下面标明：哪些必须你亲自到外部平台/运营侧去做，哪些我可以在代码里替你生成或协助。你只需完成“你做”清单，其余交给我即可。

你必须亲自完成的步骤（外部/运营/安全相关）

1. Google Cloud 项目与 OAuth 同意屏幕

* 创建或选择 GCP 项目
* 配置 OAuth consent screen（应用名称、支持邮箱、隐私政策 URL、服务条款 URL、添加测试用户）
* （若需要头像等）启用 People API

1. OAuth 客户端

* 创建 Web application OAuth Client
* 填写 Authorized JavaScript origins（本地 localhost:5173 + 生产域名）
* 填写 Authorized redirect URIs（本地 /api/auth/google/callback + 生产回调）
* 复制得到的 client\_id 与 client\_secret

1. 法务与公开页面

* 准备/部署：隐私政策页、服务条款页（必须是可公开访问的 URL）

1. 域名与 HTTPS

* 确认生产域名可用并启用 HTTPS（OAuth 同意屏幕和 redirect URI 需要）

1. Secret 管理

* 在部署环境里配置环境变量：
  + GOOGLE\_CLIENT\_ID
  + GOOGLE\_CLIENT\_SECRET
  + GOOGLE\_REDIRECT\_URI（生产回调 URL）
  + （本地 .env 里再放开发回调 URL）
* 不把 secret 写进仓库

1. 组织/限制（按需要）

* 如需只允许企业域用户：在同意屏幕或后续策略里限制或用域白名单

1. 测试账号准备

* 添加测试用户（未通过 Google 验证前对外用户无法使用）
* 准备至少两个不同 Gmail 测试登录

1. 品牌素材

* 提供产品 Logo（用于 consent screen）与支持邮箱

1. 数据合规

* 确认你收集的字段（仅 openid/email/profile）符合隐私政策声明

我可直接为你实现/补充的代码与内部配置（告诉我即可继续）

1. 后端

* /api/auth/google/start 生成 state(+PKCE)、返回授权 URL
* /api/auth/google/callback 交换 token、验证 id\_token、创建/查找用户、建立 session
* /api/auth/session 返回当前登录状态
* 会话存储（内存或可插 Redis 适配层）
* 统一错误返回格式

1. 安全

* state & PKCE 验证逻辑
* id\_token JWKS 缓存与验证
* 速率限制（简易中间件）

1. 前端

* 在 AuthModal 中实现 signIn('google')：调用 start → popup → postMessage 处理
* 全局 user / isLoggedIn store（Pinia 或现有状态模块）
* 来源页面记录与返回逻辑（侧边菜单特殊分支）
* Popup 关闭/超时处理
* Loading 与错误提示 UI

1. 辅助

* 环境变量读取与构建时注入（VITE\_GOOGLE\_CLIENT\_ID 可选）
* 文档：本地开发步骤 README 更新
* 简单单元测试 / 集成测试脚手架（可选）

你可以选择的可选手动参与（视需求）

* 是否要刷新 token（离线访问：需 scope + access\_type=offline）
* 是否要拉取更多资料（People API 额外字段 => 更新隐私政策）
* 用户数据表结构（我可给默认；你可再审阅）

最小必做清单（勾完即可让我继续写代码）：

[√] 完成 GCP OAuth consent screen（含测试用户）

[√] 创建 Web OAuth Client，拿到 client\_id / client\_secret

[√] 部署或准备隐私政策 & 服务条款 URL

[√] 确认开发/生产 redirect URLs

[√] 在部署环境配置相关环境变量

[√] 给我：是否仅需基础字段 (openid email profile)（默认是）

[√] 告诉我是否需要 PKCE（默认开启）

接下来怎么做 回复给我：

* 你已完成的打勾项
* 你的生产域名（或暂时没有）
* 是否需要离线刷新（access\_type=offline） 我就继续提交后端与前端实现代码。

需要我先生成后端/前端样板，直接说“生成代码”。