Acordo sobre o processamento de pedidos entre

CLIENTE

e

Karl Wörwag Lack- und Farbenfabrik GmbH & Co. KG

Kornwestheimer Str. 49, 70825 Korntal-Münchingen

Preâmbulo

As partes contratantes firmaram um acordo de serviços referente a uma relação de trabalho para o processamento de dados contratado, de acordo com o art. 28 do RGPD-UE e/ou o processamento de dados consagrado no acordo de serviços ocorre em nome da entidade responsável (o denominado processamento de pedidos). Para especificar os direitos e as obrigações decorrentes da relação de processamento de dados contratado, de acordo com a obrigação legal, as partes contratantes celebram o seguinte acordo.

1 Área de aplicação

O acordo será aplicável a todas as atividades que são objeto do acordo de serviços e no cumprimento das quais os colaboradores do subcontratante ou terceiros adjudicados pelo subcontratante em conformidade com este acordo entrarem em contacto com dados pessoais, dados pelos quais a entidade responsável (art. 4, n.º 7, RGPD) é encarregada.

2 Definição dos conceitos

2.1 Este acordo refere-se apenas ao processamento de dados pessoais segundo as instruções dadas pela entidade responsável.

2.2 Processamento significa qualquer procedimento ou série de procedimentos realizados com ou sem o auxílio de uma série processosem ligação com dados pessoais, como a recolha, o registo, a organização, a classificação, o armazenamento, a adaptação ou alteração, a leitura, a consulta, a utilização, a divulgação por transferência, a difusão ou outra forma de disponibilização, comparação ou associação, restrição, eliminação ou destruição.

2.3 Dados pessoais significa qualquer informação relativa a uma pessoa natural identificada ou identificável (doravante "pessoa visada"); uma pessoa singular é considerada identificável quando pode ser identificada direta ou indiretamente, em particular pela associação a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a uma ou mais características especiais que sejam a expressão da identidade física, fisiológica, genética, psíquica, económica, cultural ou social desta pessoa natural.

2.4 O subcontratante é uma pessoa singular ou jurídica, órgão governamental, instituição ou outra agência que processa dados pessoais em nome da entidade responsável.

2.5 Instrução é a ordem direcionada da entidade responsável para um determinado manuseamento relacionado com a proteção de dados (p. ex., anonimização, bloqueamento, eliminação, publicação) do subcontratante com dados pessoais. As instruções existentes (p. ex., através deste aditamento ao acordo) podem ser posteriormente alteradas, complementadas ou substituídas por instruções individuais da entidade responsável (instrução individual).

3 Especificação do conteúdo contratado

3.1 O objeto e a duração do processamento de dados contratado, bem como o âmbito, a natureza e o propósito do processamento pretendido dos dados, são consagrados no acordo de serviços.

3.2 O tipo de dados pessoais utilizados é descrito de forma precisa no **Anexo 2** ("Especificação das categorias de dados").

3.3 O círculo dos visados pelo tratamento de dados pessoais é descrito de forma precisa no **Anexo 3** ("Subcontratados autorizados ").

4 Responsabilidade e autoridade

4.1 A entidade responsável é responsável pelo cumprimento dos termos dos regulamentos de proteção de dados, especialmente pela legalidade da transmissão de dados ao subcontratante, bem como pela legalidade do processamento de dados (art. 4, n.º 7, RGPD). Ela pode exigir a publicação, correção, eliminação e o bloqueio dos dados a qualquer momento (art. 28, § 3, al. g) do RGPD), a menos que haja uma obrigação legal para armazenar os dados pessoais. Quando uma parte visada abordar diretamente o subcontratante com o objetivo de eliminar ou corrigir os seus dados, o subcontratante encaminhará imediatamente a solicitação à entidade responsável e irá auxiliá-la na concretização do pedido, em conformidade com as informações disponíveis para o subcontratante (art. 28, § 3, al. f) do RGPD).

4.2 O subcontratante só pode processar os dados de acordo com as instruções documentadas da entidade responsável, contanto que tal não seja exigido pela legislação da União ou dos Estados-membros a que o subcontratante está sujeito. Neste caso, o subcontratante deve informar imediatamente a entidade responsável sobre estas exigências legais antes do processamento. Uma instrução é a ordem escrita da entidade responsável para um tratamento específico do subcontratante com dados pessoais. As instruções são inicialmente definidas pelo acordo de serviços e podem ser alteradas, complementadas ou substituídas pela entidade responsável por escrito, através de uma única instrução (art. 28, § 3, al. a) do RGPD).

4.3 O subcontratante deve informar imediatamente a entidade responsável de acordo com o art. 28, § 3 do RGPD, se este for da opinião que uma instrução viola os regulamentos legais da proteção de dados. O subcontratante terá o direito de suspender a execução da respetiva instrução até que esta seja confirmada ou alterada pela entidade responsável perante a entidade responsável.

4.4 Alterações no objeto de processamento com alterações de procedimento devem ser decididas e documentadas em conjunto. O subcontratante só pode fornecer informações a terceiros ou aos visados com o consentimento prévio por escrito da entidade responsável. O subcontratante não usa os dados para qualquer outra finalidade e, em particular, não tem o direito de os divulgar a terceiros. Cópias e duplicados não serão feitos sem o conhecimento da entidade responsável. Qualquer outra questão só

é válida em caso de regulamentação no contrato ou nos casos mencionados na cláusula 4.2 deste acordo.

4.5 A entidade responsável mantém a lista de atividades de processamento, de acordo com o art. 30, § 1 do RGPD. O subcontratante deve, se solicitado, fornecer à entidade responsável informações para inclusão na lista de atividades de processamento.

4.6 O processamento e utilização dos dados em nome da pessoa responsável ocorrem exclusivamente no território da União Europeia ou na Área Económica Europeia da República Federal da Alemanha. Uma transferência para um estado fora do território da República Federal da Alemanha requer o consentimento prévio da pessoa responsável. Isto não se aplica às empresas afiliadas ao processador, de acordo com o § 15 da Lei das Sociedades Anônimas Alemãs, desde que regras corporativas vinculantes ou cláusulas contratuais padrão da UE tenham sido acordadas com essas empresas. Os requisitos especiais dos Art. 44 a 49 do GDPR permanecem inalterados para outros casos.

4.7 O processamento de dados pessoais em casas particulares de colaboradores do subcontratante (teletrabalho, locais de trabalho domésticos) só é permitido nas seguintes condições: Trata-se do hardware do subcontratante, que foi deixado para os colaboradores para fins profissionais e é operado por trás de uma firewall e protegido por um certificado de cliente VPN. O acesso pelo hardware dos próprios funcionários não é permitido em nenhum caso.

5 Cumprimento responsável das obrigações legais vinculativas pelo subcontratante

5.1 Além dos regulamentos contratuais deste acordo e do acordo de serviços, o subcontratante, de acordo com o art. 28, § 3, art. 30 do RGPD, tem os seguintes deveres legais.

5.2 O subcontratante deve assegurar que os colaboradores envolvidos no processamento dos dados da entidade responsável foram obrigados a respeitar, nos termos do art. 5 I c) do RGPD, e instruídos sobre as disposições de proteção referentes à legislação de proteção de dados. Isto também inclui o esclarecimento sobre a vinculação às instruções e aos objetivos existentes nesta relação de processamento contratada.

5.3 De acordo com o art. 37 do RGPD, o subcontratante nomeou um encarregado pela proteção de dados operacional, que exerce a sua atividade de acordo com o §§ art. 38 e art. 39 do RGPD. As informações de contacto do encarregado pela proteção de dados devem ser comunicadas à entidade responsável, com o objetivo de estabelecer contacto direto.

5.4 O subcontratante deve informar imediatamente a entidade responsável sobre quaisquer fiscalizações e medidas tomadas pelas autoridades supervisoras, de acordo com o art. 58 do RGPD, ou se uma autoridade supervisora tiver procedido a investigações junto do subcontratante, de acordo com o art. 83 do RGPD. Além disso, o subcontratante deve notificar a entidade responsável imediatamente se ele for processado por pedido de indemnização devido a uma violação do RGPD e deve informá-la, em intervalos regulares, sobre o processo em curso.

5.5 Após a entrada em vigor do RGPD, o subcontratante compromete-se a manter uma lista de atividades de processamento que inclua todas as categorias das atividades de processamento contratadas realizadas (art. 30, § 2 do RGPD). Esta lista contém, pelo menos,

(a) o nome e as informações de contacto do subcontratante e de cada colaborador responsável da entidade responsável, em cujo nome o subcontratante opera e, quando apropriado, o representante da entidade responsável ou do subcontratante e qualquer encarregado pela proteção de dados;

(b) as categorias de processamento realizadas em nome da entidade responsável;

(c) se for caso disso, as transferências de dados pessoais para um país terceiro ou para uma organização internacional, incluindo a indicação do país terceiro em causa ou da organização internacional em causa, bem como no caso das transferências de dados mencionadas no art. 49, parágrafo 1, subparágrafo 2, a documentação de garantias adequadas;

(d) se possível, uma descrição geral das medidas técnicas e organizacionais referidas no artigo 32, § 1 do RGPD.

O subcontratante deve, mediante solicitação, fornecer à entidade responsável acesso às informações da lista relacionadas com este processamento no prazo de 14 dias após o pedido por escrito.

6 Segurança do processamento e sua fiscalização

6.1 As partes contratantes comprometem-se com as medidas específicas de segurança técnicas e organizacionais estabelecidas no **Anexo 1** "Medidas técnicas e organizacionais" deste acordo, segundo o art. 28, § 3, al. c) do RGPD, em ligação com o art. 32, § 1 do RGPD ou § 22 do LAPD de 2018, para garantir a segurança do processamento contratado. O anexo é objeto deste acordo.

6.2 As medidas técnicas e organizacionais têm em conta a mais recente técnica no momento da celebração deste acordo e estão sujeitas ao progresso técnico. A este respeito, o subcontratante pode implementar medidas adequadas alternativas. Ao fazê-lo, o nível de segurança das medidas especificadas no anexo "Medidas técnicas e organizacionais" não deve ser inferior ao limite estabelecido. Mudanças significativas devem ser documentadas.

6.3 O subcontratante compromete-se a verificar e a avaliar periodicamente a eficácia das medidas técnicas e organizacionais específicas em relação à segurança do processamento e a documentar esta avaliação de risco.

6.4 O subcontratante irá, mediante solicitação, fornecer à entidade responsável as informações necessárias para cumprir a sua obrigação de fiscalizar a adjudicação e disponibilizar os documentos comprovativos. Devido à obrigação de fiscalização da entidade responsável, de acordo com o art. 28, § 1, § 3 do RGPD, antes do início do processamento de dados e durante a vigência da adjudicação, o subcontratante deve assegurar que a entidade responsável é capaz de se certificar do cumprimento das medidas técnicas e organizacionais tomadas. Para este efeito, o subcontratante deve, mediante pedido, informar a entidade responsável da implementação das medidas técnicas e organizacionais, de acordo com o artigo: 32, § 1, bem como da realização da avaliação dos riscos efetuada regularmente segundo a cláusula 6.3. A prova da implementação de tais medidas, que dizem respeito não apenas à adjudicação concreta, pode também ser fornecida mediante a apresentação de um certificado atual ou relatórios de instâncias independentes (por exemplo, auditores, revisão, encarregado pela proteção de dados, departamento de segurança informática, auditores de proteção de dados) ou uma certificação adequada por uma auditoria de proteção de dados ou auditoria de segurança informática (por exemplo, de acordo com a proteção básica do Serviço Federal Alemão para a Segurança da Informação, ISO 27001).

6.5 A entidade responsável pode verificar a adequação das medidas para a conformidade com os requisitos técnicos e organizacionais dos regulamentos de proteção de dados (art. 28, § 3, al. h) do RGPD) relevantes para o processamento de dados contratado durante o horário de funcionamento normal e nas instalações operacionais do subcontratante sem interromper o funcionamento do negócio.

7 Notificação por violações efetuadas pelo subcontratante

7.1 O subcontratante deve notificar a entidade responsável imediatamente após a deteção de graves perturbações às suas operações, suspeita de violação das disposições contratuais ou legais de proteção de dados, violações de tais disposições ou outras irregularidades no processamento de dados da entidade responsável (art. 28, § 3, secção 3, art. 33, art. 34 do RGPD). A informação tem, pelo menos, o seguinte conteúdo:

(a) uma descrição da natureza da violação da proteção dos dados pessoais, sempre que possível, indicando as categorias e o número aproximado das pessoas afetadas, as categorias em causa e o número aproximado dos registos de dados pessoais afetados;

(b) uma descrição das consequências prováveis da violação da proteção de dados pessoais;

(c) uma descrição das medidas já tomadas ou propostas para resolver a violação da proteção de dados pessoais e, se for caso disso, medidas para atenuar os seus potenciais efeitos adversos.

Se não puderem ser fornecidas todas as informações presentes na cláusula 7.1., al. a) - c), no momento da informação, então devem ser disponibilizadas todas as informações imediatamente após o conhecimento e, se necessário, gradualmente.

7.2 O subcontratante, em consulta com a entidade responsável, deve tomar as medidas adequadas para salvaguardar os dados e atenuar as possíveis consequências negativas para as partes visadas.

8 Eliminação e devolução dos dados

8.1 Os suportes de dados e os registos de dados transferidos permanecem propriedade da entidade responsável.

8.2 A pedido da entidade responsável, mas o mais tardar no prazo de prescrição das reivindicações no acordo de serviços subjacente, o subcontratante deve entregar todos os documentos, resultados de processamento e utilização criados, bem como as bases de dados (e quaisquer cópias ou reproduções criadas dos mesmos) em sua posse, relacionados com a relação de adjudicação à entidade responsável ou, após o consentimento prévio da entidade responsável, destruir esta informação em conformidade com a lei de proteção de dados (artigo 28, § 3, al. g) do RGPD). O mesmo se aplica ao material de teste e material rejeitado. A documentação sobre como garantir a eliminação adequada, bem como um protocolo de eliminação, deve ser submetida à entidade responsável, mediante solicitação.

8.3 O subcontratante pode manter documentação que sirva de prova sobre o processamento de dados correto e de acordo com o contratado, nos termos dos respetivos prazos de prescrição e/ou prazos de retenção, para além do final do contrato. Alternativamente, pode entregá-la à entidade responsável no final do contrato para sua quitação.

9 Subcontratados pelo subcontratante

9.1 O subcontratante não contratará qualquer outro subcontratante sem o consentimento prévio em separado por escrito da entidade responsável e compromete-se a empregar apenas subcontratados por si de acordo com as seguintes condições:

(a) O subcontratante seleciona cuidadosamente o subcontratado e verifica, antes de fazer a contratação, que ele pode cumprir os compromissos feitos entre a entidade responsável e o subcontratante. Em particular, o subcontratante deve verificar, com antecedência e regularmente durante o período do contrato, se o subcontratado tomou as medidas técnicas e organizacionais apropriadas para a proteção de dados pessoais, de acordo com o art. 32, § 1 do RGPD. O resultado da verificação deve ser documentado pelo subcontratante. O subcontratante é obrigado a fazer com que o subcontratado confirme que ele, desde que exigido por lei, nomeou um encarregado pela proteção de dados operacional, no âmbito do art. 37 do RGPD.

(b) O subcontratante deve formular os compromissos contratuais com o(s) subcontratado(s), de modo a cumprir as disposições da proteção de dados na relação contratual entre a entidade responsável e o subcontratante.

9.2 De acordo com o sentido deste regulamento, os subcontratados não são serviços que o subcontratante usa perante terceiros como um serviço adicional para auxiliar no desempenho da incumbência. Estes incluem, p. ex., serviços de telecomunicações, manutenção e assistência ao utilizador, serviços de limpeza, auditores ou eliminação de suportes de dados. No entanto, para garantir a proteção e a segurança dos dados da entidade responsável, o subcontratante é obrigado a adotar os acordos contratuais adequados e legalmente conformes e a tomar medidas de controlo, mesmo no caso de serviços adicionais externamente concedidos.

9.3 Os subcontratados contratados no momento da assinatura do contrato serão documentados no **Anexo 3** ("Subcontratados autorizados"), incluindo os locais de processamento e o tipo da prestação de serviços. Os subcontratados mencionados nesta lista são considerados legalmente encarregados desde o início, de acordo com a cláusula 9, § 1, desde que seja garantida, por parte do subcontratante, a implementação dos pré-requisitos aí especificados.

9.4 O subcontratado só poderá aceder aos dados se o subcontratado também tiver cumprido as obrigações do subcontratante neste contrato e/ou tiver assegurado isso ao subcontratante e o subcontratante verificar regularmente o cumprimento destas obrigações pelo subcontratado.

10 Serviços adicionais

As cláusulas 1 a 8 aplicam-se, de forma correspondente, se a verificação ou a manutenção de procedimentos automatizados ou do equipamento de processamento de dados for realizada por outras entidades em incumbência e o acesso aos dados pessoais não puder ser excluído.

11 Confidencialidade e controlo da proteção de dados

11.1A entidade responsável e o subcontratante comprometem-se a tratar confidencialmente todos os conhecimentos adquiridos sobre segredos comerciais e de negócios no âmbito da relação contratual. Isto também se aplica ao período acordado no acordo de serviços e também para além do término das incumbências individuais e/ou do relacionamento comercial.

11.2O subcontratante compromete-se a conceder ao encarregado para a proteção de dados operacional da entidade responsável, durante o horário comercial normal e a qualquer momento, o acesso necessário para o desempenho das suas respetivas obrigações legais relacionadas com esta incumbência.

12 Disposições finais

12.1Alterações e complementos a este anexo e todos os seus componentes - incluindo quaisquer garantias do subcontratante - devem ser efetuadas por convenção escrita e devem indicar explicitamente que se trata de uma modificação e/ou complemento destas condições. Isto também se aplica à renúncia desta exigência formal. A exigência da formalidade escrita não é aplicável se for cancelada entre as partes contratantes com base num acordo expresso e individual.

12.2Os seguintes anexos são parte integrante deste acordo:

Anexo 1 "Medidas técnicas e organizacionais"

Anexo 2 "Especificação dos tipos de dados, das categorias"

Anexo 3 "Subcontratados autorizados "

Anexo 1 para o acordo sobre o processamento de pedidos

A. Medidas técnicas e organizacionais segundo o art. 32, § 1 a-d RGPD-UE

1. Pseudonimização (art. 32, § 1, al. a do RGPD-UE)
Os dados que devem ser avaliados apenas para fins estatísticos são pseudonimizados e armazenados sem referência pessoal. Os dados que devem ser transmitidos aos subcontratados são, na medida do possível, pseudonimizados e não serão dados pessoais para o subcontratado, em conformidade com a decisão do TJCE de 19.10.2016 (C 582/2014).

2. Encriptação (art. 32, § 1, al. a do RGPD-UE)
Os dados pessoais são exclusivamente armazenados e encriptados em suportes de dados móveis e dispositivos móveis. O acesso aos dados armazenados no centro de dados só é possível através de ligações encriptadas. Os dados são transmitidos somente com encriptação forte, de acordo com a diretriz TR-2102 do Serviço Federal Alemão para a Segurança da Informação.

3. Garantia da confidencialidade (art. 32, § 1, al. b) do RGPD-UE)
A intrusão de pessoas não autorizadas nos sistemas informáticos deve ser evitada. As autorizações são geridas através de um conceito de direitos baseado em funções. Cada colaborador tem o seu próprio acesso aos sistemas informáticos, que são protegidos com uma proteção de palavra-passe. A palavra-passe deve necessariamente consistir de uma mistura de números, letras e caracteres especiais e deve ter um comprimento mínimo de oito caracteres. Os sistemas informáticos individuais são bloqueados durante os momentos de pausa. O bloqueio só pode ser superado com uma palavra-passe. As permissões terão a sua atualidade verificada regularmente. A intrusão de pessoas não autorizadas nos sistemas de computadores deve ser evitada.As autorizações são gerenciadas usando um conceito de direitos baseado em funções. Cada funcionário tem seu próprio acesso aos sistemas de computadores que são protegidos por proteção por senha. A senha deve necessariamente consistir de uma mistura de números, letras e caracteres especiais e deve ter um comprimento mínimo de oito

caracteres. Os sistemas de computadores individuais são bloqueados durante as pausas. O bloqueio só pode ser cancelado com uma senha. Permissões são verificadas regularmente para a atualidade. Inúmeras medidas garantem que os dados pessoais coletados para diferentes finalidades possam ser processados separadamente (por exemplo, através da capacidade de vários clientes e do conceito de autorização). O acesso a salas onde o processamento de dados ocorre é controlado e negado a pessoas não autorizadas. Os escritórios são protegidos por um sistema de bloqueio, os visitantes devem registrar com tempos de atendimento em uma lista. As instalações do centro de dados são protegidos por um sistema de acesso eletrônico com permissões documentados, uma estadia de pessoas não autorizadas no centro de dados só é permitida em casos de manutenção e devem ser acompanhados por uma pessoa autorizada. Os tempos de atendimento no data center são registrados eletronicamente. Os processadores só são comissionados com o processamento de dados pessoais se medidas técnicas e organizacionais equivalentes forem garantidas.Os dados pessoais são, na medida em que não são um processador, apenas transmitidos pelas instruções da pessoa responsável ou por uma base legal.

4. Garantia da integridade (art. 32, § 1, al. b) RGPD-UE)
Apenas serão concedidas permissões de registo de dados limitadas e serão efetuadas regularmente verificações de integridade. Serão efetuadas regularmente verificações de segurança como p.ex., testes de penetração.

5. Garantia de disponibilidade (art. 32, § 1, al. b) RGPD-UE)
Os dados devem ser protegidos contra destruição ou perda acidental. Basicamente, todos os dados serão armazenados de forma redundante (pelo menos através de sistemas RAID (Matriz redundante de discos independentes) à prova de falhas com nível 5 ou 6). Serão criadas várias réplicas e/ou cópias de segurança dos dados completas e redundantes, que serão guardadas fora do edifício dos dados originais. Há uma fonte de alimentação ininterrupta, uma firewall e uma proteção antivírus atualizada para garantir a disponibilidade.

6. Garantia da robustez do sistema (art. 32,§ 1 , al. b) do RGPD-UE)
A robustez das ligações de comunicação e a capacidade de computação serão asseguradas pela monitorização contínua da utilização.

7. Procedimento para restabelecer a disponibilidade dos dados pessoais após um incidente físico ou técnico (art. 32, § 1, al. c) do RGPD-UE)
São efetuados testes regulares para restaurar as cópias de dados através do armazenamento redundante em vários locais, para tentar minimizar o tempo de inatividade.

8. Procedimentos para a verificação, classificação e avaliação regulares da eficácia das medidas técnicas e organizacionais (art. 32, § 1, al. d) do RGPD-UE)
Existe um conceito de segurança informático e de proteção de dados que é constantemente verificado quanto às necessidades de ajuste. As alterações são documentadas e verificadas quanto à sua eficácia em intervalos regulares

B. Medidas técnico-organizacionais adicionais para o caso do processamento de dados sensíveis, segundo o § 22, secção 2 da Lei Alemã de Proteção de Dados de 2018:

Os funcionários serão regularmente informados no âmbito da proteção de dados sobre o estado atual. Existe um encarregado de proteção de dados nomeado.

Tendo em conta o estado da técnica, os custos de implementação e o tipo, âmbito, circunstâncias e finalidades do processamento, bem como as várias probabilidades de ocorrência e a gravidade dos riscos associados ao processamento para os direitos e liberdades das pessoas singulares, serão implementadas, perante o processamento de dados sensíveis segundo o art. 9, § 1 do RGPD-UE, as seguintes medidas adicionais de segurança no âmbito da proporcionalidade:
S1. Controlo da introdução (§ 22, secção 2, n.º 2 da Lei Alemã de Proteção de Dados de 2018)

A introdução, alteração e eliminação de dados pessoais sensíveis é registada com a especificação de um identificador de agente personalizável.

S2. Restrição de acesso a dados pessoais (§ 22, secção 2, n.º 5 da Lei Alemã de Proteção de Dados de 2018)

Os dados pessoais são bloqueados contra o acesso dos colaboradores da entidade responsável e/ou do subcontratante que, de acordo com o princípio de minimização de dados segundo o art. 5, § 1, al. c) do RGPD-UE, não precisam de acesso para o processamento legal dos dados. Para este propósito, é usado um conceito de autorização baseado em funções e grupos (comparar também A n.º 3 e n.º 8 acima)

S3. disposições processuais específicas que, no caso de uma transmissão ou processamento para outros fins, asseguram o cumprimento dos requisitos da presente lei e do Regulamento (UE) 2016/679

Para requisitos especiais de proteção de dados por regulamentos legais, estatutários ou contratuais específicos do setor, as medidas de proteção serão discutidas com a entidade responsável em casos individuais, sendo ajustadas ao nível de proteção respetivamente exigido. Isto pode incluir o cumprimento de determinadas normas de segurança de dados e normas de proteção de dados (ISO 27001, Padrões Básicos de Segurança 200-1 a 200-3 da Lei Alemã de Proteção de Dados, Lei de

Verificação de Segurança, Categorização de Classes de Proteção para Documentos no serviço público, etc.)

Os restantes pontos do § 22, secção 2 da Lei Alemã de Proteção de Dados já estão abrangidos pelas disposições do regulamento (ver A, números 1 a 8 acima).

Anexo 2 para o acordo sobre processamento de pedidos

Especificação dos tipos de dados, das categorias de dados e dos visados pelo processamento

1. Especificação dos tipos de dados e das categorias de dados:
- Dados mestre do fornecedor (por exemplo, informações de contacto do fornecedor, endereços, etc.)
- Dados de referência (por exemplo, condições de pagamento e de entrega, dados bancários, etc.)
- Dados estruturais de toda a empresa (por exemplo, produtos, serviços, responsabilidades dos colaboradores, etc.)
- Dados de transação (por exemplo, atividade empresarial, etc.)

2. Especificação dos visados pelo processamento:
- Fornecedores e seus colaboradores (parceiro de contacto)

Anexo 3 para o acordo sobre processamento de pedidos

Subcontratados autorizados