（2025 年 1 月）

目录

一、法规速递

《个人信息出境个人信息保护认证办法（征求意见稿）》

发文机关：国家互联网信息办公室

发文时间：2025.01.03

生效时间：待定

第一条 为了便利个人信息出境活动，规范个人信息出境个人信息保护认证工作，保护个人信息权益，促进个人信息高效便利安全跨境流动，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》、《中华人民共和国认证认可条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内开展个人信息出境个人信息保护认证活动，适用本办法。法律、行政法规另有规定的，依照其规定。

第三条 本办法所称个人信息出境个人信息保护认证，是指依法设立并经国家市场监督管理部门批准取得个人信息保护认证资质的专业认证机构，对个人信息处理者个人信息出境活动开展的个人信息保护认证。

本办法所称个人信息出境活动，是指个人信息处理者因业务等需要确需向中华人民共和国境外提供个人信息的行为。包括但不限于以下情形：

（一）个人信息处理者将在境内运营中收集和产生的个人信息传输至境外；

（二）个人信息处理者收集和产生的个人信息存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；

（三）符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个

人信息等其他个人信息处理活动。

第四条 中华人民共和国境内的个人信息处理者通过个人信息出境个人信息保护认证方式向境外提供个人信息的，应当同时符合下列情形：

（一）非关键信息基础设施运营者；

（二）自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息。

前款所称向境外提供的个人信息，不包括重要数据。

第五条 符合《中华人民共和国个人信息保护法》第三条第二款规定，在中华人民共和国境外处理中华人民共和国境内个人信息的个人信息处理者，获得个人信息出境个人信息保护认证，可以进行个人信息出境活动。

第六条 个人信息保护认证遵循自愿性、市场化、社会化服务原则。由具备资质的专业认证机构按照统一标准、统一规则、统一标识开展个人信息出境个人信息保护认证活动。

第七条 国家网信部门会同有关部门组织制定个人信息出境个人信息保护认证相关标准、技术法规和合格评定程序，对个人信息出境活动进行监督管理。国家市场监督管理部门会同国家网信部门组织制定个人信息出境个人信息保护认证实施规则、统一认证证书及标志。

第八条 开展个人信息出境个人信息保护认证的专业认证机构应当向国家网信部门办理备案手续。办理备案时，应当提交下列材料：

（一）取得的个人信息保护领域的认证资质情况；

（二）近 3 年从事数据安全领域、个人信息保护领域专业工作情况；

（三）个人信息保护认证实施细则及工作计划；

（四）数据安全风险防范机制；

（五）对获证个人信息处理者进行的个人信息出境活动符合认证标准情况的持续监督机制；

（六）争议受理机制和投诉处理机制；

（七）其他需要提交的材料。

第九条 中华人民共和国境内的个人信息处理者自愿向专业认证机构申请个人信息出境个人信息保护认证。

中华人民共和国境外的个人信息处理者申请个人信息出境个人信息保护认证的，应当由其在境内设立的专门机构或者指定代表协助进行申请，并承担相应的法律责任，承诺遵守中华人民共和国个人信息保护有关法律法规并接受监督管理，在认证有效期内接受专业认证机构的持续监督。

第十条 个人信息出境个人信息保护认证重点评定以下内容：

（一）个人信息出境的目的、范围、方式等的合法性、正当性、必要性；

（二）境外个人信息处理者、境外接收方所在国家或者地区的个人信息保护政策法律和网络和数据安全环境对出境个人信息安全的影响；

（三）境外个人信息处理者、境外接收方的个人信息保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

（四）个人信息处理者与境外接收方订立的有法律约束力的协议是否约定了个人信息保护的义务；

（五）个人信息处理者、境外接收方的组织架构、管理体系、技术措施能否充分有效保障数据安全和个人信息权益；

（六）专业认证机构根据个人信息保护认证相关标准认为需要评定的其他事项。

第十一条 专业认证机构在开展认证活动中，发现个人信息出境活动危害国家安

全、公共利益或者严重影响个人信息权益的，应当及时向国家网信部门及有关部门报告。

第十二条 专业认证机构应当在颁发认证证书或者认证证书状态发生变化后5个工作日内，向全国认证认可公共信息平台报送个人信息出境个人信息保护认证证书相关信息，包括认证证书编号、获证个人信息处理者名称、认证范围以及证书状态变化信息等。国家市场监督管理部门与国家网信部门建立认证信息共享机制。

第十三条 专业认证机构发现获证个人信息处理者存在个人信息出境情况与认证范围不一致等不再符合认证要求的，应当及时暂停、撤销相关认证证书，并予以公布。

国家网信部门和有关部门在个人信息保护监督管理工作中发现获证个人信息处理者存在前款情形的，专业认证机构应当配合及时暂停、撤销相关认证证书，并予以公布。

第十四条 国家市场监督管理部门会同国家网信部门对个人信息出境个人信息保护认证活动进行监督，对认证过程和认证结果进行抽查，对专业认证机构进行评价。

国家市场监督管理部门对个人信息出境安全认证活动存在服务质量等问题的，视情节予以警告、责令限期改正、停业整顿；拒不整改或规定期限内未完成整改的，以及存在弄虚作假的，撤销其认证机构资质，并予以公布。

专业认证机构通过隐瞒有关情况、提供虚假材料等不正当手段取得备案的，由国家网信部门予以撤销备案；发生严重违法情形受到停业整顿、撤销认证机构资质等行政处罚的，由国家网信部门予以注销备案。

第十五条 任何组织和个人发现获证个人信息处理者违反本办法向境外提供个人信息的，可以向省级以上网信部门和有关部门举报。

第十六条 省级以上网信部门和有关部门发现获证个人信息处理者存在较大风险或者发生个人信息安全事件的，可以依法对获证个人信息处理者进行约谈。获证个人信息处理者应当按要求整改，消除隐患。

第十七条 履行个人信息保护职责的相关部门、专业认证机构及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，并采取相应的技术措施和其他必要措施，保障相关数据不得泄露或者非法向他人提供、非法使用。

第十八条 国家促进个人信息出境个人信息保护认证活动的国际交流与合作，推动个人信息出境个人信息保护认证与其他国家、地区、国际组织之间的互认。

第十九条 违反本办法规定的，依据《中华人民共和国个人信息保护法》、《中华人民共和国认证认可条例》等法律法规处理；构成犯罪的，依法追究刑事责任。

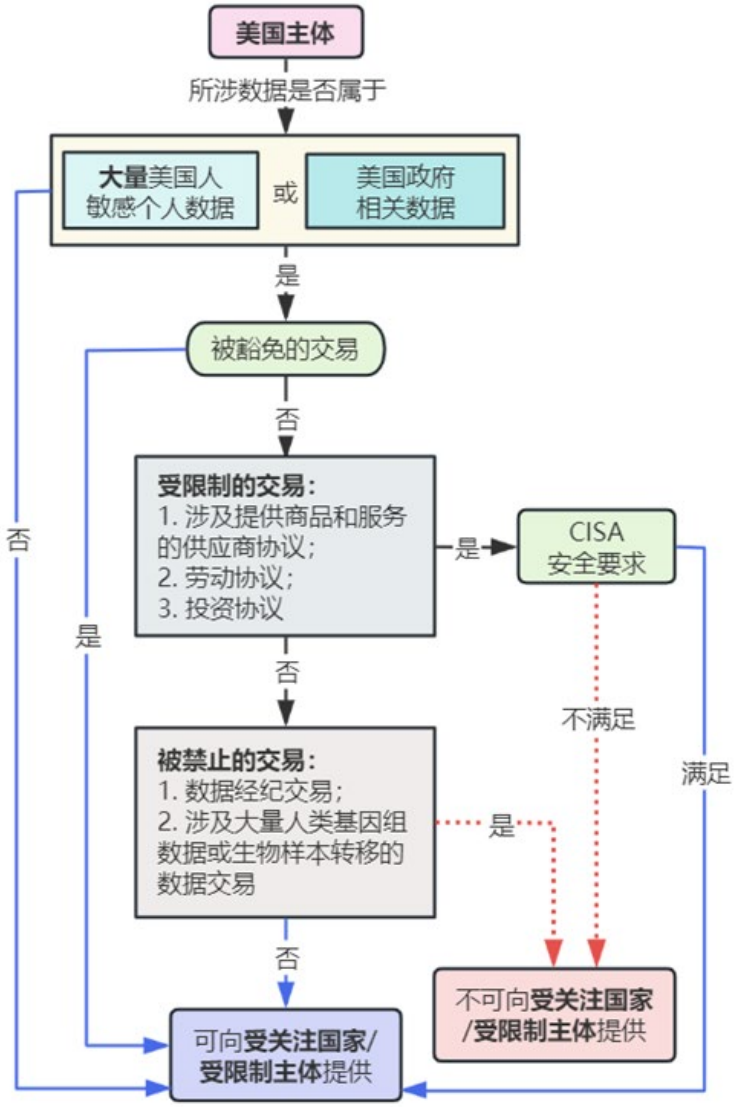
第二十条 本办法自 年 月 日起施行。

二、实务解读

1. 解读美国数据“脱钩”新规——美国第 14117 号行政令最终实施规则

供稿人：潘永建（上海市通力律师事务所）、邓梓珊（上海市通力律师事务所）、嵇若琳（上海市通力律师事务所）

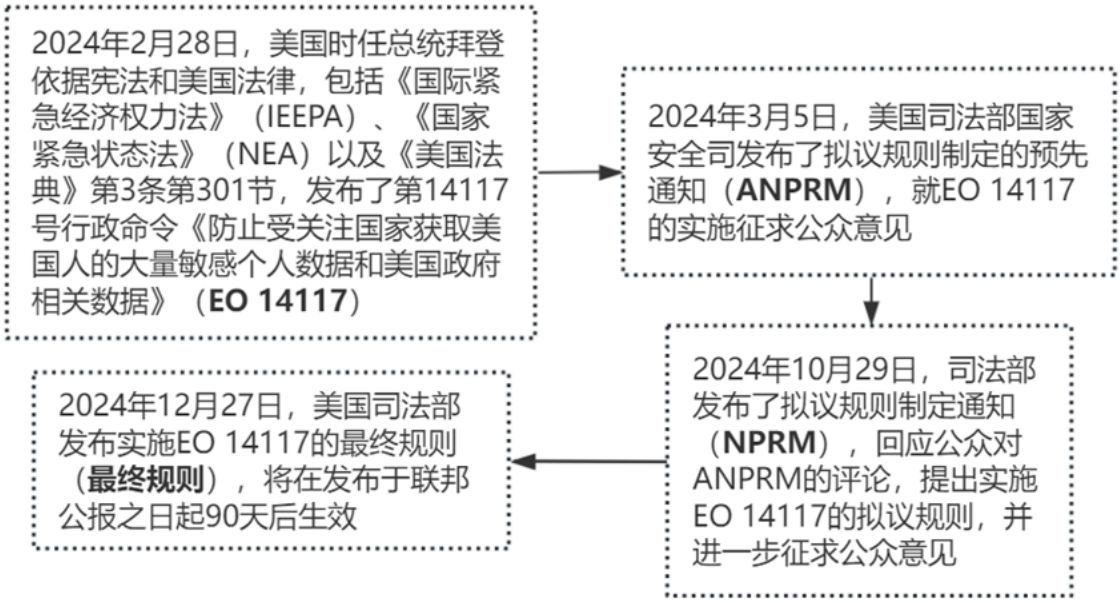
示意草图——EO 14117 管制范围



一、 背景

2024年12月27日，美国司法部正式发布了第14117号行政令（“**EO 14117**”）即《关于防止关注国家获取美国公民大量敏感个人数据和美国政府相关数据的行政命令》的**最终实施规则**（Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons，以下简称“**最终规则**”）。该行政令由拜登政府于2024年2月28日签署，要求美国司法部颁布条例，以**禁止或限制美国主体进行会导致“受关**

注国家”和“受限制实体”访问大量美国人敏感个人数据和美国政府相关数据的交易。经过十个月的起草和多轮公众意见征集与调整，最终规则得以形成，为 EO 14117 确立了具体的遵守义务。



二、重点提示

EO 14117 旨在禁止或限制美国主体进行会导致受关注国家和受限制实体访问大量美国人敏感个人数据和美国政府相关数据的交易。为了全面理解这一规则，关键在于明确几个核心概念的定义和范围。

1. “美国主体”

美国主体包含美国公民、国民或合法永居、被美国接受为难民或者提供庇护的个人、仅根据美国法或在美国司法辖区下组建的实体（含其外国分支机构），或任何位于美国境内的人士。

2.“受关注国家”和“受限制实体”

最终规则确定的受关注国家（Countries of concern）与 NPRM 中列出的保持一致，仍然包括**中国（包括中国香港和澳门）、古巴、伊朗、朝鲜、俄罗斯、委内瑞拉**六个国家。

在此基础之上，最终规则对受限制主体（Covered person）的定义进行了调整，但并未实质性改变 NPRM 中提出的范围：

(1)单独或整体上由一个或多个受关注国家或由符合第(2)的主体直接或间接持有 50%或以上股份，根据受关注国家的法律组织或特许而设立，或主要营业地位于受关注国家的实体；

(2)单独或整体上由第(1)类所述实体或第(3)、第(4)或第(5)类所述主体直接或间接持股 50%或以上实体；

(3)受关注国家或第(1)、第(2)或第(5)类所述实体的雇员或合同工的非美国人；

(4)主要居住在受关注国家领土管辖范围内的非美国人；

(5)被美国司法部长指定为：由受关注国家拥有或控制，或由受关注国家管辖或指示（Direct），或代表或声称代表受关注国家或被限制主体行事，或故意引发或指示违反规则的任何主体。对此，最终规则将包含一份由司法部指定的“**受限制主体名单**”（Covered Persons List）作为补充，并计划定期发布和更新该限制名单。

例如，以中国为例，“受限制的主体”就会包括中国政府持股 50%以上的实体（要注意这里的持股包括直接持股、间接持股，也包括单独持股，以及与其他对手国家共同持股），注册在中国的实体，或主营业务地为中国的实体；由上述列举的实体直接或间接持股 50%以上的实体。上述 50%的比例要求实质上只是一个名义上的标准，因为如果存在持股小于 50%但存在实质控制的情形，美国司法部也可以将其列为受限制的主体。此外最终规则也可能适用于外国主体，比如

上述两类中国实体的员工或合同工，以及主要居住在中国的外国主体。

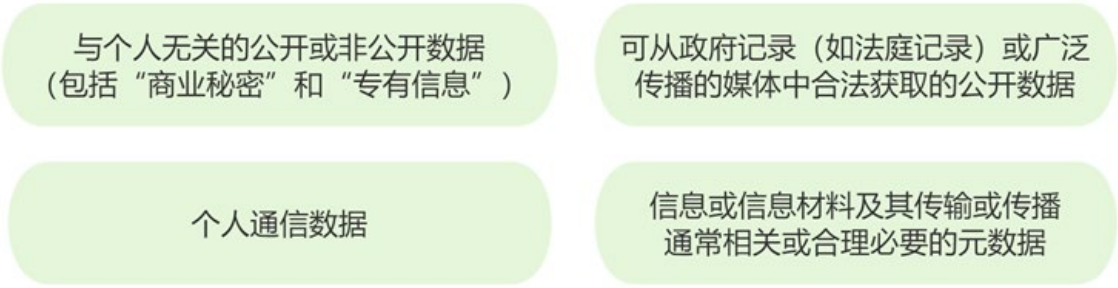
3.“大量”美国人“敏感个人数据”和美国“政府相关数据”

受管制的数据类型包括美国人**敏感个人数据**（sensitive personal data）以及**美国政府相关数据**（United States Government-related data）。

最终规则确定的美国人敏感个人数据包括以下六类：

数据类别	具体字段
1. **特定个人标识符** Covered personal identifiers	• 完整或部分政府识别或账户号码（如社保账号、驾驶证或州身份证号、护照号或外侨登记号） • 与金融机构或金融服务公司相关的完整金融账户号码或个人识别号码 • 设备或硬件标识符（如 IMEI、MAC 地址、SIM 卡号） • 人口统计或联系数据（如姓名、出生日期、出生地、邮政编码、住宅街道或邮政地址、电话号码、电子邮件地址或类似的公共账户标识符） • 广告标识符（如谷歌广告 ID、Apple 广告 ID 或其他 MAID） • 账户认证数据（如用户名、账户密码或安全问题答案） • 基于网络的标识符（如 IP 地址或 Cookie 数据） • 通话详单数据（如 CPNI）
2. **精确地理定位数据** Precise geolocation data	无论是实时数据还是历史数据，用于识别个人或设备的物理位置，精度范围在 1,000 米以内
3. **生物识别标识符** Biometric identifiers	用于识别或验证个人身份的可测量物理特征或行为，包括面部图像、声纹及其模式、视网膜和虹膜扫描、掌纹和指纹、步态以及键盘使用模式等，这些特征被录入到生物识别系统中，并由系统创建的模板
4. **人类组学数据** Human genomic data	• 人类基因组数据（human genomic data） • 人类表观基因组数据（epigenomic data） • 人类蛋白组数据（proteomic data） • 人类转录组数据（transcriptomic data）
5. **个人财务数据** Personal financial data	• 关于个人信用卡、借记卡或银行账户的数据，包括购买和支付记录 • 包括银行、信贷或其他财务报表中的资产、负债、债务和交易数据 • 信用报告或“消费者报告”[1]中的数据
6. **个人健康数据** Personal health data	包含个人过去、现在或未来身体或精神健康状况的信息；涉及向个人提供医疗保健的情况；以及与向个人提供医疗保健相关的过去、现在或未来的支付信息，包括： • 基本的身体测量和健康属性（如身体功能、身高和体重、生命体征、症状和过敏） • 社会、心理、行为和医疗诊断、干预和治疗历史 • 测试结果 • 锻炼习惯日志 • 免疫数据 • 生殖和性健康数据 • 使用或购买处方药物的数据

在此基础之上，最终规定明确将以下数据排除在敏感个人数据的定义之外：



敏感个人数据相关的交易需要达到一定数据规模才会触发监管。具体而言, 用以判断敏感个人数据规模的数据量为过去 12 个月的任一时间内，无论单次还是累计，满足或超过以下阈值的敏感个人数据总量：

(1)收集或保存超过 1,000 名美国人的人类组学数据，或者超过 100 名美国人的人类基因组数据；

(2)收集或保存超过 1,000 名美国人的生物识别标识符；

(3)收集或保存超过 1,000 个美国设备的精确地理定位数据；

(4)收集或保存超过 10,000 名美国人的个人健康数据；

(5)收集或保存超过 10,000 名美国人的个人财务数据；

(6)收集或保存超过 100,000 名美国人的特定个人标识符；或者

(7)组合数据，即包含(1)至(7)中多个类别的数据集合，或者包含与 (1)至(5)中类别相关联的任何列出的标识符，其中任何单一数据类型达到该类别中美国人或美国设备的最低人数或设备数的阈值的累积数量。

需要注意的是,在计算敏感个人数据的规模时是否达到“大量”时, **无需考虑此类数据是否经过匿名化、假名化、去标识化或者加密，也不考虑数据的存在形式。**

另一类美国政府相关数据则包括：

(1)任何位于《政府相关位置数据列表》（最终规则第 202.1401 节）中所列区域的精确地理位置数据，这些区域被司法部长认定为存在被关注国家利用的高风险，可能会泄露关于联邦政府控制地点的信息，包括这些地点的设施、活动或人口，从而对国家安全构成威胁。

(2)任何交易方在市场上推广的，声称与美国政府现任或前任雇员、承包商或

高级官员（包括军事和情报部门人员）相关联或可追溯的敏感个人数据。

与涉及美国人个人敏感数据的数据交易达到一定规模才触发规制不同，涉及美国政府相关数据的数据交易，**无论此类数据量有多大，都将受到美国司法部监管**。

3、禁止/限制/豁免的交易

禁止：由上述美国主体进行的会导致受关注国家和受限制实体访问大量美国人敏感个人数据交易将触发 EO 14117 的监管。在被监管的数据交易中，有两类数据交易类型将被禁止，分别是：

(1)数据经纪交易（Data-brokerage transactions），即数据接收方不直接从个人处收集数据，而是从数据提供方处购买数据、获得访问数据的许可的类似商业交易（不包含供应商协议、劳动协议或投资协议）；以及

(2)涉及传输大量的人类基因组数据，或者涉及传输可产生前述数据的生物学样本的交易，且这类交易是在“明知地（knowingly）”情况下进行的。

限制：同时，另有三类数据交易类型将受到限制，包括：

(1)涉及提供商品和服务的供应商协议（包括云服务协议）；

(2)劳动协议；以及

(3)投资协议。

这三类受限制的数据交易在满足规定的安全要求的前提下才可进行，适用的安全要求由国土安全部网络和基础设施保护局（CISA）另行制定。CISA 的具体安全要求包括一系列网络安全措施，例如**基本的组织网络安全政策和实践、物理及逻辑访问控制、数据脱敏和最小化处理、数据加密以及隐私增强技术的应用等。**

豁免：此外，最终规则还规定了以下几类不受限制的数据交易的豁免情形：

(1)不涉及交易金额的个人通信的数据交易；

(2)涉及表达性材料信息的进出口；

(3)旅行（包括有关个人行李、生活费用和旅行安排的数据）；

(4)政府官方的交易；

(5)金融服务、支付处理和监管合规相关的数据交易；

(6)美国跨国公司内部业务运营产生的数据交易；

(7)美国联邦法律或国际协议所要求或授权的交易；

(8)美国外国投资委员会（CFIUS）明确豁免的投资协议；

(9)提供电信服务通常涉及的数据交易；

(10)涉及药品、生物制品、器械或组合产品的审批或授权的数据交易（其中所涉及的“监管审批数据”已经根据美国食品药品监督管理局（FDA）的规定进行了去标识化或匿名处理，并且仅限于用于评估其安全性和有效性所必需的信息）；

(11)涉及其他临床研究和上市后监测数据、符合 FDA 相关要求的交易。

三、合规建议

随着最终规则的发布及其后续生效，EO 14117 下的规定将产生具体的遵守义务，针对美国敏感个人数据和政府相关数据的交易将受到严格的监管，这对我国企业在美国开展业务活动构成了新的合规挑战，特别是涉及数据处理和数据流转的业务。中资企业与美国企业之间的合作可能会直接受到该规则的约束。因此，建议中资企业在开展相关业务之前，采取以下措施，以确保合规性并降低潜在风险：

1. 核查交易中涉及的数据类型，是否属于美国敏感个人数据或美国政府相关数据；

2. 分析交易场景是否属于或可能属于被禁止或限制的“交易”；若属于/可能属于，是否存在豁免情形；

3. 若交易经过上述排查属于/可能属于 EO 14117 最终规则所限制/禁止的交易且不存在豁免情形，在业务可行的前提下，企业可考虑在美国境内处理或在其他非关注国家处理数据；

4. 加强企业合规内部审查机制，特别是在跨境数据传输与处理的环节（包括中国境内母公司与美国境内子公司之间的数据传输）。例如设立专门的合规部门，定期对数据流动、合作伙伴关系和投资协议进行审查，确保合规性与合规文档的完善，并及时与美国司法部、网络和基础设施保护局（CISA）等相关监管机构保持沟通，获取最新的监管动向和指导意见。

2. 选项越多选择越困难？个人信息出境选标准合同还是认证？

供稿人：潘永建（上海市通力律师事务所）、邓梓珊（上海市通力律师事务所）、嵇若琳（上海市通力律师事务所）

大家都已经熟知我国个人信息出境的三条政府监管路径，即数据出境安全评估、个人信息出境标准合同，以及个人信息保护认证。其中，安全评估与标准合同均已有位阶较高的法规予以明确规定（《数据出境安全评估办法》及《个人信息出境标准合同规定》均为国家互联网信息办公室（“网信办”）的部门规章），而有关认证的法规却迟迟没有出台。2022 年 11 月 4 日，网信办与国家市场监督管理总局曾联合发布《关于实施个人信息保护认证的公告》，但这仍然没有明确认证的法律地位。在近日，网信办终于发布了《个人信息出境个人信息保护认证办法（征求意见稿）》（“《认证办法》”），对出境认证的适用情形、评估内容及操作流程等进行了细化和完善。本文旨在**梳理《认证办法》的核心内容**，并分析在个人信息出境路径中，**选择标准合同备案还是认证机制的主要考量**。

1、个人信息出境活动的认定

《认证办法》沿用了《数据出境安全评估申报指南（第二版）》和《个人信

息出境标准合同备案指南（第二版）》中对于个人信息出境活动的界定，明确以下三种典型出境情形：

- 个人信息处理者将在境内运营中收集和产生的个人信息传输至境外；
- 个人信息处理者收集和产生的个人信息存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；
- 符合《个人信息保护法》（“个保法”）第三条第二款情形，在境外处理境内自然人个人信息等其他个人信息处理活动。

值得特别注意的是第三类情形，根据个保法的域外适用原则，在满足“向境内自然人提供产品或服务”或“分析、评估境内自然人行为”两种情形之一时，个人信息处理活动将直接受到个保法的规制。《认证办法》进一步明确，相关境外处理者在对境内自然人个人信息开展处理活动之前，还需就“自境外收集数据”的行为完成个人信息出境的相关合规程序。如选择适用认证，应由境外处理者在境内设立的专门机构或者指定代表协助进行申请。

2、认证的适用条件

与《促进和规范数据跨境流动规定》第八条的规定保持一致，企业在选择认证作为个人信息出境的合规路径时，需满足以下三个条件：

- 企业未被认定为关键信息基础设施运营者；
- 不涉及出境重要数据；
- 当年累计向境外提供 10 万人以上、不满 100 万人普通个人信息（不含敏感个人信息）；或者当年累计向境外提供不满 1 万人敏感个人信息。

在选择认证路径前，建议企业对自身个人信息出境活动进行全面梳理，包括明确涉及的业务场景、数据的类型以及出境规模。特别是对于出境数据是否涉及重要数据，应密切关注相关主管部门发布的政策文件，以确保符合认证的适用条件。

3、认证的评估内容

《认证办法》提出了六大方面的评估内容，与标准合同备案的评估要求有一定重叠，具体如下表：

认证	标准合同备案
（一）个人信息出境的目的、范围、方式等的合法性、正当性、必要性；	（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；
（二）境外个人信息处理者、境外接收方所在国家或者地区的个人信息保护政策法律和**网络和数据安全环境**对出境个人信息安全的影响；	（五）境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；
（五）**个人信息处理者、境外接收方**的**组织架构、管理体系、技术措施**能否充分有效保障数据安全和个人信息权益；	（三）**境外接收方**承诺承担的**义务**，以及履行义务的**管理和技术措施、能力**等能否保障出境个人信息的安全；
（四）个人信息处理者与境外接收方订立的有法律约束力的协议是否约定了**个人信息保护的义务**；	（四）**个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等**；
（三）**境外个人信息处理者、境外接收方的个人信息保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求**；	（二）**出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险**；
（六）专业认证机构根据个人信息保护认证相关标准认为需要评定的其他事项。	（六）其他可能影响个人信息出境安全的事项。

两者的**主要区别**包括：

- 认证区分了“境外个人信息处理者”和“境外接收方”两类角色，并且在第（四）项中，仅要求评估个人信息处理者与境外接收方之间订立的协议。按此理解，如果认证对象为“境外个人信息处理者”，则无需额外签署跨境传输相关协议；
- 认证的第（五）项中，要求同时对个人信息处理者和境外接收方的“组织架构、管理体系、技术措施”进行评估，而标准合同备案侧重于评估境外接收方“履行义务的管理和技术措施、能力”，对个人信息处理者的管理能力等没有特别要求。

4、信息公开与持续监督

《认证办法》强调认证过程的**透明度**和对于认证结果的**持续监督**。认证机构需在颁发认证证书后的五个工作日内，将相关信息报送至全国认证认可公共信息平台（https://cx.cnca.cn/）。

此外，认证机构需建立持续监督机制，确保认证主体在认证有效期内持续符合标准。一旦发现认证主体在证书有效期内不再符合认证要求的，认证机构可以暂停、撤销认证证书，并将相关情况予以公布。国家网信部门和相关监管部门也将对获证主体进行监督管理，并对存在问题的企业采取相应措施。

5、认证与标准合同备案，如何选择？

由于大多数企业不会触发数据出境安全评估的高门槛要求，标准合同备案和个人信息保护认证成为企业实现个人信息出境的主要合规路径。那么，企业在考

量到底选择标准合同备案还是个人信息保护认证时，应当考虑哪些因素呢？以下我们列出了两者的对比，供企业判断选择：

维度	认证	标准合同备案
评估内容	认证的评估内容更为广泛，需要同时评估个人信息处理者和境外接收方的组织架构、管理体系、技术措施。境内企业需要在内部流程优化、管理机制健全以及技术能力建设方面投入更多的资源和精力。	标准合同备案重点评估境外接收方的技术、管理措施是否可以履行标准合同所规定的义务以及保护出境个人信息安全。 备案对于境内企业的组织架构和内部管理体系关注较少，主要集中在数据“出境后”的安全保障。
公开性	认证通过后，企业的认证证书将被公开披露，能够在一定程度上证明企业的数据合规能力，对于希望提升客户信任和行业声誉的企业来说是一个加分项。	标准合同备案的信息不对外公开，缺乏类似的背书效应。但企业也可以选择将备案的通知结果提供给相关需求方。
有效期	根据《个人信息保护认证实施规则》第 5.1 条，认证证书的有效期为三年。企业需要在证书到期前六个月提出续期申请，经认证机构审核后方可延续认证。	标准合同备案的有效期由合同双方协商确定。在实践中，备案合同的有效期通常具有更大的灵活性，甚至可以约定为长期有效。
费用	认证需要通过指定的专业认证机构进行评定，会产生一定的费用。例如，根据中国网络安全审查认证和市场监管大数据中心（CCRC）公布的收费标准，认证费用包括以下项目： - 申请费：18,000 元/认证单元； - 评定注册费：24,000 元/认证单元； - 审核/验证费：6,000 元/人日； - 年金：50,000 元/年认证单元；	标准合同备案由省级网信部门负责审查，无需企业支付费用。

	- 技术验证费：另行计算。	
条款灵活性	认证允许企业与境外接收方协商出境条款内容，因此适用于境外接收方立场较为强硬、企业自身谈判能力有限的情形。	标准合同备案要求双方严格遵循国家网信部门发布的标准合同模板，条款不可修改。在实践中，部分境外接收方可能因对部分条款（如责任划分）存在异议而拒绝签署。

3. 一口气投诉了六家中国企业违反 GDPR！NOYB 到底什么来头

供稿人：潘永建（上海市通力律师事务所）、邓梓珊（上海市通力律师事务所）、嵇若琳（上海市通力律师事务所）

2025 年 1 月 16 日，奥地利非政府组织 NOYB 针对 TikTok、AliExpress（全球速卖通）、SHEIN（希音，跨境电商平台）、Temu（拼多多的跨境电商平台）、WeChat（微信）和 Xiaomi（小米）六家中企向 5 家欧盟的数据保护机构（Data Protection Authority, 以下简称“DPA”）提出《通用数据保护条例》（“GDPR”）相关的投诉，指控其“向中国非法传输数据”，并要求相应 DPA 根据 GDPR 的相关规定命令其暂停向中国传输欧盟用户的数据，同时，建议对上述被投诉人处以“有效、适当且具有威慑力”的罚款，以防止未来发生类似违规行为。

NOYB 是谁？

据其官网介绍，NOYB 作为一家总部位于奥地利维也纳的非营利组织，其团队成员包括来自欧洲各地的 20 多名法律和信息技术专家，致力于“确保私营组织尊

重基本隐私权”。2024 年 12 月 2 日，NOYB 被批准为所谓的“合格实体”，即有权在整个欧盟的法院提起集体救济诉讼。通过欧盟版的“集体诉讼”，NOYB 可以代表数千甚至数百万用户提起诉讼，例如在用户的个人数据被非法处理时要求相关公司进行赔偿。

大家或许不熟悉 NOYB 这个名字，但要说起它的名誉主席（Honorary Chairman）Max Schrems，也可算在数据保护界“赫赫有名”了。Schrems 作为奥地利隐私倡导者，曾对“欧盟-美国安全港框架”（The safe harbor privacy principles for the protection of personal data transferred from a Member State to the United States）和“欧盟-美国隐私盾协议”（EU-U.S. Privacy Shield）提出了质疑，并最终都取得了里程碑式的诉讼结果。2015 年，欧盟法院通过 Schrems I 案裁决“欧盟-美国安全港框架”因违反《1995 年数据保护指令》及侵犯欧盟公民的个人数据根本权利而无效；2020 年，欧盟法院通过 Schrems II 案，以相关机制并不足以保护欧盟公民的个人信息为理由，裁决欧盟-美国隐私盾协议无效。而目前 NOYB 已成为了名正言顺的提起集体诉讼的“合格实体”，因此，其未来是否会在数据保护领域更加踊跃也备受关注。

管辖权：为什么会涉及 5 家 DPA?

此次 NOYB 对中国 6 家出海大厂的投诉，均以相应平台注册用户的名义进行。基于 GDPR 的管辖权，GDPR 不仅适用于在欧盟内某一控制者或处理者对个人数据的处理，对于不在欧盟内设立的控制者或处理者，如果涉及向在欧盟内的数据主体提供商品或服务，或监控他们在欧盟的行为，都属于 GDPR 的管辖范围。以 TikTok 为例，NOYB 认为 TikTok 为包括欧盟用户在内的全球用户提供服务，因此，NOYB 认为上述公司受到 GDPR 的管辖并不奇怪。

而对于为什么会出现向不同的 DPA 投诉的情况（TikTok、Xiaomi：希腊 DPA；

AliExpress：比利时 DPA；SHEIN：意大利 DPA；Temu：奥地利 DPA；WeChat：荷兰 DPA），**根据 GDPR 的规定，原则上根据控制者的主要营业机构所在地来确定对应的 DPA。**但如果控制者在不止一个成员国有多处营业机构，那么其在欧盟的“中央管理机构”（Place of central administration）通常被视为主要营业机构。因此，NOYB 也在各投诉信中对于其确定 DPA 的逻辑进行了解释。以 TikTok 为例，投诉信中称，通过访问 TikTok“联系我们”部分提供的 TikTok 在爱尔兰的地址，NOYB 称并不能找到该平台的办公室或任何机构，因此，NOYB 认为该地址极有可能只是一个“信箱”地址，不能构成 GDPR 法下的主要机构。由此，NOYB 以“投诉人的惯常居住地在希腊雅典”为由，认为希腊 DPA 应为处理本投诉的主管机构，并向其提交投诉信。

主要投诉理由：傲慢与偏见？

NOYB 的投诉主要是基于所谓的“中国的法律影响了适当保障措施（Appropriate safeguards）的有效性”。NOYB 在投诉信中称，除了依赖 GDPR 第 46 条规定的适当保障措施（例如，最常见的标准合同条款（SCCs），是中欧企业之间个人信息跨境的合规传输路径之一），欧盟法院还需要核实第三国法律在何种程度上满足了相当于欧盟数据保护水平的数据保护水平。为此，需要考虑该第三国是否为数据主体（投诉人）提供可执行的数据保护权利，是否为数据主体提供有效的法律救济措施；以及保证政府机构和国家安全机构对个人数据的访问受到限制。

而对于 NOYB 来说，中国的数据保护水平的“不够格”似乎早已成为既定事实。基于对中国网络数据安全及个人信息保护相关法律的认知，其在投诉信中得出了所谓“中国法律没有限制政府机构对企业数据的访问权限”的结论；而在仅结合一些外网新闻、一家企业的透明度报告的基础上，其又试图指摘相关机构“无限制地访问由中国公司处理的个人数据的风险非常高”，甚至上升到了政治高度。

为进一步论证，NOYB 首先列举了中国关于数据本地化的法律规定，认为中国法要求企业“必须在中国境内存储‘收集和产生’的数据”，因此，企业不得不对收集的数据做本地化存储处理；投诉信中还称，“中国国家互联网信息办公室（以下简称“网信办”）具有对所有数据跨境传输授权决定的自由裁量权”（即获得事先授权），因此导致数据主体无法行使数据访问权和数据可携权。

相信对中国相关法律及数据合规实践有所了解的读者，对这些指控并不陌生。此前中国出台《网络安全法》《数据安全法》等规定时，就有外媒作出类似的曲解。中国法仅对特定主体、特定情形下的数据做本地化存储要求（例如涉及关键信息基础设施运营者、重要数据），并非简单地一以概之。而对于个人信息跨境转移，也根本不存在需要一刀切地获取网信办事先授权的监管方式，只有满足特定情况、达到一定的数据出境量的企业才需要受到政府授权形式的监管。

结语

近年来，中国大厂的出海机遇可谓风起云涌，但也因此波折不断。在如今的国际环境下，中国出海企业也需要更加重视数据及个人信息的安全与合规性，积极适应海外市场的监管要求，从而确保其跨境业务更加顺畅。