Índice

1. Finalidade, Âmbito e Destinatários

A Sintética, doravante referida como a "Empresa", esforça-se para cumprir as leis e regulamentos aplicáveis relacionados à proteção de dados pessoais nos países onde a Empresa opera. Esta Política estabelece os princípios básicos pelos quais a Empresa processa os dados pessoais de consumidores, clientes, fornecedores, parceiros de negócios, funcionários e outros indivíduos, e indica as responsabilidades dos seus departamentos comerciais e funcionários durante o processamento de dados pessoais.
Esta Política se aplica à Empresa e suas subsidiárias integrais, controladas direta ou indiretamente, que conduzem negócios dentro da Área Económica Europeia (EEA) ou processam os dados pessoais de sujeitos de dados dentro da EEA.
Os utilizadores deste documento são todos funcionários, permanentes ou temporários, e todos os contratados que trabalham em nome da Empresa.

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 de Proteção de Dados do Funcionário (02.2)
- Política de Retenção de Dados (02.6)
- Descrição do cargo de Encarregado da Proteção de Dados (02.8)
- Diretrizes do Inventário de Dados e Mapeamento de Atividades de Processamento (03.1)
- Procedimento de Acesso aos Dados pelo Titular dos Dados (04.5)
- Metodologia de Avaliação do Impacto da Proteção de Dados (AIPD) (05.1)
- Procedimento de Transferência de Dados Transfronteiras (06.1)
- Segurança de Dados Pessoais: Controlo da entrada nas instalações; controlo dos suportes de dados; controlo da inserção; controlo da utilização; controlo de acesso; controlo da transmissão; controlo da introdução; controlo do transporte
- Procedimento de Resposta e Notificação de Violação de Dados (09.1)

3. Definições

As seguintes definições de termos usados neste documento foram retiradas do Artigo 4 do Regulamento Geral de Proteção de Dados da União Europeia:

Dados Pessoais: Qualquer 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.

Dados Pessoais Sensíveis: Os dados pessoais que são, pela sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais merecem proteção específica, dado que o contexto do seu processamento pode criar riscos significativos para os direitos e liberdades fundamentais. Esses dados pessoais incluem dados pessoais revelando origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, ou associação a sindicatos, dados genéticos, dados biométricos para identificar unicamente uma pessoa singular, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular.

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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

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.

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.

Anonimização: Desidentificar de forma irreversível os dados pessoais de forma que a pessoa não possa ser identificada usando tempo, custo e tecnologia razoáveis, seja pelo responsável pelo tratamento ou por qualquer outra pessoa, para identificar esse indivíduo. Os princípios de processamento de dados pessoais não se aplicam a dados anónimos, pois não são mais dados pessoais.

Pseudonimização: 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. Pseudonimização reduz, mas não elimina completamente, a capacidade de vincular dados pessoais a um assunto de dados. Como os dados sob pseudónimo ainda são dados pessoais, o processamento de dados sob pseudónimo deve obedecer aos princípios do Processamento de Dados Pessoais.

Tratamento Transfronteiriço: O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro.

Autoridade de Controlo: uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51 do RGPD da UE.

A **Autoridade de Controlo Principal** é o organismo que tem como responsabilidade principal gerir uma atividade de tratamento transfronteiriço, por exemplo, quando está a ser investigada uma empresa que exerça atividades de tratamento em vários Estados-Membros. A autoridade principal coordena as operações que impliquem as autoridades de controlo interessadas, em conformidade com os artigos 60.º a 62.º do regulamento (por exemplo: balcão único, assistência mútua e operações conjuntas). Apresenta qualquer projeto de decisão às autoridades de controlo com interesse na matéria.

Cada **"Autoridade de Controlo Local"** continuará a manter no seu próprio território e monitorizará qualquer processamento de dados local que afete os titulares de dados ou que seja realizado por um Responsável pelo Tratamento ou subcontratante da UE ou não UE quando o seu processamento atingir os titulares de dados residentes no seu território. Suas tarefas e poderes incluem conduzir investigações e aplicar medidas administrativas e multas, promovendo a conscientização pública sobre os riscos, regras, segurança e direitos em relação ao processamento de dados pessoais, bem como obter acesso a quaisquer instalações do responsável pelo tratamento e do subcontratante, incluindo qualquer equipamento e meios de processamento de dados.

"Estabelecimento principal no que diz respeito a um responsável pelo tratamento": Quando uma organização tem vários estabelecimentos na UE, o princípio a seguir é que o estabelecimento principal é o local da administração central dessa organização. No entanto, se outro estabelecimento tomar as decisões sobre as finalidades e os meios de tratamento – e tiver competência para mandar executar tais decisões –, passa a constituir o estabelecimento principal. Cabe aos responsáveis pelo tratamento de dados estabelecer claramente onde são tomadas as decisões sobre as finalidades e os meios das atividades de tratamento de dados pessoais.

O **estabelecimento principal do subcontratante** é o local da sua administração central na União, ou, caso não tenha administração central na União, o local onde são exercidas as principais atividades de tratamento de dados na União. Nos casos que impliquem tanto o responsável pelo tratamento como o subcontratante, a autoridade de controlo principal deverá continuar a ser a autoridade de controlo do Estado-Membro onde o responsável pelo tratamento tem o estabelecimento principal, mas a autoridade de controlo do subcontratante deverá ser considerada uma autoridade de controlo interessada e deverá participar no processo de cooperação previsto pelo presente regulamento.

Grupo de Empresas: Qualquer *holding* em conjunto com as sua(s) subsidiária(s).

4. Princípios Básicos Relativos ao Processamento de Dados Pessoais

Os princípios de proteção de dados descrevem as responsabilidades básicas das organizações que lidam com dados pessoais. O Artigo 5(2) do RGPD estipula que *"o Responsável pelo Tratamento deve ser responsável e demonstrar o cumprimento dos princípios*".

4.1. Licitude, Lealdade e Transparência

Os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados.

4.2. Limitação das finalidades

Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

4.3. Minimização dos Dados

Os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados. A Empresa deve aplicar a anonimização ou pseudonimização aos dados pessoais, se possível, para reduzir os riscos para os titulares de dados em causa.

4.4. Exatidão

Os dados pessoais devem ser exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.

4.5. Limitação da Conservação

Os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.

4.6. Integridade e confidencialidade

Levando em conta o estado da tecnologia e outras medidas de segurança disponíveis, o custo de implementação e a probabilidade e gravidade dos riscos de dados pessoais, a Empresa deve usar medidas técnicas ou organizacionais apropriadas para processar Dados Pessoais de uma maneira que garanta a segurança apropriada dos dados pessoais, incluindo proteção contra destruição acidental ou ilegal, perda, alternância, acesso não autorizado ou divulgação.

4.7. Responsabilidade

O responsável pelo tratamento é responsável pela demonstração da conformidade com os princípios acima descritos.

5. Proteção de Dados nas Atividades do Negócio

Para demonstrar a conformidade com os princípios da proteção de dados, uma organização deve criar proteção de dados em todas as suas atividades de negócios.

5.1. Notificação do Titular dos Dados

(Veja a sessão Diretrizes de Processamento.)

5.2. Consentimento do Titular dos Dados

(Veja a sessão Diretrizes de Processamento.)

5.3. Recolha

A empresa deve-se esforçar para recolher a menor quantidade possível de dados pessoais. Se os dados pessoais forem recolhidos por terceiros, a Equipa de Proteção de Dados deve garantir que os dados pessoais são recolhidos legalmente.

5.4. Uso, Retenção e Destruição

Os propósitos, métodos, limitação de armazenamento e período de retenção de dados pessoais devem ser consistentes com as informações contidas na **Política de Privacidade**. A Empresa deve manter a precisão, integridade, confidencialidade e relevância dos dados pessoais com base no propósito do processamento. Mecanismos de segurança adequados, projetados para proteger os dados pessoais, devem ser usados para evitar que dados pessoais sejam roubados, mal utilizados ou violados, além de evitar violações de dados pessoais. O Responsável de TI é responsável pela conformidade com os requisitos listados nesta seção.

5.5. Divulgação a Terceiros

Sempre que a Empresa utilizar um fornecedor ou parceiro comercial para processar dados pessoais em seu nome, a Equipa de Proteção de Dados deve garantir que esse subcontratante fornece medidas de segurança para proteger os dados pessoais e que são apropriados aos riscos associados. Para este propósito, o Questionário de Conformidade do RGPD do Subcontratante (07.1) deve ser usado.
A Empresa deve exigir contratualmente que o fornecedor ou parceiro de negócios forneça o mesmo nível de proteção de dados. O fornecedor ou parceiro comercial deve apenas processar dados pessoais para cumprir suas obrigações contratuais com a Empresa ou sob as instruções da Empresa e não para quaisquer outros fins. Quando a Empresa processa dados pessoais em conjunto com um terceiro independente, a Empresa deve especificar explicitamente suas respetivas responsabilidades e as do terceiro num contrato relevante ou qualquer outro documento vinculativo legal, como o Contrato de Processamento de Dados do Subcontratante (07.2).

5.6. Transferência Transfronteiriça de Dados Pessoais

Antes de transferir dados pessoais para fora da Área Económica Europeia (EEA), devem ser adotadas proteções adequadas, incluindo a assinatura de um Acordo de Transferência de Dados, conforme requerido pela União Europeia e, se necessário, autorização da Autoridade de Controlo relevante. A entidade que recebe os dados pessoais deve cumprir os princípios de processamento de dados pessoais estabelecidos no Procedimento de Transferência de Dados Transfronteiras.

5.7. Direito ao Acesso pelo Titular dos Dados

Ao atuar como um responsável pelo tratamento, a Equipa de Proteção de Dados é responsável por fornecer aos titulares dos dados um mecanismo de acesso razoável para permitir que eles acedam aos seus dados pessoais e permitir que eles atualizem, corrijam, apaguem ou transmitam seus Dados Pessoais, se apropriado ou exigido por lei. O mecanismo de acesso será detalhado no Procedimento de Acesso aos Dados pelo Titular dos Dados (04.5).

5.8. Portabilidade dos Dados

Os titulares de dados têm o direito de receber, mediante solicitação, uma cópia dos dados que nos forneceram num formato estruturado e de transmitir esses dados para outro responsável pelo tratamento, gratuitamente. A Equipa de Proteção de Dados é responsável por garantir que tais solicitações sejam processadas dentro de um mês, que os pedidos não sejam excessivos e não afetem os direitos de dados pessoais de outros indivíduos.

5.9. Direito ao Apagamento (RtbF)

Mediante solicitação, os Titulares dos Dados têm o direito de obter da Empresa o apagamento dos seus dados pessoais. Quando a Empresa está a atuar como responsável pelo tratamento, a Equipa de Proteção de Dados deve tomar as medidas necessárias (incluindo medidas técnicas) para informar os terceiros que usam ou processam esses dados para atender à solicitação.

6. Diretrizes de Processamento

Os dados pessoais só devem ser processados quando explicitamente autorizados pela Equipa de Proteção de Dados.
A Empresa deve decidir se executa a Avaliação de Impacto de Proteção de Dados para cada atividade de processamento de dados de acordo com as **Diretrizes da Avaliação de Impacto de Proteção de Dados**.

6.1. Avisos aos Titulares dos Dados

No momento da recolha ou antes de recolher dados pessoais para qualquer tipo de atividades de processamento, incluindo, mas não limitado a, venda de produtos, serviços ou atividades de marketing, o [cargo] é responsável por informar adequadamente os titulares dos dados: os tipos de dados pessoais recolhidos, as finalidades do processamento, métodos de processamento, direitos dos titulares dos dados com relação aos seus dados pessoais, período de retenção, possíveis transferências internacionais de dados, e se os dados serão partilhados com terceiros e medidas de segurança da Empresa para proteger esses dados pessoais. Esta informação é fornecida através da **Política de Privacidade**.
Se a sua empresa possuir várias atividades de processamento de dados, será necessário desenvolver diferentes politicas dependendo da atividade de processamento e das categorias de dados pessoais recolhidos - por exemplo, uma política para o envio de correspondência e outra política para o envio de mercadoria.
Quando os dados pessoais são partilhados com terceiros, a Equipa de Proteção de Dados deve garantir que os titulares de dados tenham sido notificados por meio de uma Politica de Privacidade.
Quando os dados pessoais são transferidos para um país terceiro de acordo com a Política de Transferência de Dados Transfronteiriços, a Politica de Privacidade deve refletir isso e indicar claramente para onde e para que entidade estão a ser transferidos os dados pessoais.
Quando os dados pessoais confidenciais estiverem a ser recolhidos, a Equipa de Proteção de Dados deve certificar-se de que a política de privacidade declara explicitamente a finalidade para a qual esses dados pessoais confidenciais são recolhidos.

6.2. Obtendo Consentimento

Sempre que o processamento de dados pessoais for baseado no consentimento do titular dos dados ou em outros motivos legais, a Equipa de Proteção de Dados é responsável por manter um registo de tal consentimento. A Equipa de Proteção de Dados é responsável por fornecer aos titulares de dados opções para fornecer o consentimento e deve informar e garantir que o seu consentimento possa ser retirado a qualquer momento.
Quando a recolha de dados pessoais for relativa a uma criança menor de 16 anos, a Equipa de Proteção de Dados deve garantir que o consentimento dos pais seja dado antes da recolha, usando o Formulário de Consentimento dos Pais (4.3).
Quando surgem solicitações para corrigir, alterar ou destruir registos de dados pessoais, a Equipa de Proteção de Dados deve garantir que essas solicitações sejam tratadas dentro de um prazo razoável. A Equipa de Proteção de Dados também deve registar as solicitações e manter um registo das mesmas.

Os dados pessoais só devem ser processados para o propósito para o qual foram originalmente recolhidos. No caso em que a Empresa deseja processar dados pessoais recolhidos para outra finalidade, a Empresa deve buscar o consentimento dos seus titulares de dados numa redação clara e concisa. Qualquer solicitação desse tipo deve incluir a finalidade original para a qual os dados foram recolhidos e também a(s) finalidade(s) nova(s) ou adicional(ais). A solicitação também deve incluir o motivo da mudança na(s) finalidade(s). A Equipa de Proteção de Dados é responsável pelo cumprimento das regras deste parágrafo.
Agora e no futuro, a Equipa de Proteção de Dados deve garantir que os métodos de recolha estejam em conformidade com as leis relevantes, boas práticas e padrões do setor.
A Equipa de Proteção de Dados é responsável por criar e manter um registo das Políticas de Privacidade.

7. Organização e Responsabilidades

A responsabilidade de garantir o processamento adequado de dados pessoais é de todos que trabalham para ou com a Empresa e que têm acesso a dados pessoais processados pela Empresa.
As principais áreas de responsabilidades para o processamento de dados pessoais estão nas seguintes funções organizacionais:
A **Gerência** toma decisões e aprova as estratégias gerais da Empresa sobre a proteção de dados pessoais.
A **Equipa de Proteção de Dados** é responsável pela gestão do programa de proteção de dados pessoais e é responsável pelo desenvolvimento e promoção de políticas de proteção de dados pessoais end-to-end, conforme definido na Descrição do Cargo de Encarregado da Proteção de Dados (02.8).
O **Departamento Jurídico junto com** a **Equipa de Proteção de Dados**, monitoriza e analisa as leis de dados pessoais e mudanças nos regulamentos, desenvolve requisitos de conformidade e auxilia os departamentos de negócios a atingir suas metas de dados pessoais.

O **Responsável de TI,** é responsável por:

- Garantir que todos os sistemas, serviços e equipamentos usados para armazenar dados atendam a padrões de segurança aceitáveis.
- Realizar verificações regulares para garantir que os equipamentos e os programas de segurança estejam a funcionar adequadamente.

O **Responsável de Marketing** é responsável por:

- Aprovar todas as declarações de proteção de dados anexadas a comunicações, como correio eletrónico e correio postal.
- Abordar quaisquer questões de proteção de dados de jornalistas ou meios de comunicação, como jornais.
- Se necessário, trabalhar com a Equipa de Proteção de Dados de proteção de dados para garantir que as iniciativas de marketing respeitem os princípios de proteção de dados.

O **Responsável de Recursos Humanos** é responsável por:

- Melhorar a consciencialização de todos os funcionários no papel de utilizadores sobre a proteção de dados pessoais do usuário.
- Organizar formações de proteção de dados pessoais para os funcionários que trabalham com dados pessoais.
- Proteção dos dados pessoais dos funcionários. Deve-se garantir que os dados pessoais dos funcionários sejam processados com base nos objetivos e necessidades comerciais legítimos da entidade empregadora.

O **Responsável de Aprovisionamento** é responsável por passar as responsabilidades de proteção de dados pessoais aos fornecedores e melhorar os níveis de consciencialização dos fornecedores quanto à proteção de dados pessoais, bem como reduzir os requisitos de dados pessoais que os terceiros estejam a usar. O Departamento de Compras deve garantir que a Empresa se reserva ao direito de auditar fornecedores.

8. Diretrizes para o estabelecimento da Autoridade de Controlo Principal

8.1. Necessidade de Estabelecer a Autoridade de Controlo Principal

A identificação de uma autoridade de controlo principal só é relevante se a empresa efetuar processamento transfronteiriço de dados pessoais.
A transferência entre fronteiras de dados pessoais é realizada, se:

a) *O tratamento de dados pessoais é efetuado por filiais da Empresa com sede noutros Estados-Membros; ou*
b) *O tratamento de dados pessoais que ocorre num único estabelecimento da Empresa na União Europeia, mas que afeta substancialmente ou é suscetível de afetar substancialmente os titulares de dados em mais de um Estado-Membro.*

Se a empresa tiver apenas estabelecimentos num Estado-Membro e as suas atividades de tratamento afetarem apenas os titulares de dados desse Estado-Membro, não é necessário estabelecer uma autoridade de controlo principal. A única autoridade competente será a Autoridade Supervisora no país em que a Empresa é legalmente estabelecida.

8.2. Estabelecimento Principal e Autoridade de Controlo

8.2.1. Estabelecimento Principal para o Responsável pelo Tratamento

A Gerência precisa identificar o estabelecimento principal para que a autoridade de controlo principal possa ser determinada.
Se a Empresa estiver sediada num Estado-Membro da UE e tomar decisões relacionadas com atividades de processamento transfronteiriço no lugar da sua sede, haverá uma autoridade de controlo única responsável pelas atividades de processamento de dados realizados pela Empresa.
Se a Empresa possui vários estabelecimentos que agem de forma independente e tomam decisões sobre as finalidades e meios do processamento de dados pessoais, Gerência precisa reconhecer que existe mais de uma autoridade de controlo.

8.2.2. Estabelecimento Principal do Subcontratante

Quando a empresa está agindo como um subcontratante, o estabelecimento principal será o local da sede. No caso de o local da administração central não se situar na UE, o estabelecimento principal será o estabelecimento na UE onde se realizam as principais atividades de processamento.

8.2.3. Estabelecimento Principal para Empresas Não-UE para Responsáveis de tratamento e Subcontratantes

Se a empresa não tem um estabelecimento principal na EU, e tem subsidiaria(s) na UE, então a autoridade de controlo competente é a autoridade local de controlo.
Se a empresa não tiver um estabelecimento principal na UE nem as subsidiárias na UE, deve nomear um representante na UE, e a autoridade de controlo competente será a autoridade de controlo local onde o representante estiver localizado.

9. Resposta a Incidentes de Violação de Dados Pessoais

Quando a Empresa verifica uma violação de dados pessoais suspeita ou real, [o cargo] deve realizar uma investigação interna e tomar medidas corretivas adequadas em tempo hábil, de acordo com a **Política de Violação de Dados**. Caso exista qualquer risco para os direitos e liberdades dos titulares dos dados, a Empresa deve notificar as autoridades competentes em matéria de proteção de dados sem demora injustificada e, quando possível, no prazo de 72 horas.

10. Auditoria e Responsabilização

O Departamento de Auditoria ou é responsável por auditar como os departamentos de negócios implementam esta Política.
Qualquer funcionário que violar esta Política estará sujeito a ação disciplinar podendo também estar sujeito a responsabilidades civis ou criminais se sua conduta violar leis ou regulamentos.

11. Conflitos das Leis

Esta Política destina-se a cumprir as leis e regulamentos no lugar do estabelecimento e dos países nos quais a Sintética opera. **No caso de qualquer conflito entre esta Política e as leis e regulamentos aplicáveis, estes últimos prevalecerão**.

12. Gestão Base dos Registos deste Documento

Nome do registo	Pessoa responsável pelo armazenamento	Controlo para proteção de registo	Tempo de retenção
Formulário de Consentimento do Titular dos Dados (04.1)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	10 anos
Formulário de Eliminação do Consentimento do Títular dos Dados (04.2)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	10 anos
Formulário de Consentimento dos Pais (04.3)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	10 anos
Formulário de Eliminação de Consentimento dos Pais (04.4)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	10 anos
Contrato de Processamento de Dados do Subcontratante (Fornecedor) (07.2)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	5 anos após o término do contrato
Registo das Políticas de Privacidade (02.5)	Equipa de Proteção de Dados	Somente pessoas autorizadas podem aceder a esta pasta	Permanentemente

13. Validade e gestão do documento

Este documento é válido a partir de 24 de maio de 2018.

_____
[assinatura Gerência]

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