# IT 行业个人创业者法律风险自检手册

## LEGAL RISK SELF-INSPECTION MANUAL FOR IT ENTREPRENEURS

版本 (Version): 1.3.1 (Anonymized & Compliance Enhanced)
适用法域 (Jurisdictions): 全球通用（重点涵盖 CN/US/SG/HK/EU）
文件密级 (Classification): 内部控制 (Internal Control)

# 0. 序言 (PREAMBLE)

本手册旨在为独立开发者 (Indie Hackers)、SaaS
构建者及数字资产创作者提供一套标准化的法律风险防御体系。

# I. 资产主权与知识产权 (ASSET SOVEREIGNTY & IP)

核心原则： 确保数字资产具有排他性的法律控制权，并防止对大厂知识产权的非故意侵犯。

## 1.1 代码污染与开源合规 (Open Source Infection)

风险描述 (Risk Profile): 在闭源商业软件中混入 Copyleft 类型（如 GPL/AGPL）代码，导致衍生作品 (Derivative Works) 被迫开源。

- 触犯法规 (Legal Basis):
- CN: 《中华人民共和国著作权法》第53条（未履行许可条件即构成侵权）。
- US: _Copyright Act_, 17 U.S.C. § 101 et seq. (Breach of License Condition).
- Contract: 违反开源协议即违反合同法。
- 严重后果 (Consequences):
- 强制开源令: 法院可判决你的商业核心代码必须向公众无偿公开（如 Artifex v. Hancom 案）。
- 禁令 (Injunction): 产品被立刻下架，禁止销售。
- 商业信誉破产: 遭受开发者社区抵制，且在寻求投资/并购（M&A;）时尽职调查（Due Diligence）不通过。
- 自检清单 (Checklist):

**[ ]** 是否运行过 SCA (Software Composition Analysis) 工具扫描代码库？

**[ ]** 核心商业逻辑是否与 GPL 组件进行了进程级隔离 (Process Isolation)？

**[ ]** `package.json` 或 `pom.xml` 中是否包含未授权的商业库？

- 防御措施 (Defense Protocol):
- 建立白名单 (License Whitelist): 严格限定仅使用 Permissive Licenses (MIT, Apache 2.0, BSD-3)。
- 隔离封装 (Wrapper/Bridge): 对必须使用的 GPL 组件通过 API 调用，避免静态链接。

## 1.2 AI 生成物确权与标识义务 (AI Ownership & Labeling)

风险描述 (Risk Profile): 纯 AI 生成内容缺乏版权保护；且依据法规，未标识的 AI 内容面临行政处罚。

- 触犯法规 (Legal Basis):
- CN: 《互联网信息服务深度合成管理规定》第16条、第17条（显著标识义务）；《生成式人工智能服务管理暂行办法》。
- US: USCO (美国版权局) 指南：纯 AI 生成内容不属于“ 人类作者 ”作品，无法注册版权。
- 严重后果 (Consequences):

• 资产裸奔: 你的核心素材（如 AI
生成的游戏美术、小说章节）处于公共领域，竞争对手可合法1:1复制，无法维权。

• 行政处罚: 在中国大陆，未对 AI 生成内容进行标识，面临网信办约谈、下架整改及最高 10
万元罚款。

• 平台封杀: 主流内容平台均有权依据《社区公约》对未标识的 AI 内容限流或封号。

• 自检清单 (Checklist):

[ ] 产品生成的内容（图片/文本/视频）是否自动添加了“ AI Generated ”显性水印或隐式元数据？

[ ] 是否保留了 Prompt 工程日志及人工修饰的证据链？

• 防御措施 (Defense Protocol):

• 强制标识 (Mandatory Labeling): 在产品输出端（Export）强制写入“ 由 AI 生成 ”标识。

• 证据固化 (Evidence Retention): 归档所有人工干预的中间产物，以证明“ 人类独创性 ”。

## 1.3 权属清晰度与职务作品 (Work Made for Hire)

风险描述 (Risk Profile): 外包人员（Freelancer）或未签署协议的合伙人默认拥有其创作部分的著作权。

• 触犯法规 (Legal Basis):

• CN: 《中华人民共和国著作权法》第17条（受委托创作的作品，著作权未约定的，归受托人）。

• US: 17 U.S.C. § 101 (Work Made for Hire definition) - 必须有书面协议才能视为雇佣作品。

• 严重后果 (Consequences):

• IP 劫持: 外包程序员或合伙人离职后，有权要求你停止使用其编写的代码/设计的
UI，导致产品瘫痪。

• 融资阻断: 投资人发现核心 IP 不在公司名下，直接否决投资。

• 自检清单 (Checklist):

[ ] 所有外部协作者是否签署了 IP Assignment Agreement (知识产权转让协议)？

[ ] 是否存在口头约定的股权或分红承诺？

• 防御措施 (Defense Protocol):

• 签署 `[IP-TRANSFER]` 协议: 明确约定“ 委托创作 ”属性，权利人自始属于委托方。

## 1.4 品牌隔离与混淆防御 (Brand Isolation)

风险描述 (Risk Profile): 在产品名称或 Logo
中使用大厂元素（如“ 某平台助手 ”、“ 某App下载器 ”），构成不正当竞争。

• 触犯法规 (Legal Basis):

• CN: 《中华人民共和国商标法》第57条（商标侵权）；《反不正当竞争法》第6条（混淆行为）。

• Global: Terms of Service (ToS) of Platforms
(各大平台开发者协议中关于“ 品牌使用 ”的禁止性条款)。

• 严重后果 (Consequences):

• 惩罚性赔偿: 面临“ 赔偿损失+消除影响 ”的民事责任，且大厂通常索赔额巨大（百万级起步）。

• 生态驱逐: 应用在 App Store 被投诉下架，开发者账号被永久封禁。

• 自检清单 (Checklist):

[ ] App 名称是否包含大厂商标？

[ ] Logo 设计是否使用了大厂的配色方案或特定图形元素？

• 防御措施 (Defense Protocol):

• 去官方化命名: 使用“ For [Platform Name] ”而非“ [Platform Name] Downloader ”；在 UI 中显著声明“ 本产品与 [平台方] 无任何关联 ”。

## II. 数据边界与隐私合规 (DATA PERIMETER & PRIVACY)

核心原则： 最小化原则 (Data Minimization) 与 供应链安全。

### 2.1 数据采集与 PIPL/GDPR 合规

风险描述 (Risk Profile): 过度索取权限或无理由收集 PII (个人身份信息)，未获得充分授权。

• 触犯法规 (Legal Basis):

• CN: 《个人信息保护法》(PIPL) 第6条（最小必要原则）、第66条（法律责任）。

• EU: GDPR Art. 5 (Data minimisation), Art. 83 (Fines).

• Criminal (CN): 《刑法》第253条之一（侵犯公民个人信息罪）。

• 严重后果 (Consequences):

• 刑事责任: 违法获取、出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑；情节特别严重的，处三年以上七年以下有期徒刑（如非法获取行踪轨迹信息、通信内容等）。

• 天价罚单: PIPL 最高可罚上一年度营业额 5% 或 5000 万元；GDPR 最高 2000 万欧元或全球营收 4%。

• 通报下架: 被工信部列入“ 侵害用户权益行为APP ”名单，强制下架。

• 自检清单 (Checklist):

[ ] 是否在应用启动时强制索要非必要权限（通讯录、相册）？

[ ] 是否集成了不明来源的第三方 SDK（它们收集的数据算你的责任）？

• 防御措施 (Defense Protocol):

• 隐私套件 (Privacy Kit): 部署标准化的 Privacy Policy。

• SDK 审计: 仅集成头部厂商 SDK，并检查其隐私清单 (Privacy Manifest)。

### 2.2 数据跨境与本地化 (Cross-border Data)

风险描述 (Risk Profile): 将中国/欧盟用户数据传输至境外服务器，未通过安全评估。

• 触犯法规 (Legal Basis):

• CN: 《数据出境安全评估办法》；PIPL 第38条。

• EU: GDPR Chapter V (Transfers of personal data to third countries).

- 严重后果 (Consequences):
- 业务熔断: 监管部门责令停止数据出境，导致跨境业务直接瘫痪。
- 行政处罚: 没收违法所得，并处高额罚款；直接负责的主管人员面临罚款。
- 自检清单 (Checklist):

[ ] 服务器物理位置是否与目标用户群体重合？

[ ] 数据库中是否包含未加密的敏感个人信息？

- 防御措施 (Defense Protocol):
- 本地化存储 (Data Localization): 严格执行 CN/US/EU 数据分治，中国用户数据绝不出境。

### 2.3 未成年人防火墙 (Minor Firewall)

风险描述 (Risk Profile): 处理未成年人数据未获监护人同意。

- 触犯法规 (Legal Basis):
- CN: 《未成年人保护法》；《儿童个人信息网络保护规定》。
- US: _Children's Online Privacy Protection Act_ (COPPA).
- 严重后果 (Consequences):
- 核弹级打击: 相比成人隐私违规，针对儿童的违规在美国面临 FTC 的顶格处罚（单次违规可达 $50,000+，且按用户数累加）。
- 舆论毁灭: 品牌被贴上“危害儿童”标签，彻底丧失市场立足点。
- 自检清单 (Checklist):

[ ] 是否有识别用户年龄的机制（即使是简易的生日选择）？

[ ] 注册协议是否包含“拒绝向未满 13/14 周岁用户提供服务”的条款？

- 防御措施 (Defense Protocol):
- 拒绝服务声明: 在 ToS 中明确不向儿童提供服务，若发现儿童账号将立即删除数据。

## III. 交易协议与消费者风控 (TRANSACTION & CONSUMER PROTECTION)

核心原则： 限制责任与阻断恶意维权。

### 3.1 虚拟商品交付与退款 (Delivery & Refund)

风险描述 (Risk Profile): 数字产品被恶意退款，或因“不满意”引发纠纷。

- 触犯法规 (Legal Basis):
- CN: 《消费者权益保护法》第25条（数字化商品不适用七日无理由退货，但需消费者确认）。
- Payment Rules: Stripe/PayPal Merchant Agreements (Chargeback ratios).
- 严重后果 (Consequences):

• 资金冻结: 若 Chargeback（拒付）率超过 1%，支付网关（Stripe/PayPal）将冻结账户并扣留保证金 180 天，现金流断裂。

• 职业打假人勒索: 因条款漏洞被职业索赔，主要针对“ 虚假宣传 ”或“ 霸王条款 ”。

• 自检清单 (Checklist):

[ ] 用户协议是否包含“ No Cooling-off Period ”(无冷静期) 豁免声明？

[ ] 是否定义了“ 交付完成 ”的技术标准？

• 防御措施 (Defense Protocol):

• 反恶意维权: 借鉴电商平台逻辑，对于“ 恶意购买 ”、“ 滥用退款机制 ”的用户，保留单方面终止服务并不予退款的权利。

### 3.2 自动续费合规 (Subscription Compliance)

风险描述 (Risk Profile): 违反自动续费法规，设置“ 取消陷阱 ”。

• 触犯法规 (Legal Basis):

• CN: 《网络交易监督管理办法》第18条（自动续费前5日显著提示）。

• US: _Restore Online Shoppers' Confidence Act_ (ROSCA); California _Automatic Renewal Law_ (ARL).

• 严重后果 (Consequences):

• 集体诉讼 (US): 违反加州 ARL 是集体诉讼的重灾区，赔偿金包括退还所有历史订阅费。

• 行政罚款 (CN): 市场监管总局责令限期改正，并处以罚款。

• 自检清单 (Checklist):

[ ] 是否在扣款前发送提醒？

[ ] 取消入口是否隐蔽？

• 防御措施 (Defense Protocol):

• 透明交互: 遵循 "Click-to-Cancel" 原则，取消订阅的步骤不得多于订阅步骤。

## IV. 平台依赖与业务连续性 (PLATFORM DEPENDENCY)

核心原则： 降低“ 寄生 ”风险，防止单点故障。

### 4.1“ 卡脖子 ”条款自查 (ToS Check)

风险描述 (Risk Profile): 触犯平台“ 天条 ”（如绕过 IAP、诱导分享）。

• 触犯法规 (Legal Basis):

• Contract: 违反 Apple Developer Program License Agreement 或 微信小程序平台运营规范。

• 严重后果 (Consequences):

• 账号处决: 开发者账号被 Terminated，且关联的身份信息（身份证/信用卡）被列入黑名单，终身无法重新注册。

• 资金没收: 账户内未结算的广告费或内购收入可能被平台根据协议没收。

• 自检清单 (Checklist):

[ ] 支付流是否绕过了 App Store / 微信支付？

[ ] 营销裂变机制是否包含“强制分享”？

• 防御措施 (Defense Protocol):

• 支付路由切换 (Payment Switching): 预埋 H5 支付开关。

### 4.2 反爬虫与反向工程防御 (Anti-Crawling Defense)

风险描述 (Risk Profile): 依赖抓取/解析大型平台数据，或提供破解工具。

• 触犯法规 (Legal Basis):

• CN Criminal: 《刑法》第285条（非法侵入计算机信息系统罪；提供侵入、非法控制计算机信息系统程序、工具罪）。

• CN Civil: 《反不正当竞争法》第12条（妨碍、破坏网络产品或者服务正常运行）。

• US: _Computer Fraud and Abuse Act_ (CFAA).

• 严重后果 (Consequences):

• 刑事拘留: 只要使用了技术手段绕过平台防护（如IP代理池、模拟登录、破解签名），极易触犯刑法。这是真正的“牢狱之灾”。

• 巨额赔偿: 平台方会主张你的行为增加了其服务器负担、破坏了生态，索赔额通常以“非法获利”或“给平台造成的损失”计算，数额巨大。

• 自检清单 (Checklist):

[ ] 核心业务数据是否 100% 依赖第三方非公开接口？

[ ] 是否使用了模拟登录或 IP 代理池等对抗手段（这增加了刑事风险）？

• 防御措施 (Defense Protocol):

• 降级熔断: 设计“服务降级”模式，当大厂接口失效时，产品能回退到本地功能。

• 免责隔离: 在用户协议中明确：“本工具仅为浏览器辅助，不存储、不破解第三方数据，用户需自行承担使用风险。”（注意：此条款不能免除刑事责任，只能在一定程度上减轻民事过错）。

## V. 移动应用商店合规 (MOBILE APP STORE COMPLIANCE)

核心原则： 避免触发苹果/谷歌的“死刑条款”(Termination)，防止账号关联封禁。

### 5.1 支付绕道与虚拟商品 (IAP Bypass / Steering)

风险描述 (Risk Profile): 在 App 内销售虚拟商品（如会员、电子书、游戏币）时，试图绕过 Apple IAP (In-App Purchase) 或 Google Play Billing，接入第三方支付（如支付宝、Stripe）。

• 触犯规定 (Regulations):

• Apple: _App Store Review Guidelines_ § 3.1.1 (In-App Purchase).

• Google: _Google Play Payments Policy_.

• 严重后果 (Consequences):

• 拒绝上架 (Rejection): 审核直接被拒，无法发布。

• 下架封号 (Termination): 若通过热更新或“ 切支付 ”开关（Switch）隐蔽上线，一旦被人工复审或竞品举报发现，属于“ 欺诈行为 (Fraud) ”，会导致开发者账号及其关联账号（Associated Accounts）被永久封禁。

• 自检清单 (Checklist):

**[ ]** 销售的是“ 虚拟商品 ”还是“ 实物商品 ”？（虚拟商品必须走 IAP）。

**[ ]** App 内是否存在隐藏的 WebView 指向第三方支付页面？

**[ ]** 是否在 UI 中包含了“ 去官网购买更便宜 ”的引导性按钮（Steering）？（注：部分地区如欧盟/美国有新规豁免，但需极其严格的申报）。

## 5.2 诱导性评价与刷榜 (Incentivized Reviews & Manipulation)

风险描述 (Risk Profile):
通过给予用户奖励（如金币、解锁功能）换取五星好评，或购买虚假下载量刷榜。

• 触犯规定 (Regulations):

• Apple: _App Store Review Guidelines_ § 3.2.2 (Unacceptable) & § 5.6 (Developer Code of Conduct).

• Google: _Google Play Developer Program Policies_ (Spam and minimum functionality > User Ratings, Reviews, and Installs).

• 严重后果 (Consequences):

• 清榜: 应用评论被清空，榜单排名被强制除名。

• 信用污点: 开发者被列入商店黑名单，影响后续所有新 App 的审核权重。

• 自检清单 (Checklist):

**[ ]** App 内是否有弹窗提示“ 好评送 VIP ”？

**[ ]** 推广渠道是否承诺“ 保证排名进入前 10 ”？（此类服务商通常使用机刷，极高危）。

## 5.3 隐私标签欺诈 (Privacy Label Fraud)

风险描述 (Risk Profile): 在 App Store Connect 或 Google Play Console 填写的隐私标签（Privacy Nutrition Label）与 App 实际行为不符（例如：填写“ 不收集数据 ”，但集成的广告 SDK 在后台读取 IDFA/Android ID）。

• 触犯规定 (Regulations):

• Apple: _App Store Review Guidelines_ § 5.1.1 (Data Collection and Storage).

• Google: _Google Play User Data Policy_.

• Law: US FTC Act (Unfair or Deceptive Acts).

• 严重后果 (Consequences):

• 下架: 发现隐私声明不实，直接下架整改。

• 法律诉讼: 属于对消费者的“ 欺诈性陈述 ”，在美国可能面临集体诉讼或 FTC 调查。

• 自检清单 (Checklist):

[ ] 是否详细审查了所有第三方 SDK 的隐私披露文档？

[ ] 隐私标签是否随 App 版本更新同步更新？

### 5.4 账号关联与“马甲包”(Account Association & Spam)

风险描述 (Risk Profile): 为了获取流量，发布多个功能相似的 App（马甲包）；或因一个账号被封，注册新账号重新上架。

- 触犯规定 (Regulations):
- Apple: _App Store Review Guidelines_ § 4.3 (Spam).
- Google: _Repetitive Content Policy_.
- 严重后果 (Consequences):
- 连坐封禁 (Associated Termination): 苹果/谷歌会通过设备指纹、代码相似度、付款信用卡、登录 IP、联系人信息等建立关联图谱。一旦被判定关联，所有相关账号（包括你朋友借给你测试的账号）会被一并封禁，且申诉极难通过。
- 自检清单 (Checklist):

[ ] 是否使用了纯模板代码打包 App？

[ ] 是否在同一台电脑/网络环境下登录了多个归属不同的开发者账号？

## VI. 全球化争议阻断 (GLOBAL DISPUTE BLOCKING)

核心原则： 借鉴知名出海产品协议，通过法律技术手段提高用户诉讼门槛。

### 6.1 强制仲裁与集体诉讼弃权 (Arbitration & Class Action Waiver)

风险描述 (Risk Profile): 在美国等法域，遭遇即兴的集体诉讼（Class Action）。

- 触犯法规 (Legal Basis):
- US: _Federal Arbitration Act_ (FAA). 允许在合同中约定强制仲裁。
- 严重后果 (Consequences):
- 破产性诉讼: 若无此条款，一个简单的 UI 违规或隐私瑕疵可能导致全美用户发起集体诉讼，仅律师费和和解金就足以让一家初创公司破产。
- 自检清单 (Checklist):

[ ] 针对美国/海外用户的 ToS 中，是否包含“Class Action Waiver”条款？

[ ] 是否指定了低成本的争议解决地（如新加坡、香港或中国内地）？

- 防御措施 (Defense Protocol):
- 部署 [DISPUTE-SHIELD] 条款:

明确约定：“任何争议应首先通过非正式协商解决；协商不成的，必须提交至 [创业者所在地] 进行个案仲裁，放弃参与集体诉讼的权利。”

免责声明 (DISCLAIMER): 本手册仅供风险自检参考，不构成律师-客户关系 (Attorney-Client Relationship) 下的法律意见。具体个案请咨询具有相关司法辖区执业资格的律师。

Prepared By: Legal Assistant AI

Date: 2025-12-20