Argus 部署 DPIA 清单

Argus Gateway · 企业 AI 隐私网关 · DPIA 模板 v0.1 · 爱科拓 (agilist.cn)

本清单用于企业在部署 Argus Gateway 前，依据《个人信息保护法》第 55 条要求开展的 个人信息保护影响评估（DPIA）。清单覆盖 5 大类 22 项控制项，其中多项可由 Argus 管理后台直接导出 evidence，降低企业自评成本。

> **适用范围：** PIPL 第 55 条规定，以下四种场景必须事前开展 DPIA：
>
> - 处理敏感个人信息（身份证 / 金融账户 / 健康 / 生物识别等）；
> - 利用个人信息进行自动化决策；
> - 委托处理、对外提供或公开个人信息；
> - 向境外提供个人信息。
>
> 企业部署 Argus 转发 LLM 服务的场景通常至少涉及前两项（员工 prompt 含 PII + LLM 自动化决策）， 因此建议作为部署前强制步骤。PIPL 第 55 条同时要求 DPIA 记录**保存至少 3 年**。

1. 使用说明

- "评估记录"列由企业合规 / 法务 / 安全官共同填写；Argus 仅提供表格模板与能力映射。
- "Argus 支撑"列描述 Argus 可提供的技术证据或能力字段，作为填写参考。
- 建议按"识别 → 映射 → 必要性 → 风险 → 缓解"的顺序完成，每项需有可追溯的材料来源（文档路径 / 系统截图 / 审计日志编号）。
- 完成后的 DPIA 文档由企业 DPO 或合规负责人签署留档；Argus 后续版本会提供 DPIA 自助生成向导，自动拼接本清单与审计 evidence。

2. DPIA 清单

#	评估项	企业评估记录	Argus 支撑
A. 处理活动识别			
A1		____	

#	评估项	企业评估记录	Argus 支撑
	处理目的（如：员工代码助理 / 客服对话 / 知识问答）		业务场景由企业定义；Argus 侧可按 API Key 维度打标签对应业务场景。
A2	数据主体类别（员工 / 客户 / 供应商 / 合作方等）	____	审计日志带 `user_id` / `dept`，可按主体类别聚合。
A3	预计处理规模（月请求数 / 月 token 量级）	____	Dashboard 提供按日 / 按月聚合的请求量与 token 统计。
B. 数据流映射			
B1	涉及的个人信息类别（姓名 / 身份证 / 联系方式 / 生物识别 / 健康 / 金融等）	____	Argus 多层 PII 引擎命中统计按类型聚合（L1 结构化 / L1b 证据评分 / L2 开放词汇）。
B2	是否涉及敏感个人信息（PIPL §28）	____	审计日志标记敏感类型命中（金融 / 医疗 / 证件 / 未成年人等）。
B3	数据采集来源（员工输入 / 系统对接 / 客户提交）	____	按 API Key / 来源 IP 追溯；support 对接 SSO 身份。
B4	上游接收方（LLM 后端名单 + 部署地域）	____	路由规则与上游清单在 admin 后台可查；审计日志每条记录具体 upstream。
B5	是否跨境传输（PIPL §38-40）	____	默认路由国产后端；如启用海外上游，可按地域策略限定业务线与数据类型。
C. 必要性与合法性			
C1		____	企业自行判断；Argus 提供知情材料模板框架。

#	评估项	企业评估记录	Argus 支撑
	处理的法律依据（PIPL §13：同意 / 履行合同 / 法定职责等）		
C2	是否遵循最小必要原则（PIPL §6）	____	脱敏层保证仅必要字段传递至上游；可比对"原始 prompt"与"脱敏后 prompt"字段差异（内部）。
C3	员工 / 用户是否已知情并同意（PIPL §17）	____	企业侧走员工知情同意流程；Argus 后台可展示"数据流向"面板作为知情材料支撑。
C4	保留期限与删除策略（PIPL §19）	____	审计日志保留期可配置；过期按策略自动清理，删除行为留档。
D. 风险识别			
D1	未授权访问风险（内部越权 / 外部攻击）	____	API Key 粒度访问控制 + 审计留痕；支持按部门 / 角色隔离。
D2	数据残留 / 泄露风险（上游保存原始 prompt）	____	脱敏在网关层完成，上游收到的是脱敏后数据；企业可要求上游签约"不用于训练"。
D3	再识别风险（脱敏数据能否被还原）	____	脱敏 key 本地保存；还原操作仅在返回用户侧发生，不经过上游。
D4	自动化决策风险（PIPL §24）	____	Argus 提供每次请求的决策路径审计，可作为申诉 / 复核证据。
D5	跨境传输风险（PIPL §38-40）	____	默认国产路由；启用海外需配合企业安全评估与标准合同流程。
E. 缓解措施			

#	评估项	企业评估记录	Argus 支撑
E1	脱敏 / 加密措施	____	L1+L1b+L2 多层脱敏；传输层 TLS 1.2+；审计库支持透明加密。
E2	访问控制与权限管理	____	License / API Key / 部门三层；管理员 / 审计员 / 只读角色分离。
E3	审计与可追溯	____	每次请求结构化审计；支持按用户 / 部门 / 上游 / PII 类型聚合导出。
E4	应急响应 / 事件通报（PIPL §57）	____	日志可对接企业 SIEM；异常（如批量越权）可配置告警（v1.5 insights）。
E5	残留风险评估与可接受性判断	____	企业 DPO 基于 A-E 填写结论判断；Argus 不替代主体责任判断。

3. 签署与留存

- DPIA 文档由企业 DPO 或合规负责人签署，建议同时由法务 / 安全 / 业务负责人会签。
- 按 PIPL 第 55 条要求，DPIA 记录**至少保存 3 年**。
- 处理活动发生重大变更（新增上游 / 新增 PII 类型 / 调整路由策略）时需重新评估。
- 建议与年度合规审计周期同步复核本清单。

4. Argus 自动化支撑清单

本清单中可直接由 Argus 管理后台导出作为 evidence 的字段：

- A2 / A3：Dashboard 按主体类别与时间聚合
- B1 / B2：PII 引擎命中统计（类型 + 敏感分级）
- B4 / B5：路由审计（upstream + 地域）

- C4：审计日志保留期配置与清理记录
- D1：API Key 访问记录 + 异常访问告警
- E3：审计导出（CSV / PDF / SIEM 对接）

免责声明： 本清单为 Argus Gateway 部署场景下的 DPIA 模板起点，不构成法律意见，也不替代企业合规主体责任。 企业应由自有 DPO / 法务 / 安全团队结合具体业务场景判断残留风险是否可接受。Argus 提供的字段与 evidence 是支撑材料，最终 DPIA 文档的法律效力以企业合规签署版本为准。
