Política Global de Proteção de Dados Pessoais

Introdução

Este documento descreve a forma como a Empresa define as regras internas e cumpre a legislação aplicável à Proteção de Dados Pessoais.

A Empresa está empenhada em garantir a proteção dos Dados Pessoais dos seus colaboradores, candidatos, clientes e fornecedores. Esta Política incorpora os requisitos do novo Regulamento Geral sobre a Proteção de Dados (doravante, "Regulamento") , cuja execução é assegurada pela Lei n.º 58/2019 de 8 de agosto.

Os nossos princípios exigem que os Dados Pessoais sejam sempre:

Tratados com respeito pelos **DIREITOS DOS TITULARES DOS DADOS**	Tratados com base num **FUNDAMENTO LÍCITO**	Tratados **DE FORMA TRANSPARENTE**
Recolhidos e Tratados para **FINALIDADES DETERMINADAS, EXPLÍCITAS E LEGÍTIMAS**	**ADEQUADOS, PERTINENTES E LIMITADOS** ao que é necessário à finalidade	**EXATOS E ATUALIZADOS**
Tratados de forma que **GARANTA A SUA SEGURANÇA E CONFIDENCIALIDADE**	**CONSERVADOS APENAS PELO PERÍODO NECESSÁRIO**	**COMUNICADOS A TERCEIROS** apenas nos casos em que a lei permite ou impõe

Este documento destina-se:

- Aos colaboradores da Empresa que queiram compreender como a Empresa trata e protege os seus dados pessoais;
- Aos colaboradores da Empresa que tratam dados pessoais na sua atividade e que necessitem compreender as suas responsabilidades.

A Política é aplicável às seguintes sociedades legais do Grupo Securitas em Portugal:

- Securitas – Serviços e Tecnologia de Segurança S.A.
- Servisecuritas – Administração e Logística, Sociedade Unipessoal, Lda.
- Securitas Transport Aviation Security, Lda.
- Instalfogo – Sistemas contra Incêndios, S.A.

Esta política pode ser complementada por Informações sobre a Proteção de Dados da Empresa que serão definidas e publicitadas pelo Departamento Gestão de Risco, Jurídico e Dados.

A legislação aplicável prevalece sobre esta Política se, e na medida, exceda as normas da presente política, imponha requisitos mais rigorosos ou proporcione um grau maior de proteção.

Nos casos em que esta Política proporcionar um maior grau de proteção do que a lei aplicável ou proporcionar salvaguardas e direitos adicionais para os Titulares dos Dados, a presente política será aplicável.

O Encarregado da Proteção de Dados da Empresa pode ser contactado através do e-mail - dpo@securitas.pt.

Todas as dúvidas relacionadas com esta Política ou sobre a proteção de dados pessoais em geral devem ser dirigidas ao Encarregado da Proteção de Dados.

A Empresa atualizará este documento periodicamente. A atualização será feita anualmente ou conforme for adequado, procurando dar resposta às alterações legislativas, às necessidades de negócio e ao desenvolvimento da tecnologia.

1. Resumo dos Princípios Fundamentais

Todas as entidades Securitas devem cumprir esta Política de Proteção de Dados, independentemente do país onde se encontram estabelecidas, a menos que definido apenas como um requisito da União Europeia/ Espaço Económico Europeu.

Para além disso, todas as entidades da Securitas devem cumprir as leis e regulamentos locais sobre proteção e tratamento de dados pessoais.

2. Objetivo

A cultura do Grupo Securitas tem como base fortes valores, compartilhamos um grande senso de responsabilidade perante os nossos clientes, colaboradores e comunidades em que operamos, protegendo as pessoas e bens.

Os nossos valores, são fundamentais no Grupo Securitas, e formam a base dos nossos padrões éticos assim como o respeito pela privacidade dos indivíduos. O Conselho de Administração da Securitas Portugal ("Securitas") adotou esta política interna de proteção de dados ("Política Global de Proteção de Dados Pessoais"), que visa manter o alto nível ético e garantir que a Securitas conduz os negócios de acordo com os valores e mantém uma boa reputação aos olhos do público e do mercado de capitais.

Esta Política Global de Proteção de Dados descreve os **quatro princípios da proteção de dados** com base nos valores do Grupo Securitas, bem como os **princípios básicos da proteção de dados**, estes, em conjunto, devem integrar todas as atividades, serviços e produtos, independentemente do local onde a entidade da Securitas esteja estabelecida.

O Grupo Securitas adotou, com base nos seus valores, os **quatro princípios da proteção de dados** que se aplicam a todas as entidades do Grupo Securitas:

1. **Conformidade** – A nossa operação é realizada de acordo com as leis e regulamentos aplicáveis sobre a matéria de dados pessoais. Os colaboradores que lidam com os dados pessoais no seu trabalho devem familiarizar-se e cumprir com as leis e regulamentos. Para a Securitas, a conformidade inclui o respeito pelos indivíduos e pelo direito à proteção de dados, independentemente do desenvolvimento tecnológico se mover mais rápido do que a estrutura legal;

2. **Integridade** – A atuação da Securitas na recolha e tratamento de dados pessoais pauta-se por princípios de honestidade e de confiança. Este princípio significa que a comunicação dos fundamentos da recolha de dados pessoais é pautada por regras de transparência.

3. **Prevenção de danos** - Devemos desenvolver serviços e produtos que procuram prevenir danos financeiros, físicos ou de reputação, diretos ou indiretos. Os dados pessoais devem ser protegidos de forma a evitar qualquer dano.

4. **Colaboração e Prestação** – Prestamos toda a colaboração e ajudamos no exercício e garantia dos direitos dos titulares de dados pessoais. Quando existirem direitos adicionais, como por exemplo, a retificação de dados pessoais e/ou o apagamento dos dados pessoais ("esquecimento"), ajudamos oportunamente, a exercer tais direitos.

3. Definições

(i) Responsável pelo tratamento

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

(ii) Titular dos dados

O titular dos dados é o indivíduo a quem os dados pessoais se relacionam (como um colaborador, uma pessoa de contacto num cliente ou mesmo um cliente).

(iii) Dados Pessoais

Informação relativa a uma pessoa singular identificada ou identificável ("Titular dos dados"); é considerada identificável uma pessoa singular 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. Exemplos: nome, data de nascimento, n.º de filhos, n.º mecanográfico, fumador / não fumador, matrícula do veículo entre outros.

(iv) Tratamento

Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de 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;

(v) Subcontratante

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

(vi) Categorias especiais de dados pessoais ou "Dados Pessoais Sensíveis"

Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

4. Responsabilidade, Organização e Estrutura de Governo

4.1. Equipa de Encarregados de Proteção de Dados do Grupo

O CEO da Securitas é o principal responsável pela conformidade com a proteção de dados. A responsabilidade de desenvolver e gerir uma estratégia de proteção de dados pessoais do Grupo Securitas foi delegada ao Group Data Proteccion Officer/Global Privacy Officer que o administrará em conjunto com o Group Privacy Officer CDSO para as matérias de Segurança da Informação e o Management Assurance Director para as matérias de auditoria. ("**The Group DPO Team**").

4.2. Entidades Securitas da União Europeia/ Espaço Económico Europeu

É da responsabilidade do Administrador-Delegado do país, em cada país da União Europeia/Espaço Económico Europeu, garantir a conformidade oportuna com a Política Global de Proteção de Dados Pessoais, assim como todas as leis e regulamentos de proteção de dados aplicáveis, incluindo o Regulamento Geral de Proteção de Dados da UE ("RGPD").

A responsabilidade inclui a avaliação de leis e regulamentos aplicáveis, bem como a avaliação da extensão e o escopo dos dados pessoais tratados no país e garantir o exercício das ações apropriadas para assegurar a conformidade.

De acordo com o RGPD, é obrigatório que determinadas entidades designem um Encarregado da Proteção de Dados ("EPD").

Assim, um EPD é uma nomeação formal com registo na Autoridade de Proteção de Dados local, Comissão Nacional de Proteção de Dados, e deve ter competência e ser responsável por determinadas tarefas.

4.3. Todas as entidades do Grupo Securitas

Helena Silling foi nomeada internamente Diretora de Proteção de Dados do Grupo Securitas (esta nomeação não está registada em nenhuma autoridade de supervisão) e pode ser contactada por email através: dpo@securitas.com.

Ann Blomqvist é oficialmente a EPD da Securitas AB.

Em Portugal, foi nomeada como Encarregado de Proteção de Dados, Andreia Soares.

Quaisquer dúvidas relacionadas com os requisitos ao abrigo da presente Política ou outros relacionados com questões de proteção de dados devem ser dirigidas ao seguinte endereço eletrónico: dpo@securitas.pt

Para obter mais informações sobre a nomeação e tarefas de um Encarregado de Proteção de Dados de acordo com a legislação da União Europeia/Espaço Económico Europeu, consulte os conceitos de chave de proteção de dados (DPKC).

5. Princípios relacionados com o tratamento de dados pessoais

5.1 Esta Política visa garantir que o Tratamento de Dados Pessoais é realizado de acordo com a legislação aplicável, de uma forma justa e salvaguardando os direitos dos Titulares de Dados.

Todos os colaboradores da Empresa devem cumprir os seguintes **sete princípios de boas práticas**.

(i) **Legalidade, justiça e transparência -** Todos os dados pessoais devem ser tratados de forma legal, justa e transparente em relação ao titular dos dados.
Para que o tratamento conduzido por uma entidade da Securitas seja legal, o mesmo deve ter por base um fundamento legal.
O princípio do tratamento justo e transparente exige que o titular dos dados seja informado da existência da operação de tratamento, dos objetivos e possíveis consequências.

Fundamento legal: Existem determinadas condições que devem ser cumpridas para que os Dados Pessoais sejam tratados legalmente. Estas podem incluir, entre outras, que:

- O Titular dos Dados tenha autorizado o Tratamento (por exemplo, através do opt in para receber comunicações de marketing); ou
- O Tratamento é absolutamente necessário para a realização da atividade comercial ou para a execução de um contrato (por exemplo, a recolha de dados de clientes para fornecer serviços e processar a faturação e pagamento, ou o Tratamento de informações sobre o salário do colaborador e detalhes da conta bancária para que os salários possam ser pagos); ou
- O Tratamento está em conformidade com uma obrigação legal à qual a Empresa está sujeita (por exemplo, a comunicação dos dados salariais de colaboradores à segurança social ou à Administração Tributária);
- O Tratamento visa os interesses legítimos prosseguidos pela Empresa (por exemplo, segurança física, TI e segurança de rede), desde que esses interesses não se sobreponham aos direitos dos Titulares dos Dados; ou
- O Tratamento é realizado em situações de emergência para proteger os interesses fundamentais do Titular dos Dados (por exemplo, por motivos de segurança ou de saúde e segurança).

Quando procedemos à recolha de Dados Pessoais Sensíveis, será geralmente necessário obter a autorização explícita do Titular dos Dados, por exemplo, através da assinatura de um formulário a confirmar que este concorda com a recolha e utilização de tais informações.

No entanto, é importante ter em conta que no contexto da relação laboral o consentimento dos colaboradores é geralmente insuficiente para fundamentar um tratamento de dados pessoais.

A Empresa apenas solicitará o consentimento para tratamento de dados pessoais em casos devidamente avaliados, nos quais se considere que o Titular dos Dados pode efetivamente conceder ou negar a prestação do consentimento de forma livre.

Tratamento Transparente: É essencial garantir que o Titular dos Dados entenda quem é o Responsável pelo Tratamento, quais as finalidades para as quais os dados são tratados, como serão tratados, a identidade de qualquer pessoa ou entidade a quem os dados possam ser divulgados (por exemplo, clientes e outras sociedades do grupo da Empresa), para onde serão transferidos, a partir de onde serão acessíveis e quais são os seus direitos relativamente à sua informação ao abrigo da lei aplicável.

(ii) Limitação da finalidade - A Securitas deve garantir que a finalidade do tratamento de dados pessoais seja específica, explícita e legítima antes de iniciar o tratamento e deve ser mencionado que os dados pessoais que foram recolhidos para uma finalidade específica não podem ser tratados de maneira incompatível com esse(s) objetivo(s).

Tratamento para finalidade limitada: Os Dados Pessoais só podem ser tratados para as finalidades específicas comunicadas ao Titular dos Dados no momento em que os dados foram originalmente recolhidos ou para qualquer outra finalidade especificamente autorizada pela lei aplicável.

Isto significa que os Dados Pessoais não podem ser recolhidos para uma finalidade e, em seguida, utilizados para outra. Se for necessário alterar a finalidade para a qual os dados são tratados, o Titular dos Dados tem de ser informado sobre a nova finalidade antes de qualquer Tratamento ocorrer, podendo ser necessário dar-lhe a oportunidade de se opor ao mesmo.

Para a Securitas, as finalidades podem, entre outras, referir-se- às seguintes:

- Gestão de relação contratual com clientes e fornecedores;
- Gestão de ativos da empresa;
- Aquisição e manutenção dos bens e serviços;
- Gestão financeira;
- *Compliance* interna,
- Marketing;
- Assessoria e gestão do contencioso da Empresa;
- Criação, gestão e manutenção dos sistemas de informação e de telecomunicações.

Os dados dos colaboradores da Empresa, em particular, serão tratados para as seguintes finalidades:

- Gestão de recursos humanos;
- Seleção de pessoal e recrutamento;
- Gestão contabilística e gestão de relação com auditores;
- Comunicação interna, envio da Revista Securitas, realização do *Employee Survey* Securitas (Inquérito aos Colaboradores da Securitas);
- Processamento de renumerações, incluindo penhoras de vencimentos e reembolso de despesas;
- Segurança e Saúde no trabalho;
- Gestão de sanções disciplinares;
- Formação profissional;
- Videovigilância.

O fundamento jurídico é a necessidade do tratamento para a execução de contrato de trabalho, ou para diligências pré-contratuais a pedido do titular dos dados.

O tratamento de dados para efeito de medicina no trabalho encontra fundamento na alínea h) do n.º 2 do art.º 9 do Regulamento.

A videovigilância é realizada com base no interesse legítimo da Empresa, com a finalidade de proteção de pessoas e bens.

Os dados pessoais dos trabalhadores são conservados pelo período de 1 (um) ano após o término da relação laboral, sem prejuízo i) de tal prazo se estender pelo tempo de duração de eventual processo judicial ou de eventual processo que corra os seus termos perante uma entidade administrativa e ii) dos prazos de conservação de documentos impostos por disposição legal, designadamente pela legislação laboral, fiscal e contributiva.

Os dados dos colaboradores poderão ser comunicados a: i) entidades do grupo de empresas da Empresa; ii) a empresas que lhe prestem serviços, designadamente, de prestação de serviços de segurança e saúde no trabalho ou outras relacionadas com a gestão de pessoal e de recursos humanos; a iii) entidades públicas que tenham legitimidade legal para proceder ao tratamento dos dados em questão, tendo em vista designadamente, procedimentos decorrentes do exercício da atividade de segurança privada, o cálculo e pagamento de retribuições, prestações acessórias, outros abonos e gratificações; o cálculo, retenção na fonte e operações relativas a descontos na retribuição, obrigatórios ou facultativos, decorrentes de disposição legal; bem como a iv) auditores internos e externos da Empresa.

(iii) **Minimização de dados** - Os dados pessoais recolhidos e tratados devem ser adequados, relevantes e limitados ao necessário em relação aos propósitos para os quais são tratados.

Adequação, relevância e limitação ao necessário relativamente à finalidade: Os Dados Pessoais só devem ser recolhidos e tratados na medida em que sejam necessários para as finalidades da Empresa e que tenham sido informados ao Titular dos Dados. Quaisquer dados pessoais que não são necessários para essa finalidade não devem ser recolhidos.

O Tratamento de Dados Pessoais deve limitar-se aos Dados razoavelmente adequados e relevantes para a finalidade comercial aplicável.

Devem ser tomadas medidas razoáveis para manter os Dados Pessoais num formulário que permita a identificação do Titular dos Dados por um período que não seja superior ao necessário para as finalidades para as quais os Dados Pessoais são tratados.

(iv) **Precisão** - A Securitas procurará que os dados pessoais sejam precisos e, quando necessário, atualizados. Por conseguinte, as entidades da Securitas devem tomar todas as medidas razoáveis para garantir que os dados pessoais imprecisos ou desatualizados, tendo em conta os fins para os quais são tratados, sejam apagados ou retificados sem demora desnecessária.

Rigor, e quando necessário, atualização dos Dados: Os Dados Pessoais devem ser rigorosos e mantidos atualizados. Devem ser tomadas medidas para verificar o rigor de quaisquer dados pessoais no ponto de recolha e, posteriormente, em intervalos regulares.

Os Dados Pessoais que sejam incorretos ou enganosos não são rigorosos e devem ser tomadas medidas para verificar o rigor de quaisquer Dados Pessoais no ponto de recolha e, posteriormente, em intervalos regulares.

(v) **Limitação de armazenamento** – os dados pessoais não devem ser mantidos por um período mais longo do que o necessário para a sua finalidade de tratamento, é recomendável que os dados ou sejam apagados ou sejam anonimizados.

Manutenção apenas pelo tempo necessário: Os períodos de retenção de Dados Pessoais devem ser definidos e documentados.

Os Dados Pessoais que não estão a ser ativamente utilizados, os Dados Pessoais relativamente aos quais não tenhamos uma obrigação legal de reter (por exemplo, para finalidades fiscais); os Dados Pessoais que não estejamos autorizados a manter por motivos legais ou de conformidade; ou os Dados Pessoais que não são necessários para finalidades de histórico ou análise estatística, devem ser eliminados de forma segura.

Os dados imprecisos ou desatualizados devem ser destruídos ou eliminados o mais rapidamente possível, exceto se esses dados sejam retidos ao abrigo de qualquer período de retenção legal.

(vi) **Integridade e confidencialidade** - Os dados pessoais devem sempre ser tratados de maneira a garantir a integridade e a confidencialidade. Para garantir a integridade dos dados, devem ser adotadas medidas para proteger os dados contra perda, destruição ou alteração não autorizada ou acidental, por exemplo, recorrendo a software antivírus, realizando backups regulares do banco de dados ou dar formação aos colaboradores sobre o perigo de abrir e-mails de fontes não confiáveis. Para garantir a confidencialidade dos dados, devem ser adotadas medidas para proteger os dados contra uso ou divulgação não autorizada ou acidental, por exemplo, criptografar os dados, limitar o número de pessoas que têm acesso a dados confidenciais, protegendo os edifícios contra invasores ou proteger o acesso a servidores com senhas.

A Empresa deve processar os Dados Pessoais de uma forma que garanta um nível de segurança dos Dados Pessoais adequado ao risco, incluindo a proteção contra o tratamento não autorizado ou ilegal e contra perdas, destruições ou danos acidentais, utilizando medidas técnicas ou organizacionais adequadas e respeitando os requisitos das leis aplicáveis.

Quando exigido pela lei aplicável, a Empresa deve realizar e manter um registo das avaliações de impacto da Proteção de Dados em novas iniciativas suscetíveis de resultar num risco elevado para os direitos de privacidade e Proteção de Dados

(vii) **Responsabilidade** - No papel de responsável pelo tratamento de dados, as entidades da Securitas serão responsáveis por, e deverão poder demonstrar conformidade, com os princípios acima mencionados. As medidas, por forma a demonstrar o seu sentido de responsabilidade, podem incluir a implementação de, por exemplo, uma política de retenção e/ou um processo para realizar avaliações de risco de proteção de dados, por exemplo na União Europeia/ Espaço Económico Europeu, uma Avaliação de Impacto na Proteção de Dados ("AIPD").

Os Dados Pessoais têm de ser tratados de uma forma justa e em conformidade com os direitos do Titular dos Dados.

A Empresa deve implementar procedimentos que visem facilitar os seguintes direitos do Titular relativamente aos seus Dados Pessoais, onde e até ao limite previsto pela legislação aplicável:

- Direito ao acesso
- Direito à retificação
- Direito ao apagamento ("direito a ser esquecido")
- Direito à limitação do tratamento
- Direito à portabilidade de dados
- Direito à oposição ao tratamento
- Direito a não estar sujeito a decisões automatizadas, incluindo a definição de perfis

Os colaboradores da Empresa podem exercer os direitos acima referidos junto do Encarregado da Proteção de Dados (dpo@securitas.pt).

Os Titulares de Dados têm o direito a retirar o consentimento, nos casos em que o tratamento se baseia neste. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.

Os Titulares de Dados, incluindo os colaboradores da Empresa, tem o direito de apresentar uma reclamação à Comissão Nacional de Proteção de Dados ("CNPD").

5.2. Fundamentos legais para o tratamento de dados pessoais

A Securitas apenas processará dados pessoais quando tenha uma base legal e uma finalidade comercial justificável conforme previsto no 5.1.

O tratamento de dados pessoais deve ter como base, pelo menos um fundamento legal, quando exista, de acordo com a lei aplicável.

5.3. Direito do titular dos dados

Dependendo da regulamentação aplicável no país, uma entidade da Securitas poderá prever diferentes direitos em relação ao tratamento de dados pessoais.

No entanto, todas as entidades da Securitas devem levar em consideração esses direitos ao tomar decisões comerciais ou administrativas, pois podem limitar a capacidade da entidade de tratar legalmente dados pessoais ou exigir que a entidade tome algumas ações específicas.

Cada entidade da Securitas deve tomar todas as medidas razoáveis (por exemplo, estabelecer e implementar procedimentos e políticas internas) para permitir o exercício dos direitos aplicáveis pelos titulares dos dados em tempo hábil.

5.4. Proteção de dados desde a conceção e por defeito

As considerações sobre a proteção de dados devem ser incorporadas nos produtos, operações e sistemas de tratamento desde os estágios iniciais de desenvolvimento e ao longo do ciclo de vida do tratamento. O objetivo da privacidade por defeito é permitir que a privacidade efetue todo o ciclo de vida do sistema usado para o tratamento de dados pessoais.

A extensão e os padrões aos quais isso será aplicado dependerão da legislação aplicável em matéria de proteção de dados em que o tratamento ocorrerá.

As **regras de Segurança da Informação** definem medidas de segurança que precisam estar em vigor para proteger informações e dados pessoais.

5.5. Medidas Técnicas e Organizativas

Todas as entidades Securitas devem implementar medidas técnicas e organizativas para garantir um nível de proteção e segurança adequado ao risco para o tratamento de dados pessoais.

Dependendo da natureza do tratamento, as medidas podem incluir:

(i) Anonimização ou pseudonimização e criptografia de dados pessoais;
(ii) A capacidade de garantir confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento;
(iii) A capacidade de manter e restaurar a disponibilidade e acesso a dados pessoais;
(iv) Um processo para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais.

As regras de Segurança da Informação definem mais orientações sobre medidas de segurança para informações e dados pessoais.

6. Responsável pelo tratamento de dados e Subcontratante

6.1. Responsabilidade

Quando uma entidade da Securitas da União Europeia/Espaço Económico Europeu estiver a tratar dados pessoais, atua como responsável pelo tratamento ou como subcontratante.

Em cada relação, em que a entidade da Securitas trate dados pessoais, é importante que seja realizada uma avaliação para aferir se a entidade da Securitas, em questão, está a atuar como responsável pelo tratamento ou subcontratante em relação ao tratamento.

6.2. Contrato de tratamento de dados

A Securitas celebrará um Contrato de Tratamento de Dados ("CTD"), quando a entidade da Securitas estiver a executar a sua prestação como responsável pelo tratamento ou quando atuar como subcontratante.

Existem certos requisitos obrigatórios a que o CTD deve obedecer.

A Securitas adotou dois modelos diferentes para esse fim, dependendo se a entidade da Securitas relevante estiver a atuar como responsável pelo tratamento ou como subcontratante.

É de notar, que é da responsabilidade da entidade Securitas, ao atuar como responsável pelo tratamento, garantir que os procedimentos forneçam garantias suficientes para implementar medidas técnicas e organizativas apropriadas para serem compatíveis e

proteger os dados pessoais sob sua responsabilidade.

A responsabilidade da entidade da Securitas, que atua como subcontratante, é garantir que apenas se compromete com as medidas técnicas e organizativas que poderá cumprir.

Os dois modelos de contrato de tratamento de dados são controlados pelo Departamento de Gestão, Risco, Jurídico e Dados e foram enviados para todas as Direções, com relevância para a matéria de proteção de dados, os respetivos modelos.

O modelo de contrato de tratamento de dados em que a Securitas atua como subcontratante está disponibilizado no SGE.

6.3. Registo de atividades de Tratamento

Cada entidade da Securitas deve manter um registo das suas atividades de tratamento.

O conteúdo desse registo deve seguir as leis e regulamentos aplicáveis. Se for fornecido um processo ou sistema para todo o Grupo Securitas ou Divisão para manter um registo das atividades de tratamento, cada entidade da Securitas dentro do escopo será responsável por seguir o processo.

6.4. Serviços baseados em Cloud

Quando se recorra a serviços de outsourcing para terceiros, como prestadores de serviços de IT ou ao recorrer a prestadores de serviços em cloud para o tratamento de dados pessoais, é necessário fazer considerações de proteção de dados e os requisitos de segurança das informações devem ser garantidos pela Securitas como parte da implementação ou outsourcing.

6.5. Transferência de dados pessoais

Quando os dados pessoais são transferidos da União Europeia/Espaço Económico Europeu para um país fora da União Europeia/Espaço Económico Europeu (um "país terceiro"), a entidade da Securitas que transfere ou dá acesso aos dados pessoais do país terceiro é responsável por garantir um nível adequado de proteção.

Os Dados Pessoais só podem ser transferidos para outra entidade se esta transferência estiver em conformidade com os princípios de Proteção de Dados e outras regras estabelecidas na presente política, nas leis e deliberações aplicáveis à Proteção de Dados. Como tal, essa transferência só pode ocorrer se estiver em conformidade com a finalidade para a qual os dados foram recolhidos e se a transferência for necessária para essa finalidade.

- **Tratamento realizado por um Subcontratante em benefício da Empresa**

Quando o Tratamento deva ser realizado por um Subcontratante em benefício da Empresa, deve existir um acordo escrito ou outro ato normativo.

O Subcontratante deve aceitar as obrigações contratuais para garantir o cumprimento da presente política e de outras obrigações contratuais necessárias para assegurar um nível adequado de proteção para a transferência e qualquer Tratamento subsequente (incluindo quaisquer transferências subsequentes).

- **Transferências de Dados Pessoais para um Responsável pelo Tratamento**

Nalguns casos pode ser necessário transferir Dados Pessoais para terceiros que não atuem como Subcontratantes de Dados perante a Empresa. Tal transferência pode ser permitida se o Titular dos Dados a tiver autorizado, ou se for necessária para a execução de um contrato com o Titular dos Dados, para cumprir as disposições obrigatórias da legislação nacional (por exemplo, uma transferência de Dados Pessoais para a segurança social, para autoridades fiscais ou para a inspeção do trabalho), para proteger os direitos legais (por exemplo, em litígios) ou em situações de emergência em que a transferência seja necessária para proteger os interesses fundamentais do Titular dos Dados (por exemplo, por motivos de segurança ou saúde).

Noutros casos, o Departamento de Gestão, Risco, Jurídico e Dados e o Encarregado da Proteção de Dados da Empresa devem ser consultados antes dos Dados Pessoais serem transferidos para terceiros.

- **Transferências transfronteiras de dados pessoais**

Ao implementar a presente política, a Empresa deve respeitar os requisitos legais que impõem condições específicas às transferências internacionais de Dados Pessoais.

Regras específicas para o Espaço Económico Europeu

Os Dados Pessoais só podem ser transferidos de um país do Espaço Económico Europeu (EEE) para países fora do EEE ("países terceiros") que a Comissão Europeia considere que garantem um nível adequado de proteção. No momento da publicação da presente política, estes incluem, entre outros, Andorra, Argentina, Canadá, Suíça e Nova Zelândia. A lista completa e atualizada de decisões sobre a adequação da proteção de dados pessoais em países terceiros pela Comissão Europeia pode ser consultada em: http://ec.europa.eu/justice/dataprotection/internationaltransfers/adequacy/index_en.htm.

6.6. Data Governance

As entidades da Securitas devem ter uma estrutura de gestão de dados sólida e compatível.

A estrutura de gestão de dados deve incluir pelo menos as seguintes funções: *Business Owner*, *System Owner* e *Data Owner*.

A tabela abaixo descreve os diferentes papéis e suas respetivas responsabilidades.

Função	Descrição	Responsibilidade
Business Owner	O *Business Owner* da empresa possui o processo comercial que usa os sistemas e os dados. Os *Business Owners* são responsáveis por garantir que os sistemas e o tratamento de dados suportam os processos de negócios.	• Verificar se os sistemas e o tratamento de dados dão suporte aos negócios; • Supervisionar a gestão do sistema do ponto de vista financeiro; • Aprovar decisões relacionadas à implementação de novos sistemas e principais desenvolvimentos; • Garantir que as Avaliações de Impacto na Proteção de Dados (AIPD) sejam executadas quando necessário.
System Owner	O *System Owner* é responsável por garantir que os dados sejam tratados no sistema de maneira segura e de acordo com a política acordada ao longo do seu ciclo de vida.	• Desenvolver um plano de segurança do sistema em coordenação com os proprietários dos dados, o administrador do sistema, o *security manager* e os usuários finais funcionais; • Manter o plano de segurança do sistema e garantir que o sistema seja implantado e operado de acordo com os requisitos de segurança acordados; • Atualizar o plano de segurança do sistema sempre que ocorrer uma alteração significativa; • Suporte na identificação, implementação e avaliação dos controlos de segurança comuns; • Garantir que os usuários do sistema e a equipa de suporte recebam instruções apropriadas sobre o uso do sistema, como regras de procedimento (ou uma política de uso aceitável); • Coordenar usuários, terceiros e gestão de sistemas técnicos.
	O *Data Owner* dos dados possui uma atividade de tratamento de dados, por exemplo o tratamento de dados	• Estabelecer as regras para o uso e proteção adequados dos dados; • Fornecer informações aos *System Owner* sobre os requisitos de segurança e controlo de segurança para o(s) sistema(s) de informação em que a informação reside; • Decidir quem tem acesso aos dados e

Data Owner	para pagamento de salários, pode pertencer à chefia de RH. O *Data Owner* é responsável por estabelecer o controlo para criação, recolha, tratamento, divulgação e eliminação dos dados.	com que tipos de privilégios ou direitos de acesso serão concedidos; • Auxiliar na identificação e avaliação dos controlos de segurança comuns onde as informações residem; • Garantir que os dados pessoais sejam processados por motivos legais e de acordo com os princípios do RGPD; • Definir períodos de retenção apropriados para os dados junto com o *System Owner*; • Informar o Encarregado de Proteção de Dados das atividades de tratamento e procurar aconselhamento quando necessário.

6.7. Violação de dados

As entidades da Securitas devem ter processos e garantir que exista um amplo conhecimento para reportar incidentes de segurança que envolvam dados pessoais dentro dos prazos exigidos. Se for fornecido um processo ou sistema para todo o grupo ou divisão para reportar a violação de dados pessoais, cada entidade da Securitas dentro do escopo será responsável por seguir o processo.

Se os incidentes reportados forem uma violação da segurança que levou à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou tratados de outra forma, deve ser incluído, por exemplo, transmissão acidental ou ilegal a terceiros, acesso acidental ou ilegal por terceiros ou perda de dados, independentemente de estar em ambientes internos ou externos ou devido à perda de hardware em que os dados pessoais foram armazenados ou acedidos.

Quando a Securitas for subcontratante, notificará o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais. Portanto, é importante:

1. A existência de um procedimento para entrar em contacto com o responsável pelo tratamento de dados, fornecendo informações relevantes, o mais rápido possível após uma violação de dados, nos casos em que a Securitas estiver a atuar como subcontratante.

2. Certifique-se de que é claro quem é o responsável por receber informações sobre violações de dados dos subcontratantes, quando a Securitas estiver como responsável pelo tratamento e a recorrer a subcontratados.

Quando exigido pela lei aplicável, a Empresa em questão deve notificar a Comissão Nacional de Proteção de Dados após a descoberta de uma violação de Dados Pessoais

dentro do prazo legal, isto é, sem demora injustificada e, sempre que possível, até 72h após ter conhecimento da mesma.

Da mesma forma, quando exigido pela lei aplicável, a sociedade da Empresa em questão deve notificar o Titular dos Dados, a menos que uma autoridade responsável pela aplicação da lei ou autoridade de supervisão determine que a notificação impediria uma investigação criminal ou causaria danos à segurança nacional. Nesse caso, a notificação deve ser adiada conforme instruído por essa autoridade.

A Empresa deve responder prontamente às consultas dos Titulares dos Dados relativas a tais violações de Dados Pessoais.

6.8. Avaliação de impacto na proteção de dados

As entidades da Securitas devem ter um processo para avaliar os riscos relacionados ao tratamento de dados pessoais. A avaliação de risco, obrigatória para os responsáveis pelo tratamento de dados pessoais, é denominada por Avaliação de Impacto na Proteção de Dados ("AIPD").

Cada entidade da Securitas deve avaliar e documentar os riscos relacionados ao tratamento de dados pessoais que possam constituir alto risco para os titulares dos dados.

7. Obrigações Gerais

A Empresa deve assegurar e poder demonstrar que o Tratamento de Dados Pessoais é realizado de acordo com a presente Política e com a lei aplicável.

Quando exigido pela lei aplicável, as empresas da Empresa devem tomar as medidas necessárias para manter um registo das atividades de Tratamento sob a sua responsabilidade.

Tanto no momento da determinação dos meios de Tratamento como no momento do próprio Tratamento, a Empresa deve implementar medidas adequadas para cumprir os princípios de Proteção de Dados listados na Política Global de Proteção de Dados Pessoais de uma forma eficaz e integrar as salvaguardas necessárias nas atividades de Tratamento ("Proteção de Dados desde a Conceção").

Quando uma sociedade da Empresa determinar as finalidades e meios para o Tratamento de Dados Pessoais em conjunto com outra empresa, estes, de uma forma transparente, determinarão as respetivas responsabilidades. Quando exigido pela lei aplicável, a essência do acordo pode ser disponibilizada ao Titular dos Dados.

Quando uma sociedade da Empresa atuar como um Subcontratante, comprometemo-nos a tratar os Dados Pessoais apenas segundo instruções documentadas do

Responsável pelo Tratamento para garantir que os envolvidos nas atividades de Tratamento assumiram um compromisso com vista à confidencialidade e ao cumprimento da legislação aplicável e dos requisitos do cliente.

8. Obrigação perante a Autoridade responsável pela Proteção de Dados – Comissão Nacional de Proteção de Dados

A Empresa responderá em tempo útil e de uma forma adequada a qualquer pedido por parte da Comissão Nacional de Proteção de Dados ("CNPD").

As questões podem estar relacionadas com quaisquer notificações de Tratamento de dados junto da CNPD ou, em geral, com o cumprimento das leis aplicáveis.

Os colaboradores da Empresa que receberem tal pedido da CNPD devem entrar em contacto com o Encarregado da Proteção de Dados ou com o departamento jurídico da Empresa para os envolver na comunicação com a CNPD.

9. Aplicabilidade

Esta Política de Proteção de Dados aplica-se a todas as unidades de report, em todos os níveis organizacionais dentro do Grupo Securitas Portugal, ou seja, empresas onde a Securitas AB (publ.) detém controlo acionista direto ou indireto em Portugal.

Esta Política deve ser comunicada e implementada, na medida do possível, em todas as parcerias comerciais (incluindo parceiros de joint venture) e nas relações contratuais de fornecedores.

10. Execução e Responsabilidade

Administrador – Delegado

- Responsável por conduzir a atividade no âmbito da sua área de responsabilidade de acordo com a presente Política;
- Presta apoio a todos os departamentos no desempenho das suas funções em conformidade com a presente Política;
- Confirma o cumprimento da presente Política.

Encarregado da Proteção de Dados da Empresa

- Aconselha a Administração e outras Direções da Empresa em matéria de Proteção de Dados;

- Recomenda a modificação à presente política para garantir que cumpre os requisitos legais aplicáveis e continua a satisfazer as nossas necessidades comerciais;
- Colabora em matéria de Proteção de Dados com os outros departamentos da empresa, nomeadamente as Áreas de Negócio, e outros departamentos com atuação relevante na proteção de dados;
- Presta apoio e orientação à Empresa que implementa a presente política e os procedimentos relacionados;
- Presta aconselhamento no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização;
- Resolve conflitos ou desentendimentos relacionados com os requisitos ao abrigo da presente política ou outros relacionados com questões de proteção de dados;
- Resolve conflitos entre a lei aplicável e a presente política;
- Mantém-se atualizado relativamente aos desenvolvimentos em matéria de Proteção de Dados e permanece informado sobre as leis, obrigações locais e orientações regulatórias aplicáveis, e as melhores práticas relacionadas com o respeito pela Proteção de Dados;
- Mantém uma visão global e monitoriza o desempenho das avaliações do impacto da proteção de dados e, quando solicitado, fornece orientação e aconselhamento adicionais
- Coopera com a CNPD e serve de ponto de contacto com esta autoridade sobre questões relacionadas com o tratamento de dados

É da responsabilidade de todos os colaboradores do Grupo Securitas conhecer e, cumprir esta Política, padrões e procedimentos de suporte.

11. Formação

É responsabilidade de cada Entidade da Securitas garantir que seja dada formação adequada a todos os colaboradores que lidam com dados pessoais regularmente, para garantir a conformidade com esta Política Global de Proteção de Dados Pessoais.

O Encarregado pela Proteção de Dados deve contribuir para desenvolver essa formação.

O Securitas desenvolveu um módulo de e-learning para o RGPD ministrado a todos os colaboradores.

12. Revisão e Seguimento da presente política

O cumprimento desta Política Global de Proteção de Dados Pessoais por todas as entidades e colaboradores da Securitas será monitorizado como parte do processo de Gestão corporativa de riscos da Securitas, que inclui autoavaliações, auditorias internas

e externas e acompanhamento de rotina de todos os assuntos relatados.

13. Referência a documentos e modelos adicionais

No SGE foram disponibilizados os seguintes documentos relacionados com a proteção de dados e em conformidade com o RGPD:

(i) DPKC – Phase I and II – *Data Protection Key Concepts*;
(ii) Política de Conservação de documentos;
(iii) Procedimento de Resposta a Violação de Dados Pessoais;
(iv) Modelo de Contrato de Tratamento de Dados – Securitas como Subcontratante;
(v) Procedimento de avaliação de impacto sobre a proteção de dados;
(vi) Diretriz sobre a avaliação de impacto na proteção de dados
(vii) Modelo da tabela de avaliação de impacto na proteção de dados;
(viii) Modelo de Declaração de Privacidade.

14. Aprovação

Esta Política Global de Proteção de Dados Pessoais foi aprovada pelo Conselho de Administração da Securitas.