ARBONIA

Política de tratamento de dados (Política de Proteção de Dados)

16 de junho de 2020

ARBONIA

ÍNDICE

1 FINALIDADE E OBJETIVO 3
2 CONCEITOS E DEFINIÇÕES 4
3 ÂMBITO 6
3.1 Âmbito organizativo 6
3.2 Leis, regulamentos, normas e políticas 6
4 BASE REGULAMENTAR 7
5 PAPÉIS E RESPONSABILIDADES 7
6 PRINCÍPIOS DE PROTEÇÃO DOS DADOS NO TRATAMENTO DE DADOS PESSOAIS 10
6.1 Equidade, licitude e transparência 10
6.2 Limitação das finalidades 12
6.3 Minimização de dados 12
6.4 Corretos e atualizados 12
6.5 Período de conservação limitado 12
6.6 Confidencialidade e segurança dos dados 13
7 OUTRAS OBRIGAÇÕES AO ABRIGO DO RGPD OU OUTRAS NORMAS DE PROTEÇÃO DE DADOS SIMILARES APLICÁVEIS 13
7.1 Princípio da responsabilidade 13
7.2 Regras para o subcontratante (sobretudo parceiros de prestação de serviços) 14
7.2.1 Disponibilização de dados pessoais ao subcontratante (saída de dados) 14
7.2.2 Receção de dados pessoais como subcontratante (entrada de dados) 15
7.3 Transmissão transfronteiriça de dados pessoais 15
7.4 Tratamento de um pedido de um titular dos dados 16
7.5 Realização de uma avaliação de impacto sobre a proteção de dados 17
8 SEGURANÇA DOS DADOS PESSOAIS 18
9 NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA DOS DADOS 20
10 CONSEQUÊNCIAS DO INCUMPRIMENTO 21
11 DIVERGÊNCIAS 21
12 INFORMAÇÕES 21
13 ENTRADA EM VIGOR 21

ARBONIA

1 FINALIDADE E OBJETIVO

Para cumprir as obrigações legais e contratuais, é imprescindível recolher e tratar dados pessoais. Neste contexto, é obrigatório cumprir as normas de proteção de dados aplicáveis em cada país. Esta política apresenta o modo como a Arbonia AG e as sociedades do grupo (adiante designadas conjuntamente por "Arbonia", ou cada sociedade do grupo é adiante designada por "sociedade do grupo") tratam os dados pessoais. As disposições aqui estipuladas são consideradas normas mínimas. Se a lei de proteção de dados local previr normas mais rigorosas, estas deverão ser cumpridas. Deverão ser igualmente respeitadas todas as normas locais relativas à implementação desta política.

A finalidade desta política de tratamento de dados ("Política de Proteção de Dados") é a definição, implementação, conservação e melhoria contínua, pela Arbonia, do cumprimento da proteção de dados, de acordo com os requisitos do Regulamento Geral de Proteção de Dados da União Europeia 2016/679 (**RGPD**) e todas as demais leis de proteção de dados locais aplicáveis (conjuntamente, as **leis de proteção de dados aplicáveis**).

O incumprimento das leis de proteção de dados aplicáveis coloca a Arbonia em risco de danos para a reputação e de multas pecuniárias substanciais (por ex. até 4 % do volume de negócios mundial, ao abrigo do RGPD). Pode além do mais expor os nossos clientes e colaboradores a determinados riscos de proteção de dados, como por exemplo furto de identidade ou perdas financeiras. O cumprimento das leis de proteção de dados aplicáveis ajuda-nos a manter a confiança na organização da Arbonia e a garantir o sucesso da nossa atividade de negócio.

O objetivo desta Política de Proteção de Dados é disponibilizar o enquadramento para esse cumprimento da proteção de dados no seio da Arbonia. Em particular, visa implementar princípios de base para o tratamento de dados pessoais (**princípios de proteção de dados**), conforme definidos no Ponto 6, e pelos quais as empresas da Arbonia são responsáveis quando agem como responsáveis pelo tratamento ao abrigo do RGPD, regulamenta a necessidade de medidas técnicas e organizativas adequadas e a notificação de incidentes de proteção de dados, como normas mínimas para todas as empresas da Arbonia e aplica-se a todos os colaboradores da Arbonia, bem como aos membros do conselho de administração da Arbonia AG.

Disponibiliza ainda um enquadramento para requisitos adicionais, aplicável aos responsáveis pelo tratamento e aos subcontratantes ao abrigo do RGPD (ou leis de proteção de dados similares aplicáveis), conforme descrito no Ponto 7.

2 CONCEITOS E DEFINIÇÕES

Para os fins desta Política de Proteção de Dados, aplicam-se os seguintes conceitos e definições:

Dados anonimizados significa que a identidade pessoal nunca poderá ser rastreada por ninguém ou que a identidade pessoal só poderia ser rastreada mediante um esforço desproporcionado de tempo, custos e trabalho.

Leis de proteção de dados aplicáveis são o Regulamento Geral de Proteção de Dados da União Europeia 2016/679 (**RGPD**) ou todas as demais leis de proteção de dados nacionais aplicáveis que prevejam normas similares.

Responsável do processo de negócio é uma pessoa singular que assume responsabilidade por esta Política de Proteção de Dados e que é responsável pelo tratamento de dados pessoais e pela respetiva aplicação de TI.

Consentimento corresponde ao consentimento do titular dos dados, ou seja, qualquer manifestação de vontade livre, específica, informada e inequívoca, sob a forma de uma declaração outro ato positivo claro, com a qual o titular dos dados dê a conhecer que consente o tratamento dos dados pessoais que lhe digam respeito.

Responsável pelo tratamento é a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento de dados pessoais.

Incidente de segurança dos dados é um acontecimento relativamente ao qual existe uma legítima suspeita de terem sido registados, recolhidos, alterados, copiados, transmitidos e utilizados dados pessoais de forma ilegítima. Pode dizer respeito a ações de terceiros ou de colaboradores da empresa.

Titular dos dados é uma pessoa singular identificada ou identificável. Uma pessoa singular identificável é uma pessoa que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

O **subcontratante** é uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Registo das atividades de tratamento dos dados é um registo do tratamento de dados sob a responsabilidade do responsável pelo tratamento. Este registo inclui todos os seguintes

dados: (i) nome e dados de contacto do responsável pelo tratamento e, se aplicável, do corresponsável pelo tratamento, do substituto do responsável pelo tratamento e do coordenador da proteção de dados local; (ii) as finalidades do tratamento, (iii) uma descrição das categorias de titulares dos dados e da categoria de dados pessoais; (iv) as categorias dos destinatários a quem foram ou serão divulgados dados pessoais, incluindo destinatários em países terceiros; (v) se aplicável, transmissão de dados pessoais a um país terceiro, incluindo a identificação do país terceiro e a documentação de garantias adequadas; (vi) os períodos previstos para o apagamento das diversas categorias de dados pessoais; (vii) uma descrição geral das medidas de segurança técnicas e organizativas.

Encarregado da proteção de dados ou coordenador da proteção de dados ou **CPD** é a pessoa descrita no Ponto 5.

Dados pessoais significa todas as informações (incluindo dados pessoais de categorias especiais) relativas ao titular dos dados, ou seja, relativas a uma pessoa singular identificada ou identificável, como por exemplo nome, data de nascimento, endereço de correio eletrónico, religião, dados de localização, dados eletrónicos (endereço IP, dados de localização, etc.), números de identificação (número da segurança social, número de identificação pessoal, etc.), características físicas (sexo, cor da pele, cor do cabelo, etc.), dados de cliente, e muitos outros), que estejam protegidos ao abrigo de um regulamento de proteção de dados aplicável.

Tratamento ou **tratar** significam qualquer operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Pseudonimização significa o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Dados pessoais de categorias especiais são dados sobre a origem racial ou étnica, opinião política, perspetivas religiosas ou filosóficas, condenações criminais, pertença a sindicatos, saúde ou orientação sexual do titular dos dados, ou dados genéticos, dados biométricos, para fins de identificação inequívoca de uma pessoa singular.

Países terceiros são todas as nações não pertencentes à União Europeia ou ao Espaço Económico Europeu ou um país com um nível de proteção adequado, considerado adequado pela Comissão Europeia (ver Lista de países com nível de proteção de dados adequado:

< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Terceiros significa qualquer outra pessoa, que não o titular dos dados, o responsável pelo tratamento ou o subcontratante (incluindo, por ex. parceiros de negócios, subempreiteiros, agências de notação de crédito e outros), bem como pessoas que, sob a autoridade direta do responsável pelo tratamento ou subcontratante, estão autorizadas a fazer o tratamento de dados pessoais. No contexto do tratamento de dados pessoais ao abrigo de uma autorização, os subcontratantes não são, do ponto de vista legal, considerados terceiros, a abrigo da lei de proteção de dados, já que estão legalmente atribuídos ao responsável pelo tratamento.

3 ÂMBITO

3.1 Âmbito organizativo

Esta Política de Proteção de Dados aplica-se a todas as sociedades do grupo Arbonia, a todos os colaboradores da Arbonia e aos membros do conselho de administração da Arbonia AG. É obrigatória por lei a sua implementação em todas as sociedades do grupo.

3.2 Leis, regulamentos, normas e políticas

Esta Política de Proteção de Dados abrange os requisitos do RGPD e os princípios de proteção de dados reconhecidos internacionalmente, sem que substitua a lei nacional em vigor. É um complemento às leis de proteção de dados nacionais aplicáveis. A lei nacional em vigor terá precedência em caso de conflito com esta Política de Proteção de Dados ou se previr requisitos mais exigentes do que esta Política de Proteção de Dados. Os conteúdos desta Política de Proteção de Dados têm igualmente de ser cumpridos se não estiver disponível legislação nacional correspondente.

Se esta Política de Proteção de Dados estiver em contradição com as disposições legais de um determinado país, as disposições específicas desta Política de Proteção de Dados poderão ser integradas numa política local, em conciliação com o Head Legal & Compliance. Não podem no entanto ser alterados os conteúdos de base e a finalidade das disposições em causa.

4 BASE REGULAMENTAR

Esta Política de Proteção de Dados baseia-se no RGPD e nos princípios de base de proteção de dados globalmente aceites.

5 PAPÉIS E RESPONSABILIDADES

- O diretor executivo de uma sociedade do grupo[1] é responsável por:
  1. garantir, em última instância, que cada pessoa coletiva cumpre as suas obrigações relativas ao tratamento de dados pessoais.
  2. garantir o cumprimento dos requisitos decorrentes desta Política de Proteção de Dados (incluindo a notificação de incidentes no domínio da segurança dos dados).
  3. garantir que o responsável do processo de negócio preenche e atualiza o "Registo de atividades de tratamento" ao nível da sociedade do grupo.
  4. nomear um encarregado da proteção dos dados formal (interno ou externo) (adiante designado por "encarregado da proteção de dados") se a lei de proteção de dados local aplicável o exigir, e comunicar anualmente esta pessoa nomeada, durante o ano, ao Head Legal & Compliance e à Internal Audit.
  5. nomear um gestor da proteção de dados local (adiante designado por "coordenador da proteção de dados") se a lei de proteção de dados local aplicável não estipular um encarregado da proteção de dados local formal. Esta pessoa nomeada deverá ser comunicada anualmente, durante o ano, ao Head Legal & Compliance e à Internal Audit.

- O coordenador da proteção de dados ou encarregado da proteção de dados local definido[2] pelo diretor executivo de uma sociedade do grupo tem de:
  1. monitorizar o cumprimento desta Política de Proteção de Dados e das instruções do responsável pelo tratamento ou do subcontratante relativamente à proteção dos dados pessoais, incluindo a transmissão de responsabilidades e as respetivas verificações.
  2. informar, aconselhar e supervisionar o responsável pelo tratamento ou o subcontratante e os colaboradores que executam as obrigações de tratamento ao abrigo desta Política de Proteção de Dados.
  3. se tal lhe for solicitado, fornecer conselhos sobre uma avaliação de impacto sobre a proteção de dados e monitorizar os respetivos resultados, bem como responder a outras perguntas sobre dados pessoais que sejam da sua competência ao abrigo desta Política de Proteção de Dados.
  4. monitorizar e manter atualizado o "Registo de atividades de tratamento" que deve ser mantido por cada sociedade do grupo e preenchido pelos responsáveis dos

[1] Para sociedades do grupo sem atividade operacional, esta responsabilidade será definida separadamente, em conjunto com o Head Legal & Compliance.
[2] Para sociedades do grupo sem atividade operacional, esta responsabilidade será definida separadamente, em conjunto com o Head Legal & Compliance.

processos de negócio, bem como, anualmente, durante o ano, confirmar a integridade e atualidade desta lista junto do Head Legal & Compliance.
5. servir de ponto de contacto do Head Legal & Compliance e manter este último atualizado sobre a responsabilidade, riscos e problemas relacionados com a proteção de dados pessoais.
6. apoiar o TI responsável pela aplicação de TI na verificação e autorização de novas aplicações de TI, ao nível da sociedade do grupo, para tratamento de dados pessoais, e qualquer aplicação de TI de tratamento de categorias especiais de dados pessoais, da perspetiva da proteção de dados.
7. aprovar a transmissão de dados pessoais para um país terceiro, da perspetiva da proteção de dados (ver também abaixo, n.º 14).
8. servir de ponto de contacto local para a autoridade de controlo para questões relacionadas com o tratamento de dados e colaborar com a autoridade de controlo,
9. tratar de pedidos de informação de colaboradores envolvidos no tratamento de dados pessoais.
10. responder a pedidos de titulares dos dados, sobre os respetivos dados pessoais na posse da Arbonia ou, em caso de pedido a várias sociedades do grupo Arbonia, tratar o pedido em coordenação com o Corporate IT (ver também abaixo, n.º 7.4)
11. juntamente com o subcontratante, analisar e aprovar contratos ou acordos elaborados ou previamente analisados pelos responsáveis de processos de negócio que possam implicar o tratamento dos dados pessoais por conta da Arbonia, conforme definido no ponto 7.2.
12. monitorizar o encarregado da proteção de dados local externo, caso tenha sido nomeado.
13. notificar incidentes no domínio da segurança dos dados , de acordo com a instrução de Data Breach Notification (ver abaixo n.º 9, bem como a "Arbonia Data Breach Policy").

- O IT-Board, conjuntamente com o Corporate IT, é responsável por:
  1. definir as normas aplicáveis em todo o grupo, bem como controlos de TI gerais (GITC) que deverão ser cumpridos aquando do armazenamento de dados.

- O TI responsável em cada caso e que presta assistência a uma sociedade do grupo é responsável por:
  1. mediante normas correspondentes, políticas e a execução de controlos de TI gerais (GITC), garantir que os sistemas, os serviços e o equipamento utilizados para armazenar dados cumprem normas de segurança plausíveis (controlo de acessos/apagamento de dados), considerando o estado mais atual da tecnologia, os custos de implementação e o tipo, âmbito, contexto e finalidade do tratamento, bem como as diversas probabilidades e gravidade dos efeitos sobre s direitos e liberdades das pessoas singulares.
  2. envidar esforços no sentido de o responsável pelo tratamento e o subcontratante implementarem medidas técnicas e organizativas adequadas, a fim de garantir um nível de proteção ajustado ao risco, conforme previsto no ponto 8.

3. após consulta do coordenador da proteção dos dados ou do responsável pelo tratamento, analisar e aprovar, da perspetiva da proteção dos dados, novas aplicações de TI para o tratamento de dados pessoais.
4. realizar verificações e análises regulares para garantir que o hardware e o software de segurança funcionam corretamente. Os resultados dos controlos de proteção dos dados têm de ser comunicados ao encarregado da proteção dos dados competente.
5. avaliar a segurança dos dados de todos os serviços de terceiros (por ex. subcontratante) a que a empresa recorre para o tratamento de dados pessoais (por ex. serviços de *cloud computing*, etc.)
6. manter uma lista de incidentes no domínio da segurança dos dados e comunicar incidentes de segurança dos dados ao Corporate IT.
7. coordenar e responder a pedidos de titulares dos dados de informações sobre os dados pessoais sobre o titular dos dados que estejam na posse da sociedade do grupo Arbonia a que o TI em causa presta assistência (ver também abaixo o n.º 7.4)
8. notificar os incidentes ou riscos detetados no domínio da segurança dos dados, conforme definido na política de Data Breach Notification (ver abaixo o n.º 9, bem como a "Arbonia Data Breach Policy")

- O Corporate IT, em colaboração com o TI responsável pela assistência a uma sociedade do grupo, é responsável por
  1. realizar verificações e análises regulares para garantir que o hardware e o software de segurança funcionam corretamente. Os resultados dos controlos de proteção dos dados têm de ser comunicados ao encarregado da proteção dos dados competente.
  2. Manter uma lista central de incidentes no domínio da segurança dos dados.
  3. notificar os incidentes ou riscos detetados no domínio da segurança dos dados, conforme definido na política de Data Breach Notification (ver abaixo o n.º 9, bem como a "Arbonia Data Breach Policy").

- A Internal Audit é responsável por:
  1. por ocasião das auditorias realizadas de acordo com o plano de auditorias ordinário, no âmbito de uma auditoria baseada no risco, verificar se os procedimentos organizativos cumprem as especificações essenciais desta Política de Proteção de Dados.

- Os responsáveis dos processos de negócio são responsáveis por:
  1. garantir a participação adequada e atempada do encarregado da proteção de dados local em todos os assuntos necessários para avaliar o tratamento de dados pessoais.
  2. juntamente com o subcontratante, elaborar ou pré-aprovar todos os contratos ou acordos que possam implicar o tratamento de dados pessoais por conta da Arbonia, conforme descrito no ponto 7.2.
  3. preencher e manter atualizado o "Registo de atividades de tratamento" mantido pela respetiva sociedade do grupo e, anualmente, até ao final de abril, confirmar a integridade e atualidade das respetivas entradas junto do coordenador da proteção dos dados ou do encarregado da proteção dos dados.

4. antes da implementação de novas atividades de tratamento de dados pessoais, avaliar os riscos que daí podem resultar para a personalidade e os direitos fundamentais do titular dos dados e, em caso de risco previsivelmente elevado do tratamento, realizar previamente uma avaliação de impacto sobre a proteção de dados.

6 PRINCÍPIOS DE PROTEÇÃO DOS DADOS NO TRATAMENTO DE DADOS PESSOAIS

Qualquer sociedade do grupo que atue como responsável pelo tratamento de dados pessoais tem de garantir que consegue **comprovar o cumprimento dos seguintes 6 (seis) princípios fundamentais de proteção dos dados:**

1. Tratar dados pessoais apenas se for possível comprovar uma base legal válida entre as leis de proteção de dados em vigor e se o titular dos dados for informado sobre a identidade e os dados de contacto do responsável pelo tratamento, o tipo e os fundamentos legais dos dados pessoais registados, os respetivos períodos de conservação e a finalidade de registo dos dados pessoais

2. cumprir sempre a finalidade para a qual os dados pessoais foram registados

3. registar/tratar apenas dados pessoais que sejam realmente necessários

4. manter dados pessoais corretos e apagar dados pessoais incorretos

5. conservar dados pessoais apenas durante os períodos de conservação legais efetivamente necessários

6. tratar os dados pessoais com confidencialidade e partilhar apenas o estritamente necessário

6.1 Equidade, licitude e transparência

Os dados pessoais podem ser tratados apenas para fins especialmente permitidos, conforme descrito abaixo; este procedimento tem de ser transparente. Por conseguinte, os dados pessoais deverão ser tratados com licitude e equidade, respeitando os direitos individuais dos titulares dos dados. Tal pode incluir dados pessoais que a Arbonia receba diretamente de um titular dos dados (por ex. mediante o preenchimento de formulários ou correspondência postal, telefónica, por correio eletrónico ou outra), bem como dados pessoais que a Arbonia receba de terceiros.

Ao abrigo das leis de proteção de dados em vigor, os dados pessoais podem ser tratados legitimamente com base em **cinco fundamentos legítimos** (**fundamentos legítimos**), de acordo com o RGPD. Estes fundamentos incluem:

1. **Contrato:** O tratamento de dados pessoais é necessário para a execução de um contrato em que uma das partes é o titular dos dados ou para a execução de medidas pré-contratuais a pedido do titular dos dados, ou

2. **Consentimento:** O tratamento de dados pessoais baseia-se no consentimento (modelo de *opt-in*) do titular dos dados para uma ou várias finalidades específicas. O consentimento tem de ser documentado ou

3. **Obrigação legal:** O tratamento de dados pessoais baseia-se numa obrigação legal da Arbonia. O tipo e o âmbito do tratamento dos dados tem de ser necessário para a atividade de tratamento legalmente permitida e cumprir as condições legais em vigor, ou

4. **Interesse público:** O tratamento é necessário para a realização de uma tarefa de interesse público, ou

5. **Legítimos interesses de negócio:** O tratamento é proporcional face a legítimos interesses de negócio da Arbonia ou do terceiro a quem são divulgados os dados pessoais, exceto se tiverem precedência os interesses ou os direitos e liberdades fundamentais do titular dos dados. Legítimos interesses são, em geral, interesses de cariz legal geral (por ex. cobrança de dívidas pendentes/através de convenção coletiva com o conselho de empresa/reivindicação/exercício de ou defesa contra reivindicações legais relativamente ao titular dos dados) ou comerciais (por ex. prevenção de violações contratuais).

A transparência exige que o titular dos dados tem de ser informado sobre a forma de manuseamento dos seus dados pessoais. Regra geral, recomenda-se assim que os dados pessoais sejam obtidos diretamente do titular dos dados (e não através de terceiros). Caso seja necessário o tratamento de dados pessoais, o titular dos dados tem de ser informado sobre o seguinte:

- nome e dados de contacto do responsável pelo tratamento, bem como, se aplicável, do seu substituto na UE
- se aplicável, os dados de contacto do coordenador da proteção de dados ou do encarregado da proteção de dados
- a finalidade do tratamento de dados pessoais, bem como as bases legais para esse tratamento,
- destinatários terceiros ou categorias de destinatários terceiros aos quais possam ser transmitidos dados

- se aplicável, informações sobre o tratamento num país terceiro e referência à existência de garantias adequadas

6.2 Limitação das finalidades

Os dados pessoais podem ser tratados apenas para a finalidade comunicada ao titular dos dados antes do seu registo. São possíveis alterações posteriores à finalidade apenas de caráter restrito e carecem de justificação. O responsável pelo tratamento tem de informar o titular dos dados da finalidade de tratamento dos seus dados pessoais pela Arbonia no momento em que a Arbonia recolhe os dados pessoais pela primeira vez ou, posteriormente, logo que possível. Em cada tratamento para fins promocionais ou em programas de marketing, o titular dos dados tem de ter o direito de se opor ao tratamento dos seus dados pessoais e tem de ser expressamente informado acerca desses fins. Nesta medida, cada responsável pelo tratamento tem de implementar um tratamento de reclamações que garanta o respeito pela opção de *opt-out*.

6.3 Minimização de dados

Registar/tratar apenas dados pessoais que sejam realmente necessários Antes do tratamento de dados pessoais, é preciso determinar se e em que medida é necessário esse tratamento para alcançar a finalidade pretendida. Os dados pessoais não podem ser registados previamente e armazenados para potenciais finalidades futuras, a menos que a lei nacional o exija ou permita.

6.4 Corretos e atualizados

Os dados pessoais têm de estar corretos, completos e – se ocorrerem alterações – mantidos atualizados. Devem ser tomadas medidas adequadas para garantir que dados pessoais incorretos ou incompletos são apagados, retificados, complementados ou atualizados. Todas as pessoas que trabalham com dados pessoais têm de tomar as medidas adequadas para este fim (por ex. mediante confirmação dos dados de um titular se este telefonar ou removendo um número de telefone guardado da base de dados se o titular dos dados já não o utilizar).

6.5 Período de conservação limitado

Os dados pessoais podem ser conservados durante o período efetivamente necessário. Os dados pessoais têm de ser apagados logo que já não sejam necessários para as finalidades previstas, se o consentimento for revogado ou se for apresentada oposição à sua utilização com base em legítimo interesse, e se a Arbonia não puder apresentar motivos legítimos prioritários. Nalguns casos, períodos de armazenamento superiores podem permitir a conservação de dados pessoais durante mais tempo se tal for exigido legalmente (por ex. ao abrigo das leis tributárias e comerciais) ou se os dados pessoais forem necessários para a reivindicação, exercício ou defesa de direitos.

6.6 Confidencialidade e segurança dos dados

Os dados pessoais deverão ser sempre tratados com confidencialidade e deverão ser partilhados apenas na medida do estritamente necessário. Aplica-se o princípio da "informação necessária", pelo que os colaboradores e terceiros deverão ter acesso a dados pessoais apenas e na medida em que seja necessário ao cumprimento da finalidade. Tal exige um conceito cautelosamente concebido que defina os direitos de acesso específicos para cada processo de negócio, incluindo a implementação e aprovação dos papéis e responsabilidades (conceito de direito de acesso). Os destinatários de dados pessoas deverão ser informados da confidencialidade dos dados pessoais **e têm de se submeter a um acordo de confidencialidade** (o qual poderá fazer parte do contrato de trabalho ou similar). Exceção: o destinatário está submetido a uma obrigação de confidencialidade profissional ou legal.

Os dados pessoais deverão ser protegidos com medidas organizativas e técnicas adequadas, a fim de impedir o acesso ilegítimo, a disseminação ou divulgação ilegal ou a perda, alteração ou destruição acidentais (ver ponto 8).

7 OUTRAS OBRIGAÇÕES AO ABRIGO DO RGPD OU OUTRAS NORMAS DE PROTEÇÃO DE DADOS SIMILARES APLICÁVEIS

7.1 Princípio da responsabilidade

Uma sociedade do grupo Arbonia que esteja sujeita ao RGPD (ou norma de proteção de dados similar aplicável) tem de garantir que consegue comprovar o cumprimento das leis de proteção de dados aplicáveis (princípio da "responsabilidade"). Por conseguinte, estas sociedades do grupo, além dos requisitos gerais ao abrigo da presente Política de Proteção de Dados, têm de implementar e cumprir os seguintes aspetos, cabendo a responsabilidade última desta implementação e cumprimento da responsabilidade ao diretor executivo da sociedade do grupo em causa:

1. Coordenador da proteção de dados ou encarregado da proteção de dados local: nomeação de um coordenador da proteção de dados ou encarregado da proteção de dados local especial

2. Manutenção do "Registo de atividades de tratamento": deve gerir-se e manter-se atualizado um inventário das atividades de tratamento de dados pessoais

3. Verificação de legitimidade: deverá verificar-se o tratamento legítimo dos dados pessoais e que se verificam motivos legítimos, sobretudo no tratamento de categorias especiais de dados pessoais

4. Controlo do subcontratante: celebração de um contrato de subcontratação com o subcontratante ou como subcontratante de fornecimento ou receção de dados

pessoais com uma autorização segundo o artigo 28.º do RGPD.

5. No caso de responsáveis conjuntos pelo tratamento, deve prever-se um acordo entre os responsáveis conjuntos pelo tratamento segundo o artigo 26.º do RGPD.

6. Os colaboradores da Arbonia devem ser informados sobre a atividade de tratamento de dados pessoais.

7.2 Regras para o subcontratante (sobretudo parceiros de prestação de serviços)

O responsável pelo tratamento trabalha apenas com subcontratantes que ofereçam garantias suficientes de que serão tomadas medidas técnicas e organizativas adequadas que garantam que o tratamento dos dados pessoais será fará de acordo com os requisitos do artigo 28.º do RGPD e assegurem a proteção do titular dos dados.

Para serviços partilhados dentro da Arbonia, existe um acordo que autoriza a transmissão de dados pessoais, desde que existam fundamentos legais legítimos para essa transmissão ao abrigo das leis de proteção de dados em vigor.

7.2.1 Disponibilização de dados pessoais ao subcontratante (saída de dados)

O tratamento de dados pessoais ao abrigo de uma autorização significa que um prestador de serviços é encarregado de tratar dados pessoais sem que lhe seja transferida a responsabilidade pelo processo de negócio correspondente (ou seja, prestadores de serviços, serviços externos). Neste caso, deve ser celebrado prestadores externos um contrato de subcontratação para o tratamento de dados pessoais com autorização. A sociedade do grupo Arbonia em causa é o responsável pelo tratamento e assume a inteira responsabilidade pela execução correta do tratamento dos dados pessoais pelo subcontratante.

O responsável do processo de negócio em causa tem de garantir que para a subcontratação de tais serviços é utilizado o acordo modelo atual para a subcontratação do tratamento ou um contrato similar correspondente disponibilizado pelo prestador de serviços para cumprimento dos requisitos decorrentes do artigo 28.º do RGPD. Em alternativa, o prestador de serviços pode documentar o seu cumprimento dos requisitos de segurança dos dados, apresentando uma certificação adequada e homologada pela UE. Qualquer desvio a uma tal norma de segurança tem de ser autorizado pelo encarregado da proteção de dados ou coordenador da proteção de dados, em colaboração com o Corporate IT. Os contratos atualmente existentes têm de ser revistos no prazo de um ano após a entrada em vigor desta Política de Proteção de Dados e têm de incluir um contrato de subcontratação do tratamento escrito.

7.2.2 Receção de dados pessoais como subcontratante (entrada de dados)

Se um terceiro transmitir dados pessoais a uma sociedade do grupo Arbonia, é preciso garantir que os dados pessoais (i) podem ser utilizados para a finalidade prevista, (ii) são recolhidos com base em motivos legítimos (recomenda-se a obtenção de uma confirmação por escrito) e (iii) que existe um contrato de subcontratação do tratamento de acordo com o artigo 28:º do RGPD.

7.3 Transmissão transfronteiriça de dados pessoais

No caso de transmissão transfronteiriça de dados pessoais, têm de ser cumpridos os requisitos nacionais de cada país relativos à divulgação de dados pessoais no estrangeiro. Ao abrigo do RGPD, é permitida a transmissão de dados pessoais dentro da UE, do EEE ou num país que a Comissão Europeia tenha constatado cumprir garantias adequadas de assegurar um nível de proteção de dados adequado. Esta transmissão de dados não carece de autorização especial. A Comissão Europeia classificou, entre outros, a Suíça como um país que proporciona uma proteção adequada (consultar a lista de países atual: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Só é permitida a transmissão de dados pessoais a um país terceiro se este apresentar garantias adicionais adequadas. Ou seja, se o destinatário conseguir comprovar que mantém uma norma de proteção de dados correspondente a esta Política de Proteção de Dados (por ex. i) aplicação de regras empresariais vinculativas, ii) celebração de cláusulas de contratação padrão da UE para a subcontratação do tratamento em países terceiros com o prestador de serviços e outras empresas subcontratadas[3], iii) existência de regras de conduta aprovadas pela autoridade de controlo, iv) em caso de participação do prestador de serviços num sistema de certificação acreditado pela UE para obtenção de um nível de proteção de dados suficiente ou v) com acordos individuais entre o responsável pelo tratamento e o subcontratante, com a autorização da autoridade de controlo competente) e com informação do titular dos dados. Esta obrigação não se aplica se a transmissão tiver por base uma obrigação legal. Uma tal transmissão carece da autorização do coordenador da proteção de dados ou encarregado da proteção de dados.

Se forem transmitidos dados pessoais dentro da Arbonia, a sociedade do grupo que importa os dados pessoais é obrigada a cooperar em todos os pedidos de informação da autoridade de controlo competente do país onde tem sede a sociedade do grupo que exporta os dados e a ir ao encontro de todas as observações efetuadas pela autoridade de controlo relativamente ao tratamento dos dados pessoais transmitidos.

[3] Consultar a Decisão da Comissão de 5 de fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

7.4 Tratamento de um pedido de um titular dos dados

Os titulares dos dados têm o direito de apresentar um pedido formal de informações sobre os dados pessoais na posse da Arbonia e podem exigir o seguinte:

Direito de informação sobre:

- as finalidades do tratamento;
- as categorias de dados pessoais sujeitas a tratamento;
- os destinatários ou as categorias de destinatários aos quais foram ou serão divulgados os dados pessoais, em particular destinatários em países terceiros ou em organizações internacionais;
- se possível, o período previsto de armazenamento dos dados pessoais ou, caso tal não seja possível, os critérios de determinação deste período;
- a existência do direito de retificação ou apagamento dos dados pessoais que lhe dizem respeito ou de restrição do tratamento pelo responsável pelo tratamento ou de oposição a este tratamento;
- existência de um direito de reclamação junto de uma autoridade de controlo;
- todas as informações disponíveis sobre a origem dos dados, se os dados pessoais não forem recolhidos junto do titular dos dados;
- existência de uma tomada de decisão automatizada, incluindo a definição de perfis;
- Se forem transmitidos dados pessoais a um país terceiro ou a uma organização internacional, o titular dos dados tem o direito de ser informado sobre as garantias adequadas.

Direito de retificação:

- O titular dos dados tem o direito de solicitar a imediata retificação de dados pessoais incorretos que lhe digam respeito. Considerando as finalidades do tratamento, o titular dos dados tem o direito de solicitar que sejam complementados os seus dados pessoais que estejam incompletos – igualmente mediante uma declaração complementar.

Direito de apagamento ("direito a ser esquecido")

- O titular dos dados tem o direito de solicitar ao responsável pelo tratamento que os seus dados pessoais sejam imediatamente apagados e o responsável pelo tratamento é obrigado a apagar de imediato os dados pessoais, desde que se aplique um dos seguintes motivos:
    1. Os dados pessoais deixaram de ser necessários para as finalidades para as quais foram recolhidos ou de outro modo sujeitos a tratamento;
    2. O titular dos dados revoga o consentimento que está na base do tratamento segundo a alínea a) do n.º 1 do artigo 6.º do RGPD ou a alínea a) do n.º 2 do artigo 9.º do RGPD, não havendo outro fundamento legal para o tratamento;
    3. Nos termos do n.º 1 do artigo 21.º do RGPD, o titular dos dados opõe-se ao tratamento e não existem motivos legítimos e prioritários para o tratamento

ou o titular dos dados opõe-se ao tratamento nos termos do n.º 2 do artigo 21.º do RGPD;
4. Os dados pessoais foram submetidos a tratamento ilegal;
5. O apagamento dos dados pessoais é necessário para cumprir uma obrigação legal segundo a lei dos Estados-Membros em causa à qual o responsável pelo tratamento está sujeito;
6. Os dados pessoais foram recolhidos no âmbito de serviços da sociedade da informação nos termos do n.º 1 do artigo 8.º do RGPD.

Direito de restrição do tratamento:

- O titular dos dados tem o direito de solicitar a restrição do tratamento ao responsável pelo tratamento, caso se verifiquem as seguintes condições:
- se for contestada a correção dos dados pessoais que dizem respeito ao titular durante o tempo que o responsável pelo tratamento demorar a verificar a correção dos dados pessoais:
- se o tratamento for ilegal e se o titular dos dados recusar o apagamento dos dados pessoais, solicitando ao invés a restrição da utilização dos dados pessoais;
- se o responsável pelo tratamento já não precisar dos dados pessoais para as finalidades do tratamento, mas o titular dos dados ainda precisar deles para declaração, exercício ou defesa de um direito,
- se o titular dos dados se opuser ao tratamento nos termos do n.º1 do artigo 21.º, enquanto ainda não se tiver determinado se existem motivos legítimos do responsável pelo tratamento que tenham precedência sobre os motivos do titular dos dados.

Deverá solicitar-se ao titular dos dados que apresente o seu pedido por escrito, quer seja por correio eletrónico ou correio postal, dirigido ao respetivo encarregado da proteção de dados local. O encarregado da proteção de dados local deverá disponibilizar imediatamente informações ao titular dos dados, mas em todo o caso no prazo de um mês após a receção do pedido. Este prazo pode ser prolongado por mais dois meses se tal se revelar necessário considerando a sua complexidade e o número de pedidos. O coordenador da proteção dos dados ou encarregado da proteção dos dados do responsável pelo tratamento, no prazo de um mês após a receção do pedido, informa o titular dos dados do prolongamento do prazo, juntamente com os motivos do atraso. O titular dos dados não deverá incorrrer em nenhum custo associado ao pedido de informação sobre os dados que lhe dizem respeito na posse da Arbonia, na medida em que os pedidos do titular não sejam claramente infundados ou excessivos, em particular se forem efetuados repetidamente. Os pedidos de um titular dos dados relativos a várias sociedades do grupo deverão ser encaminhados para o Corporate IT para fins de coordenação e resposta.

7.5 Realização de uma avaliação de impacto sobre a proteção de dados

Se uma nova forma prevista de tratamento de dados pessoais, em particular mediante a utilização de novas tecnologias, considerando o tipo, o âmbito, as circunstâncias e as

finalidades do tratamento, apresentar previsivelmente um risco elevado para os direitos e liberdades do titular dos dados, deve realizar-se previamente uma avaliação de impacto das atividades de tratamento previstas sobre a proteção de dados pessoais.

Antes da implementação de novas atividades de tratamento devem assim ser avaliados os riscos que daí podem resultar para a personalidade e os direitos fundamentais do titular dos dados. No caso de novas aplicações de TI, este procedimento deve ser considerado no âmbito do processo de autorização. Se uma primeira avaliação conduzir à conclusão de que uma nova forma prevista de tratamento de dados pessoais apresenta previsivelmente um risco elevado para o titular dos dados, deve ser realizada uma avaliação de impacto sobre a proteção de dados.

Eventuais questões que surjam sobre a necessidade ou durante a realização da avaliação de impacto sobre a proteção de dados deverão ser encaminhadas para o coordenador da proteção de dados ou encarregado da proteção de dados local. Após a sua realização, a avaliação de impacto sobre a proteção de dados deverá ser comunicada ao coordenador da proteção de dados ou encarregado da proteção de dados local, devendo este último emitir um parecer.

Se uma avaliação de impacto sobre a proteção de dados indicar que o tratamento apresentaria um risco elevado para o titular dos dados, e se não forem tomadas medidas de contenção do risco, antes da implementação das novas atividades de tratamento deverá consultar-se a autoridade de controlo.

8 SEGURANÇA DOS DADOS PESSOAIS

Os dados pessoais têm de ser protegidos contra o acesso ilegítimo e o tratamento e a divulgação ilegítimos, bem como contra a perda, alteração ou destruição acidentais. Tal aplica-se independentemente de os dados serem tratados eletronicamente ou em papel.

O responsável pelo tratamento e o subcontratante têm de tomar medidas técnicas e organizativas adequadas para proteger os dados de um tratamento ilegítimo. Estas medidas têm de se basear em (i) boas práticas, (ii) riscos do tratamento e (iii) necessidade de proteger os dados pessoais (determinada mediante o processo de classificação de informações); estes incluem, entre outros, de acordo com o que for adequado caso a caso:

(a) a pseudonimização e a cifragem dos dados pessoais;

(b) a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento;

(c) a capacidade de repor rapidamente a disponibilidade dos dados pessoais e o acesso aos mesmos em caso de incidente físico ou técnico;

(d) um procedimento de verificação, análise e avaliação regulares da eficácia das medidas técnicas e organizativas de garantia da segurança do tratamento

As medidas técnicas e organizativas de proteção dos dados pessoais fazem parte da gestão interna da segurança da informação e têm de ser permanentemente ajustadas aos desenvolvimentos técnicos e às alterações organizativas.

Os procedimentos de segurança podem incluir, no mínimo:

- Controlos de acessos: deverá ser comunicada cada pessoa estranha que seja detetada em áreas com controlo de acessos.

- Gavetas ou arquivadores com fecho seguro: secretária e armários devem manter-se trancados se contiverem algum tipo de informação confidencial. Os dados pessoais são sempre informações confidenciais. Os colaboradores devem garantir que o papel e as impressões contendo dados pessoais não são deixados em locais globalmente visíveis, por exemplo, numa impressora. Se os dados pessoais forem, com autorização, armazenados num suporte de cedência de dados (por ex. CD, pen de dados ou DVD), este suporte deve ser guardado em local seguro quando não estiver em utilização.
- Métodos de eliminação: quando deixarem de ser necessários, os documentos em papel devem ser destruídos em máquina própria e eliminados em segurança. Tal aplica-se igualmente a dados pessoais normalmente armazenados em suporte eletrónico, mas que tenham sido impressos.

- Dados armazenados eletronicamente: os dados pessoais devem ser protegidos por palavras-passe de acordo com as diretrizes atuais relativas a palavras-passe e nunca devem ser partilhados entre colaboradores. Se forem armazenados eletronicamente, os dados pessoais têm de ser guardados e consultados em sistemas de servidores de TI e em aplicações de tecnologia da informação estruturadas, e não cifrados em computadores locais.

- Dados pessoais recolhidos eletronicamente disponibilizados pelo titular: deve verificar-se a identidade do titular dos dados, preferencialmente mediante um duplo processo de *opt-in* (ou seja, um segundo endereço eletrónico para validação do endereço eletrónico indicado). Se o acesso a um sítio web ou aplicação estiver limitado a utilizadores registados (i.e. conta de utilizador), a identificação e autenticação do titular dos dados têm de proporcionar uma proteção de segurança que, durante o acesso, seja proporcional aos conteúdos em causa.

- Precaução na partilha de dados pessoais: os dados pessoais nunca devem ser partilhados de modo informal. Aplica-se o princípio de "informações necessárias". É

obrigatório um sistema de discriminação e separação por processo de negócio, bem como a implementação de papéis e responsabilidades. Os dados pessoais devem ser cifrados antes da sua transmissão eletrónica. O gestor de tecnologias da informação pode explicar como os dados pessoais são enviados para pessoas de contacto externas autorizadas.

- Pedir orientações: em caso de dúvidas ou inseguranças sobre um aspeto da proteção de dados ou relativamente às obrigações ao abrigo desta Política de Proteção de Dados, deve obter-se aconselhamento junto do superior direto, do encarregado da proteção de dados local ou do Legal & Compliance.

O RGPD exige que a privacidade seja tida em conta o mas precocemente possível. A privacidade desde a conceção exige que as organizações considerem a privacidade nas primeiras fases da conceção da tecnologia e durante todo o processo de desenvolvimento de novos produtos, procedimentos ou serviços relacionados com o tratamento de dados pessoais. A privacidade por defeito significa que, se um sistema ou serviço implicar a decisão individual de quantos dados pessoais poderá partilhar com terceiros, deverão aplicar-se as definições por defeito que proporcionem a maior proteção da privacidade. Por conseguinte, qualquer nova aplicação de TI está sujeita a um processo de autorização interno, sendo que, no âmbito da avaliação, esta nova aplicação de TI também deverá ser avaliada sob pontos de vista da proteção de dados.

9 NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA DOS DADOS

Muitas normas de proteção de dados em vigor exigem que os incidentes de segurança dos dados sejam diretamente notificados ao legislador. Exige-se assim que todos os incidentes de segurança dos dados sejam imediatamente notificados ao coordenador da proteção dos dados ou ao encarregado da proteção dos dados, independentemente de o sistema afetado ser local ou do grupo, de acordo com o processo descrito na política da Arbonia relativa a incidentes de segurança dos dados ("Arbonia Data Breach Policy"). Se o TI detetar incidentes ou riscos no domínio da segurança dos dados, estes deverão ser comunicados conforme definido na política de Data Breach Notification.

O objetivo é cumprir as obrigações de notificação de violações às obrigações de proteção de dados em vigor ao abrigo das leis de proteção de dados aplicáveis (por ex. segundo o RGPD, o mais tardar 72 horas após a tomada de conhecimento).

Nesse caso, deve sublinhar-se a necessidade de cumprimento dos prazos indicados para a notificação de violações da proteção de dados e de tomada de medidas mediatas para investigar incidentes e determinar se foram efetivamente violados os dados pessoais. O Corporate IT tem de manter um registo interno de violações de segurança na Arbonia, para assim cumprir os deveres de notificação ao abrigo da lei nacional e garantir que são aplicadas as regras de representação aplicáveis para notificar em qualquer altura eventuais

violações. Antes da notificação de uma autoridade nacional, deve informar-se o Corporate IT ou o departamento Legal and Compliance do grupo.

Todas as restantes políticas do Corporate IT e dos departamentos de TI locais devem ser rigorosamente cumpridas.

10 CONSEQUÊNCIAS DO INCUMPRIMENTO

O cumprimento desta Política de Proteção de Dados assume extrema importância para a Arbonia e para a perceção pública da Arbonia. Um tratamento inadequado de dados pessoais ou outras violações às leis de proteção de dados podem, em muitos países, estar sujeitas a consequências penais e dar origem ao pagamento de indemnizações. No seio da Arbonia, uma violação das regras constantes desta Política de Proteção de Dados pode dar origem a sanções ao abrigo da lei e/ou do respetivo contrato (de trabalho).

11 DIVERGÊNCIAS

Só serão admitidas divergências relativamente às disposições desta Política e dos seus suplementos após conciliação com o Head of Legal & Compliance.

12 INFORMAÇÕES

As informações relacionadas com a Política de Proteção de Dados serão fornecidas pelo Head of Legal & Compliance.

13 ENTRADA EM VIGOR

Esta Política entra em vigor no dia 17 de junho de 2020 e substitui a política de tratamento de dados (política de proteção de dados) de 5 de dezembro de 2013.

Arbon, 16 de junho de 2020

Arbonia AG

Alexander von Witzleben
Presidente do conselho de administração e CEO

Andrea Wickart
Head of Legal & Compliance/Secretária Geral

ARBONIA

Suplementos a esta Política de Proteção de Dados da Arbonia:

Os seguintes suplementos, na sua versão atual, concretizam a presente Política de Proteção de Dados:

- Política relativa a pedidos de titulares dos dados e de apagamento de dados
- Política relativa a violações de proteção de dados
- Declaração de proteção de dados para os colaboradores

Este documento é válido sem assinatura.