业务流程设计与合规落地指引：开发类专用版

BUSINESS PROCESS & COMPLIANCE GUIDELINES: DEV-OPS LEGAL (REV. 3.0)

适用对象： 独立开发者 (Independent Developers)、SaaS 构建者 (SaaS Builders)、外包技术服务商 (Outsourcing Vendors)、AI 工具开发者。

核心法理： 基于合同法、知识产权法及全球数据合规要求（PIPL/GDPR），构建全周期的法律防御工事。

阶段一：需求锚定与缔约 (Initiation & Scoping)

目标： 确立合同标的（Subject Matter）的刚性边界，通过程序正义规避范围蔓延（Scope Creep）与管辖风险。

1.1 核心定义与法律适用 (Definitions & Governing Law)

- 流程动作： 在合同首部明确定义“ 知识产权归属原则 ”及“ 争议解决路径 ”。
- 关键合规点：
- 排斥“ 职务作品 ”(Exclusion of "Work Made for Hire")： 针对美国及英美法系客户，必须在显眼位置声明：“ 双方明确同意，本合同不构成美国《版权法》17 U.S.C. § 101 意义上的‘ Work Made for Hire ’。所有知识产权归属严格依照本合同知识产权条款约定。 ”
- 分层管辖策略 (Jurisdiction Strategy)：
- 境内客户： 适用中华人民共和国法律。争议解决推荐深圳国际仲裁院 (SCIA)（科技案件专业度高）或中国国际经济贸易仲裁委员会 (CIETAC)。
- 跨境客户： 推荐适用新加坡法律 + 新加坡国际仲裁中心 (SIAC)（高性价比、执行力强）；或香港法律 + 香港国际仲裁中心 (HKIAC)。
- 注： 避免默认适用中国法院管辖，以免遭海外客户抵触。

1.2 需求规格说明书 (SOW) 的法律排他性

[V] 流程动作： 将技术需求转化为具备法律效力的《工作说明书》（Statement of Work）。

- 关键合规点：
- 排他性定义 (Exclusivity of Scope)： 设置“ 消极清单（Negative List） ”，明确未列入 SOW 的功能视为“ 不在范围内（Out of Scope） ”。
- 变更控制机制 (Change Control Procedure)： 确立“ 无 CR (Change Request) 不变更 ”原则。任何变更必须书面确认其对价格（Fees）和交付日（Delivery Date）的影响。

1.3 灵活化报价与支付里程碑 (Pricing & Payment Milestones)

- 流程动作： 根据客户类型提供差异化支付方案，提高签约率。
- 关键合规点：
- 方案 A（稳健型 - 适合中大型项目）： 40% 签约预付 - 40% Beta 版本交付 - 20% 最终验收。
- 方案 B（激进型 - 适合敏捷开发）： 50% 签约预付 - 30% 上线/部署 - 20% 质保期结束或最终验收。

• 中止权 (Right of Suspension)：约定“若甲方逾期付款超过 [X] 日，乙方有权暂停开发、切断 API 访问，且不承担违约责任。”

阶段二：开发与资产管理 (Development & Asset Mgmt)

目标：实施 IP 污染隔离（IP Contamination Isolation）、AI 合规流转与资产确权。

2.1 开源组件准入与隔离机制 (OSS Compliance & Isolation)

• 流程动作：采用“工具扫描 + 人工复核”的双重审查机制。

• 关键合规点：

• 自动化合规工具链：

• 依赖扫描：使用 Dependabot / Renovate + Snyk / Socket.dev 进行实时监控。

• License 审计：使用 FOSSA / ClearlyDefined / Open Source License Checker 生成合规底稿。

• Copyleft 物理隔离：针对 GPL/AGPL 组件，强制采用独立进程（Independent Process）架构，仅通过 API 通信，阻断开源义务向主程序传染。

2.2 AI 辅助开发与 Prompt 保护 (AI Governance & Asset Protection)

• 流程动作：记录 AI 工具使用日志，明确数据流转条款。

• 关键合规点：

• AI 工具服务条款流转 (Terms Flow-down)：“乙方保证，开发过程中使用的 AI 工具（如 GitHub Copilot, Claude, GPT）均已接受其服务条款中关于‘数据保密’与‘非训练用途（Opt-out of Training）’的约束，不会将甲方的特定业务逻辑用于模型训练。”

• Prompt 商业秘密保护 (Prompt as Trade Secret)：“甲方不得通过逆向工程 (Reverse Engineering)、反编译或恶意诱导等方式，尝试获取、复制或使用乙方用于生成代码/UI 的提示词 (Prompts)、参数配置或微调模型权重。”

• 中间件确权：明确通用算法逻辑、数据库设计归乙方所有（Background IP），仅授权甲方使用。

阶段三：交付与验收闭环 (Delivery & Acceptance)

目标：确立交付完成的法律事实，实施分层交付策略。

3.1 数字化交付与默示验收 (Digital Delivery & Deemed Acceptance)

• 流程动作：发送标准化《交付确认函》或 Release Tag，并设置差异化验收期。

• 关键合规点：

• 差异化验收时效： 纯代码交付：7-10 个工作日；SaaS/已上线系统：3-5 个工作日（基于“ 上线即使用 ”的法理）。

• 默示验收条款： 约定“ 逾期未提书面异议（需附带 Bug 复现路径），视为验收合格。 ”

3.2 源代码分层交付策略 (Layered Source Code Delivery)

• 流程动作： 将交付物在物理层面进行分包。

• 关键合规点：

• 业务层（Business Layer）： 提供完整可编辑源代码，转让著作权（或独家许可）。

• 通用层（Infrastructure/Middleware Layer）： 仅提供编译后的二进制文件、压缩包或只读访问权限（Read-only Access）。保留开发者核心框架的知识产权。

阶段四：运维、数据合规与责任限制 (Maintenance, Data & Liability)

目标： 构建风险防火墙，明确数据处理者角色。

4.1 数据安全与跨境合规 (Data Compliance & Cross-border)

• 流程动作： 在 DPA (Data Processing Agreement) 中明确角色划分。

• 关键合规点：

• 角色划分 (Controller vs Processor)： 明确甲方为数据控制者 (Controller)，对数据来源合法性及用户授权负责；乙方仅为数据处理者 (Processor)，依照甲方指令处理数据。

• 安全义务： 乙方承诺采取行业标准的技术措施（加密、访问控制、日志审计）。

• 跨境传输 (Cross-border Data Transfer)： 若涉及数据出境（如中国用户数据传至海外服务器），明确双方需配合签署“ 标准合同条款 (SCCs) ”或通过相关安全评估，费用及合规责任由数据控制者（甲方）主要承担。

4.2 务实的责任限额 (Liability Cap)

• 流程动作： 设定更具可执行性的赔偿上限。

• 关键合规点：

• 保底限额机制：“ 在法律允许范围内，乙方承担的赔偿总额不超过以下较高者：(i) 甲方在本合同项下已实际支付给乙方的服务费用总额；或 (ii) 人民币 [500,000] 元（或等值外币）。 ”

• 现状提供 (As-Is)： 重申不保证软件无 Bug，并明确排除对云厂商（AWS/Azure）故障导致的连带责任。

[DELIVERABLES] 配套法律文件包清单 (Rev. 3.0)

[V] 《技术开发主服务协议 (MSA - International)》：含 WMFH 排除、管辖权选项、分层交付条款。

[V] 《工作说明书 (SOW)》：含变更控制 (CR) 流程、支付方案 A/B。

- 《数据处理协议 (DPA)》：含 Controller/Processor 划分、跨境传输条款。
- 《开源组件合规报告》：由 Snyk/FOSSA 导出的自动化清单。
- 《SaaS 订阅协议 (ToS)》：含放弃撤回权、AI 使用声明。