Índice

1. Finalidade, Âmbito e Destinatários

Esta política define os períodos de retenção necessários para todas as categorias específicas de dados pessoais e define os padrões mínimos a serem aplicados ao destruir certas informações dentro da Sintética, doravante denominada "Empresa".
Esta Política aplica-se a todas as unidades de negócios, processos e sistemas em todos os países nos quais a Empresa conduz negócios e possui negócios ou outras relações comerciais com terceiros.
Esta Política aplica-se a todos os executivos, diretores, trabalhadores, agentes, afiliadas, contratados, consultores ou prestadores de serviços da Empresa que possam recolher, processar ou ter acesso a dados (incluindo dados pessoais e/ou dados pessoais confidenciais). É responsabilidade de todos os acima familiarizarem-se com esta Política e garantir o cumprimento adequado.
Esta política aplica-se a todas as informações usadas na empresa. Exemplos de documentos incluídos:

- Endereços Eletrónicos
- Documentos impressos
- Documentos digitais
- Vídeo e áudio
- Dados gerados por sistemas de controlo de ponto

2. Documentos de Referência

- EU GDPR 2016/679 (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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados))
- Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016
- 10 Medidas para Preparar a Aplicação do Regulamento Europeu de Proteção de Dados (CNPD)
- Política Geral de Proteção de Dados Pessoais (02.1)

3. Regras de Retenção

3.1. Princípio Geral de Retenção

No caso de qualquer categoria de documentos não especificamente definidos em outra parte desta Política (e em particular, no Calendário de Retenção de Dados) e a menos que exigido de outra forma pela lei aplicável, o período de retenção exigido para esse documento será de 10 anos a partir da data de criação do documento.

3.2. Programa Geral de Retenção

A Equipa de Proteção de Dados define o período de tempo durante o qual os documentos e registos eletrónicos devem ser retidos por meio do Calendário de Retenção de Dados.

Poderão existir exceções aos períodos de retenção no Calendário de Retenção de Dados nos seguintes casos:

- Investigações em andamento das autoridades dos Estados Membros, se houver uma necessidade de registos de dados pessoais serem necessários pela Empresa para comprovar o cumprimento de quaisquer requisitos legais; ou
- Quando exercem direitos legais em casos de processos judiciais pela legislação local.

3.3. Backup dos Dados durante o Período de Retenção

A possibilidade de que os meios de dados usados para backup se desgastem deve ser considerada. Se forem escolhidos meios de backup eletrónicos, todos os procedimentos e sistemas que garantem o acesso à informação durante o período de retenção (tanto no que diz respeito ao portador da informação quanto na legibilidade dos formatos) também serão guardados de maneira a proteger as informações contra perdas como resultado de futuras mudanças tecnológicas. A responsabilidade pelo armazenamento é da Equipa de Proteção de Dados.

3.4. Destruição de Dados

A Empresa e os seus funcionários devem regularmente rever todos os dados, sejam eles mantidos eletronicamente ou em papel, para decidir eliminar ou excluir quaisquer dados, uma vez que a finalidade para a qual esses documentos foram criados já não é mais relevante. Veja o Anexo do Calendário de Retenção de Dados. A responsabilidade geral pela destruição de dados é da Equipa de Proteção de Dados.

Uma vez tomada a decisão de eliminar de acordo com o Calendário de Retenção, os dados devem ser excluídos, triturados ou destruídos tendo em atenção se é papel ou em formato eletrónico dependendo da sua forma e tendo em conta sempre o grau equivalente ao seu valor para os outros e o seu nível de confidencialidade. O método de destruição varia e depende da natureza do documento. Por exemplo, quaisquer documentos que contenham informações sensíveis ou confidenciais (e dados pessoais particularmente sensíveis) devem ser destruídos como lixo confidencial e estar sujeitos à eliminação eletrónica segura; alguns contratos expirados ou substituídos podem apenas garantir a destruição interna. A seção destruição de documentos abaixo define o modo de destruição.

Neste contexto, o trabalhador deve executar as tarefas e assumir as responsabilidades relevantes para a destruição da informação de forma adequada. O processo específico de eliminação ou destruição pode ser realizado por um trabalhador ou por um prestador de serviços interno ou externo que a Equipa de Proteção de Dados subcontrate para este fim. Quaisquer disposições gerais aplicáveis ao abrigo das leis de proteção de dados relevantes e da Política Geral de Proteção de Dados Pessoais da Empresa devem ser cumpridas.

Devem existir controlos apropriados que impeçam a perda permanente de informações essenciais da empresa como resultado da destruição maliciosa ou não intencional de informações - esses controlos são descritos nas Políticas de Segurança da Informação.

A Equipa de Proteção de Dados deve documentar e aprovar totalmente o processo de destruição. Os requisitos legais aplicáveis para a destruição de informações, particularmente os requisitos sob as leis de proteção de dados aplicáveis que devem ser integralmente observados.

3.5. Violação, Execução e Conformidade

A pessoa designada com responsabilidade pela Proteção de Dados, a Equipa de Proteção de Dados, tem a responsabilidade de garantir que cada um dos escritórios da Empresa cumpra esta Política. É também da responsabilidade deste auxiliar qualquer escritório local com perguntas de qualquer proteção de dados local ou autoridades governamentais.

Qualquer suspeita de violação desta Política deve ser reportada imediatamente à Equipa de Proteção de Dados. Todos os casos de suspeita de violações desta Política devem ser investigados e tomadas as medidas apropriadas.

O não cumprimento desta Política pode resultar em consequências adversas, incluindo, mas não limitado a perda de confiança do cliente, litígio e perda de vantagem competitiva, perda financeira e danos à reputação da Empresa, danos pessoais, danos ou perdas. O não cumprimento desta Política pelos trabalhadores permanentes, temporários ou contratados, ou quaisquer terceiros, que tenham tido acesso às instalações ou informações da Empresa, pode, portanto, resultar em processos disciplinares ou no término de seu contrato de trabalho. Tal não conformidade também pode levar a ação(ões) legal(ais) contra as partes envolvidas em tais atividades.

3.6. Destruição de Documentos

3.6.1. Calendarização da Rotina de Destruição

Os registos que podem ser regularmente destruídos, a menos que sujeitos a uma investigação legal ou regulatória em andamento, são os seguintes:

- Anúncios e avisos de reuniões diárias e outros eventos, incluindo aceitações e pedidos de desculpas;
- Solicitações de informações comuns, como rotas de viagem;
- Reservas para reuniões internas sem cobranças / custos externos;
- Transmissão de documentos, tais como cartas, folhas de rosto de fax, mensagens de correio eletrónico ou postal, folhetos e itens semelhantes que acompanham documentos, mas não adicionam qualquer valor;
- Recados de mensagens;
- Lista de endereços substituída, listas de distribuição, etc.
- Duplicação documentos como cópias de documentação de identificação pessoal, rascunhos inalterados, impressões de Snapshots ou extratos de bancos de dados e arquivos diários;
- Publicações internas de stock(s) obsoletas; e

- Revistas comerciais, catálogos de fornecedores, folhetos e boletins informativos de fornecedores ou outras organizações externas.

Em todos os casos, a eliminação encontra-se sempre sujeita a quaisquer requisitos que possam existir no contexto de um litígio.

3.6.2. Método de Destruição

Os documentos de Nível I são aqueles que contêm informações de mais alta segurança e confidencialidade e aquelas que incluem dados pessoais. Estes documentos devem ser eliminados como lixo confidencial (triturado transversalmente e incinerado) e sujeitos a uma eliminação eletrónica segura. A destruição dos documentos deve incluir prova de destruição.
Os documentos de nível II são documentos proprietários que contêm informações confidenciais, como nomes, assinaturas e endereços de terceiros, ou que podem ser usados por terceiros para cometer fraudes, mas que não contêm dados pessoais. Os documentos devem ser cortados transversalmente e depois colocados em lixeiras trancadas para recolha por uma empresa de eliminação aprovada, e os documentos eletrónicos estarão sujeitos à eliminação eletrónica segura.
Documentos de nível III são aqueles que não contêm informações confidenciais ou dados pessoais e são documentos da empresa publicados. Estes devem ser triturados ou descartados através de uma empresa de reciclagem e incluir, entre outras coisas, anúncios, catálogos, panfletos e boletins informativos. A destruição dos documentos não necessita incluir prova de destruição.

3.7. Gestão Base dos Registos deste Documento

Nome do registo	Pessoa responsável pelo armazenamento	Controlo para proteção de registo	Tempo de retenção
Calendário de Retenção de Dados (02.7)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	Permanentemente

3.8. Validade e gestão do documento

Este documento é válido a partir de 15 de setembro de 2018.

3.9. Anexos

Anexo – Calendário de Retenção de Dados

_____
[assinatura Gerência]

	Registo do motivo de alteração
Versão 2 __/__/___	
Versão 3 __/__/___	
Versão 4 __/__/___	
Versão 5 __/__/___	
Versão 6 __/__/___	