DIRETRIZ DO GRUPO

DA voestalpine AG

RELATIVA AO TRATAMENTO DE DADOS PESSOAIS

DIRETRIZ DE PROTEÇÃO DE DADOS

voestalpine
ONE STEP AHEAD.

Preâmbulo

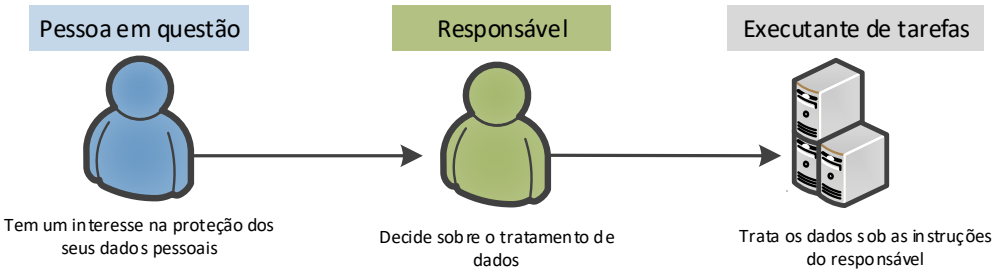
Prezadas Senhoras e Senhores,

na era digital é comum coletar e tratar dados. Nesta matéria, na voestalpine, o princípio básico é: onde se guardam e tratam dados pessoais tem de se assegurar uma elevada proteção e segurança dos dados. Isto é válido não apenas para os dados dos colaboradores, mas também para os dados dos clientes, fornecedores e outros parceiros comerciais e outras pessoas.
Enquanto parceiro confiável, consideramos ser nossa obrigação salvaguardar a privacidade de cada um e garantir uma norma unificada e válida em todo o mundo relativa ao manuseio de dados pessoais.
Nesta diretriz do Grupo sobre proteção de dados está definido o princípio básico referente à prevenção de dados e à economia de dados, e estão ancorados os pressupostos para o tratamento de dados pessoais de colaboradores, clientes, fornecedores e outros parceiros comerciais e outras pessoas. Deste modo, estabelecemos uma norma válida em todo o mundo de proteção e segurança dos dados de nosso Grupo.
Nossos gerentes e colaboradores estão obrigados a observar esta diretriz de proteção de dados, bem como toda a respectiva legislação aplicável. No contexto do tratamento de dados pessoais é de se observar que, além desta diretriz de proteção de dados, são também válidas e devem ser respeitadas em especial as eventuais IT Policies & Guidelines, como a norma mínima de segurança de TI para colaboradores.

Por questões de simplificação da leitura desta diretriz relativa à proteção de dados utilizamos apenas a forma masculina. Naturalmente que o seu teor se aplica automaticamente a ambos os sexos.

A OS CONCEITOS DE FORMA SIMPLES E CONCISA

a) Intervenientes na proteção de dados



b) Dados abrangidos

Pelos regulamentos jurídicos estão abrangidos exclusivamente dados pessoais, incluindo dados sensíveis (categorias especiais de dados pessoais), que não estejam anonimizados. Em caso de anonimização, os dados pessoais são alterados de forma que possam ser mais correlacionados a uma pessoa.

Nesse caso, estão incluídas todas as informações que se referem a uma pessoa (física) identificada ou identificável.

Essas são, entre outras:

- Nome
- Nome da empresa, caso se trate de pessoas jurídicas que se enquadrem no âmbito da aplicação das leis em matéria de proteção de dados
- Data de nascimento
- Número pessoal/identificação única
- Contatos privados e profissionais (endereço, número de telefone, e-mail)
- Estado civil
- Sexo
- Registros de imagem e som (vídeos, fotos, etc.)
- Dados sensíveis (categorias especiais de dados pessoais) como por ex.:
  - Religião
  - Dados biométricos (por ex.: impressão digital)
  - Opiniões políticas (por ex.: filiação partidária)
  - Filiação sindical
  - Dados sobre saúde e dados genéticos

B TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais é proibido, exceto se existir (pelo menos) um dos motivos e/ou justificação legítimos seguidamente indicados:

- Interesses legítimos prevalecentes do responsável
- Cumprimento de obrigações contratuais
- Concordância da pessoa em questão
- Cumprimento de obrigação legal
- Proteção dos interesses vitais da pessoa em questão

Dados sensíveis (categorias especiais de dados pessoais – ver acima) **são considerados especialmente suscetíveis de proteção**, razão pela qual o tratamento desses dados requer um cuidado maior. O mesmo é válido para dados sobre condenações e infrações penais.
Qualquer tratamento de dados pessoais precisa ter como base uma **determinada finalidade**. Além disso, a pessoa em questão tem de ser **informada** sobre o tratamento de seus dados pessoais.
Só pode ser compilada, tratada e utilizada a quantidade de dados pessoais necessária para alcançar a finalidade legítima (**"menos possível, e somente o necessário!"**).
Além disso, os bancos de dados têm de estar corretos e completos. Os dados poderão ser **deletados** passados os períodos de conservação de registros legais ou referentes a processos de negócios. Os dados antigos ou incorretos deverão ser **corrigidos**, complementados ou atualizados.

C PRINCÍPIO DA NECESSIDADE DE INFORMAÇÃO

O acesso a dados pessoais por colaboradores só está autorizado quando for necessário ao cumprimento dos respectivos trabalhos.

D NENHUM PRIVILÉGIO DO GRUPO

DEVE-SE OBSERVAR que não existe **nenhum privilégio do Grupo**. A transferência de dados pessoais dentro do Grupo – ou seja de uma empresa do Grupo para outra – está igualmente sujeita às normas de proteção de dados, assim como às disposições desta diretriz de proteção de dados.

E TRANSFERÊNCIA TRANSFRONTEIRIÇAS DE DADOS PESSOAIS

Em cada transferência transfronteiriça de dados pessoais, o gerente de proteção de dados local deverá ser envolvido e deverão ser observados os respectivos requisitos locais para a transmissão de dados pessoais para o país estrangeiro.
Em cada transferência transfronteiriça de dados pessoais, o receptor (e eventuais subcontratados do receptor) dos dados tem de garantir um nível de proteção equivalente ao desta diretriz de proteção de dados e ao dos regulamentos europeus em matéria de proteção de dados.
Instrumentos adequados, que comprovem um nível de proteção de dados equivalente, poderão ser, entre outros:

- O receptor tem sede no Espaço Econômico Europeu e, por conseguinte, está sujeito aos regulamentos de proteção de dados;

- O receptor tem sede em um país que, de acordo com a determinação da Comissão Europeia, dispõe de um nível adequado de proteção de dados ("países com estatuto equivalente");
- Acordo com as cláusulas contratuais padrão da UE;
- Participação do receptor em um sistema de certificação reconhecido pela UE para a garantia de um nível de proteção de dados apropriado (por ex.: *EU-U.S. Privacy Shield*).

Em determinados casos, é permitida também a transferência transfronteiriças de dados pessoais sem prova de um nível de proteção de dados suficiente.

F REGULAMENTOS COMPLEMENTARES PARA EMPRESAS DO GRUPO COM SEDE OU ATIVIDADE ECONÔMICA NO ESPAÇO ECONÔMICO EUROPEU[1]

Empresas do Grupo com sede no Espaço Econômico Europeu, assim como empresas do Grupo que disponibilizam serviços (bens/serviços) a entidades dentro do Espaço Econômico Europeu ou que observam sua conduta, deverão registrar todos os tratamentos de dados em um **diretório interno de procedimentos**, sendo que esse diretório de procedimentos completo tem de estar implementado, no máximo, a partir de 1.5.2018, nos termos do regulamento base sobre proteção de dados. Para assegurar um procedimento uniforme de criação dos diretórios de procedimentos, deverão ser utilizadas as tabelas ou ferramentas de informática disponibilizadas pela Comissão de Proteção de Dados do Grupo.

No âmbito da criação do diretório de procedimentos, deverá ser previamente realizada uma avaliação de riscos pelo responsável da respectiva área em colaboração com o gerente de proteção de dados local. Se for provável que o tratamento de dados represente um elevado risco para os direitos e a liberdade da pessoa em questão, então o responsável da respectiva área em colaboração com o gerente de proteção de dados local deverá realizar **previamente** uma **avaliação do impacto da proteção de dados**. O resultado e eventuais medidas encontradas no âmbito da avaliação de riscos, assim como da avaliação do impacto da proteção de dados, deverão ser registrados no diretório de procedimentos.

[1] Os Estados signatários do Espaço Econômico Europeu são os 28 Estados-Membro da UE, assim como a Islândia, o Liechtenstein e a Noruega.

Índice

1 INTRODUÇÃO E DEFINIÇÃO DE OBJETIVOS

A voestalpine leva muito a sério a obrigação de proteção de privacidade e, assim, a exigência de prevenção e economia de dados pessoais de seus colaboradores, clientes e outros parceiros comerciais e outras pessoas.
Nesta diretriz de proteção de dados são esclarecidos os princípios básicos que devem ser observados no tratamento de dados pessoais no Grupo voestalpine.
Em caso de violação dos regulamentos de proteção de dados ou das disposições da diretriz de proteção de dados, todo colaborador estará sujeito a medidas disciplinares e do direito trabalhista. Além disso, em alguns países, tratamentos de dados pessoais abusivos ou outras violações do direito de proteção de dados terão igualmente consequências de responsabilidade penal e civil.

2 ÂMBITO DE APLICAÇÃO

Esta diretriz de proteção de dados é aplicável a todas as empresas e colaboradores do Grupo voestalpine.
Pertencem ao Grupo voestalpine todas as empresas nas quais, direta ou indiretamente, a voestalpine AG detenha uma participação de, pelo menos, 50% ou nas quais exerça qualquer outro tipo de controle. Todas as outras empresas, nas quais a voestalpine AG detenha, direta ou indiretamente, pelo menos 25% e não exerça controle, tomarão conhecimento desta diretriz de proteção de dados com a solicitação de reconhecimento autônomo no âmbito de suas estruturas de decisão estatutárias, tornando-a igualmente aplicável.
Esta diretriz de proteção de dados é válida para o tratamento de dados pessoais de pessoas físicas. Nos países, nos quais os dados de pessoas jurídicas são protegidos da mesma forma, esta diretriz de proteção de dados será igualmente válida para pessoas jurídicas[2]. Dados anonimizados (dados que não podem ser atribuídos a nenhuma pessoa), por exemplo, para avaliações ou análises estatísticas, não estão abrangidos por esta diretriz de proteção de dados.

2.1 VALIDADE DA LEGISLAÇÃO LOCAL

Esta diretriz de proteção de dados inclui os princípios básicos que devem ser mantidos pelo Grupo voestalpine no tratamento de dados pessoais, sem pretender substituir a legislação local. A respectiva legislação local prevalece sobre esta diretriz de proteção de dados, caso existam divergências obrigatórias ou requisitos mais exigentes. Deverão ser observadas, em especial, eventuais obrigações de informação e requisitos de autorização de acordo com a legislação local relacionadas ao tratamento de dados.
Cada empresa do Grupo é responsável pela observância desta diretriz de proteção de dados e dos requisitos da legislação local. Em caso de conflito, a empresa do Grupo em questão tem de informar imediatamente o gerente de proteção de dados local. Se for necessário de acordo com a legislação local, o gerente de proteção de dados local estará autorizado, em conjunto com o respectivo gerente de proteção de dados responsável da divisão e o gerente de proteção de dados do Grupo a derrogar de forma divergente a esta diretriz de proteção de dados.

[2] Por exemplo, na Áustria e devido às disposições da DSG 2000, os dados de pessoas jurídicas se enquadram no âmbito de aplicação desta diretriz relativa à proteção de dados

3 DEFINIÇÕES DE TERMOS

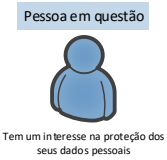
3.1 RESPONSÁVEL VS. EXECUTANTE DE TAREFAS

Responsável é aquela pessoa física ou jurídica e/ou conjunto de pessoas, que toma a decisão de utilizar os dados pessoais para uma determinada finalidade, e/ou que decide sobre as finalidades e os meios do tratamento. Responsável no contexto profissional, por exemplo, cálculos de salários, gestão de recursos humanos etc., portanto, é a empresa do Grupo enquanto empregador. No tratamento de dados pessoais, o responsável tem de observar os princípios indicados no item n.º 4.

Executante de tarefas (ou prestador de serviços no âmbito da legislação sobre proteção de dados) é uma pessoa física ou jurídica e/ou grupo de pessoas, que trata os dados pessoais exclusivamente em nome do responsável. Como um executantes de tarefas se qualificam com frequência, por exemplo, os *Shared Service* da voestalpine group-IT GmbH ou prestadores de recursos humanos[3]. Também no caso de terceirização, refere-se a um executante de tarefas. No entanto, deverá se observar que os executantes de tarefas são considerados responsáveis em relação à proteção dos dados pessoais dos seus próprios colaboradores, fornecedores etc.

Toda vez que se recorrer a um executante de tarefas, independentemente se ele for uma empresa do Grupo voestalpine, será necessário um acordo por escrito entre o responsável e o executante de tarefas ("**acordo do** executante de tarefas"), que descreve, pelo menos, o objeto e a duração do tratamento e do tipo de dados pessoais, as categorias das pessoas em questão e as obrigações e direitos do responsável. Através da celebração de um acordo do executante de tarefas, as obrigações do responsável permanecem inalteradas. DEVE-SE OBSERVAR neste contexto, que não existe nenhum privilégio do Grupo. A transferência de dados dentro do Grupo está sujeita, sem restrições, a esta diretriz de proteção de dados.

3.2 DADOS PESSOAIS



Por "dados pessoais" se entendem todas as informações que se referem a uma pessoa identificada ou identificável ("**Pessoa em questão**"). Estão assim abrangidos todos os dados sobre a pessoa em questão, com os quais a sua identidade é determinada ou determinável. Em alguns países[4], essas pessoas em questão também podem ser pessoas jurídicas.

Dessa forma, em regra geral, os dados pessoais qualificam-se, no âmbito da definição acima, por exemplo:

- Nome, datas de nascimento, números em geral de identificação pessoal, estado civil, sexo, registros de imagem e de som (vídeos, fotos), contatos particulares e profissionais de pessoas físicas;
- Nome da empresa, dados de contato de pessoas jurídicas, quando essas se enquadram no âmbito de aplicação das leis em matéria de proteção de dados;
- etc.

[3] Por exemplo, na Áustria, a voestalpine Personal Services GmbH

[4] Por exemplo, na Áustria

3.3 CATEGORIAS ESPECIAIS DE DADOS PESSOAIS

3.3.1 Dados sensíveis (categorias especiais de dados pessoais)

Por “dados sensíveis” (categorias especiais de dados pessoais) consideram-se dados, através dos quais se pode saber a origem de raça ou étnica, opiniões políticas, convicções religiosas ou filosóficas ou filiação sindical, assim como dados genéticos, dados biométricos que levam a uma identificação clara de uma pessoa física, dados sobre saúde ou outros dados relativos à vida sexual ou à orientação sexual de uma pessoa física. Por conseguinte, dados sensíveis são, por exemplo:

- Religião
- Diagnósticos médicos
- Impressão digital
- Filiação partidária
- etc.

Esses dados são considerados especialmente suscetíveis de proteção, razão pela qual o tratamento desses dados requer um cuidado maior. Em função da legislação local, outros dados poderão ser classificados como especialmente dignos de proteção. Assim, dados sobre condenações e infrações penais usufruem de uma proteção especial.

3.3.2 Dados pseudonimizados

A “pseudonimização” é uma forma de tratamento de dados pessoais, através da qual, sem a obtenção de informações adicionais se torna impossível atribuí-los a uma pessoa em questão específica, se essas informações adicionais forem mantidas em separado e estiverem sujeitas a medidas técnicas e organizacionais que assegurem que os dados pessoais não possam ser atribuídos a uma pessoa física identificada ou identificável. Os dados pseudonimizados estão abrangidos pelo âmbito de aplicação das normas de proteção de dados e da presente diretriz de proteção de dados.

3.3.3 Dados anonimizados

No caso de dados anonimizados não existe qualquer identificação. Tratam-se de dados, para os quais é impossível restabelecer a identidade das pessoas em questão. Este tipo de dados não é abrangido pela proteção de dados e, consequentemente, também não está sujeito a esta diretriz de proteção de dados.

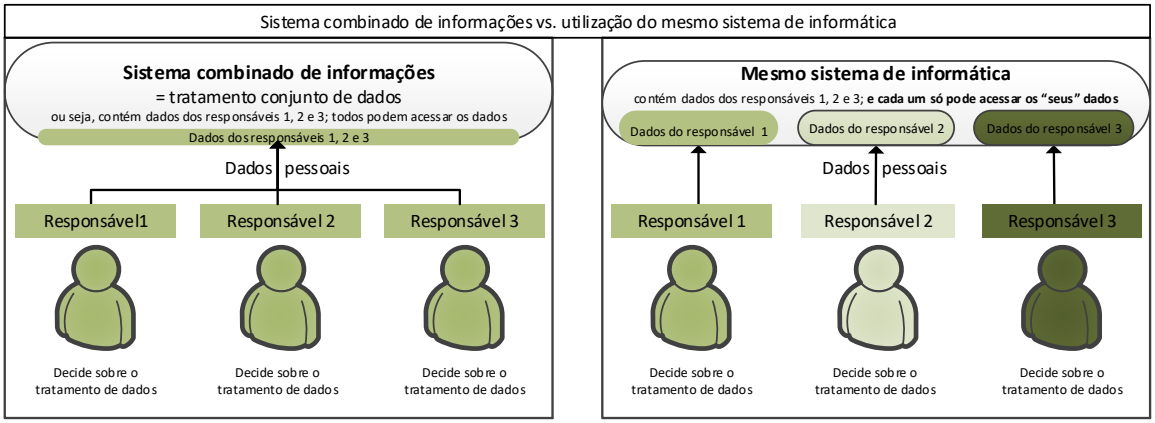
3.4 TRATAMENTO DE DADOS

Por “tratamento” se entende qualquer procedimento, com ou sem recursos a processos automatizados, ou qualquer conjunto de operações relacionado aos dados pessoais, como registro, coleta, organização, ordenação, armazenamento, adaptação ou alteração, seleção, consulta, utilização, divulgação através de transmissão, difusão ou qualquer outra forma de distribuição, comparação ou ligação, limitação, exclusão ou destruição.

3.5 TRATAMENTO CONJUNTO DE DADOS PESSOAIS (SISTEMA COMBINADO DE INFORMAÇÕES)

Fala-se de sistema combinado de informações quando há um **tratamento e uma utilização conjuntos** de dados pessoais por vários responsáveis e cada responsável pode acessar os

dados. A utilização das mesmas ferramentas de informática por várias empresas do Grupo voestalpine não é considerada um sistema combinado de informações.



Em regra geral, os sistemas combinados de informações podem ser adotados em sistemas conjuntos de gestão de fornecedores ou em sistemas de *Customer-Relationship* dentro de um Grupo. Por exemplo, podemos encontrar sistemas combinados de informações também na área do turismo (sistemas de reservas de voos e hotéis), sob a forma das designadas "listas de nomes sujos" de relações comerciais indesejadas em determinados setores, na "lista de alerta" de bancos ou ainda na administração pública (por exemplo, registro central). Ao existir um sistema combinado de informações ou quando vários responsáveis determinarem em conjunto os fins e os meios para o tratamento, os responsáveis serão, em conjunto, responsáveis pela legitimidade do tratamento de dados. Por conseguinte, antes da implementação do sistema combinado de informações o gerente de proteção de dados responsável local deverá ser informado imediatamente.

4 PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

Qualquer tratamento de dados pessoais deverá ser realizado protegendo os direitos, em especial o direito à privacidade, e a liberdade das pessoas em questão segundo os princípios básicos abaixo.

4.1 PRINCÍPIO BÁSICO: LEGALIDADE DO TRATAMENTO

Basicamente, qualquer tratamento de dados pessoais é proibido, exceto se existir uma autorização. A exceção é quando existe uma regulamentação legal expressa ou quando a pessoa em questão tiver autorizado o tratamento de seus dados pessoais (justificativa legal/autorização). Tal autorização é também necessária quando a finalidade de qualquer tratamento de dados for alterada rem relação à finalidade original.
As autorizações e/ou justificativas legais para o tratamento de dados pessoais são:

4.1.1 Interesses legítimos prevalecentes

O tratamento de dados pessoais é legal quando esse ocorrer para a concretização de um interesse legítimo do responsável e não prevalecer sobre os interesses dignos de proteção da pessoa em questão.
Interesses legítimos podem ser, por exemplo, a reivindicação, o exercício e a defesa de direitos legais, o combate à a fraude, as diligências prévias no âmbito de aquisições de empresas etc.

4.1.2 Cumprimento de obrigações contratuais

O tratamento é autorizado desde que seja necessário para o cumprimento de um contrato, cuja parte contratante seja a pessoa em questão ou para a execução de diligências prévias em curso, a pedido da pessoa em questão. Por exemplo, o tratamento de dados pessoais do empregador é legal para realizar cálculos de salários e remunerações para o cumprimento de suas obrigações decorrentes dos contratos de serviços.

4.1.3 Declaração de consentimento (autorização da pessoa em questão)

O tratamento de dados pessoais não está sujeito a quaisquer limitações desde que a pessoa em questão tenha dado a sua autorização inequívoca para um ou vários fins específicos. Uma declaração de consentimento pode ser revogada a qualquer momento e terá de ser obtida de forma prévia, livre e fundamentada. Além disso, por motivos de comprovação, as declarações de consentimento têm de ser obtidas e conservadas por escrito.

4.1.4 Leis, regulamentos e outros normas vinculativas

O tratamento de dados de caráter pessoal é também permitido quando for necessário para o cumprimento de uma obrigação legal por parte do responsável.
Aqui se incluem igualmente obrigações do responsável provenientes de regimes coletivos. Regimes coletivos são acordos corporativos, contratos coletivos, acordos salariais entre o empregador e os representantes dos trabalhadores no âmbito das possibilidades do respectivo direito trabalhista local. Os regulamentos têm de se destinar a uma finalidade concreta do acordo desejado e são aplicáveis contexto do direito local de proteção de dados.

4.1.5 Interesses vitais da pessoa em questão

Um tratamento de dados é ainda autorizado para proteger interesses vitais da pessoa em questão ou de uma outra pessoa física.

4.1.6 Tratamento de dados sensíveis (categorias especiais de dados)

O tratamento de dados sensíveis (categorias especiais de dados) só ser realizado de forma muito limitada no âmbito das disposições de proteção de dados. Por exemplo, quando isso for requerido por lei, se a pessoa em questão o tiver especificamente autorizado ou for necessário para efeitos de assistência médica para a avaliação da capacidade de trabalho. Portanto, antes do tratamento de dados sensíveis (categorias especiais de dados) é necessário informar o respectivo gerente de proteção de dados local responsável.

4.2 PRINCÍPIO DA LIMITAÇÃO DA FINALIDADE E MATERIALIDADE

Qualquer tratamento de dados pessoais precisa ter como base uma **determinada finalidade legítima**. O tratamento não pode ser realizado de uma forma que não esteja de acordo com as finalidades definidas.

4.3 PRINCÍPIO DA TRANSPARÊNCIA

O princípio da transparência implica a garantia de salvaguardar a visão do indivíduo, ao qual se refere o tratamento de dados pessoais. A pessoa em questão tem de ser informada sobre o tratamento dos seus dados pessoais. Além disso, os dados pessoais têm de ser obtidos junto da própria pessoa em questão.
Para atender ao princípio da transparência, os responsáveis têm obrigações de informação e de divulgação. No caso do tratamento de dados pessoais, a pessoa em questão tem de, pelo menos, reconhecer o seguinte ou ser informada de forma correspondente:

- **Identidade** do responsável (ou seja, onde serão obtidos os dados);
- **Finalidade (s) e base(s) jurídica(s)** odo tratamento, bem como os interesses legítimos que assistem ao tratamento de dados;
- Terceiros, a quem os dados poderão ser reencaminhados (**círculo de receptores**);
- Tipos e categorias de dados compilados, bem como a base jurídica para a transferência internacional de dados;
- Duração do tratamento de dados, direitos da pessoa em questão, direitos de recurso, se a disponibilização dos dados pessoais teve indicação legal ou contratual ou se é necessária para uma celebração de contrato, se a pessoa em questão está obrigada a disponibilizar os dados pessoais, e quais as possíveis consequências que teria a sua não disponibilização: decisões automatizadas.

4.4 PREVENÇÃO E ECONOMIA DE DADOS

Por prevenção e economia de dados se entende que só deverá ser compilada, tratada e utilizada a quantidade de dados pessoais necessária à concretização da finalidade pretendida e legítima.
Quando for possível para a concretização da finalidade e o esforço for proporcional à finalidade pretendida, então deverão ser utilizados dados anonimizados ou pseudonimizados.
Os dados pessoais não podem ser guardados para potenciais finalidades futuras, a menos que a legislação local o estipule ou autorize.

4.5 EXCLUSÃO

Os dados pessoais, que já não sejam necessários após os prazos legais ou que estejam relacionados a processos corporativos, terão de ser excluídos. Para isso, as empresas do Grupo voestalpine estão obrigadas, em conjunto com o gerente de proteção de dados local, a elaborar procedimentos de exclusão de dados pessoais.
Se, em casos individuais, existirem indícios de que os dados pessoais sejam importantes por motivos de interesse público para efeitos de arquivo, econômicos ou de pesquisa histórica ou para efeitos estatísticos, terá de se esclarecer em conjunto com o gerente de proteção de dados da divisão e do Grupo, se a continuidade do tratamento dos dados é admissível para essa finalidade.

4.6 DECISÕES/CARACTERIZAÇÃO DE PERFIL

O tratamento automatizado de dados pessoais, através do qual características individuais de personalidade (por ex.: avaliação dos perfis de capacidade ou outras avaliações no âmbito do desempenho laboral, análise da situação econômica etc.) são analisadas, não pode constituir a base exclusiva para decisões com consequências jurídicas ou efeitos

negativos consideráveis para as pessoas em questão. A pessoa em questão tem de ser informada sobre o fato e o resultado de uma decisão automatizada, sendo-lhe dada a possibilidade de tomar uma posição e de contestar a decisão.

4.7 EXATIDÃO

Os dados pessoais a tratar têm de ser corretos, completos e, sempre que necessário, atualizados. Deverão ser encontradas medidas para assegurar que os dados não pertinentes, incompletos ou desatualizados sejam excluídos, corrigidos, complementados ou atualizados.

4.8 CONFIDENCIALIDADE E SEGURANÇA DE DADOS

Os dados pessoais estão sujeitos ao sigilo de dados e devem ser tratados de forma rigorosamente confidencial. O acesso a dados pessoais por colaboradores só está autorizado na medida em que seja necessário ao cumprimento dos respectivos trabalhos (“princípio *need-to-know*”). Os colaboradores não podem usar dados pessoais para efeitos particulares ou econômicos, transmiti-los a pessoas não autorizadas ou disponibilizá-los de qualquer outra forma.
No início da relação trabalhista, o colaborador tem de ser orientado sobrea obrigação de manter o sigilo de dados. Essa obrigação se mantém igualmente depois de terminada a relação trabalhista.
No tratamento de dados pessoais, deverão ser implementadas medidas organizacionais e técnicas apropriadas para impedir o acesso de pessoas não autorizadas, os tratamentos indevidos ou transmissões, assim como a perda, a alteração e a destruição intencionais. No geral, através da implementação de medidas técnicas e organizacionais é necessário que seja alcançado um nível de proteção adequado contra o risco de violação aos direitos e à liberdade da pessoa em questão. Essas medidas têm de se orientar pelo desenvolvimento tecnológico, pelos custos de implementação, pelos riscos decorrentes do tratamento e pela necessidade de proteção dos dados.

4.9 INTERNET E TELECOMUNICAÇÕES

Se forem coletados, tratados e utilizados dados pessoais provenientes de páginas na internet ou de aplicativos de empresas do Grupo, as pessoas em questão deverão ser informadas sobre o fato através de avisos sobre proteção de dados e, se for o caso, através de avisos sobre *cookies*. Os avisos sobre a proteção de dados e cookies deverão ser integrados de forma a serem facilmente identificáveis e estarem imediatamente sempre acessíveis e disponíveis às pessoas em questão.
Se as empresas do Grupo os criarem para a geração de perfis do usuários com base na avaliação do comportamento de utilização de páginas na internet e aplicativos (*tracking*), então as pessoas em questão precisarão sempre ser informadas através dos avisos sobre proteção de dados e *cookies*. Esse *tracking* só se poderá ocorrer quando a legislação local o autorizar. Sempre que necessário deverá ser obtida a autorização da pessoa em questão para a geração de perfis do usuário.

4.10 DIREITOS DA PESSOA EM QUESTÃO

As pessoas em questão têm não apenas o direito à informação sobre seus dados tratados (ver 4.3), mas também o direito sobre a informação, correção, exclusão, limitação do tratamento, transmissão de dados e contestação do tratamento de dados.
Em caso de perguntas das pessoas em questão dirigidas a uma empresa do Grupo, elas deverão ser imediatamente transmitidas ao gerente de proteção de dados local, devendo ser acordado com ele o procedimento a seguir. Caso os dados apenas sejam tratados por representação, a solicitação deverá ser reencaminhada ao gerente de proteção de dados local responsável.

5 TRANSFERÊNCIA TRANSFRONTEIRIÇAS DE DADOS PESSOAIS

Em cada transferência transfronteiriça de dados pessoais, o gerente de proteção de dados local deverá ser envolvido e deverão ser observados os respectivos requisitos locais de transferência de dados pessoais ao país estrangeiro.
Em caso de transferência de dados pessoais de uma empresa do Grupo voestalpine para um receptor em um outro país diferente da empresa voestalpine em questão, o receptor tem, independentemente de se tratar de uma outra empresa do Grupo voestalpine, de garantir um nível de proteção equivalente ao desta diretriz de proteção de dados e ao dos regulamentos europeus de proteção de dados.
Neste contexto, é DEVE-SE OBSERVAR que o mesmo é válido no caso de o receptor dos dados de caráter pessoal se localizar no mesmo país da empresa voestalpine, mas recorrer a um subcontratado que tenha sede em outro país que não o da empresa voestalpine em questão.
Instrumentos adequados que comprovem um nível de proteção de dados equivalente poderão ser, entre outros:

- O receptor tem sede no Espaço Econômico Europeu e, por conseguinte, está sujeito aos regulamentos de proteção de dados;
- O receptor tem sede em um país que, de acordo com a determinação da Comissão Europeia, dispõe de um nível adequado de proteção de dados ("países com estatuto equivalente");
- Acordo com as cláusulas contratuais padrão da UE em sua versão atualmente em vigor;
- Participação do receptor em um sistema de certificação reconhecido pela UE para a garantia de um nível de proteção de dados apropriado (por ex.: *EU-U.S. Privacy Shield*).

Se não puder ser comprovado um nível de proteção de dados equivalente, a transferência transfronteiriça de dados pessoais também poderá, sujeita a outros requisitos locais, ser autorizada em determinados casos. Exemplos disso são:

- A pessoa em questão autorizou expressamente a transferência de dados proposta depois de ter sido devidamente informada sobre riscos existentes possíveis decorrentes de tal transferência de dados;
- A transferência é necessária para a celebração ou o cumprimento de um contrato do interesse da pessoa em questão realizado pelo responsável com outra pessoa física ou jurídica;
- A transferência é necessária para a reinvindicação, o exercício ou a defesa de direitos legais.

DEVE-SE OBSERVAR neste contexto, que não existe nenhum privilégio do Grupo. Uma transferência transfronteiriça dentro do Grupo de dados pessoais está igualmente sujeita a essas disposições.

6 REGULAMENTOS COMPLEMENTARES PARA EMPRESAS DO GRUPO COM SEDE OU ATIVIDADE ECONÔMICA NO ESPAÇO ECONÔMICO EUROPEU

Empresas,

- com sede no Espaço Econômico Europeu, e
- aquelas, que realizam o tratamento de dados, que oferecem bens e/ou serviços à pessoa em questão no Espaço Econômico Europeu ou observam seu comportamento,

têm, além disso, de observar as disposições que se seguem relativas ao diretório de procedimentos, assim como à avaliação de riscos/do impacto da proteção de dados:

6.1 DIRETÓRIO DE PROCEDIMENTOS

As empresas anteriormente referidas (tanto os responsáveis como o executante de tarefas) têm de introduzir eventuais tratamentos de dados pessoais em um diretório de procedimentos interno[5] em conformidade com as disposições legais aplicáveis, em especial o DSGVO[5], devendo dispor de um diretório de procedimentos completo, nos termos do DSGVO[5], o mais tardar a partir de 1 de maio de 2018.

No diretório de procedimentos para responsáveis deverão constar, pelo menos, os seguintes dados:

Categoria de dados	Informações relativas a gestão administração de recursos humanos e pagamento de pessoal
Pessoa de contato	» *Pessoa de contato responsável da organização de proteção de dados* » *Nome e dados de contato (endereço, endereço e e-mail e número de telefone) do responsável, assim como* » *Nome e dados de contato de um eventual responsável pela proteção de dados nos termos do DSGVO[5];*
Finalidades do tratamento	*Gerenciamento de dados de colaboradores para cálculo de salários, remunerações e pagamentos e cumprimento de obrigações de registro, informação e notificações, na medida em que isso seja necessário devido a leis ou legislação coletiva ou obrigações trabalhistas, bem como para a conservação eletrônica e geração de documentos em eFile/eForms para o cumprimento de obrigações de registro, informação, notificações.*

[5] Nos termos das disposições do DSGVO – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas física no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretriz 95/46/CE (Regulamento Geral sobre a Proteção de Dados – DSGVO).

Descrição das categorias das pessoas em questão	» *Colaboradores ativos ou aposentados, grupos de pessoas em situação semelhante a colaboradores, colaboradores temporários, colaboradores autônomos, aprendizes, voluntários e estagiários* » *Instituições bancárias, companhias de seguros e outros prestadores de serviços* » *Usuário do sistema (externo e interno)*
Descrição das categorias de dados pessoais	» *Número pessoal* » *Nome* » *Cargo* » *Data e local de nascimento* » *Estado civil* » *Nacionalidade* » *Endereço do local de trabalho* » *Tipo de medida (nova contratação, recontratação, transferência, alteração de salário, termo da relação contratual, subsídio, entrada para a aposentadoria etc.)* » *Estatuto profissional (inativo/ativo/saiu da empresa/aposentado)* » *etc.*
As categorias de receptores, aos quais os dados pessoais foram ou serão divulgados	» *Autoridades, entidades públicas* » *Credores da pessoa em questão* » *Representante legal* » *Empresa do grupo, no âmbito de aplicação do DSGVO*[5] » *Empresas de terceirização de pessoal* » *Companhias de seguros etc.*
Transferências de dados pessoais em um país fora do Espaço Econômico Europeu	*Empresas (do Grupo); endereço, dados de contato de uma pessoa de contato, finalidade e base jurídica para a transferência de dados*
Avaliação de riscos, bem como, se necessário, avaliação do impacto da proteção de dados	*Breve apresentação dos riscos identificados, medidas encontradas para minimizar os riscos e as razões para a decisão da introdução do tratamento de dados em questão face aos riscos estabelecidos.*
Quando possível: » Períodos de armazenamento » Descrição geral das medidas técnicas e organizacionais nos termos do artigo 32.º, n.º 1 do DSGVO[5]	

Para assegurar um procedimento uniforme, o Grupo de criação dos diretórios de procedimentos deverá utilizar as tabelas ou ferramentas de informática disponibilizadas pela Comissão de Proteção de Dados do Grupo.

6.2 AVALIAÇÃO DE RISCOS/DO IMPACTO DA PROTEÇÃO DE DADOS

No âmbito da criação do diretório de procedimentos, deverá ser previamente realizada uma avaliação de riscos pelo responsável da respectiva área em colaboração com o gerente de proteção de dados local. Se o tratamento de dados pessoais estiver associado a um provável risco elevado aos direitos e à liberdade de pessoas físicas devido ao tipo, ao âmbito, às circunstâncias e às finalidades do tratamento ou devido à utilização de novas tecnologias, então o responsável pela respectiva área deverá, em conjunto com o gerente de proteção de dados, realizar uma avaliação prévia das consequências dos procedimentos de tratamento previstos com vista à proteção dos dados pessoais ("**avaliação do impacto da proteção de dados**"). O resultado e as eventuais medidas encontradas no âmbito da avaliação do impacto da proteção de dados deverão ser igualmente registrados no diretório de procedimentos. Uma avaliação do impacto da proteção de dados deverá ser efetuada em especial, quando:

- forem tratados dados sensíveis (categorias especiais de dados pessoais) ou dados pessoais sobre condenações e infrações penais de uma forma abrangente;
- ocorrer uma avaliação sistemática e abrangente de aspectos pessoais de pessoas físicas, baseada em tratamento automatizado, incluindo a caracterização de perfil, que por sua vez servirá de base à tomada de decisões que possam ter consequências legais para pessoas físicas ou que as possam afetar de forma semelhante;
- houver um monitoramento sistemático e abrangente de áreas de acesso público.

Em caso de dúvida, a necessidade de uma avaliação do impacto da proteção de dados deverá ser previamente acordada entre o responsável pela respectiva área em conjunto com o gerente de proteção de dados local.

7 VIOLAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS ("VIOLAÇÃO DA PROTEÇÃO DE DADOS")

São consideradas violações de proteção de dados pessoais a destruição, a perda, a alteração ou a divulgação acidental ou indevida de dados. Em caso de violação da proteção de dados pessoais (por exemplo, devido a *hacking*, perda de disco externo de dados etc.) deverão ser cumpridas as obrigações de comunicação e de informação do Grupo (Service Desk da voestalpine group-IT GmbH, Linz/Áustria[6]) nos termos da diretriz da organização de proteção de dados da voestalpine AG, assim como em conformidade com a legislação local.

Além disso, o gerente de proteção de dados local deverá comunicar o fato o mais rapidamente possível aos gerentes de proteção de dados da divisão e do Grupo em conformidade com a diretriz da organização de proteção de dados da voestalpine AG.

[6] Atendimento ao cliente: Fone: +43 50304 15 9191; E-mail: helpdesk@voestalpine.com

8 ENTRADA EM VIGOR

Esta diretriz do Grupo na presente versão entra em vigor em 1 de abril de 2017 e serve como instrução a todos os colaboradores do Grupo voestalpine.
Esta diretriz de proteção de dados será, se necessário, atualizada por decisão da diretoria da voestalpine AG e, eventualmente, complementada apenas para determinados países ou regiões em conformidade com os regulamentos e diretrizes em vigor.

Linz, 6 de março de 2017

W. Eder	H. Eibensteiner	F. Kainersdorfer
R. Ottel	F. Rotter	P. Schwab