dados a apresentar uma reivindicação contra ele com relação a suas próprias operações de processamento sob a Política de Privacidade de Dados do Grupo DHL como se ele fosse o exportador de dados ou o importador de dados, a menos que qualquer entidade sucessora tenha assumido todas as obrigações do exportador de dados ou do importador de dados por contrato ou por operação de lei, caso em que o titular dos dados pode fazer cumprir seus direitos contra essa entidade. A responsabilidade do sub-processador será limitada às suas próprias operações de processamento sob a Política de Privacidade de Dados do Grupo DHL.

(4) A jurisdição para este fim é no país de estabelecimento do exportador de dados.

3. Direitos de terceiros

Os titulares de dados têm o direito de fazer cumprir como beneficiário terceiro, capítulo II, seção III parágrafo 5 parágrafo 1 e IV da Política de Privacidade de Dados do Grupo DHL contra o exportador de dados e/ou - dependendo das circunstâncias - o importador de dados ou sub-processador por sua respectiva violação de suas obrigações da Política de Privacidade DP DHL, no que diz respeito aos seus dados pessoais.

4. Resolução alternativa de disputas

(1) Os titulares de dados que acreditam que seu direito de proteção de sua esfera individual de vida foi prejudicado por um ato real ou suposto de processamento de seus dados pessoais podem se aplicar ao Oficial de Proteção de Dados competente da respectiva empresa do grupo, solicitando arbitragem. O Oficial de Proteção de Dados examinará a legitimidade da reclamação e aconselhará o titular dos dados com relação aos seus direitos. Ao fazer isso, o Oficial de Proteção de Dados é obrigado a manter a confidencialidade de outros dados pessoais dos quais o Oficial de Proteção de Dados foi informado pelo reclamante, na medida em que este último

não libere o Oficial de Proteção de Dados desta obrigação. A pedido do titular dos dados, pode ser feita uma tentativa de chegar a um acordo sobre a reclamação com a participação do titular dos dados e o Oficial de Proteção de Dados. Tal acordo pode também incluir uma recomendação relativa a danos em conexão com a violação do direito de proteção de sua esfera individual de vida.

(2) O direito de fazer uma reclamação à Autoridade Supervisora de Proteção de Dados competente e/ou de tomar medidas permanece inalterado por esta disposição.

V. ANEXO: DEFINIÇÕES

Anonimização
Significa alterar um dado pessoal de modo que detalhes individuais sobre relações pessoais ou factuais não possam ser atribuídos à uma pessoa física especifica ou identificável sem que seja necessária uma quantidade desproporcional de tempo, dinheiro ou esforço.

Categorias especiais de dados pessoais
são dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical e o processamento de dados genéticos ou biométricos com o propósito de identificar exclusivamente uma pessoa física, dados referentes à saúde ou referentes à vida sexual ou orientação sexual de uma pessoa física no sentido do Artigo 9 (1) da GDPR.

Controlador
É a pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, sozinho ou em conjunto com outros, determina os propósitos e meios do processamento de dados pessoais onde os propósitos e meios de tal processamento são determinados pela lei da União ou do Estado-Membro, o controlador ou os critérios específicos para sua nomeação podem ser fornecidos pela lei da União ou do Estado-Membro. O controlador não é o ramo/estabelecimento comercial legalmente dependente de uma pessoa jurídica, mas sim a empresa como um todo; veja o Artigo 4 (7) da GDPR.

CPA (Acordo controlador-processador)
É um acordo estipulado pelo Artigo 28 da GDPR referente ao processamento de dados pessoais por um processador em nome de um controlador.

Dados pessoais
é qualquer informação relativa a uma pessoa física identificada ou identificável (titular dos dados); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos à identidade física, fisiológica, genética, mental, econômica, cultural ou social da pessoa física; veja o Artigo 4 (1) GDPR.

DPO (Oficial de Proteção de Dados)
pode ser - onde previsto pelas leis nacionais - nomeado como Encarregado de Proteção de Dados de acordo com tais leis ou, em qualquer outro caso, nomeado como Coordenador de Proteção de Dados. Se um Coordenador de Proteção de Dados for nomeado em uma empresa do Grupo além de um Encarregado de Proteção de Dados estatutário, os direitos e obrigações da Política de Privacidade de Dados do Grupo DHL serão aplicados na gestão de proteção de dados pelo Encarregado de Proteção de Dados, sendo que este processo será apoiado pelo Coordenador de Proteção de Dados em questão.

Empresa do Grupo
Refere-se a Deutsche Post AG, bem como todas as empresas nas quais a Deutsche Post AG tem uma participação direta ou indireta de mais de 50%, ou sobre as quais exerce controle financeiro. Além disso, no contexto da Política de Privacidade de Dados do Grupo DHL, as empresas que aderiram voluntariamente à Política de Privacidade de Dados do Grupo DHL são equiparadas às empresas do grupo.

Exportador de Dados
É a empresa sediada em um país da União Europeia (EU) que transfere dados pessoais para uma Importadora de Dados.

GDPR
Regulamento Geral de Proteção de Dados 2016/679/EU do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de indivíduos com relação ao processamento de dados pessoais e sobre a livre circulação de tais dados.

Importadora de Dados
É a empresa sediada em um país terceiro que recebe dados pessoais de uma Exportadora de Dados.

País terceiro
Qualquer país localizado fora da União Europeia.

Processador
significa qualquer pessoa física ou jurídica, autoridade pública, agência ou outro corpo que processe dados pessoais em nome do controlador; veja o Artigo 4 (8) GDPR.

Profiling
Profiling significa qualquer forma de processamento automatizado de dados pessoais que consiste no uso de dados pessoais para avaliar certos aspectos pessoais relacionados a uma pessoa física, em particular para analisar ou prever aspectos referentes ao desempenho de trabalho dessa pessoa física, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.

Pseudonimização
é a alteração de dados pessoais usando um sistema de alocação, de modo que detalhes individuais não possam mais ser atribuídos a uma pessoa física sem conhecimento ou uso do sistema de alocação.

Sub-processador
significa qualquer processador contratado pelo importador de dados ou por qualquer outro sub-processador do importador de dados que concorda em receber do importador de dados, ou de outro sub-processador do importador de dados, dados pessoais exclusivamente destinados a atividades de processamento a serem realizadas em nome do exportador de dados de acordo com suas instruções, os termos relevantes da Política de Privacidade de Dados do Grupo DHL e os termos do subcontrato escrito.

Terceiro
é uma pessoa física ou jurídica, autoridade pública, agência ou corpo que não seja o titular dos dados, controlador, processador e pessoas que, sob a autoridade direta do controlador ou processador, estão autorizadas a processar dados pessoais.

Titular dos dados
é toda pessoa física identificada ou identificável cujos dados pessoais são processados; veja o Artigo 4 (1) do GDPR.

Transferência Adicional
Existe transferência adicional se um importador de dados encaminha dados para outros terceiros que têm sua sede em um terceiro país ou se envolve na transferência transfronteiriça de dados.

Transferência de Dados
significa a divulgação por transmissão, por exemplo, a passagem de dados pessoais armazenados, ou dados pessoais adquiridos por meio de processamento, para um terceiro, ao encaminhá-los ativamente ou permitindo que terceiros os recuperem.

Tratamento de Dados
São todas as operações ou conjunto de operações realizadas em dados pessoais ou conjuntos de dados pessoais, sejam por meios automáticos ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, disseminação ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, exclusão ou destruição; veja o Artigo 4 (2) da GDPR.

Bonn, 01 de julho de 2023