

中国制造企业工业设备联网与数据采集合规分析

****重要说明：****本报告基于截至 **2026 年 10 月 13 日** 有效的公开法规、监管规则、标准与执法案例，以及所提供原 PDF 的披露内容形成，属于合规研究与整改建议，不构成正式法律意见。涉及重要数据认定、关基身份、数据出境申报及重大事件报告时，建议由中国执业律师与属地主管部门进一步确认。

首要结论

原报告包含多项会直接扩大监管与生产安全风险的错误结论，尤其是明文工控通信、直连公网云、无需分类分级、无需等保、任意跨境和事后再报告。

立即止损

暂停未经评估的数据出境和公网直连；禁止共享管理员账号；恢复并集中留存日志；启动工业数据分类分级、等保定级和跨境数据盘点。

管理层决策点

应将该项目从单纯“设备联网工程”升级为 OT 安全、数据安全、个人信息保护和跨境合规的联合治理项目。

原 PDF 明确主张“无需分类分级、无需采集日志、优先明文 Modbus/TCP、公网云无需隔离、统一保存六个月”，并允许核心工艺数据直接传往境外总部。¹同时还主张无需等保、共享管理员账号、系统卡顿即可关闭审计功能、三年一次自查、发生泄露后再报告等做法。¹这些结论不能作为项目上线或安全验收依据。

一、关键错误纠正清单

原报告结论	评级	正确口径	管理层建议动作
工业数据无需分类分级	不符合	工业数据处理者应定期梳理数据，识别一般、重要和核心数据；重要/核心数据还需形成目录并备案。生产运行、工艺参数、系统日志本身即属于需梳理的数据类别。 2	立即建立“设备—数据项—系统—用途—流向—级别”台账
设备日志无需记录采集行为	不符合	工业数据处理、权限管理、人员操作日志应留存不少于六个月；《网络安全法》也要求网络运行和安全事件日志不少于六个月。 2 3	恢复日志，接入集中审计；禁止业务部门自行关闭
优先使用明文 Modbus/TCP	条件性错误/高风险	法律没有指定唯一工业协议，但重要/核心数据传输应采用密码、校验、安全通道或安全协议；工信部指南要求远程访问使用 IPsec、SSL、VPN 等安全通道。 2 4	明文 Modbus 仅限严格隔离的本地 OT 段；跨区、远程、上云必须通过安全网关/隧道

原报告结论	评级	正确口径	管理层建议动作
工业数据库可直接部署公网云且无需隔离	不符合	工控网络与管理网或互联网连接时，应分区分域、实施边界防护和行为审计；上云设备应双向认证，不同业务环境应隔离。 4	取消数据库公网暴露，建设 OT-DMZ、私网接入、云安全组和堡垒机
所有数据统一保存六个月	不符合	“六个月”主要是网络及工业处理日志的最低留存期，不是所有数据的统一保存期；个人信息应按实现目的所必需的最短时间保存。 5 2	建立按数据类型、用途、法规及合同区分的留存矩阵
核心工艺数据可直接传境外总部	不符合	重要数据出境原则上必须通过安全评估；个人信息还要根据身份、规模和敏感性选择安全评估、标准合同或认证路径。 6	在完成分类、出境数据盘点和路径判定前暂停相关传输

原报告结论	评级	正确口径	管理层建议动作
所有工业数据都不是重要数据	错误	并非所有工艺数据都自动构成重要数据，但也不能自行一概排除。企业须识别、申报；未被主管部门告知或公开列入重要数据的，出境时可不按重要数据申报。 7 6	建立重要数据识别工作底稿，并保留向属地工信部门咨询的记录
无需等保	不符合	网络安全等级保护是法定义务；工业控制系统、物联网、云及大数据平台均属于等保对象范围。 3 8	对 PLC/SCADA、MES、工业数据库、边缘平台、云平台分别确定合理边界并定级
等保三年做一次即可	错误	二级以上系统应在定级或上线后 30 日内备案；三级系统至少每年测评一次、四级至少每半年一次。二级周期需结合属地和行业要求，不可统一写成“三年一次”。 9	先定级再确定测评周期，不以供应商口头意见替代定级

原报告结论	评级	正确口径	管理层建议动作
泄露以后再报告	严重不符合	发生或可能发生数据/个人信息泄露时应立即处置并按规则报告；较大以上网络安全事件中，关基最迟 1 小时，其他网络运营者最迟 4 小时报告。 5 10	建立小时级内部升级机制和监管报告预案
共享管理员账号、可关闭审计	不符合	法规要求合理权限、访问控制、安全认证和可追溯日志；工控指南明确最小授权、关键系统双因素认证。 7 4	取消共享账号，推行实名账号、PAM/堡垒机、MFA 和紧急账号审批
“未自报关基，所以一定不是关基”	未知/错误逻辑	关基由保护工作部门依据认定规则组织认定并通知运营者，并非企业仅靠自我判断即可排除。 11	核实是否收到认定通知，并评估所属行业及系统失效影响

二、适用法规与效力层级

1. 强制性法律和行政法规

规范	对本场景的核心作用
修订后的《网络安全法》	自 2026 年 1 月 1 日起适用修订文本；确立等保、网络日志、事件响应、数据分类、备份和加密义务。 12
《数据安全法》	要求全流程数据安全制度、分类分级、重要数据负责人、年度风险评估、漏洞和事件处置。 13
《个人信息保护法》	员工姓名、工号、操作记录、账号、位置、生物特征等可识别操作员信息适用；规定合法性基础、告知、权利、影响评估和跨境规则。 5
《网络数据安全条例》	自 2025 年起细化加密、备份、访问控制、第三方管理、重要数据识别、年度评估和跨境规则。 7
《关键信息基础设施安全保护条例》	仅在系统被主管部门认定为关基后触发增强义务，包括专门机构、年度评估、供应链审查和境内存储。 11

2. 现行工业领域规则

原报告所列“《工业数据安全管理办法（征求意见稿）》”已经过时。当前应采用正式发布且自 **2023 年 1 月 1 日** 施行的《工业和信息化领域数据安全管理办法（试行）》；该规则覆盖研发设计、生产制造、经营管理、运行维护和平台运营数据。[2](#)

还应纳入：

- 《工业控制系统网络安全防护指南》（2024）：属于指导性安全基线，并非每一项都是独立罚则，但对判断企业是否采取“必要措施”具有重要参考价值；官方定位为 33 项指导性基线要求。 [14](#)
- 《工业和信息化领域数据安全事件应急预案（试行）》（2024）：工业数据处理者应制定本单位预案，较大以上事件立即向地方行业监管部门报告。 [15](#)
- 《网络数据安全风险评估办法》（2026）：重要数据处理者每年评估；一般数据处理者至少每三年评估一次属于鼓励性要求。 [16](#)
- 《个人信息保护合规审计管理办法》（2025）：处理超过 1000 万人个人信息者至少每两年审计一次；处理 100 万人以上个人信息者应指定个人信息保护负责人。 [17](#)
- 《国家网络安全事件报告管理办法》（2025）：建立统一的较大以上事件报告时限和报告字段。 [10](#)

3. 标准的正确定位

- ****GB/T 43697-2024《数据安全技术 数据分类分级规则》****为现行推荐性国家标准，可用于分类分级方法和重要数据识别工作底稿。 [18](#)
- ****GB/T 22239-2019《网络安全等级保护基本要求》****为现行推荐性国家标准，但等保制度本身属于法定义务，该标准是落实义务的重要技术依据。 [19](#)
- ****GB/T 45577-2025《数据安全风险评估方法》****是推荐性标准，可用于年度风险评估方法、报告及证据结构。 [20](#)

三、要求映射

类别	主要要求
收集	合法、正当、必要；工业重要/核心数据须记录来源、时间、类型、数量、频度和流向。 2

类别	主要要求
告知与合法性基础	员工个人信息应在处理前告知主体、目的、方式、类型、保存期和权利渠道。可基于同意，也可在依法制定劳动制度和集体合同框架内基于人力资源管理必要性处理；不能简单以“经理口头同意”替代。 5
分类分级	数据资产应按研发、生产运行、管理、运维、服务等分类，并识别一般、重要、核心数据；高等级数据混合处理时按最高等级保护。 2
存储与删除	重要/核心数据采用校验、密码、备份和介质管理；个人信息采用最短必要保存期，并具备删除或匿名化能力。 2 7
安全保护	建立制度、权限、培训、应急、监测；个人信息采用加密、去标识化等措施；OT实施分区分域和边界隔离。 5 4
对外提供/委托	合同需约定目的、期限、方式、范围、数据类型、保护措施和责任；重要数据委托或共同处理前进行风险评估，对供应商履约进行监督。 7
出境	重要数据、关基运营者的个人信息以及达到数量阈值的个人信息适用不同出境机制；所有个人信息出境原则上仍需履行告知、单独同意和个人信息保护影响评估。 6
事件通知	立即补救；按事件等级向网信、公安、工信等渠道报告，并在可能损害个人权益时通知相关个人。 5 10

类别	主要要求
数据主体权利	建立查阅、复制、更正、删除、限制处理、撤回同意及投诉渠道。 5
负责人和记录	重要数据处理者设数据安全负责人及机构；达到规定规模的个人信息处理者设个人信息保护负责人；影响评估记录至少保存三年，委托/提供记录至少保存三年。 7 5

四、建议目标架构

工信部现行指南要求 OT 分区分域、与管理网或互联网之间实施纵向防护和审计，上云设备实行双向认证并隔离不同业务环境。[4](#)建议采用以下结构，而不是“PLC—互联网—公网数据库”直连。



Figure 1: 制造企业工业数据从设备到境内平台再到境外总部的受控流动架构；跨境前必须先完成重要数据识别、个人信息路径判断及相应安全措施。

五、技术控制清单

法律或现行规则明确要求

1. 网络与系统分级保护：完成定级、备案、建设整改、测评和持续运营。
2. 身份与权限：实名唯一账号、最小权限、离职立即撤权；重要数据操作纳入审批和留痕。
3. 日志：覆盖采集、处理、传输、权限变更、人员操作和安全事件，至少保存六个月。
4. 重要/核心数据保护：传输使用密码、安全协议或安全通道；存储实施校验、密码、备份和恢复测试。
5. 个人信息保护：加密或去标识化、权限隔离、最短必要保存、删除能力、权利响应。
6. 事件管理：监测、预案、分级、报告、通知、证据保全和事后总结。

基于工控标准和风险的推荐控制

- PLC 与采集层保留必要的传统协议，但通过工业防火墙、协议代理、安全网关或单向传输装置限制范围。
- 建立现场控制区、监控区、OT-DMZ、企业 IT 区和云区，禁止跨区任意路由。
- 远程运维采用 VPN/零信任接入、MFA、堡垒机、临时授权、命令审计和会话录像。
- 数据库启用静态加密、密钥独立管理、字段级脱敏；法规通常不指定唯一算法或密钥长度，应结合商用密码、等保等级及实际风险选择。
- 补丁先在仿真或测试环境验证；无法及时修补时采取白名单、端口封禁、虚拟补丁和网络隔离。
- 建设离线或不可变备份，定期恢复演练；备份不得成为绕过删除和出境控制的渠道。
- 监测不得因“系统卡顿”直接关闭；性能问题应通过异步日志、边缘缓存、采样或容量扩展解决。

六、跨境传输决策路径

1. 是否包含重要数据？

如已被主管部门告知或公开列入重要数据，出境必须申报安全评估。未被告知或公开列入的，不需要仅因企业内部猜测而按重要数据申报，但仍要保留识别和申报过程证据。

[6](#)

2. 是否包含个人信息？

即使只是员工工号、姓名和操作日志，只要能够识别自然人，即适用个人信息规则。[5](#)

3. 非关基个人信息规模路径：

- 不满 10 万人普通个人信息且不含敏感信息：通常免于安全评估、标准合同和认证；
- 10 万至不足 100 万普通个人信息，或不足 1 万敏感个人信息：标准合同或认证；
- 100 万以上普通个人信息或 1 万以上敏感个人信息：安全评估。[6](#)
- 认证路径仅适用于非关基且处于上述中间阈值的主体。[21](#)

4. 豁免不等于无义务。

告知、单独同意、个人信息保护影响评估、境外接收方合同约束和安全保护仍应落实。

[6](#)

5. 国内内容灾中心之间传输不属于数据出境，但仍需访问控制、加密、分类分级、第三方合同和等保管理。

七、供应商和第三方影响

角色	典型定位	关键要求
云服务商	通常委托处理者；若自行决定用途可能转为独立或共同处理者	数据区域、管理员访问、加密、备份、转委托、删除返还、审计权、事件时限
设备厂商/运维商	委托处理者或远程访问方	临时账号、MFA、访问窗口、会话审计、禁止擅自留存和转委托
系统集成商	建设和迁移过程中的受托方	测试数据管理、漏洞责任、代码安全、交付删除、供应链审查
境外总部/境外平台	境外接收方；如共同决定用途，可能为共同处理者	出境机制、PIA、单独同意、境外接收方义务、权利响应和再转移限制
安全/测评机构	评估受托方	保密、最小访问、项目结束删除、不得擅自转委托

《网络数据安全条例》要求个人信息和重要数据提供、委托及共同处理通过合同约定目的、方式、范围和安全义务，并监督接收方，相关记录至少保存三年。⁷

八、风险暴露与执法关注度

风险	主要后果	执法关注度
个人信息违法处理/出境	一般可责令整改、没收所得；拒不整改最高 100 万元。情节严重可达 5000 万元 或上一年度营业额 5% ，责任人员 10 万—100 万元，并可能停业或吊销许可。 ⁵	高
数据安全义务缺失	一般 5 万—50 万元；严重后果 50 万—200 万元；违反核心数据制度 200 万—1000 万元。 ¹³	高
重要数据违法出境	一般 10 万—100 万元；情节严重 100 万—1000 万元，并可停业整顿或吊销许可。 ¹³	高
等保/网络安全义务缺失	修订《网络安全法》对严重后果可处 50 万—200 万元，特别严重可达 200 万—1000 万元。 ¹²	高
关基义务缺失	未设置机构、未年度评估、未签安全保密协议等，拒不整改或造成后果可处 10 万—100 万元。 ¹¹	条件性高

近期官方案例显示，监管已直接处罚弱口令、未授权访问、未加密传输、测试数据未删除、等保缺失、日志不足和供应商合同缺陷。^{22 23} 2026 年网信执法案例还包括企业未经安全评估向境外传输姓名、手机号、邮箱和设备使用信息的案件。²² 因此，对本报告中已明确暴露的实践，风险不宜评为“低”。

九、整改路线图

以下时间窗口和成本等级属于本报告建议，不是法定统一期限。

优先级	时间窗口	行动	责任团队	成本
紧急	0-15 天	暂停未经评估的境外传输；关闭公网暴露；恢复日志；冻结共享管理员账号；保留现状证据	CIO/CISO、OT、法务、总部 IT	低—中
紧急	0-30 天	完成数据流图、资产台账、境外接收方清单；识别个人信息、重要数据候选项	数据治理、OT、隐私、业务	中
短期	30-60 天	开展等保定级；形成网络分区整改方案；完成跨境路径判定和PIA	安全、法务、测评机构	中

优先级	时间窗口	行动	责任团队	成本
短期	30–90 天	部署 OT-DMZ、防火墙、VPN、MFA、堡垒机、集中日志；整改云访问和数据库权限	OT、基础设施、云团队	中—高
短期	60–90 天	更新供应商合同、员工告知、数据留存制度、事件预案并开展桌面演练	法务、HR、采购、安全	中
中期	3–6 个月	完成等保整改/测评；建立数据标签、去标识化、删除和备份恢复能力	IT、OT、数据平台	高
中期	6–9 个月	形成年度风险评估、审计、供应商复核、漏洞管理和监管报告常态机制	CISO、内审、合规	中

十、持续合规与文档模板

持续机制

- 每季度：数据资产、跨境流向、供应商和高权限账号变化复核。
- 每半年：OT 事件演练、备份恢复测试、供应商远程访问抽查。
- 每年：重要数据/核心数据目录复核；重要数据年度风险评估；等保和关基适用性复核；个人信息审计计划。
- 重大变更时：新设备联网、新云平台、网络边界变化、数据出境范围变化、并购或供应商更换需触发专项评估。

需要创建或更新的文件

文件	核心字段/章节
数据资产与分类分级制度	数据名称、来源、系统、责任人、级别、个人信息属性、重要数据依据、流向
个人信息处理规则/员工告知	处理者、目的、依据、类别、接收方、保存期、权利渠道、跨境事项
数据处理活动记录	目的、系统、数据项、主体类别、共享方、出境国、保留和删除
PIA/DPIA 模板	合法性、必要性、个人权益影响、风险、控制、剩余风险和审批人
委托处理协议/DPA	目的、期限、范围、访问、转委托、事件通知、返还删除、审计
跨境评估文件包	数据清单、重要数据判断、数量统计、境外接收方、PIA、机制选择
日志与留存制度	日志类型、字段、保存期、完整性、访问权限、关闭审批、销毁

文件	核心字段/章节
安全事件响应计划	分级标准、1/2/4 小时报告路径、联系人、证据保全、通知模板
等保档案	系统边界、定级报告、备案、测评、整改、变更记录
供应商安全附件	远程访问、MFA、漏洞、SLA、数据位置、转委托、审计和退出
删除与介质销毁制度	触发条件、审批、技术方法、备份处理、完成证明
风险评估与审计计划	范围、频率、标准、发现项、整改负责人、截止日期、关闭证据

最终管理判断

****原 PDF 不应通过合规审核或作为工业联网项目实施依据。 ****最危险的不是单一技术选型，而是其总体治理逻辑：先联网、默认明文、默认公网、默认共享账号、默认允许跨境、出了问题再报告。正确路径应为：

先盘点和分类 → 再定网络与等保边界 → 按风险设计技术控制 → 判断关基和重要数据 → 确定个人信息及跨境路径 → 完成合同、评估和审批 → 上线后持续监测、审计和报告。