Santander Asset Management/

Santander Pensões

Política de Proteção de Dados

(Global)

2022

ÍNDICE

1. INTRODUÇÃO

A Política de Proteção de Dados Pessoais tem por objetivo definir critérios em matéria de proteção de dados, desenvolvendo o Marco Corporativo de Cumprimento e Conduta relativamente ao controlo da informação, confidencialidade e cumprimento das exigências legais em matéria de proteção de dados.

Desta forma, está associada aos valores éticos e reafirma o firme compromisso de manter uma conduta de respeito das normas e padrões que os empregados do Grupo SAM devem ter em consideração nas suas operações diárias.

Esta Política é estruturada com base na seguinte regulamentação:

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- Lei n.º 58/2019, de 8 de agosto que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- Lei n.º 59/2019, de 08 de Agosto, relativa a Dados Pessoais para prevenção, deteção, investigação ou repressão de infrações penais;
- Lei n.º 41/2004, de 18 de Agosto, relativa à Proteção De Dados Pessoais E Privacidade Nas Telecomunicações, na sua redação atualizada pela Lei n.º 46/2012, de 29 de Agosto;
- Lei n.º 43/2004, de 18 de agosto, Lei de Organização e Funcionamento da Comissão Nacional de Proteção de Dados, com as alterações introduzidas pela Lei n.º 55-A/2010 e pela Lei n.º 58/2019, de 08.08.

2. DEFINIÇÕES E ÂMBITO

A presente Politica é aplicável a dados de natureza pessoal e respetivo tratamento.

Para uma melhor compreensão do documento, são definidos os seguintes termos/conceitos:

- **Dados pessoais:** qualquer informação numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo (por exemplo, dados biométricos), relativa a pessoas singulares identificadas ou identificáveis.
  - Informações de identificação direta: dados que incluem informações que permitem identificar ou distinguir uma pessoa singular diretamente e por si mesmas, sem a necessidade de combiná-los com outros dados, como: nome, endereço, número de telefone, número de fax, endereço de email, perfis identificativos exclusivos, como o número de segurança social, número de passaporte, etc.

- Dados de identificação: documentos de identificação (cartão do cidadão, número de identificação ou passaporte), endereço, imagem, voz, número de segurança social, telefone, marcas físicas, nome e sobrenome, assinatura, impressão digital e assinatura eletrónica.
- Dados biométricos: dados pessoais obtidos a partir de um tratamento técnico específico, relacionados com as características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitem ou confirmam a identificação exclusiva dessa pessoa, como imagens faciais ou dados de impressões digitais.

- Informações de identificação indireta: dados pessoais que incluem informação que, embora não possa identificar ou distinguir diretamente a pessoa, a SAM Investment Holdings, SL (Grupo SAM ou Topco) ou um terceiro podem associá-los ou ligá-los a uma pessoa singular, tendo em consideração todos os meios possíveis e razoáveis que possam ser usados. São, portanto, dados que, por si só, não permitem a identificação de pessoas, mas que combinados com outros fatores podem permitir a identificação.

- Dados pseudoanónimos: aqueles que não podem ser atribuídos a uma parte interessada específica sem o uso de informações adicionais, desde que essas informações adicionais sejam armazenadas separadamente e estejam sujeitas a medidas técnicas e organizacionais que garantam que não sejam atribuídos a uma pessoa física identificada ou identificável. Estes dados continuarão a ser considerados dados pessoais enquanto a pessoa singular à qual eles correspondem puder ser identificada. De qualquer forma, o procedimento de pseudonimização dos dados será uma das medidas a serem aplicadas para minimizar os riscos em termos de proteção de dados.

- Dados anónimos: dados que não permitem que uma pessoa seja identificada nem a tornam, de qualquer forma, identificável e, portanto, estão excluídos do âmbito dos regulamentos de proteção de dados. Os dados anonimizados nunca serão considerados dados pessoais.

- Interessado(s): pessoa singular titular dos dados submetidos ao tratamento, ou seja, é a pessoa singular que os dados identificam ou tornam identificável.

- Responsável pelo tratamento: pessoa singular ou coletiva que determina os objetivos e meios do tratamento. Aplicará as medidas técnicas e organizativas adequadas com o propósito de garantir e poder demonstrar que os seus tratamentos são conformes com a lei e regulamentação de proteção de dados em vigor.

- Subcontratante: pessoa singular ou coletiva que processa dados pessoais em nome do Responsável pelo Tratamento. Deverá cumprir das instruções do Responsável pelo Tratamento e com as exigências da normativa de proteção de dados em vigor. Colocará à disposição do Responsável pelo

Tratamento toda a informação necessária para demonstrar o cumprimento das suas obrigações e deverá oferecer as garantias suficientes, de forma q que o tratamento seja conforme com os requisitos da lei e regulamentação e garantir a proteção dos direitos dos titulares.

- Autoridade de Controlo: Autoridade independente encarregue de supervisionar a aplicação da lei e regulamentação em matéria de proteção de dados, como objetivo de proteger os direitos e liberdades fundamentais dos titulares dos dados.

- Incidente de segurança: incidente que afeta os dados pessoais:

  - Violação de confidencialidade: acesso, comunicação e/ou utilização não autorizada dos dados pessoais de uma ou mais pessoas singulares.

  - Violação de integridade: modificação, destruição, perda ou alteração acidental ou ilegal dos dados pessoais transmitidos, armazenados ou tratados de uma ou mais pessoas singulares, sem a sua autorização.

  - Violação de disponibilidade: impossibilidade de acesso aos dados pessoais.

- Transferência internacional de dados: fluxo de dados pessoais entre estados com diferentes regimes legais em matéria de proteção de dados.

- *Cookies* e tecnologias similares de rastreio ("local shared objects", "web beacons", "web bugs", "tracking pixels", etc.): ficheiros que são transferidos e armazenados no equipamento (computador/Smartphone/Tablet) do utilizador que navega na Internet ao aceder a determinadas páginas da web e aplicações e que são usados para armazenar e recuperar informações sobre a navegação feita nesse equipamento.

- Encarregado da Proteção de Dados: Figura encarregue de zelar e assessorar o cumprimento da lei e regulamentação de proteção de dados pela entidade; por outro lado, é o ponto de contacto com a Autoridade de Controlo e com os Interessados.

- Função Corporativa de Proteção de Dados: Encarregue de supervisionar o cumprimento nas distintas entidades do Grupo Santander envolvidas pela lei /regulamentação de proteção de dados. Por outro lado, é encarregue do controlo direto dos negócios e funções corporativas do Centro Corporativo.

As entidades do Grupo SAM, neste caso SAM SGOIC e a Santander, devem garantir a confidencialidade, segurança e integridade das informações pessoais pelas quais cada entidade é

responsável, bem como garantir que todos os terceiros com acesso aos dados da entidade, ou seja, os subcontratantes, cumprem as garantias e obrigações legais e contratuais relativas ao tratamento de dados e informações aos quais acedem.

Esta Política foi preparada pela SAM e disponibilizada às unidades locais, de entre as quais a **Santander Asset Management, SGOIC, S.A. (**adiante SAM SGOIC ou SAM Portugal) e a **Santander Pensões**, **Sociedade Gestora de Fundos de Pensões, S.A.** (adiante Santander Pensões) em cada jurisdição como documento de guia, estabelecendo o regime a ser aplicado à matéria em referência.

3. ÂMBITO DE APLICAÇÃO E TRANSPOSIÇÃO NAS FILIAIS

Esta Política foi elaborada pela SAM Investment Holdings, SL (Topco) e é disponibilizada às entidades do Grupo SAM como documento de referência, entre as quais a SAM SGOIC e a Santander Pensões, estabelecendo o regime de proteção de dados aplicável.

Cada entidade do Grupo SAM é responsável por preparar e aprovar nos seus órgãos sociais os documentos internos que permitam a aplicação, dentro do seu âmbito, das disposições contidas nos documentos do Grupo, com as adaptações que, se adequado, sejam estritamente essenciais para os tornarem compatíveis e cumprirem os requisitos regulamentares e normativos ou com as expectativas dos seus supervisores.

Essa aprovação deve ter a validação da SAM Investment Holdings, SL.

A SAM SGOIC e a Santander Pensões procedem à adaptação da Política de Proteção de Dados, e à validação previa junto da área Global da SAM Investment Holdings, SL antes da sua aprovação pelos respectivos Conselhos de Administração.

4. CRITÉRIOS

Todos os empregados estão obrigados a respeitar a privacidade de todas as pessoas cujos dados têm acesso em resultado da própria atividade da entidade ou do desempenho de suas funções, sejam estas clientes, outros colaboradores ou qualquer outra pessoa singular

Como princípio geral deverá zelar-se pela confidencialidade e segurança e integridade da informação de caracter pessoal e procurar que todos os fornecedores (contrapartes) com acesso a dados pessoais cumpram as garantias e obrigações legais e contratuais relativas ao tratamento de dados pessoais e informação a que tenham acesso.

A seguir, são detalhados os principais critérios corporativos destinados a assegurar o correto cumprimento das obrigações da normativa aplicável em matéria de proteção de dados pessoais:

4.1 Licitude, proporcionalidade e transparência.

Os dados pessoais devem ser tratados de forma:

- Lícita: os dados serão obtidos seguindo os requisitos estabelecidos pelos regulamentos aplicáveis.

O tratamento dos dados será sempre realizado tendo em conta alguma das seguintes bases legitimadoras:

- O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.
- O tratamento é necessário para a execução de um contrato no qual a parte interessada é parte ou para a aplicação, a pedido desta última, de medidas pré-contratuais.
- O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o Responsável pelo Tratamento e o Subcontratante estejam sujeitos;
- O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o Responsável pelo Tratamento;
- O tratamento for necessário para efeito dos interesses legítimos do Responsável pelo Tratamento ou de terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for um menor.

O âmbito da utilização de *cookies* ou outros dispositivos de seguimento, deverão ser analizados e adaptados, otendo o consentimento em caso necessário.

- Proporcional: os dados serão tratados unicamente de acordo com os fins necessários, adequados e relevantes.

- Transparente: As informações a proporcionar em relação à proteção de dados devem ser claras, concisas, transparentes, inteligíveis e facilmente acessíveis, com uma linguagem clara e simples, sem ambiguidades, ou seja, fáceis de entender pelo Interessado.

4.2 Fins compatíveis com a origem da recolha.

Deve ser assegurado que o tratamento de dados pessoais se limita às finalidades específicas, expressas e legítimas para as quais os dados foram originalmente recolhidos e que não serão posteriormente tratados de forma incompatível com tais finalidades.

Nesse sentido, cumpre esclarecer que as atividades de tratamento ulterior para fins de documentos oficiais e de interesse público, para pesquisa científica e histórica ou para fins estatísticos devem ser consideradas atividades de tratamento lícito compatíveis.

Como regra geral, será necessário solicitar o consentimento expresso dos Interessados quando o tratamento dos dados for para além dos fins para os quais foram inicialmente recolhidos e não seja compatível com os mesmos. A fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, dever ter-se em conta:

- Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
- O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
- A natureza dos dados pessoais, em especial se se tratar de dados especialmente protegidos;
- As eventuais consequências do tratamento posterior pretendido para os Interessados;
- A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Assim, desde que o tratamento de dados não seja baseado no consentimento, o tratamento de dados pessoais para fins distintos daqueles para os quais foram inicialmente recolhidos só deve ser permitido quando for compatível com os fins da recolha inicial. Em qualquer caso, os requisitos de transparência impostos pela regulamentação local aplicável devem ser cumpridos.

4.3 Minimização e precisão dos dados pessoais.

Os dados pessoais serão adequados, relevantes e limitados ao necessário em relação aos fins específicos para os quais são objeto de tratamento. Devem ser analisados em cada caso concreto (no tratamento ou quando ocorra uma modificação substancial do mesmo) os tipos de dados recolhidos e os processos associados ao tratamento com um critério de minimização, para que sejam acedidos o menor número possível de dados pessoais necessários para a sua execução.

Da mesma forma, devem ser adotadas todas as medidas razoáveis devem ser tomadas para suprimir ou retificar todos os dados que possam resultar desnecessários, ser imprecisos ou incompletos, em relação aos fins para os quais são objeto tratamento. Devem ser estabelecidos processos periódicos de revisão sobre a necessidade, exatidão e completude dos dados.

4.4 Integridade, confidencialidade, disponibilidade e resiliência

Deve ser assegurado que os dados são tratados com o devido nível de segurança, incluindo a proteção contra tratamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, através da aplicação de medidas técnicas ou organizacionais apropriadas, como por exemplo a pseudonimização ou a encriptação de dados pessoais. De acordo com a Política Corporativa de Gestão de Governo de Dados, todos os dados envolvidos num evento de dados (incluindo dados pessoais) deverão estar categorizados de acordo com a semântica usada no Grupo.

Além disso, devera garantir-se que os colaboradores, os terceiros que prestam serviços, as empresas subcontratadas pelos terceiros e os empregados destas, que no desempenho das suas funções tenham acesso a dados pessoais, se comprometem a manter em sigilo e a não se comunicar, em nenhum caso, a terceiros, essas informações pessoais, a menos que haja autorização expressa ou uma obrigação legal. Nesse sentido, todas as pessoas com acesso a dados pessoais devem assinar um acordo de sigilo e confidencialidade.

4.5 Conservação de Dados Pessoais

Deverá ser assegurado que os dados pessoais são sujeitos a tratamento de forma a permitir unicamente a identificação dos Interessadas apenas para fins legítimos do tratamento e durante o tempo estritamente necessário. Decorrido esse tempo, para a determinação dos períodos de manutenção mais extensos, as entidades devem ter em consideração os regulamentos locais que lhes são aplicáveis, em particular em matéria de prevenção de branqueamento de capitais e financiamento do terrorismo, bem como os prazos de prescrição para ações penais, comerciais, civis e laborais aplicáveis.

Não obstante o exposto, e desde que os regulamentos locais aplicáveis o permitam, os dados pessoais podem ser mantidos por um período além do necessário, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos, sem prejuízo da aplicação das medidas técnicas e organizacionais adequadas para proteger os direitos e liberdades das partes interessadas, de acordo com os regulamentos aplicáveis em vigor.

4.6 Dever de informação

Antes de recolher qualquer tipo de dados pessoais, devem ser comunicadas aos Interessados, de forma simples, precisa e de fácil compreensão as seguintes informações:

- Os dados da pessoa de contacto da entidade jurídica Responsável pelo Tratamento dos dados.
- Os detalhes de contacto do Encarregado da Proteção de dados;
- As finalidades a que se destina o tratamento dos dados pessoais.
- O fundamento jurídico para o tratamento (legitimador);
- Os destinatários ou as categorias de destinatários dos dados pessoais.
- As categorias e tipologia dos dados pessoais objeto de tratamento.
- O prazo (período) durante o qual os dados pessoais serão conservados, ou, quando não seja possível, os critérios utilizados para determinar esse período.
- A possibilidade dos Interessados exercerem os seus direitos sobre os seus dados pessoais.
- O direito de apresentar uma reclamação junto da autoridade competente, se aplicável.
- Se a recolha de dados pessoais é um requisito legal, contratual ou pré-contratual.
- Quando dados pessoais são obtidos por meio de terceiros, a origem de onde procedem os dados pessoais e, quando apropriado, se procedem de fontes de acesso público.

4.7 Direitos dos Interessados

Os Interessados ou os terceiros que facilitem os dados destes interessados devem ser informdos sobre a normativa (lei e regulamentação) aplicável, os riscos, as salvaguardas e direitos relacionados com o tratamento dos seus dados pessoais, através das cláusulas ou avisos de privacidade adequados.

Nesse sentido, são facilitados aos Interessados os meios necessários para o exercício dos seus direitos associados ao tratamento, de forma gratuita e simples e será realizada a gestão atempada e necessária desse exercício de direitos.

A título exemplificativo, os direitos dos Interessados previstos no Regulamentos Europeu de Proteção de Dados são os seguintes:

- Direito de acesso: direito de solicitar ao Responsável pelo Tratamento acesso aos dados pessoais que lhe digam respeito,

- Direito de retificação: o direito de solicitar ao Responsável pelo Tratamento a retificação, sem demora injustificada, no que diz respeito aos seus dados pessoais;

- Direito de cancelamento ou eliminação (direito ao esquecimento): o direito de solicitar ao Responsável pelo Tratamento, sem demora injustificada, o apagamento dos seus dados pessoais;

- Direito à limitação do tratamento: o direito de solicitar ao Responsável pelo Tratamento, sem demora injustificada, a limitação do tratamento dos dados pessoais de que seja titular em caso de inexatidão, ilicitude ou que já não sejam necessários para o Responsável pelo Tratamento e/ou o direito de se, verificadas as condições, se opor a esse tratamento;

- Direito à portabilidade dos dados: o direito de receber em formatos interoperáveis, de uso comum e leitura mecânica, os dados pessoais de que é titular e que sejam objeto de um tratamento assente no consentimento e seja efetuado por meios automatizados;

- Direito de oposição: direito de solicitar ao Responsável pelo Tratamento que cesse o tratamento dos seis dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

- Direito de não ser objeto de uma decisão baseada unicamente no tratamento automático: direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado e que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

4.8 Proteção de dados desde a conceção (*by design*) e por defeito

A privacidade desde a conceção tem por objetivo que a proteção dos dados pessoais esteja presente desde a primeira fase de criação de um produto ou serviço, enquanto o princípio da proteção de dados por defeito prevê que sejam objeto de tratamento os dados que sejam estritamente necessários para cada uma das finalidades legítimas.

Para o efeito, serão adotadas as medidas técnicas e organizativas destinadas a aplicar com eficácia os princípios da proteção de dados, que incorporem a todo o momento as garantias necessárias no tratamento, como por exemplo a pseudonimização, a minimização de acessos aos dados, o prazo de conservação dos dados, a homologação de fornecedores com acesso aos dados, as garantias adequadas em caso de transferências internacionais, a análise de novos produtos e serviços, etc.

4.9 Responsabilidade proativa

Em linha com o princípio da responsabilidade proactiva, em regra, deverá dispor-se de todas as evidências que acreditem o cumprimento de todos os requisitos na matéria, como por exemplo, um registo de atividades de tratamento, avaliações de impacto sobre proteção de dados, um inventário de fornecedores homologados em matéria de proteção de dados, procedimentos de gestão de incidentes de segurança que afetem dados pessoais, etc

4.10 Incidentes de Segurança dos Dados Pessoais

Devem ser disponibilizadas as ferramentas e procedimentos de resposta necessários para responder a qualquer violação de segurança que cause a destruição, perda ou alteração acidental ou ilegal de dados pessoais transmitidos ou mantidos, ou à comunicação ou acesso não autorizado a esses dados.

Por outro lado, deve contar-se com os meios necessários devem estar disponíveis para demonstrar que toda a proteção tecnológica apropriada foi aplicada e as medidas organizacionais apropriadas foram tomadas para determinar, o mais rapidamente possível: (i) se houve uma violação da segurança dos dados pessoais; (ii) se constitui um risco para a privacidade de pessoas singulares, e (iii) se é necessário informar a autoridade de controlo e o(s) Interessado(s).

Devem existir procedimentos claros e acessíveis para todos os colaboradores que permitam uma diligência devida ("Due Dilligence") em incidentes de segurança que afetem os dados pessoais e que facilitem a coordenação rápida de todas as áreas envolvidas.

4.11 Transferências internacionais

Conforme definido acima, a transferência internacional de dados significa um fluxo de dados pessoais entre estados com diferentes regimes legais que concedem diferentes graus de proteção de dados.

Devem ser aplicadas garantias adequadas tanto no país de origem como no país de destino dos dados para manter todas as transferências internacionais de dados pessoais dentro de um nível apropriado de segurança, que podem ser previstas por cláusulas contratuais – tipo, códigos de conduta, mecanismos de certificação aprovados ou regras corporativas vinculativas.

5. MODELO DE *GOVERNO* E COMPETÊNCIAS

O governo corporativo em matéria de proteção de dados é descrito infra, sem prejuízo do cumprimento da normativa corporativa geral que seja aplicável.

A Função Global de Proteção de Dados informa periodicamente a Comissão delegada de Riscos das questões relevantes em matérias de dados dentro do Grupo SAM e, pelo menos, anualmente, o estado do cumprimento das unidades de negócio sob sua supervisão e seguimento.

6. TITULARIDADE, INTERPRETAÇÃO, DATA DE VALIDADE E REVISÃO PERIÓDICA

A elaboração desta Política é da responsabilidade da Função de Riscos e Compliance da SAM Investment Holdings, SL.

A adaptação desta politica para a SAM SGOIC e Santander Pensões foi preparada pelo Departamento de Riscos & Compliance, que previamente a validou junto da área Global, tendo sido submetida à aprovação dos respetivos Conselhos de Administração em Maio de 2022.A interpretação desta Política é da responsabilidade de cada área de Riscos & Compliance (inclusive na SAM SGOIC e na Santander Pensões)

Esta política entra em vigor a partir da data da sua publicação. O seu conteúdo estará sujeito a revisão periódica, sendo realizadas as alterações ou modificações consideradas apropriadas.

7. CONTROLO DE VERSÕES

Versão	Área responsável	Descrição	Comité aprovação	Data de Aprovação
1	Risk & Compliance Global/Raul Garcia	Politica inicial aprovada	Board SAM Investment Holdings SL.	26/04/2018
2	Risk & Compliance Global/Raul Garcia	Adaptação à nova Política corporativa	Board SAM Investment Holdings SL.	06/06/2020

3	Risk & Compliance Global/Raul Garcia	Inclusão de: (i) detalhe do exercício de direitos;(ii) principio da privacidade por conceção e por defeito (iii) responsabilidade proactiva (iv) transferências internacionais de dados	Board SAM Investment Holdings SL	17.06.2022[1]

Adaptação da política à SAM Portugal e à Santander Pensões:

Versão	Área responsável	Descrição	Comité aprovação	Data de Aprovação
1.1	Riscos & Compliance SAM PT e SPensões	Politica inicial aprovada	Conselho de Administração da SAM Portugal e Santander Pensões	19/05/2018
2.1	Riscos & Compliance SAM PT e SPensões	Adaptação da nova política corporativa	Conselho de Administração da SAM Portugal e Santander Pensões	08/06/2020
3.1	Riscos & Compliance SAM PT e SPensões	Adaptação da nova política corporativa	Conselho de Administração da SAM Portugal e Santander Pensões	25.05.2022

[1] Pendente de aprovação pelo Conselho de Administração da TopCo.