Acordo de Tratamento de Dados (DPA) — Beew4y Clinic v1.0

AQN INNOVATION LTDA — CNPJ 48.143.641/0001-21
Versão 1.0 · Vigência: 2026-04-19
RASCUNHO — AGUARDANDO REVISÃO JURÍDICA — NÃO CONSTITUI DOCUMENTO FINAL

TEMPLATE — Contrato de Processamento de Dados (DPA)

Beew4y (Operadora) !” Clínica (Controladora)

Status: Rascunho técnico — REQUER REVISÃO E APROVAÇÃO JURÍDICA antes de qualquer assinatura.
Aviso: este documento é um rascunho preparatório. Não constitui aconselhamento jurídico. Não assinar sem revisão por advogado especializado em proteito de dados.

CONTRATO DE PROCESSAMENTO DE DADOS PESSOAIS

Entre:

CONTROLADORA: [NOME DA CLÍNICA], pessoa jurídica de direito privado, CNPJ nº [__], com sede em [ENDEREÇO], neste ato representada por [NOME DO REPRESENTANTE], doravante denominada simplesmente "CONTROLADORA" ou "Clínica";

E

OPERADORA: [RAZÃO SOCIAL DA BEEW4Y], pessoa jurídica de direito privado, CNPJ nº [__], com sede em [ENDEREÇO], neste ato representada por [NOME DO REPRESENTANTE], doravante denominada simplesmente "OPERADORA" ou "Beew4y";

As partes acima identificadas celebram o presente Contrato de Processamento de Dados Pessoais ("DPA"), que é parte integrante e inseparável do Contrato de Prestação de Serviços celebrado entre as partes ("Contrato Principal"), nos termos seguintes:

CLÁUSULA 1 — OBJETO

1.1 O presente DPA disciplina o tratamento de dados pessoais pela OPERADORA em nome e por instrução da CONTROLADORA, no âmbito da prestação dos serviços de software de gestão de clínicas descritos no Contrato Principal.

1.2 A OPERADORA tratará dados pessoais de pacientes e profissionais da CONTROLADORA exclusivamente para viabilizar as funcionalidades contratadas, em especial o módulo de registro de evoluções clínicas por sessão ("Módulo Clínico").

CLÁUSULA 2 — CATEGORIAS DE DADOS TRATADOS

2.1 A OPERADORA tratará, em nome da CONTROLADORA, as seguintes categorias de dados:

Dados pessoais sensíveis (LGPD art. 5º, II):

- Conteúdo de evoluções clínicas (registros de atendimento, dados de saúde)
- Instrumentos clínicos utilizados (protocolos, escalas, abordagens)

Dados pessoais não sensíveis:

- Identificadores técnicos de pacientes (UUID interno)
- Metadados de atendimento (data, duração)
- Dados de profissionais (nome, conselho, número de registro)
- Dados de auditoria pseudonimizados (IP hash, UA hash, timestamp, role)

2.2 Os dados sensíveis de saúde são tratados com base na tutela da saúde (LGPD art. 11, II, f), por operador de dados devidamente contratado.

CLÁUSULA 3 — FINALIDADES E LIMITAÇÕES

3.1 A OPERADORA tratará os dados pessoais exclusivamente para:

- (a) Armazenar e disponibilizar registros clínicos criados pela CONTROLADORA e seus profissionais;
- (b) Registrar trilha de auditoria de acesso aos dados clínicos, conforme exigência LGPD;
- (c) Calcular e aplicar prazos de retenção configurados pela CONTROLADORA;
- (d) Garantir isolamento multi-tenant (isolação de dados entre clínicas distintas);
- (e) Operar funcionalidades de suporte contratadas (backup, monitoramento, atualização de sistema).

3.2 É vedada à OPERADORA:

- (a) Utilizar os dados para qualquer finalidade própria não prevista neste DPA;
- (b) Compartilhar dados com terceiros não previstos na Cláusula 7;
- (c) Transferir dados a outros países sem ciência prévia da CONTROLADORA;
- (d) Criar perfis ou fazer inferências sobre os titulares além do necessário à prestação do serviço.

CLÁUSULA 4 — OBRIGAÇÕES DA OPERADORA

4.1 A OPERADORA compromete-se a:

- Tratar dados apenas conforme instruções documentadas da CONTROLADORA e os termos deste DPA;
- Implementar e manter medidas técnicas e organizacionais adequadas (descritas no Anexo I);
- Garantir confidencialidade dos dados por todos os seus colaboradores com acesso;
- Notificar a CONTROLADORA, sem demora injustificada, de qualquer incidente de segurança que afete dados pessoais sob sua gestão;
- Apoiar a CONTROLADORA no cumprimento de obrigações legais, incluindo atendimento a direitos de titulares;
- Após o encerramento do contrato, devolver ou eliminar os dados, conforme opção da CONTROLADORA;
- Fornecer as informações necessárias para demonstrar conformidade com este DPA, incluindo permitir auditorias razoáveis.

4.2 A OPERADORA manterá registro das atividades de tratamento realizadas em nome da CONTROLADORA.

CLÁUSULA 5 — OBRIGAÇÕES DA CONTROLADORA

5.1 A CONTROLADORA compromete-se a:

- Garantir que possui base legal adequada para o tratamento dos dados antes de inserir qualquer dado na plataforma;
- Informar os titulares (pacientes) sobre o uso do sistema e o tratamento de seus dados;
- Configurar corretamente os acessos de profissionais e administradores;
- Manter os dados cadastrais de profissionais atualizados no sistema;
- Tratar como confidenciais as credenciais de acesso à plataforma;
- Comunicar à OPERADORA qualquer solicitação de titular de dados recebida diretamente que exija cooperação da OPERADORA;
- Não inserir dados pessoais sensíveis fora do módulo clínico designado.

5.2 A CONTROLADORA declara expressamente que:

- (a) qualquer conteúdo inserido no sistema que reproduza protocolo, checklist, fases estruturadas ou material identificável como obra de autor ou instituto de método clínico específico é de sua exclusiva responsabilidade, incluindo a obtenção de licença do respectivo titular antes da inserção;
- (b) o uso do sistema Beew4y não implica certificação, habilitação, validação ou endosso de qualquer método clínico pela OPERADORA;
- (c) a OPERADORA não fornece, não endossa e não reproduz protocolos, checklists ou materiais proprietários de métodos clínicos de terceiros — o catálogo de métodos disponível no sistema é fornecido apenas para fins organizacionais de registro;
- (d) a responsabilidade pela correta aplicação dos métodos clínicos, pela habilitação dos profissionais e pelo cumprimento das normas dos respectivos conselhos profissionais é exclusiva da CONTROLADORA e de seus profissionais.

CLÁUSULA 6 — INCIDENTES DE SEGURANÇA

6.1 Em caso de incidente de segurança que afete dados pessoais processados no âmbito deste DPA, a OPERADORA notificará a CONTROLADORA em prazo não superior a 72 (setenta e duas) horas após tomar conhecimento.

6.2 A notificação conterá, no mínimo:

- (a) Natureza do incidente e dados afetados;
- (b) Número aproximado de titulares afetados;
- (c) Medidas adotadas para mitigar os efeitos do incidente;
- (d) Ponto de contato para informações adicionais.

6.3 A CONTROLADORA é responsável por avaliar a necessidade de notificação à ANPD e aos titulares afetados (LGPD art. 48).

CLÁUSULA 7 — SUBOPERADORES

7.1 A CONTROLADORA autoriza a OPERADORA a utilizar os seguintes suboperadores:

Suboperador | Serviço | Localização | DPA disponível
Supabase Inc. | Banco de dados PostgreSQL + Autenticação | AWS us-east-2 (EUA) | supabase.com/legal/dpa
[Provedor VPS] | Servidor de aplicação e logs | [País] | [Verificar]

7.2 A OPERADORA garante que os suboperadores listados oferecem garantias de proteção de dados equivalentes às deste DPA.

7.3 Qualquer alteração na lista de suboperadores será comunicada à CONTROLADORA com antecedência mínima de 30

(trinta) dias, que poderá se opor à alteração.

CLÁUSULA 8 — TRANSFERÊNCIA INTERNACIONAL

8.1 Os dados pessoais são armazenados em servidores da Supabase localizados nos EUA (AWS us-east-2).

8.2 Tal transferência é realizada com base em mecanismo de adequação previsto no DPA Supabase (Standard Contractual Clauses — SCCs da Comissão Europeia, adotadas como referência para adequação internacional).

8.3 A OPERADORA se compromete a não realizar outras transferências internacionais sem comunicação prévia e consentimento da CONTROLADORA.

CLÁUSULA 9 — PRAZO DE RETENÇÃO E ENCERRAMENTO

9.1 Os dados serão retidos pelo prazo configurado pela CONTROLADORA na plataforma, observados os limites técnicos:

- Mínimo: 2 (dois) anos
- Máximo: 20 (vinte) anos
- Padrão (sem configuração): 5 (cinco) anos

9.2 Após o encerramento do Contrato Principal, a CONTROLADORA poderá, no prazo de 30 (trinta) dias, solicitar:

- (a) A exportação dos dados (sujeito à disponibilidade de funcionalidade de export no sistema);
- (b) A eliminação segura dos dados.

9.3 Findo o prazo do item 9.2 sem manifestação, a OPERADORA poderá eliminar os dados após notificação prévia.

9.4 A trilha de auditoria (auditoriaacessoclinico) é eliminada em cascata com as evoluções correspondentes.

CLÁUSULA 10 — RESPONSABILIDADE

10.1 Cada parte responderá por danos causados em decorrência do descumprimento deste DPA.

10.2 A OPERADORA não responde por tratamentos realizados pela CONTROLADORA fora do sistema, por uso indevido das credenciais de acesso pela CONTROLADORA, ou por dados inseridos pela CONTROLADORA em violação à lei.

10.3 A responsabilidade da OPERADORA limita-se ao previsto no Contrato Principal.

CLÁUSULA 11 — DISPOSIÇÕES FINAIS

11.1 Este DPA é regido pela legislação brasileira, em especial pela Lei nº 13.709/2018 (LGPD).

11.2 As partes elegem o foro da comarca de [CIDADE] para dirimir quaisquer controvérsias.

11.3 Alterações a este DPA devem ser feitas por escrito e assinadas por ambas as partes.

[LOCAL], [DATA]

CONTROLADORA:

_____
[Nome do representante]
[Cargo]
[Nome da Clínica]
CNPJ: [__]

OPERADORA:

_____
[Nome do representante]
[Cargo]
Beew4y
CNPJ: [__]

ANEXO I — MEDIDAS TÉCNICAS E ORGANIZACIONAIS DE SEGURANÇA

As medidas implementadas pela OPERADORA para proteção dos dados processados estão detalhadas no documento docs/clinical/lgpd-medidas-seguranca.md, incorporado a este DPA por referência.

Resumo das principais medidas:

- Autenticação JWT via Supabase Auth com validação JWKS no backend
- RBAC por role com isolamento por empresa (empresa_id sempre do JWT)
- Row-Level Security (RLS) no PostgreSQL
- Trilha de auditoria Nível 2 fail-closed — dado clínico não entregue sem registro de acesso
- IP e User-Agent pseudonimizados (SHA256)
- Plain text obrigatório — HTML rejeitado em conteúdo clínico
- TLS em trânsito (nginx HTTPS)

- Backup automático gerenciado pelo Supabase (7 dias)
- Feature flag de desativação instantânea do domínio clínico

RASCUNHO TÉCNICO — SUJEITO A REVISÃO JURÍDICA — NÃO ASSINAR SEM APROVAÇÃO DO ADVOGADO RESPONSÁVEL