Política de Privacidade

Atualização 0.6.0
14 de novembro de 2026

1. Identificação e responsabilidades

A SINZIX AI 360, disponível em https://app.sinzix360.com/, é explorada em nome individual por Marco Paulo Fagundes Correia Rodrigues, sob a marca SINZIX AI 360. Contacto para privacidade, direitos e apoio: marco.pavmr@gmail.com. Esta política aplica-se aos utilizadores da aplicação e às pessoas cujos dados sejam introduzidos no serviço.

Marco Paulo Fagundes Correia Rodrigues é o responsável pelo tratamento dos dados de registo, autenticação, gestão da conta, apoio, segurança e cumprimento das obrigações legais próprias da exploração da SINZIX. A marca, por si só, não constitui uma pessoa coletiva distinta.

Quanto aos processos de peritagem, é responsável pelo tratamento a entidade ou o profissional que determina as finalidades e os meios essenciais desse tratamento. Um utilizador que trabalha por conta de uma seguradora ou gabinete pode atuar sob a autoridade dessa entidade, de acordo com o mandato e a relação contratual aplicáveis. Não se presume que todos os utilizadores sejam responsáveis autónomos.

Quando disponibiliza armazenamento e funcionalidades sobre os conteúdos de processos por conta e segundo as instruções desse responsável, a SINZIX atua como subcontratante. Essa relação deve estar regulada por acordo nos termos do artigo 28.º do RGPD. Esta política informa os titulares; não substitui esse acordo. A confirmação do utilizador não exclui obrigações nem responsabilidades próprias da SINZIX.

O acesso de novos utilizadores depende de aprovação do administrador. O administrador consulta os dados de registo e o estado de autorização para gerir acessos; essa função não lhe apresenta os conteúdos dos processos de outros clientes. As instruções globais dos relatórios são privadas e geridas pelo administrador.

2. Categorias de dados, origem e necessidade

O Google fornece o identificador da conta, nome e e-mail verificado para criar e autenticar a conta SINZIX. A SINZIX não recebe a palavra-passe Google.

Os utilizadores introduzem dados de segurados, representantes, lesados e outros intervenientes: identificação e contactos, moradas, referências de processos e apólices, datas, danos patrimoniais, valores, notas, relatórios, documentos e fotografias. A SINZIX guarda também instruções do utilizador e identificadores das pastas, ficheiros e eventos associados às integrações.

São tratados dados técnicos necessários ao funcionamento e segurança, incluindo sessão e registos técnicos do alojamento. As credenciais de integração guardadas no servidor são cifradas. Não devem ser introduzidos dados excessivos, palavras-passe, documentos de identificação integralmente reproduzidos sem necessidade, ou dados de saúde e outros dados especialmente protegidos sem necessidade e fundamento legal próprio.

O identificador Google e o e-mail verificado são necessários ao acesso pela modalidade disponível. As integrações externas são opcionais. A falta da autorização correspondente impede essa integração, mas não constitui autorização para utilizar outra conta ou outros dados.

3. Finalidades e fundamentos jurídicos

Os dados de conta são tratados para criar e autenticar o acesso, guardar preferências, prestar apoio e executar a relação de utilização do serviço, nos termos do artigo 6.º, n.º 1, alínea b), do RGPD, quando aplicável à relação com o titular.

A proteção da aplicação, prevenção de acessos indevidos e investigação de incidentes assentam no interesse legítimo de manter um serviço seguro, sujeito à ponderação dos direitos dos titulares. As obrigações legais próprias assentam no artigo 6.º, n.º 1, alínea c). Quando um tratamento específico dependa de consentimento, este será solicitado separadamente e poderá ser retirado sem afetar a licitude do tratamento anterior.

Nos conteúdos de processos tratados por conta de clientes, compete ao respetivo responsável definir e demonstrar os fundamentos jurídicos, cumprir os deveres de informação e emitir instruções lícitas. A SINZIX utiliza os dados para executar essas instruções e as funcionalidades pedidas. Uma autorização técnica Google ou a leitura desta política não substituem o fundamento jurídico exigido para tratar dados de terceiros.

4. Google Drive, Calendar e Maps

O início de sessão, o acesso ao Drive e o acesso ao Calendar são autorizações distintas, efetuadas nos ecrãs oficiais Google. O cliente não tem de criar chaves API Google.

O Drive utiliza a permissão drive.file, para trabalhar com ficheiros criados pela aplicação ou autorizados pelo utilizador. A pasta é escolhida no seletor Google. Quando solicitado, a aplicação cria ou atualiza pastas, documentos, fotografias e cópias da ficha nessa localização. Não disponibiliza a outros clientes os ficheiros ou configurações desta conta.

O Calendar utiliza a permissão calendar.app.created para criar um calendário próprio SINZIX AI 360 - Peritagens e gerir os eventos desse calendário. A sincronização envia referência, nome do segurado, morada da peritagem, datas e descrição de ligação à ficha. Os lembretes ficam associados aos eventos Google. A sincronização automática após guardar a ficha é uma opção do utilizador; a aplicação pode pedir nova autorização quando a sessão Google expira. Esta permissão não dá acesso geral aos outros calendários do utilizador.

O botão Google Maps abre um pedido de direções com a morada escolhida. A morada é enviada ao Google quando o utilizador carrega nesse botão. A SINZIX não exige localização GPS para este atalho e não efetua acompanhamento contínuo da localização. A eventual utilização da localização pelo Maps é gerida pelo próprio Google e pelas permissões do dispositivo.

O acesso Google pode ser revisto ou revogado em https://myaccount.google.com/connections. Desligar uma integração não elimina os ficheiros ou eventos já criados no Google, nem equivale a encerrar a conta SINZIX.

5. Utilização limitada dos dados Google

A utilização e a transferência para outras aplicações de informação recebida das APIs Google respeitam a Google API Services User Data Policy, incluindo os requisitos Limited Use: https://developers.google.com/terms/api-services-user-data-policy.

Os dados Google são utilizados para as funcionalidades solicitadas. Não são vendidos, utilizados para publicidade personalizada ou utilizados pela SINZIX para treinar modelos de IA de finalidade geral. O acesso humano limita-se às situações admitidas pela política Google, designadamente apoio autorizado, segurança, cumprimento legal ou outras situações permitidas.

6. Inteligência artificial e revisão profissional

Ao pedir a geração de um rascunho, são enviados à OpenAI os dados da ficha, notas e instruções indicados na confirmação da aplicação. Na importação, os documentos e fotografias expressamente selecionados são enviados à OpenAI apenas depois de confirmação específica, para extrair os dados da ficha, transcrever o preliminar e propor a classificação das páginas. Podem ser enviados PDFs, imagens e texto de documentos Word. Todos os originais são conservados. A separação física dos PDFs é executada no servidor após revisão e confirmação dos dados. O teste da ligação envia um pedido curto de teste. As chaves API pessoais ficam cifradas no servidor e não são apresentadas a outros utilizadores.

A utilização da API OpenAI está sujeita às condições, controlos e regras de conservação do serviço contratado. Informação do fornecedor: https://openai.com/policies/privacy-policy/ e https://platform.openai.com/docs/guides/your-data. O envio deve limitar-se aos dados necessários e autorizados pelo responsável pelo processo.

A utilização direta do plano ChatGPT depende da disponibilização e aprovação dessa integração e não está ativa nesta versão. A SINZIX não solicita nem guarda a palavra-passe ChatGPT. Uma modalidade de IA gratuita só estará disponível quando expressamente identificada como ativa na aplicação.

Os resultados são rascunhos sujeitos a revisão humana. A aplicação não toma decisões exclusivamente automatizadas com efeitos jurídicos sobre cobertura, responsabilidade, indemnização ou direitos dos titulares.

7. Destinatários e transferências internacionais

O alojamento e infraestrutura de suporte utilizam PTisp. Google recebe os dados necessários à autenticação e às integrações que o utilizador ativa; OpenAI recebe os dados enviados nos pedidos de IA que o utilizador confirma. Podem intervir prestadores técnicos autorizados e autoridades quando exista obrigação legal.

O papel de cada fornecedor depende da operação e dos contratos aplicáveis. Quando um fornecedor trate conteúdos por conta do responsável, aplicam-se as exigências de subcontratação, incluindo autorização e garantias contratuais adequadas.

Os fornecedores podem recorrer a infraestruturas fora do Espaço Económico Europeu. Quando haja transferência internacional, devem aplicar-se os mecanismos previstos no capítulo V do RGPD, incluindo decisão de adequação aplicável ou cláusulas contratuais-tipo e medidas adicionais quando necessárias. Pode ser pedida informação sobre os destinatários e garantias através do contacto de privacidade; esta política não afirma que todos os dados permanecem exclusivamente em Portugal.

8. Conservação, encerramento e cópias de segurança

Os dados de conta são conservados enquanto a conta estiver ativa e forem necessários à prestação do serviço. Após encerramento, são eliminados ou anonimizados quando deixem de ser necessários, ressalvando obrigações legais e a conservação estritamente necessária ao exercício ou defesa de direitos.

Os conteúdos de processos são conservados de acordo com as instruções do respetivo responsável, durante a prestação do serviço. O responsável deve definir o prazo adequado à sua atividade. Não existe, nesta versão, um prazo automático único de eliminação de todos os processos. Pode ser pedida exportação, devolução e eliminação pelo contacto de privacidade.

As cópias de segurança destinam-se à recuperação e ficam em área privada. Um pedido de eliminação abrange as cópias sob controlo da SINZIX: são eliminadas quando tecnicamente executável ou isoladas de utilização corrente até à sua substituição ou eliminação, salvaguardadas obrigações legais. Se uma cópia for reposta, devem ser reaplicadas as instruções de eliminação.

As atualizações de software são preparadas para preservar dados e configurações e são precedidas de cópia de segurança. Isto não constitui garantia absoluta de ausência de falhas. Os documentos e eventos já enviados para a conta Google mantêm-se nessa conta até serem eliminados pelo seu titular ou por uma

operação autorizada.

O botão Eliminar processo remove os dados e ficheiros ativos desse processo na SINZIX, move a pasta específica do processo para o lixo Google Drive e remove os eventos SINZIX associados. Não elimina a pasta principal do utilizador. As cópias de segurança seguem as regras de conservação e eliminação descritas nesta política.

9. Segurança, confidencialidade e incidentes

A aplicação utiliza HTTPS, autenticação Google, sessões protegidas, separação lógica de dados por conta, proteção de pedidos de alteração e cifragem das credenciais de integrações no servidor. Os conteúdos e ficheiros não são, por esse facto, integralmente cifrados de ponta a ponta. O acesso técnico deve limitar-se às pessoas autorizadas, sujeitas a confidencialidade e necessidade de acesso.

Os incidentes são avaliados e tratados de acordo com o RGPD. Quando atuar como subcontratante, a SINZIX deve comunicar violações de dados ao responsável sem demora injustificada após delas tomar conhecimento. Quando atuar como responsável, aplica os deveres de notificação à autoridade e de comunicação aos titulares nas circunstâncias legalmente exigidas.

O utilizador deve proteger a sua conta Google e os dispositivos, limitar acessos e comunicar suspeitas de utilização indevida para marco.pavmr@gmail.com.

10. Cookies e armazenamento no dispositivo

São utilizados cookies necessários à autenticação e armazenamento local do navegador para apoiar o funcionamento e a recuperação das alterações na conta. A SINZIX não integrou publicidade nem análise publicitária. Os componentes Google seguem também as políticas próprias desse fornecedor.

Em dispositivos partilhados, o utilizador deve terminar a sessão e proteger ou limpar o perfil do navegador, tendo em conta que podem existir cópias locais de dados. A revogação de uma integração não limpa automaticamente o armazenamento local do dispositivo.

11. Direitos dos titulares e reclamação

Nos termos aplicáveis, o titular pode pedir acesso, retificação, apagamento, limitação, oposição e portabilidade, e retirar consentimento quando este seja o fundamento do tratamento. Pode contactar marco.pavmr@gmail.com. A identidade será verificada por meios proporcionais, sem pedir documentação excessiva.

Os pedidos são respondidos, em regra, no prazo de um mês. Quando legalmente admissível, o prazo pode ser prorrogado por mais dois meses, com informação sobre a prorrogação e respetivos motivos no primeiro mês.

Quando o pedido diga respeito a dados de um processo gerido por um cliente responsável, a SINZIX articula a resposta com esse responsável e presta a assistência devida. A aplicação permite exportar fichas e instruções em JSON e descarregar separadamente documentos e fotografias.

O titular pode apresentar reclamação à Comissão Nacional de Proteção de Dados: https://www.cnpd.pt/. A confirmação de leitura da política e a aceitação dos termos não representam renúncia aos direitos dos titulares.

12. Confirmação e alterações

Antes de utilizar as funcionalidades de alteração de dados, cada utilizador confirma que leu esta política, aceita os termos e dispõe de autorização para tratar os dados que introduz, de acordo com as suas funções. Ficam registados a conta, a versão confirmada e a data da confirmação. As integrações e os envios de IA têm controlos próprios.

Esta atualização tem a referência 2026-11-14-v2 e data de 14 de novembro de 2026. A leitura de documentos com IA exige a confirmação específica apresentada na importação. Alterações materiais serão comunicadas e, quando exigível, haverá nova confirmação ou autorização antes de novos tratamentos. Uma alteração futura de entidade exploradora exige atualização da identificação e cumprimento dos deveres legais correspondentes.