AI与数据出境合规决策表（2026 Q4版）

AI上线与数据出境是两组需要分别判断的义务：先确认服务对象、功能和数据流，再核对AI评估备案、出境路径及个人信息保护措施。本表纳入2026年生效的出境认证、拟人化互动服务和小型处理者简化规则，可供产品、技术与法务共同自查。

作者：王冠律师｜北京浩略律师事务所联合创始人｜执业证号：11101202111297085

版本：v1.1｜原稿日期：2026-10-20｜本次修订：2026-10-24。条文与适用时点见文末官方来源。

一、先画数据流，再判断AI服务适用范围

先记录：谁提供服务、面向谁、有什么功能；处理目的、数据种类、人数和来源；数据存储位置、境外接收方、远程访问权限及再转移链路。数据存放境内但可被境外查询、调取或下载，也应核对是否构成数据出境。去标识化数据仍可能属于个人信息，不能把“已脱敏”直接等同匿名化。

内部研发或内部应用、未向境内公众提供的生成式AI服务，不适用《生成式人工智能服务管理暂行办法》第2条规定的该类公众服务管理范围；个人信息、数据安全、商业秘密、知识产权等义务仍须履行。向境内公众提供生成式AI服务时，应履行相应内容和数据治理义务，其中具有舆论属性或者社会动员能力的，按第17条开展安全评估并履行算法备案手续。评估与备案各有规则，不能概括为所有AI服务都必须“先评估、后备案”。

2026-07-15施行的拟人化互动服务办法另有专门要求：面向境内公众提供模拟自然人人格、思维或沟通风格的持续性情感互动服务，应按其第22条判断上线、功能新增、重大变化、用户规模等安全评估触发情形，并按第26条履行算法备案及变更、注销。普通客服、问答、工作助手等不涉及持续性情感互动的，不适用该办法第2条的定义。

二、数据出境路径决策表：先核对豁免，再算人数

以下以2024年跨境流动规定和2025年起施行的网络数据条例为基础。主体是否为关键信息基础设施运营者（CIIO）、是否含重要数据、特定场景与自贸试验区规则应先核对；人数门槛表不能脱离这些前提使用。重要数据以识别申报、相关目录及告知为基础，未被相关地区、部门告知或公开发布为重要数据的，不需要作为重要数据申报出境安全评估。

出境路径分流表：按适用条件逐层判断

顺序 / 情形	适用条件	路径或动作	适用边界与依据
不含个人信息和重要数据	国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中的数据	免予安全评估、标准合同和认证三项制度	仍履行数据安全等义务；跨境规定第3条
境外数据回传	境外收集产生的个人信息传入境内处理后回传，未引入境内个人信息或重要数据	免予三项制度	保留来源、加工和回传证据；第4条

顺序 / 情形	适用条件	路径或动作	适用边界与依据
特定必要场景 / 自贸区	个人作为一方的合同、依法实施的跨境人力资源管理、紧急保护等；自贸区负面清单另核资格与范围	符合具体条件时免予三项制度；履行法定职责义务另看条例第35条等	第5—6条、条例第35条；重要数据不能借个人信息场景豁免，必要性不能无限扩张
CIIO或重要数据	CIIO出境个人信息或重要数据；非CIIO出境重要数据，且无适用的特别规定	通过所在地省级网信部门向国家网信部门申报安全评估	跨境规定第7条；第3—6条适用情形从其规定；行业要求另核
非CIIO：达到评估门槛	当年累计出境个人信息（不含敏感）达到100万人，或敏感个人信息达到1万人	申报并通过数据出境安全评估	“以上”含本数；不能用数量拆分或认证替代；第7条
非CIIO：合同或认证区间	当年累计普通个人信息≥10万人且＜100万人，或敏感个人信息大于0且＜1万人；不含重要数据	订立并使标准合同生效，依法备案；或取得个人信息出境认证	跨境规定第8条、2026认证办法第5条；如任一指标达到评估门槛，走评估
非CIIO：小规模普通信息	当年累计出境不满10万人个人信息，不含敏感个人信息、重要数据；无其他适用限制	免予三项制度	跨境规定第5条；告知、合法性基础、影响评估等分别判断

计数以数据处理者为单位，按当年1月1日起累计出境的自然人数统计，对同一个人多次提供不按传输次数重复计数；普通与敏感个人信息分别计算，适用场景豁免的数据依主管部门申报指南口径处理并单独留账。不能让各项目各算一套，也不能将业务线人数未经去重直接相加。

豁免的是评估、标准合同、认证三项制度，不能推导成全部保护义务免除。出境前仍须依法核对处理合法性基础、告知、个人单独同意是否适用、最小必要、境外接收方约束及个人信息保护影响评估；有法定不依同意处理依据的，应记录依据及范围，不宜统一要求每名员工一律签同意书。

2026年7月官方问答进一步明确：出境活动属于个保法第13条第1款第2至7项规定情形的，不需取得个人同意，但仍应履行出境告知义务；依同意处理时，单独同意须具体明确，不能捆绑成“一揽子”授权。招聘简历也不能直接套用员工管理豁免：境外总部不参与录用决策时，简历出境不具备必要性；参与决策的，也应限于必要人员和数据项，并依法落实出境路径及保护义务。

三、高频场景：动作和期限分别管理

场景、动作与期限对照（不同手续不能互相替代）

场景	先判断什么	应落实的动作	期限 / 留档重点
公众生成式AI	是否属于暂行办法第2条范围，是否具有舆论属性或社会动员能力	落实训练数据与内容、个人信息、投诉处置；符合条件时开展安全评估和算法备案	按适用评估规则安排上线；算法备案提供服务之日起10个工作日内填报，不是全体AI统一审批期限

场景	先判断什么	应落实的动作	期限 / 留档重点
算法备案及变更	算法推荐规定第2、24条的服务与主体条件是否满足	填报、自评估、编号公示及链接；重大变化另核安全评估	备案10个工作日；变更10个工作日；终止服务起20个工作日内注销；材料齐全后30个工作日内备案并公示
拟人化情感互动	是否持续模拟人格或沟通风格提供情感互动；不按普通客服一概处理	按专门办法开展安全评估、报省级网信部门；备案、未成年人保护、退出与防沉迷提示	2026-07-15起适用；第22条上线或增设功能即是评估触发情形，另有用户规模与风险条件
AI生成合成内容	服务提供、内容传播或用户发布分别是什么角色	按标识办法及强制性标准核对显式、隐式标识、传播提示和用户声明	2025-09-01起适用；文本、图片、音频、视频和虚拟场景等按类别实施，不仅图片视频
标准合同	处于合同 / 认证区间，境外接收方及用途是否明确	事前影响评估、签署并生效标准合同，再依法备案；变更情形重新评估、签订或补充并备案	标准合同生效之日起10个工作日内向所在地省级网信部门备案；不得以尚未备案忽略其他前置义务
出境认证	符合2026认证办法第5条，专业机构具备资质并完成备案	按第6条完成告知、同意适用性及影响评估等，向专业机构申请并取得认证	证书有效期3年；到期继续使用的，应在届满前6个月提出认证申请；达安全评估门槛后另行申报
出境安全评估	CIIO、重要数据或人数触发，且无适用豁免	风险自评估、法律文件、向省级网信部门提交并由国家网信部门评估	通过后依评估范围出境；结果有效期3年；符合条件的在届满前60个工作日内申请延长，须经批准
境外AI / 云 / 总部访问	输入内容、日志、运维或远程权限是否使境外获得个人信息或重要数据	先最小化数据和权限，核清接收方、再利用、训练及再转移；再按路径分流	采购和上线前核查，持续监控人数、用途、接收方及技术架构变化

四、三类评估和合规审计：分别留报告

评估、审计及报送对照

事项	触发与内容	对外提交 / 频次	保存与变更
个人信息保护影响评估	个保法第55条：敏感信息、自动化决策、委托 / 提供 / 公开、出境及其他重大影响情形，事前评估	一般内部形成报告；出境合同、认证等按各自要求提交材料	报告和处理情况记录至少保存3年；小型处理者可按符合条件的简便方式开展
数据出境安全评估	触发强制评估情形；事前完成数据出境风险自评估并准备申报	通过所在地省级网信部门向国家网信部门申报；取得通过结果后依范围实施	现行结果有效期3年；变化、到期及延长按规定处理

事项	触发与内容	对外提交 / 频次	保存与变更
重要数据风险评估	识别为重要数据的处理活动；提供、委托、共同处理另核事前风险评估	按条例第32条每年度评估并向省级以上有关主管部门报送报告	依行业规则和项目档案制度留存；不能用个人信息影响评估替代
个人信息保护合规审计	审计处理活动是否遵守法律、行政法规	处理超过1000万人个人信息的，审计办法第4条要求至少每两年一次；其他处理者依风险合理确定频次，特别规则另核	小型处理者有2026年简化规则；未成年人、监管指定审计及行业要求分别核对

安全评估延期须核对第三版申报指南及2026年7月问答的完整条件，包括目的范围、处理者和接收方未变化，未来三年人数或重要数据规模增幅不超过原批准过去三年规模的20%，法律文件符合要求，以及过去三年依评估结果合规开展且未发生重大数据安全事件。提出申请不等于自动获准延期。

五、四组人数口径，不能相互替代

出境10万 / 100万 / 1万：前两项是当年累计出境个人信息（不含敏感）人数门槛；1万是敏感个人信息安全评估门槛。少量敏感个人信息也可能进入合同或认证区间，不能因“总数不到10万”直接豁免。

处理100万人以上：合规审计办法第12条明确应指定个人信息保护负责人。依2025年7月18日报送公告，公告发布后达到100万人的，应自达到之日起30个工作日内完成向所在地设区的市级网信部门的信息报送；报送信息实质性变更的，自变更起30个工作日内办理。个保法第52条另要求公开负责人联系方式。这是处理规模口径，不是当年出境人数。

处理1000万人以上：网络数据条例第28条要求遵守第30、32条有关负责人、管理机构和年度风险评估等规定，并不把这些个人信息自动认定为重要数据。合规审计办法第4条的“超过1000万人、至少每两年审计一次”另有严格措辞，不能把两者混写。

处理不满10万人：这是2026年小型个人信息处理者简化措施的主体规模条件，与“当年出境普通个人信息不满10万人”的路径豁免不同。前者统计处理规模，后者统计符合条件的年度出境规模。

六、小型处理者：可以简化，但先满足条件

2026-09-01施行的小型处理者规定，对境内处理不满10万人个人信息的处理者提供简化措施。可按附件自查表至少每五年开展一次合规审计并保存至少五年；可按简便表开展影响评估并保存至少三年。处理未成年人信息的特别审计规定仍需核对。通过个人信息保护认证的，在认证有效期内可依第17条免予开展合规审计。

第8条允许符合严格条件的平台内小型处理者在平台规则、权责约定、处理范围及平台已经覆盖相应审计和影响评估时避免重复开展。超出平台规则范围的处理活动须另行落实义务。不能把“平台有隐私政策”当成所有商户均自动免评估，也不能把小型企业身份当作敏感信息或数据出境的全面豁免。

七、季度监管更新与项目留档模板

法规的发布日期、施行日与本企业整改日分开填写；下表是已核对事项的项目管理示例，不把旧文件编造成2026年某季度的新规。

季度更新台账示例与空白记录行

文件 / 时点	本次更新纳入事项	企业需记录的动作	责任与证据
2026-01-01：出境认证办法施行	认证条件、证书3年、届满前6个月申请	检查是否适用认证以及后续人数是否达到评估门槛	负责人、证书范围、到期提醒、人数台账
2026-07-15：拟人化互动办法施行	持续情感互动产品、评估与算法备案	核对服务功能、评估触发、未成年人和退出措施	产品清单、评估报告、备案及改版记录
2026-09-01：小型处理者简化规定施行	主体人数、简化表、平台覆盖及例外	核对资格，选择适用措施，记录不适用部分	规模证明、平台协议、简化表与保存期限
2026-09-11：出境政策问答发布	认证可申请范围及达量后的评估衔接	区分自愿认证与法定路径，不用认证替代强制评估	认证申请、增长预警、整改排期
待填：实际文件及施行日	受影响的具体业务或数据流	条款、整改动作、完成日、复核方式	实际责任人、版本、官方链接、存档路径

项目最低留档包：服务与数据流图、主体及接收方清单、分类与人数统计口径、合法性基础和必要性说明、告知及同意适用记录、影响评估、合同或认证或安全评估材料、上线与变更记录、应急联系人和下一次检查日期。科技初创企业融资时，可与初创公司股权架构及尽调准备清单一并使用。

八、常见问题

问：公司内部使用AI，也必须做算法备案吗?

答：不能只凭“使用AI”判断。应区分内部使用与对公众提供服务，核对算法推荐、生成式AI及2026年拟人化互动规则的具体适用条件；内部使用仍须核查数据、商业秘密和个人信息保护。

问：不到10万人出境，是否一定不需要手续?

答：不一定。小规模普通个人信息豁免有非CIIO、不含敏感信息和重要数据等条件；少量敏感信息也可能需要标准合同或认证。场景豁免及其他适用规则应先判断。

问：标准合同必须备案通过后才能首次出境吗?

答：办法要求合同生效后10个工作日内备案，不能把它表述为统一的事前行政审批。但首次出境前应完成适用的影响评估、合法性基础、告知同意及有效合同等义务；触发安全评估的则不能用标准合同替代。

问：处理1000万人个人信息，就属于重要数据处理者吗?

答：不能直接这样认定。网络数据条例第28条要求适用第30、32条的部分加重义务，不等于这些个人信息自动被认定为重要数据；重要数据仍须按识别、目录、告知与公布规则判断。

问：通过出境认证后，人数增长到安全评估门槛怎么办？

答：应按规则申报数据出境安全评估，认证不能代替。2026年9月政策问答明确可把已认证情况附后供评估参考；要持续统计当年累计出境人数。

问：小型处理者可以完全不做影响评估吗？

答：一般可采用简便评估表并至少保存三年；仅在平台内处理等条件及平台评估已覆盖时，可按第8条避免重复开展。不能从小型身份直接推出全面免除。

九、官方来源与版本记录

1. 《个人信息保护法》：2021-11-01施行；第13、38—40、52、55—56条。
2. 《促进和规范数据跨境流动规定》：2024-03-22施行；第2—10、13条。
3. 《网络数据安全管理条例》：2025-01-01施行；第28—32、35—38条。
4. 《数据出境安全评估办法》：2022-09-01施行；门槛、有效期等按2024年新规调整。
5. 《个人信息出境标准合同办法》：2023-06-01施行；第5—8条；门槛按2024年新规调整。
6. 《个人信息出境认证办法》：2026-01-01施行；第5—8条。
7. 《数据出境安全评估申报指南（第三版）》发布说明：2025-06-27发布；申报材料、线上入口和评估延期。
8. 数据出境安全管理政策法规问答（2026年7月）：2026-07-24发布；告知同意、评估延期及求职者简历必要性。
9. 数据出境安全管理政策法规问答（2026年9月）：2026-09-11发布；认证适用、达量后的安全评估与申请。
10. 《生成式人工智能服务管理暂行办法》：2023-08-15施行；第2、9、12、14—17条。
11. 《互联网信息服务算法推荐管理规定》：2022-03-01施行；第2、24—26条。
12. 《人工智能生成合成内容标识办法》：2025-09-01施行；第2—6、9—10条及配套强制性标准。
13. 《人工智能拟人化互动服务管理暂行办法》：2026-07-15施行；第2、18、22—23、26条。
14. 《小型个人信息处理者个人信息保护简化措施规定》：2026-09-01施行；第2、8、10、13—14、17条。
15. 《个人信息保护合规审计管理办法》：2025-05-01施行；第4、12条。
16. 关于开展个人信息保护负责人信息报送工作的公告：2025-07-18发布；负责人信息报送。

版本v1.1，2026-10-24修订：纠正AI评估备案泛化、出境门槛边界、标准合同备案时点及1000万人等同重要数据的表述；补入2026年出境认证、拟人化互动、小型处理者规则与9月问答；删除未经实际签审的团队审核署名。v1.0原稿日期为2026-10-20。

本文提供一般性法律信息和项目自查工具。具体安排须结合公司文件、业务事实、行业及所在地规则判断；不构成个案法律意见。

王冠律师｜北京浩略律师事务所｜咨询电话：17813108512｜联系与咨询准备