Segurança e LGPD

Ficha técnica para o time de segurança e o encarregado de dados de quem contrata. O que está aqui está publicado no site, com o rótulo do estado de cada item.

Chaves e cifragem

Envelope por registro

disponível

Cada registro sensível tem a sua chave de dados, embrulhada pela chave-mestra no módulo de chaves. Decifrar um registro não abre nenhum outro; a decifragem privilegiada só acontece num serviço separado.

Trilha de decifragem

disponível

Toda decifragem privilegiada entra numa trilha só de acréscimo, com cadeia de hash: buraco, reordenação e bifurcação aparecem.

Chave dos recibos

disponível

ECDSA P-256 no módulo de chaves; a chave privada nunca sai. Só o serviço que emite recibos assina; a pública é publicada como JWKS.

Componente certificado

disponível

A presença viva vem de um componente da AWS certificado pela iBeta (ISO/IEC 30107-3), declarado no recibo com o fornecedor e a versão do software da Hummand que o chamou, com o opt-out de uso para treino de IA aplicado.

Isolamento e acesso

Isolamento por linha

disponível

Segurança por linha real no Postgres, com um papel de aplicação que não pode contorná-la. Uma consulta sem cliente não devolve nada.

Chaves, sessões e MFA

disponível

Chaves de API por cliente e por escopo. Painel com MFA por aplicativo, códigos de recuperação e limite de tentativas.

Níveis dentro do cliente

disponível

Analista, supervisor e administrador, com autorização por piso em cada rota e testes que provam que nenhuma ficou sem piso.

O console da Hummand deixa rastro

disponível

Toda visualização de dado de cliente pelo console fica registrada e atribuída a uma pessoa. Abrir o conteúdo cifrado de um ato exige motivo, e o cliente vê no painel quem abriu.

Operação

Transporte, borda e release

disponível

TLS automático, transporte estrito com pré-carga, resposta da API sem cache por padrão; cada release aplica a migração com backup antes.

Limites declarados

arquitetura-alvo

mTLS do cliente por camadas, ainda desligado no vínculo com o contrato; mTLS entre serviços internos fica para depois. Limite de requisições por chave, por cliente e por IP.

Dados pessoais

Consentimento por etapa
disponível

Geral antes de tudo, biométrico antes de qualquer captura; textos versionados, com instante, hash e versão gravados no recibo. O consentimento geral nunca desbloqueia biometria.

Nenhuma imagem, nenhum template
disponível

A presença viva e o match devolvem o resultado, e a imagem e o template são descartados. É invariante do produto, não configuração.

Referências em hash
disponível

A referência da pessoa entra como compromisso HMAC com a chave de referência do cliente e um sal novo a cada recibo; o contexto, como hash. É pseudonimização (art. 13, §4º), não anonimização.

Apagamento por destruição de chave
disponível

Pelo ato ou pela referência do cliente, síncrono, com registro de quem apagou e quando. Apagar tem escopo próprio, que nenhuma integração recebe por padrão.

Retenção por prazo
disponível

Veredito e CPF cifrados: 90 dias. Evidência de consentimento e trilha de eventos: cinco anos. Varredura a cada seis horas.

Papéis

O cliente é o controlador; a Hummand, operadora. Registro de tratamento e relatório de impacto preenchidos pelo encarregado em 2026-09-21, revistos a cada mudança de fluxo de dados.

Onde os dados ficam

A instalação de hoje

Servidor e banco na União Europeia, backups cifrados também na União Europeia; presença viva, match e módulo de chaves na AWS, nos Estados Unidos, sem retenção de quadros; a borda e os sites na rede global da Cloudflare; a telemetria com a Grafana Labs, com stack em São Paulo. O mecanismo de transferência de cada fornecedor, nos termos do art. 33, está descrito no registro de tratamento, que o cliente recebe na contratação.

Residência nacional por acordo

Por contrato, a operação pode ser inteiramente nacional: servidor, banco, backups, chaves e a própria presença viva, que também roda em região brasileira.

Registros e pedidos

Registros de acesso
disponível

Por obrigação legal (Marco Civil, art. 15), 190 dias: data, hora, IP e protocolo, num registro separado do banco, dos backups e do recibo.

Ordens legais

Dado pessoal só sai mediante ordem escrita de autoridade competente, no menor escopo, com parecer jurídico antes e registro depois; o cliente é comunicado salvo vedação legal.

Encarregado de dados identificado na Política de privacidade; canal do titular: dados@hummand.com.br. Divulgação responsável: security@hummand.com.br.

contato@hummand.com.br

hummand.com.br/seguranca · hummand.com.br/lgpd