MedAct — Acordo de Subcontratação de Dados (DPA)

Versão 2.0 · 2 de novembro de 2026 · Para contas criadas antes desta data, entra em vigor a 17 de novembro de 2026

Este acordo cobre os requisitos do art. 28.º, n.º 3, do RGPD.

Cláusula 1: Partes e definições

1.1. Este contrato é celebrado entre:

- **Responsável pelo Tratamento:** o utilizador da aplicação MedAct, identificado pelo email da conta e pelos dados que indique no seu perfil (nome e profissão), adiante "Responsável";
- **Subcontratante:** Ana Costa, pessoa singular, NIF 272660507, morada Rua São Ciro 40, 1200-831 Lisboa, contacto de privacidade apoio@medact.net, adiante "Subcontratante".

1.2. "Serviço" é a aplicação web MedAct, disponível em medact.net, que permite registar atos clínicos diários, importá-los de ficheiros e fotografias, e reconciliá-los com extratos de pagamento das clínicas.

1.3. Os termos "dados pessoais", "tratamento", "titular dos dados", "violação de dados pessoais" e "autoridade de controlo" têm o significado do Regulamento (UE) 2016/679 ("RGPD"). "CNPD" é a Comissão Nacional de Proteção de Dados.

1.4. O Responsável trata os dados dos pacientes para uma finalidade própria, o controlo e a reconciliação dos seus honorários profissionais, distinta das finalidades da clínica onde presta serviços. Quanto a este tratamento, atua como responsável pelo tratamento autónomo (art. 4.º, 7), RGPD), e não por conta da clínica.

Cláusula 2: Objeto, natureza, finalidade e duração

2.1. O Subcontratante trata dados pessoais por conta do Responsável, exclusivamente para prestar o Serviço: guardar, organizar, importar, comparar e exportar os registos que o Responsável introduz.

2.2. Os dados tratados incluem dados de saúde, na medida em que o nome do paciente associado a um ato médico ou dentário revela informação sobre a sua saúde (art. 9.º RGPD). A descrição completa está no Anexo I.

2.3. O contrato vigora enquanto o Responsável tiver conta ativa no Serviço e, depois, durante o prazo de apagamento da cláusula 11.

2.4. Quanto aos dados da conta do Responsável (email, perfil e dados de acesso), a MedAct é a responsável pelo tratamento. Esses dados são tratados nos termos da Política de Privacidade e não ao abrigo deste contrato.

Cláusulas 3 e 4: Instruções e confidencialidade

3. Instruções documentadas. 3.1. O Subcontratante trata os dados apenas mediante instruções documentadas do Responsável, incluindo quanto a transferências para países fora do Espaço Económico Europeu, salvo se o direito da União ou nacional o obrigar a outro tratamento; nesse caso informa o Responsável antes, a menos que a lei o proíba.

3.2. Este contrato e a utilização normal das funcionalidades do Serviço são as instruções completas do Responsável. Instruções adicionais serão dadas por escrito para apoio@medact.net.

3.3. O Subcontratante informa imediatamente o Responsável se considerar que uma instrução viola o RGPD ou outra norma de proteção de dados.

3.4. O Subcontratante não trata os dados dos pacientes para fins próprios, não os vende, não os usa para publicidade e não os usa para treinar modelos de inteligência artificial.

4. Confidencialidade. 4.1. O Subcontratante garante que as pessoas autorizadas a tratar os dados estão sujeitas a um dever de confidencialidade, contratual ou legal.

4.2. O Subcontratante não acede ao conteúdo dos registos do Responsável, exceto se necessário para resolver um problema técnico pedido por este ou para cumprir a lei.

Cláusulas 5 a 7: Segurança, assistência e violações

5. Segurança (art. 32.º RGPD). O Subcontratante aplica as medidas técnicas e organizativas descritas no Anexo II, adequadas ao risco dos dados de saúde, e revisa-as pelo menos uma vez por ano.

6. Assistência ao Responsável. 6.1. Tendo em conta a natureza do tratamento, o Subcontratante ajuda o Responsável, por medidas adequadas, a responder aos pedidos dos titulares (acesso, retificação, apagamento, limitação, portabilidade, oposição). Se receber um pedido diretamente de um titular, encaminha-o ao Responsável em 5 dias úteis sem lhe responder. O Subcontratante presta a assistência pedida pelo Responsável no prazo de 10 dias úteis.

6.2. O Subcontratante ajuda o Responsável a cumprir os arts. 32.º a 36.º do RGPD (segurança, notificação de violações, avaliação de impacto e consulta prévia), fornecendo a informação que tiver, incluindo a avaliação de impacto da MedAct.

6.3. A funcionalidade de apagar conta e a de exportar dados dentro do Serviço permitem ao Responsável exercer por si os direitos de apagamento e portabilidade sobre os registos que introduziu.

7. Violações de dados pessoais. 7.1. O Subcontratante notifica o Responsável sem demora injustificada e, sempre que possível, no prazo de 48 horas após ter conhecimento de uma violação, por email para o endereço da conta.

7.2. A notificação descreve, tanto quanto conhecido: a natureza da violação, as categorias e o número aproximado de titulares e registos, as consequências prováveis e as medidas tomadas ou propostas.

7.3. A notificação à CNPD (72 horas, art. 33.º) e aos titulares (art. 34.º) compete ao Responsável. O Subcontratante colabora e fornece a informação necessária.

Cláusulas 8 e 9: Subcontratantes ulteriores e transferências

8. Subcontratantes ulteriores. 8.1. O Responsável autoriza, de forma geral, o recurso aos subcontratantes ulteriores listados no Anexo III.

8.2. O Subcontratante informa o Responsável por email de qualquer alteração prevista (adição ou substituição) com pelo menos 15 dias de antecedência ou, se o subcontratante ulterior lhe der um aviso mais curto, logo que tenha conhecimento da alteração. O Responsável pode opor-se por escrito nesse prazo; se não houver solução, pode terminar o contrato e apagar a conta sem encargos.

8.3. O Subcontratante impõe a cada subcontratante ulterior, por contrato (incluindo os acordos de tratamento de dados normalizados de cada fornecedor), obrigações de proteção de dados equivalentes às deste contrato e responde perante o Responsável pelo cumprimento delas.

9. Transferências internacionais. 9.1. Os dados são alojados na União Europeia (Irlanda).

9.2. Quando um subcontratante ulterior trate dados fora do Espaço Económico Europeu, o Subcontratante assegura que a transferência assenta num mecanismo válido do capítulo V do RGPD (decisão de adequação, incluindo o Quadro de Privacidade UE-EUA, ou cláusulas contratuais-tipo) e, quando necessário, em medidas suplementares. O mecanismo aplicável a cada fornecedor está indicado no Anexo III.

Cláusula 10: Obrigações do Responsável

10.1. O Responsável declara e garante que:

- tem fundamento de licitude para tratar os dados dos pacientes, nomeadamente o interesse legítimo no controlo e na reconciliação dos seus honorários e, quando aplicável, o cumprimento de obrigações legais, incluindo fiscais (art. 6.º, n.º 1, als. f) e c), RGPD), e uma condição válida para tratar dados de saúde (art. 9.º, n.º 2, al. h), RGPD, conjugado com o art. 29.º da Lei n.º 58/2019), e que o faz no âmbito da sua atividade profissional, sujeito ao dever de sigilo;
- informou os pacientes do tratamento, nos termos dos arts. 13.º e 14.º do RGPD, quando exigido;
- introduz no Serviço apenas os dados necessários para o registo e a reconciliação dos seus atos;
- não escreve informação clínica detalhada (diagnósticos, histórico clínico) nos campos de texto livre, como "Notas";
- mantém confidenciais as credenciais de acesso e não partilha a conta com terceiros.

10.2. O Responsável é responsável por avaliar se a sua utilização do Serviço cumpre as regras da sua profissão, da clínica onde trabalha e dos contratos que tenha com essa clínica.

10.3. O Responsável compromete-se a seguir as boas práticas do Anexo IV.

Cláusulas 11 a 13: Termo, auditorias e responsabilidade

11. Termo e apagamento. 11.1. Quando a conta é apagada ou o contrato termina, o Subcontratante apaga os dados pessoais do Responsável, incluindo cópias, no prazo de 30 dias (de imediato, se o Responsável apagar a conta no próprio Serviço), salvo se o direito da União ou nacional exigir a sua conservação. O mesmo se aplica às contas sem início de sessão durante 12 meses, após aviso por email com 30 dias de antecedência. Fica excetuado o registo mínimo da aceitação dos documentos contratuais (email, documento, versão, data e hash), que o Subcontratante conserva durante 3 anos, apenas para provar essa aceitação e se defender em caso de reclamação, e que apaga depois automaticamente (arts. 6.º, n.º 1, f), e 17.º, n.º 3, e) do RGPD).

11.2. Antes do termo, o Responsável pode exportar os seus dados pelo Serviço. Se pedir, o Subcontratante entrega-os num formato legível por máquina (Excel ou JSON).

11.3. O Subcontratante faz cópias de segurança diárias da base de dados, cifradas antes de saírem do servidor (AES-256, com chave só na posse da MedAct) e guardadas num repositório privado do GitHub durante 7 dias; os dados apagados desaparecem delas no fim desse prazo. As cópias servem apenas para recuperar o Serviço em caso de falha ou incidente e não são usadas para repor uma conta apagada pelo Responsável. Se o Subcontratante fizer exportações manuais para sua proteção, guarda-as cifradas e apaga-as no mesmo prazo da cláusula 11.1.

12. Informação e auditorias. 12.1. O Subcontratante disponibiliza ao Responsável a informação necessária para demonstrar o cumprimento do art. 28.º do RGPD.

12.2. O Responsável pode pedir uma auditoria ou inspeção, com 30 dias de aviso prévio, no máximo uma vez por ano (ou mais, após uma violação de dados). O Subcontratante pode responder primeiro por escrito, com a documentação de segurança e os DPAs dos seus fornecedores, e só se isso não bastar permite uma verificação presencial ou remota, sem acesso a dados de outros utilizadores.

13. Responsabilidade. Cada parte responde perante os titulares e as autoridades nos termos do art. 82.º do RGPD. Entre as partes, cada uma responde pelos danos que causar ao incumprir este contrato ou o RGPD, nos termos da lei, sem prejuízo do direito de regresso previsto no art. 82.º(5) do RGPD.

Cláusulas 14 e 15: Aceitação, lei aplicável e foro

14. Aceitação eletrónica. 14.1. O Responsável aceita este contrato marcando a caixa correspondente no registo, antes do primeiro acesso ao Serviço. A aplicação guarda a versão do contrato, a data e a hora da aceitação, e permite descarregar uma cópia em PDF.

14.2. Quando o Subcontratante alterar este contrato, pede nova aceitação, com aviso prévio de 15 dias. Sem ela, o acesso ao Serviço pode ser suspenso.

14.3. Em caso de conflito entre este contrato e os Termos de Uso ou a Política de Privacidade, prevalece este contrato quanto aos dados dos pacientes.

15. Lei aplicável e foro. Este contrato rege-se pela lei portuguesa e pelo RGPD. Para litígios que dele decorram, as partes escolhem o foro da comarca de Lisboa, com renúncia a qualquer outro.

Anexo I: Descrição do tratamento

Elemento	Descrição
Objeto e finalidade	Registar atos clínicos diários e reconciliá-los com os extratos de pagamento das clínicas, para o Responsável confirmar os valores que lhe são devidos
Titulares dos dados	Pacientes do Responsável
Categorias de dados	Nome do paciente, número de processo, data do ato, ato médico e código, dente, convénio ou seguradora, valor, custos de laboratório, clínica, estado de pagamento, indicação de falta ou desmarcação, notas do Responsável

Categoria especial (art. 9.º)	Sim, dados de saúde, na medida em que o nome do paciente ligado a um ato revela informação de saúde
Ficheiros importados	Ficheiros Excel e PDF de extratos e fotografias de agendas. As fotografias são enviadas à Anthropic para leitura e não são guardadas pelo Subcontratante. Os ficheiros Excel e PDF são lidos no navegador do Responsável e não são enviados ao servidor; ficam em cache no navegador, ligados à conta, e só os registos resultantes são guardados.
Operações	Recolha, registo, organização, conservação, consulta, comparação, importação, exportação, apagamento; leitura automática de fotografias de agendas por um modelo de inteligência artificial
Duração	Enquanto a conta estiver ativa, mais o prazo de apagamento da cláusula 11
Local de alojamento	União Europeia (Irlanda)

Anexo II: Medidas técnicas e organizativas

Só ficam neste anexo as medidas que existem de facto. Quando a aplicação passar a ter novas medidas, como a autenticação em dois passos para os utilizadores, este anexo é atualizado.

- **Isolamento entre utilizadores:** segurança ao nível da linha (RLS) ativa em todas as tabelas, com políticas que só dão a cada utilizador acesso aos seus registos; permissões anónimas retiradas das tabelas.
- **Autenticação:** palavra-passe com um mínimo de 12 caracteres e sessão por utilizador; as funções de servidor exigem o token de sessão válido.
- **Proteção contra abuso:** limites de tentativas de registo e login, e CAPTCHA no login, registo e recuperação de palavra-passe.
- **Sessão:** termina automaticamente após 8 horas de inatividade; a cache local é limpa ao terminar sessão, ao trocar de conta no mesmo navegador e após a inatividade, só depois de confirmado que tudo está gravado na base de dados.
- **Ficheiros:** validação de tipo e de tamanho máximo nos carregamentos.
- **Navegador:** cabeçalhos de segurança no alojamento (Content-Security-Policy, proteção contra incorporação noutros sites e contra deteção de tipo de conteúdo), que limitam a ligação apenas aos serviços indicados no Anexo III.
- **Cifragem:** ligações cifradas (HTTPS/TLS); cifragem dos dados em repouso (AES-256) pelo fornecedor da base de dados.
- **Cópias de segurança:** cópias de segurança diárias da base de dados, cifradas antes de saírem do servidor (AES-256, com chave só na posse da MedAct) e guardadas num repositório privado do GitHub durante 7 dias; o GitHub não tem acesso à chave. O Responsável deve conservar na mesma os extratos originais das clínicas.
- **Email:** envio a partir de um domínio próprio com SPF, DKIM e DMARC.
- **Acessos do Subcontratante:** acesso administrativo restrito a uma pessoa, com autenticação forte (autenticação em dois passos ativa nas contas Supabase, Netlify, GitHub e Google).
- **Registo de aceitação:** versão, data e hora da aceitação dos documentos contratuais, guardadas na base de dados; depois de a conta ser apagada, fica 3 anos um registo mínimo (email, documento,

versão, data e hash), apagado automaticamente.

- **Organizativas:** procedimento escrito de violação de dados; revisão anual destas medidas; não utilização de dados reais de pacientes em testes e desenvolvimento.

Anexo III: Subcontratantes ulteriores autorizados

Fornecedor	Função	Dados	Localização	Mecanismo de transferência
Supabase	Base de dados, autenticação e funções de servidor	Todos os dados do Anexo I	UE (Irlanda)	O DPA da Supabase faz parte dos Termos de Serviço e incorpora cláusulas contratuais-tipo (módulos dois e três), com a aceitação dos termos a produzir o efeito de as assinar
Anthropic	Leitura automática de fotografias de agendas	Imagem enviada pelo Responsável, que pode conter nomes de pacientes	EUA	O DPA da Anthropic faz parte dos Termos Comerciais e incorpora cláusulas contratuais-tipo
Netlify	Alojamento da aplicação	Dados técnicos de ligação (endereço IP)	EUA	Quadro de Privacidade UE-EUA (Netlify está certificada), com cláusulas contratuais-tipo se a certificação cessar
Google Workspace	Email de apoio	Conteúdo das mensagens que o Responsável enviar	Vários países, definidos pela Google	Cloud Data Processing Addendum da Google, incorporado no contrato do Google Workspace, com cláusulas contratuais-tipo quando não exista outra solução de transferência
Cloudflare (Turnstile)	CAPTCHA no acesso	Dados técnicos do dispositivo	EUA	DPA incorporado no contrato de subscrição; Quadro de Privacidade UE-EUA, com cláusulas contratuais-tipo como alternativa
GitHub	Armazenamento de cópias de segurança	Cópias cifradas de todos os dados do Anexo I (sem acesso à chave)	EUA	GitHub Customer Agreement com DPA (organização MedAct-app); Quadro de Privacidade UE-EUA, com cláusulas contratuais-tipo como alternativa

Anexo IV: Boas práticas de proteção de dados para o Responsável

Estas regras ajudam o Responsável a cumprir o RGPD. Não substituem as obrigações que tem enquanto profissional de saúde, incluindo o dever de sigilo.

A. Escrever o mínimo

1. Sempre que possível, identifica o paciente pelo número de processo ou de paciente da clínica, ou por iniciais, em vez do nome completo. Mantém o nome completo só se precisares dele para conferir os valores.

2. Não escrevas diagnósticos, histórico clínico, queixas ou outra informação de saúde nas "Notas" nem noutro campo de texto livre. Escreve só o que precisas para a faturação, por exemplo "aguarda autorização da seguradora".

3. Não introduzas morada, contactos, número de utente, NIF ou documentos de identificação do paciente.

B. Fotografias e ficheiros

4. Antes de tirares uma foto da agenda, recorta ou tapa o que não for necessário (outros profissionais, outros dias, contactos, notas clínicas). A imagem é enviada a um serviço de inteligência artificial de um subcontratante.

5. Revê sempre os registos criados a partir de uma foto. Podem conter erros e ficam pendentes até os confirmares.

6. Importa só os ficheiros Excel e PDF de que precisas, e apaga do teu dispositivo os ficheiros e exportações que já não sejam necessários.

C. Segurança da conta e do dispositivo

7. Usa uma palavra-passe longa e única para a MedAct, de preferência num gestor de palavras-passe, e não a partilhes com ninguém.

8. Termina sempre a sessão em computadores e tablets partilhados ou públicos. Mantém o bloqueio de ecrã ativo e o sistema e o navegador atualizados.

9. Ativa a autenticação em dois passos assim que estiver disponível na aplicação.

D. Comunicação com o apoio

10. Não envies dados de pacientes (nomes, capturas de ecrã, ficheiros de extratos) por email para apoio@medact.net. Para pedir ajuda, tapa ou substitui os nomes.

E. Pacientes e clínicas

11. Confirma que tens fundamento legal para tratar os dados e que informaste os pacientes, quando exigido. Se trabalhas numa clínica, confirma que o teu contrato com ela não te proíbe de registar estes dados numa ferramenta própria. Se proibir, usa só o número de processo.

12. Se um paciente exercer um direito (acesso, retificação, apagamento), podes apagar os registos dele na aplicação e exportar os teus dados. Se precisares de ajuda, avisa-nos por apoio@medact.net.

F. Se algo correr mal

13. Se suspeitares de acesso indevido à tua conta, perda de um dispositivo com sessão aberta ou envio de dados a quem não devia, avisa-nos de imediato por apoio@medact.net e muda a palavra-passe. Avisamos-te em 48 horas de qualquer violação que nos diga respeito; a notificação à CNPD, em 72 horas, é tua responsabilidade enquanto responsável pelo tratamento.

G. Testes e formação

14. Para experimentar funcionalidades ou mostrar a aplicação a alguém, usa dados fictícios, nunca pacientes reais.

Ana Costa · NIF 272660507 · Rua São Ciro 40, 1200-831 Lisboa · apoio@medact.net · medact.net