PIPL 合规白皮书

Argus Gateway · 企业 AI 隐私网关 · 示意版 v0.1 · 更新于 2026-04-19 · 爱科拓 (agilist.cn)

本白皮书示意《中华人民共和国个人信息保护法》（PIPL）主要条款与 Argus Gateway 能力的对应方向。 所列 Argus 能力为方向性描述，具体实现细节、字段 schema 与 evidence 导出形式，以实际部署后的 admin 后台和合规文档为准。

> **阅读说明：** 本文件面向企业安全 / 法务团队做 Argus 选型评估时的方向性参考。 它不是完整的法律意见，也不是详细的 Argus 实现文档。 详细映射 / evidence 字段 / DPIA 模板等，请在申请 demo 后由 Argus 团队随部署方案一起提供。

1. Argus 在 PIPL 合规链路中的定位

PIPL 下，使用 AI 服务的企业既可能是"个人信息处理者"（直接收集员工 / 客户数据并输入到 LLM）， 也可能委托外部 LLM 服务进行处理。无论哪种，AI 调用链上都会出现 PII 被传递、被存储、被跨境的情况。

Argus Gateway 处于企业和上游 LLM 服务之间，承担三类 PIPL 相关的技术职责：

- **输入侧脱敏：**在请求进入上游 LLM 前，对常见 PII 做脱敏处理，降低"必需字段之外的 PI"泄露的概率。
- **审计留痕：**记录每次 LLM 请求的身份、时间、脱敏类型、路由决策、上游后端等信息，形成合规证据。
- **路由可控：**企业可以选择国产 LLM 后端以避免数据出境，或对特定敏感业务走本地 / 私有云部署。

2. PIPL 条款 × Argus 能力方向

条款	要求	Argus 能力方向
第 10 条	合法、正当、必要处理个人信息	多层 PII 脱敏，尽量只向上游 LLM 传递完成任务所必需的字段。
第 17 条		

条款	要求	Argus 能力方向
	告知用户数据处理情况	管理后台提供数据流向可视化，可作为员工 / 用户知情材料的支撑。
第 19 条	合理期限内存储	审计日志保留期可配置，过期自动清理。
第 21 条	委托处理关系需签订协议	Argus 提供标准 DPA 模板框架，供法务按企业合规流程完善。
第 38-40 条	数据出境评估	默认路由国产 LLM（数据不出境）。如需海外后端，配合企业出境评估流程与地域路由策略。
第 55 条	DPIA（数据保护影响评估）	提供 Argus 部署场景下的 DPIA 模板（即将上线），可直接作为评估文档起点。

3. 多层 PII 识别能力概述

Argus 的 PII 识别不是单一 regex，而是多层协同：

- **L1 规则层：**基于规则的快速识别，覆盖中国常见结构化 PII（身份证 / 银行卡 / 手机 / 邮箱 / 地址 / 港澳台证件 / 企业统一社会信用代码等）。
- **L1b 证据评分层：**结合上下文判断识别结果的置信度，降低误判率。
- **L2 开放词汇层：**面向中文姓名 / 组织名 / 地名等规则难以穷尽的开放词汇 PII 类型。

具体每层的识别规则、置信度阈值、性能数据将在后续《多层 PII 引擎技术白皮书》中披露。 核心算法部分（argus-redact）已开源，企业可独立验证中文 PII 识别效果。

4. 审计与证据链

Argus 为每次 LLM 请求生成结构化审计日志，包含：

- 请求方身份（API Key / 部门 / 员工）
- 脱敏层命中情况与 PII 类型分布
- 路由决策与上游后端
- 响应时长与成本归因

审计数据可按部门 / PII 类型 / 上游 / 用户等维度聚合导出，对接企业已有的 SIEM 或合规审计系统。 字段详细 schema 随部署方案提供。

5. 数据出境与国产 LLM 路由

在 PIPL 第 38-40 条框架下，企业使用海外 LLM 服务涉及"个人信息出境"， 需走安全评估 / 标准合同备案 / 认证三条路径之一。

Argus 的默认方案是路由至国产 LLM 后端（DeepSeek / Kimi / 豆包 / 通义等）， 从网络链路上避免"个人信息出境"的合规成本。 如果业务必须使用海外后端，Argus 通过地域路由策略配合企业出境评估流程， 在脱敏层叠加隔离。

6. 使用建议

- 企业部署前应由法务 / 安全官共同完成一次 Argus 场景下的 DPIA。
- 基于实际业务风险等级选择脱敏层组合与路由策略，不同部门 / 业务线可设置不同策略。
- 审计日志保留期需与企业现有日志留存策略、PIPL 第 19 条、网安法第 21 条（6 个月）协调。
- Argus 提供的 DPA 模板、备案材料模板、DPIA 模板均为起点，最终法律效力以企业法务审定版本为准。

免责声明： 本文件为 Argus Gateway 合规能力方向性介绍，不构成法律意见。 企业落地 AI 合规应由自有合规 / 法务团队结合具体业务场景判断， Argus 提供的模板和能力是支撑材料，不替代企业合规主体责任。