Legal

Documentação MOC Fidelidade — Legal

- Acordo de Tratamento de Dados (DPA modelo)

Acordo de Tratamento de Dados (DPA modelo)

Acordo de Tratamento de Dados (DPA)

> **Modelo padrão** — entrega-se ao cliente sob demanda quando solicitado por área jurídica, compliance ou DPO. Não publicado no Site institucional.

ACORDO DE TRATAMENTO DE DADOS PESSOAIS — DPA

Este Acordo de Tratamento de Dados Pessoais ("**DPA**") integra os Termos de Uso celebrados entre:

- **OPERADOR: MOC Soluções LTDA**, CNPJ 00.000.000/0001-00, com sede em [endereço], doravante denominada "**MOC**".
- **CONTROLADOR:** [Razão social do cliente], CNPJ [00.000.000/0001-00], com sede em [endereço], doravante denominado "**CLIENTE**".

As partes celebram o presente DPA com o objetivo de regulamentar o tratamento de dados pessoais realizado pela MOC em nome do CLIENTE, em cumprimento à **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD)**.

---

1. Objeto

A MOC, na condição de **Operador** (art. 5º, VII, LGPD), realiza tratamento de dados pessoais coletados pelo CLIENTE em sua plataforma SaaS "MOC Fidelidade", utilizada pelo CLIENTE para operar seu programa de fidelidade (o "**Serviço**").

2. Papéis das partes

- **CLIENTE** atua como **Controlador** dos dados pessoais de seus próprios clientes finais (consumidores), sendo responsável por decisões sobre finalidade e forma do tratamento, base legal aplicável e atendimento aos titulares.
- **MOC** atua como **Operador**, realizando o tratamento exclusivamente conforme instruções do CLIENTE e nos limites técnicos do Serviço contratado.

3. Natureza e finalidade do tratamento

A MOC trata os dados pessoais com a finalidade de viabilizar a operação do programa de fidelidade do CLIENTE, incluindo:

- Identificação e autenticação de clientes finais;
- Registro de marcações/pontuações por consumo;
- Gestão de catálogo de recompensas e resgates;
- Envio de comunicações transacionais (notificações de saldo, recompensa disponível, confirmação de resgate);
- Geração de relatórios agregados pro CLIENTE.

4. Categorias de dados pessoais tratados

Categoria	Origem	Finalidade
Nome completo	Cliente final cadastra	Identificação
E-mail	Cliente final cadastra	Login + notificação
Telefone/celular	Cliente final cadastra (opcional)	Suporte + notificação
Foto de perfil	Cliente final envia (opcional)	UX
Histórico transacional	Gerado pelo Serviço	Operação do programa
Dispositivo (FCM token)	App coleta	Push notification
IP + user-agent	Captura automática	Segurança + audit log

A MOC **não trata** dados sensíveis (origem racial/étnica, saúde, biometria etc.) nem dados de crianças/adolescentes intencionalmente; o CLIENTE compromete-se a não inserir tais categorias.

5. Categorias de titulares

- Clientes finais (consumidores) do CLIENTE;
- Operadores/funcionários autorizados pelo CLIENTE pra usar o painel admin.

6. Duração do tratamento

Pelo período de vigência do contrato + 30 dias para fins de exportação dos dados pelo CLIENTE. Após esse período, dados pessoais identificáveis são excluídos. Registros transacionais anonimizados podem ser mantidos para cumprimento de obrigação legal/tributária.

7. Obrigações da MOC (Operador)

A MOC compromete-se a:

7.1. **Tratar dados somente conforme instruções documentadas** do CLIENTE (neste DPA, no contrato e nas configurações do Serviço).

7.2. **Garantir confidencialidade**, exigindo dos seus colaboradores contratos de confidencialidade equivalentes.

7.3. **Implementar medidas técnicas e administrativas de segurança**, incluindo:

- Criptografia TLS 1.2+ em trânsito;
- Hash bcrypt de senhas;
- Tokens JWT com expiração;
- Validação de assinatura HMAC em webhooks de pagamento;
- Isolamento lógico por empresa no banco de dados;
- Backups diários com retenção mínima de 7 dias;
- Audit log de ações administrativas;
- Rate limiting nos endpoints públicos.

7.4. **Notificar o CLIENTE em até 48 horas** sobre qualquer incidente de segurança que envolva dados pessoais, fornecendo detalhes técnicos da natureza, dados afetados, medidas tomadas e mitigação.

7.5. **Não compartilhar dados pessoais com terceiros**, salvo:

- Sub-operadores essenciais ao funcionamento (vide Anexo I);
- Por determinação judicial expressa;
- Com consentimento explícito do CLIENTE.

7.6. **Auxiliar o CLIENTE** no atendimento a solicitações de titulares (acesso, correção, exclusão, portabilidade) e em eventual relatório de impacto.

7.7. **Devolver ou eliminar dados** ao término do contrato, conforme instrução do CLIENTE, ressalvada obrigação legal de retenção.

7.8. **Manter registros** das operações de tratamento e disponibilizá-los ao CLIENTE quando solicitado para fins de demonstração de conformidade.

8. Obrigações do CLIENTE (Controlador)

8.1. Coletar dados pessoais com base legal adequada (consentimento, contrato, legítimo interesse ou outra prevista em lei).

8.2. Informar titulares de forma clara sobre finalidade do tratamento, manter sua própria Política de Privacidade.

8.3. Atender às solicitações dos titulares (LGPD art. 18), podendo solicitar auxílio à MOC para operações técnicas (exclusão, exportação, etc.).

8.4. Não inserir no Serviço dados sensíveis ou de crianças sem base legal adequada.

8.5. Manter atualizado o cadastro do responsável (DPO) na plataforma.

9. Sub-operadores

A MOC utiliza sub-operadores listados no **Anexo I** deste DPA, com os quais mantém contratos de proteção de dados equivalentes a este DPA. Mudanças na lista de sub-operadores serão comunicadas com antecedência mínima de 30 dias; o CLIENTE pode se opor por escrito.

10. Transferência internacional

Alguns sub-operadores estão sediados fora do Brasil (vide Anexo I). A MOC exige desses fornecedores cláusulas contratuais padrão ou outras garantias adequadas previstas no art. 33 da LGPD.

11. Direito de auditoria

O CLIENTE pode auditar, mediante aviso prévio de 30 dias e custas próprias, o cumprimento deste DPA pela MOC, uma vez por ano, em horário comercial e sem interromper a operação. Em alternativa, a MOC pode disponibilizar relatórios de auditoria de terceiros independentes (SOC 2, ISO 27001) quando existentes.

12. Vigência e rescisão

Este DPA vigora pelo mesmo prazo do contrato principal. Sua rescisão antecipada acompanha a rescisão do contrato principal.

13. Lei aplicável e foro

Este DPA é regido pela legislação brasileira, em especial a LGPD. Fica eleito o foro da comarca de [Cidade/UF], com renúncia a qualquer outro, para dirimir controvérsias.

Local: _____ **Data:** _____

MOC SOLUÇÕES LTDA Nome: _____ Cargo: _____ Assinatura: _____

CLIENTE Nome: _____ Cargo: _____ Assinatura: _____

ANEXO I — Lista de sub-operadores

Sub-operador	País	Serviço prestado	Categorias de dados
Mercado Pago (Mercado Livre Inc.)	Brasil	Processamento de pagamento (PIX, boleto, cartão)	Identificação do pagador, CNPJ/CPF, valor
Google LLC (Firebase Cloud Messaging)	EUA	Entrega de push notification	Token de dispositivo, payload de mensagem
Google LLC (Google Analytics 4)	EUA	Métricas agregadas de uso do Site	IP truncado, user-agent (sem dados pessoais)
Google LLC (Google Sign-In)	EUA	Login social (opcional ao cliente final)	E-mail, nome, foto pública do perfil
Meta (Facebook Auth)	EUA	Login social (opcional ao cliente final)	E-mail, nome, foto pública do perfil
Sendinblue/Brevo (Sendinblue SAS)	França	Envio de e-mails transacionais	E-mail destinatário, conteúdo da mensagem
Hostgator (HostGator.com LLC)	EUA/Brasil	Hospedagem de e-mail (recepção em contato@)	E-mail destinatário
MOC Soluções (infraestrutura própria)	Brasil	MinIO (storage de imagens), Postgres, app servers	Todos os dados pessoais tratados

> A lista é atualizada conforme necessário. Versão sempre disponível em `docs/legal/dpa-modelo.md` e em docs.mocsolucoes.com.br.

ANEXO II — Medidas técnicas e organizacionais (MTO)

Segurança da informação

- **Criptografia em trânsito:** TLS 1.2+ obrigatório, HSTS preload no Site.
- **Criptografia em repouso:** disco do servidor com LUKS (quando aplicável) ou criptografia nativa do provedor de cloud.
- **Senhas:** bcrypt com 10 rounds.
- **Tokens:** JWT com expiração configurável (default 7 dias), refresh obrigatório pra escopos sensíveis.
- **Webhook de pagamento:** assinatura HMAC-SHA256 validada server-side.

Controle de acesso

- Autenticação obrigatória pra acessar painéis admin (e-mail+senha ou OAuth).
- Escopos hierárquicos (cliente / operador / adm / superadmin).
- Audit log de eventos críticos (login OK/falha, troca de plano, cobrança manual).

Disponibilidade e backup

- Backup diário do banco Postgres, retenção mínima 7 dias.
- Cópia espelhada em storage S3-compatible (MinIO).
- RTO objetivo: 4h. RPO: 24h.

Resposta a incidentes

- Equipe técnica disponível 24/7 pra incidentes P0/P1.
- Comunicação ao Controlador em até 48h, com plano de mitigação.
- Pós-mortem público (ou ao Controlador afetado) quando aplicável.

Pessoal

- Acessos administrativos restritos a 2 pessoas + auditados em audit_logs.
- Onboarding de novo colaborador inclui treinamento de LGPD e assinatura de termo de confidencialidade.