Compromisso com a Soberania e Privacidade Total dos Dados

O Formatra foi desenvolvido com foco em privacidade desde o design (Privacy by Design). Imagens, documentos, áudios, vídeos, nomes e caminhos de arquivos nunca saem do aparelho. Em produção, somente diagnósticos técnicos de estabilidade são enviados ao Firebase Crashlytics, conforme detalhado nesta política.

1. Processamento 100% Local no Dispositivo (On-Device)

- Isolamento de Hardware: Todas as operações de decodificação, transformação e renderização (imagens, PDFs, documentos, áudios e vídeos) utilizam threads isoladas (isolates/compute) do processador do seu smartphone ou tablet.
- Arquitetura Zero-Cloud: A conversão não utiliza servidor remoto, banco de dados em nuvem nem web service. O acesso à internet é usado exclusivamente pelo Crashlytics para enviar relatórios técnicos de estabilidade.
- Funcionamento Completo Offline: Todas as conversões funcionam perfeitamente no Modo Avião ou sem qualquer conectividade de rede, comprovando a inexistência de fluxo externo de dados.

2. Arquivos Temporários e Sandbox Isolada

- Armazenamento Temporário Restrito: Quando um pipeline de conversão (como transcodificação de vídeo ou áudio via FFmpeg) requer arquivos intermediários de buffer, estes são gravados estritamente na pasta de cache privado do aplicativo gerida pelo sistema operacional (Directory.systemTemp).
- Isolamento de Sandbox: Nenhum arquivo intermediário fica visível para outros aplicativos ou exposto publicamente no armazenamento do dispositivo durante o processamento.

3. Política de Retenção de Dados (Zero Retenção Externa)

- Descarte Imediato de Buffers: Assim que a conversão é concluída, cancelada ou interrompida por erro, todos os arquivos temporários são imediatamente purgados e apagados do armazenamento de cache.
- Zero Histórico Remoto: O Formatra não retém cópias de arquivos em servidores, não mantém histórico de conversões em nuvem e não armazena metadados dos seus arquivos.
- Persistência sob Vontade do Usuário: Apenas o arquivo final que você decide salvar voluntariamente através do seletor nativo permanece guardado na pasta que você escolheu no seu dispositivo.

4. Política de Logs e Diagnósticos Técnicos

- Sem Coleta de Conteúdo em Logs: Logs rotineiros permanecem locais e são sanitizados. Eventos de início ou sucesso de conversão, idioma, formato, quantidade, seleção e salvamento de arquivos não são enviados ao Crashlytics.
- FFmpeg Silencioso em Produção: Em compilações de lançamento (release), os logs nativos do FFmpeg são totalmente silenciados (Level.avLogQuiet e FFmpegKitConfig.disableLogs()), prevenindo qualquer vazamento de detalhes técnicos.
- Telemetria de Estabilidade com Firebase Crashlytics: O app utiliza o Firebase Crashlytics para falhas e diagnósticos de estabilidade. Textos definidos pelo Formatra e stack traces passam por sanitização de caminhos, URIs, nomes de arquivos, e-mails, URLs e padrões de credenciais. O SDK também coleta metadados técnicos, identificadores de instalação e sessão. Não há Firebase Analytics nem identificadores publicitários (AD_ID/IDFA).

5. Compartilhamento e Exportação de Arquivos

- Controle Exclusivo do Usuário: A exportação ou compartilhamento de arquivos convertidos é 100% deliberada e realizada apenas quando o usuário aciona expressamente os botões de Salvar ou Compartilhar.
- Seletores e Folha de Compartilhamento Nativos: A gravação utiliza o seletor nativo do sistema operacional (File Picker / SAF no Android e Document Picker no iOS). O compartilhamento utiliza a folha nativa do sistema (Share Sheet), sem intermediários.

- **Sem Integração com Terceiros:** O Formatra não compartilha dados com redes de publicidade, redes sociais embutidas, anunciantes ou corretores de dados (data brokers).

6. Garantias de Não Coleta

NÃO NÃO envia conteúdo de arquivos para servidores ou nuvens de terceiros.

NÃO NÃO armazena seus dados em servidores ou bancos de dados remotos.

NÃO NÃO exige contas, senhas, cadastros, e-mails ou números de telefone.

NÃO NÃO utiliza identificadores de anúncios (como IDFA no iOS ou AAID no Android).

NÃO NÃO rastreia hábitos de uso ou comportamento de navegação.

7. Declarações Oficiais para Lojas de Aplicativos

• Google Play (Data Safety): declarar Crash logs, Diagnostics, Device or other IDs e atividade técnica de sessão. A coleta é obrigatória para estabilidade, criptografada em trânsito e não inclui arquivos nem conteúdo. AD_ID e Analytics não são usados.

• Apple App Store (App Privacy): declarar Crash Data, Performance Data, Other Diagnostic Data, Product Interaction e Device ID como não vinculados ao usuário e não usados para rastreamento. Nenhum conteúdo de arquivo é coletado.

• LGPD e GDPR: Plena conformidade com os princípios de minimização, segurança e Privacy by Default.

8. Contato e Auditoria Aberta

O Formatra respeita os mais altos padrões de transparência. Qualquer dúvida ou solicitação de auditoria pode ser endereçada no repositório oficial do projeto.

© 2026 Formatra • Arquivos 100% On-Device • Sem publicidade