

数据出境安全评估的适用范围

重要数据的识别与未评估出境的责任

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要: 数据出境有三条合规路径: 安全评估、标准合同、保护认证。其中, 安全评估的门槛最高、程序最严, 适用的范围也最容易引发争议。数据安全法、个人信息保护法与《数据出境安全评估办法》共同构筑了评估的制度框架, 但框架之中仍有模糊之处。其一, 重要数据的识别标准不清。何谓重要数据, 法律只作了定义, 未列清单, 企业难以自我判断。其二, 触发条件的技术口径不明。累计传输量如何计算、统计周期如何确定、一人一次与一人多次如何区分, 实务中做法不一。其三, 未评估出境的法律后果不明。是行政处罚、合同无效, 还是刑事责任, 规范之间缺乏衔接。其四, 与标准合同、保护认证的关系不清。评估是否为其他两条路径的前置, 未经评估而签订标准合同的, 效力如何。本文认为, 安全评估的适用范围应作限缩解释, 以重要数据与法定情形为限, 不宜扩张至一般个人信息。重要数据的识别, 应采取行业目录加企业自主识别相结合的模式, 并引入事前沟通机制。触发条件的计算, 应以自然人为单位累计, 以年度为统计周期。未评估出境的行为, 在行政法上应受处罚, 在民法上不当然无效, 但相对方有权解除。

关键词: 数据出境; 安全评估; 重要数据; 触发条件; 合规路径

中图分类号: D922.17 **文献标识码:** A **文稿编号:** WJLT(2021)01-0038-12

The Scope of Security Assessment for Outbound Data Transfer

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Three compliance paths exist for outbound data transfer: security assessment, standard contract and protection certification. Security assessment has the highest threshold, the strictest procedure and the most contested scope. The Data Security Law, the Personal Information Protection Law and the Measures for Security Assessment of Outbound Data Transfer together establish the framework, yet ambiguities remain. First, the criteria for identifying important data are unclear; the law defines but does not list them. Second, the technical standard for triggering the assessment is uncertain, including how cumulative volume is calculated and over what period. Third, the consequences of transferring without assessment are unclear, whether administrative penalty, contractual invalidity or criminal liability. Fourth, the relationship with the standard contract and certification is undefined. This article argues that the scope should be narrowly construed, limited to important data and statutory situations. Identification should combine sectoral catalogues with self-assessment and prior consultation. Volume should be counted per natural person on an annual basis. Transfer without assessment should be administratively sanctioned, but the contract is not automatically void.

Key words: outbound data transfer; security assessment; important data; triggering threshold; compliance path

说明: (本文为作者个人研究观点, 不代表所在单位意见)

作者简介: 赵跃, 安徽国运律师事务所执业律师, 主要研究数据法与网络法。

一、问题的提出

数据出境, 是数字经济发展中的一道必答题。企业要开展跨境业务, 须把数据传输至境外; 国家要维护数据安全, 须对出境行为加以管理。二者之间的平衡, 靠制度设计实现。

我国选择了三条路径并行的模式: 安全评估、标准合同、保护认证。三条路径的门槛不同, 适用的情形也不同。安全评估是门槛最高的一条, 适用于重要数据与达到法定数量

的个人信息。

制度建立以来，适用的范围一直是争议的焦点。企业最关心的问题有三个：我的数据是不是重要数据；我的传输量是否达到了触发标准；没有评估就出境，会有什么后果。三个问题，都不容易回答。

第一个问题的困难，在于重要数据没有清单。数据安全法第二十一条只作了定义，要求各地区、各部门确定重要数据目录。目录的制定进展缓慢，多数行业尚无目录，企业只能自行判断。

第二个问题的困难，在于计算口径。办法规定，自当年一月一日起累计向境外提供一百万人以上个人信息或者一万条以上敏感个人信息的，须申报评估。累计如何计算，是以人为单位还是以条为单位，法律没有明确。

第三个问题的困难，在于责任竞合。未评估出境，可能违反数据安全法、个人信息保护法、网络安全法，三部法律的处罚不同；在民法上，相关合同的效力如何，也没有定论。

三个问题的背后，是一个更根本的问题：安全评估的适用范围，究竟应当宽还是窄。宽，则企业合规成本高，跨境业务受阻；窄，则数据安全的风险难以控制。

本文认为，应当作限缩解释。理由是：安全评估是事前许可性质的管制措施，对营业自由的限制最强，应严格依照法律保留与比例原则适用；重要数据的范围应通过目录明确，不宜由执法机关逐案认定；触发条件应作有利于企业的解释。

这一立场，不是放松管制，而是使管制可预期。可预期的管制，企业才能遵守；不可预期的管制，只会催生规避。规则的明确，是最好的合规激励。

本文的结构如下：第二节梳理三条路径的规范体系，第三节讨论重要数据的识别，第四节讨论触发条件，第五节讨论评估的程序，第六节讨论未评估出境的后果，第七节讨论与另两条路径的关系，第八节讨论企业的合规义务，第九节为结语。

概念上还须区分数据出境与数据跨境。前者指数据从境内流向境外，后者含义更广，包括境外主体在境内收集数据、境内主体访问境外数据等情形。本文以出境为限。

出境的主体，是数据处理者。个人为生活需要传输数据的，不属于规制对象。这一区分，体现了规制重点在经营性的数据处理活动。

出境的客体，是数据。数据与信息的界分，在法理上仍有争议，但在出境管理中，二者基本同义，均指以电子或者其他方式记录的各类信息。

二、三条路径的规范体系

数据出境的规范体系，由三部法律、一部行政法规与若干部门规章构成。三部法律是网络安全法、数据安全法、个人信息保护法；行政法规是《网络数据安全条例》；规章是《数据出境安全评估办法》《个人信息出境标准合同办法》等。

网络安全法第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储；因业务需要，确需向境外提供的，应当按照规定进行安全评估。这是安全评估制度的最初依据。

数据安全法第二十一条建立数据分类分级保护制度，要求确定重要数据目录；第三十一条规定，关键信息基础设施的运营者和其他数据处理者处理重要数据的出境安全管理，适用有关法律、行政法规的规定。

个人信息保护法第三十八条列举了个人信息出境的四类条件：通过安全评估；经专业机构认证；订立标准合同；法律、行政法规或者网信部门规定的其他条件。第三十九条要求取得个人的单独同意。

四类条件，构成了三条路径的法律基础。安全评估是第一类，标准合同是第三类，保护认证是第二类。三条路径并列，企业可以选择，但选择的自由受适用范围的限制。

《数据出境安全评估办法》第四条明确了应当申报评估的四种情形：数据处理者向境外提供重要数据；关键信息基础设施运营者向境外提供个人信息或者重要数据；数据处理者向境外提供个人信息，达到法定数量的；网信部门规定的其他情形。

四种情形，可以分为两类：以数据性质为标准的情形，即重要数据；以主体身份为标准的情形，即关键信息基础设施运营者；以数量为标准的情形，即达到法定数量的个人信息。三类标准，构成本文的讨论框架。

三类标准的适用关系，值得注意。它们是并列的，只要符合其一，即须申报。这意味着，即使不是关键信息基础设施运营者，只要处理重要数据或者达到数量标准，也须申报。

还有一层，是三条路径的层级。安全评估是强管制，标准合同与保护认证是弱管制。强管制适用于风险较高的情形，弱管制适用于风险较低的情形。这一层级，体现了比例原则。

从比较法看，欧盟的《通用数据保护条例》以充分性认定、适当保障措施与例外情形三层机制管理数据出境，其中适当保障措施包括标准合同条款与行为准则。我国的三条路径，与之功能相近。

差异在于，我国的路径选择与数据分类分级绑定，重要数据一律走评估；欧盟则以个人数据保护水平为核心，不区分重要数据。这一差异，反映了两种不同的规制理念。

综上，三条路径构成了数据出境的规范体系，安全评估是最强的一环。理解其适用范围，须把握三类触发标准与层级关系。这是后续讨论的基础。

重要数据何时触发安全评估、不申报会承担何种责任，实务中的梳理可参见

重要数据何时触发安全评估、不申报会承担何种责任，实务中的梳理可参见向境外提供重要数据何时必须报安全评估一文的归纳，本文不再重复其处罚标准，只就适用范围的界定展开。

分类分级是识别的制度前提。数据安全法要求建立分类分级保护制度，分类解决是什么的问题，分级解决多重要的问题。二者结合，才能确定保护的措施。

分类分级的落地，须有标准支撑。国家标准已经发布若干，但行业标准参差不齐，企业适用时常常无所适从。标准的统一，是识别的前提。

三、重要数据的识别

重要数据是安全评估的核心概念，也是适用范围中最模糊的部分。数据安全法第二十一条的定义是：一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

这一定义，有三个特点：后果导向，以危害后果为判断标准；国家安全导向，以国家安全为核心；不确定性，危害的可能性难以量化。三个特点，使定义难以直接适用于个案。

为此，法律要求制定重要数据目录。数据安全法第二十一条规定，各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录。目录制度，是把抽象定义具体化的路径。

目录的制定进展如何？截至目前，汽车、证券、医疗、工信等领域已发布或者正在制定目录，多数行业尚无目录。这一状况，使企业难以自我判断，也使执法缺乏统一标准。

在目录缺失的情况下，企业如何识别？实践中形成了三种做法：一是参照已发布的本行业目录；二是参照相邻行业的目录；三是自行组织评估。三种做法，都有局限。

参照本行业目录，是最可靠的做法，但多数行业无目录。参照相邻行业目录，存在类比不当的风险。自行评估，缺乏统一标准，结论难以获得认可。

本文主张，建立行业目录加企业自主识别相结合的模式。行业目录解决共性问题，企业自主识别解决个性问题。二者结合，既保证统一性，又保留灵活性。

企业自主识别，须有方法。建议采用四步法：第一步，梳理数据资产，明确数据的类型、来源、规模；第二步，评估危害后果，分析数据泄露对国家安全、经济运行、社会稳定的影响；第三步，对照目录，有目录的按目录判断，无目录的按定义判断；第四步，形成识别报告，留存备查。

四步法的关键，是第二步的危害后果评估。评估的维度，包括数据的规模、敏感性、关联性、可聚合性。规模越大、敏感性越高、关联性越强、越易聚合，危害越大。

举例而言，地理信息数据，若涉及军事设施、重要基础设施的位置，属于重要数据；若仅为一般的导航数据，则不属于。人口健康数据，若涉及大规模人群的健康状况，可能属于重要数据；若为个别患者的诊疗记录，则属于个人信息。

还有一个方法，是事前沟通。企业在难以判断时，可以向网信部门或者行业主管部门咨询，请求确认。沟通的结论，可以作为企业合规的依据。这一机制，可以降低企业的

确定性。

事前沟通的规范化，须有程序保障。建议明确沟通的申请材料、答复期限、答复效力。答复应具有约束力，执法机关不得事后反悔，否则企业的信赖利益无从保护。

重要数据与个人信息的界分，也须明确。二者可能重叠：大规模的个人信息，经聚合分析后可能成为重要数据；但个人信息本身，不因数量大而当然成为重要数据。

界分的标准，是危害的对象。危害个人权益的，是个人信息问题；危害国家安全、公共利益的，是重要数据问题。这一标准，与定义的后果导向一致。

实践中，有一种扩大化的倾向，把大量个人信息一概视为重要数据，从而要求申报评估。这一倾向，混淆了二者，加重了企业负担，应予纠正。

综上，重要数据的识别，须以目录为基础，以自主识别为补充，以事前沟通为保障。识别的核心，是危害后果的评估。范围的扩大化，应当避免。

还有一层，是数据出境与数据中转的区分。境内主体将数据传输至境外服务器，再由境外主体回传境内的，是否属于出境？本文认为，属于，因为数据已经为境外主体所获取。

反之，境外主体在境内设立的机构处理境内数据，未向境外提供的，不属于出境。判断的标准，是数据是否被境外主体实际获取，而非服务器的物理位置。

四、触发条件的计算

触发条件的计算，是实务中最易产生争议的技术问题。办法规定，数据处理者向境外提供个人信息，累计达到一百万人以上或者一万条以上敏感个人信息的，须申报评估。

计算的首要问题，是计算单位。是以人数为单位，还是以条数为单位？办法的表述是一百万人以上与一万条以上，前者以人为单位，后者以条为单位。这一区分，蕴含了立法的考量。

一般个人信息，以人为单位。理由是：一般个人信息的敏感性较低，单条泄露的危害有限，须达到一定人数才构成风险。以人为单位，可以避免因重复传输而夸大风险。

敏感个人信息，以条为单位。理由是：敏感个人信息的敏感性高，单条泄露即可能造成严重后果，须以条数控制。以条为单位，可以更准确地反映风险。

这一区分，在计算时须严格遵循。一般个人信息不得按条累计，敏感个人信息不得按人折算。混淆二者，会导致触发标准的误用。

计算的第二个问题，是重复计算。同一自然人的个人信息被多次传输的，是按一人计算，还是按多次计算？本文认为，一般个人信息应按一人计算，敏感个人信息应按条计算。

按一人计算的理由，是避免重复。同一自然人的信息，无论传输多少次，其人格权益的主体只有一个，风险不因次数而倍增。若按次计算，企业将因业务模式而承担不同的合

规义务，有失公平。

但去重须有技术支撑。企业须建立个人信息的传输台账，记录传输的对象、时间、数量，并能识别重复的自然人。技术上，可通过标识符的去重实现，但须注意不得额外收集个人信息。

计算的第三个问题，是统计周期。办法规定自当年一月一日起累计，即以自然年为周期。这一规定，明确了起算点，但未明确跨年度的处理。

跨年度的处理，有两种理解：一是每年重新起算，上年度的传输不计入；二是连续计算，跨年度的传输累计。本文认为，应采用第一种，理由是条文明文规定自当年一月一日起。

每年重新起算，可能被企业规避：年末少传、年初多传，即可规避评估。这一风险，须通过其他机制弥补，例如把规避行为认定为违反诚信原则，或者以连续十二个月为周期补充计算。

计算的第四个问题，是传输的方式。直接传输、间接传输、境外访问，是否都计入？办法的表述是向境外提供，包括传输、存储、访问等提供行为。三种方式，均应计入。

境外访问的计入，值得注意。境外主体通过系统查询境内数据，虽未物理传输，但实质上使境外主体获得了数据，应视为提供。这一理解，与国际上的通行做法一致。

计算的第五个问题，是集团内部的传输。跨国公司的境内子公司向境外母公司传输数据，是否计入？本文认为，应计入。数据出境的风险，不因传输对象是关联方而降低。

但集团内部的传输，可以在程序中予以便利。例如，允许集团统一申报、允许一次评估覆盖多个接收方。这些便利，须在制度上明确，不能靠个案裁量。

计算的第六个问题，是数据的类型。个人信息、重要数据、非个人数据的非重要数据，计算方式不同。重要数据不按数量计算，只要传输即须评估；非重要数据的非个人数据，原则上不适用评估。

综上，触发条件的计算，须把握五个要点：一般个人信息按人、敏感个人信息按条；同一自然人去重；以自然年为周期；访问亦计入；集团内部传输计入。五个要点，构成计算的基本规则。

评估的实质审查，还须关注数据的聚合效应。单项数据看似无关紧要，聚合之后可能形成重要的画像，进而危害国家安全。评估时，应把聚合的可能性纳入考量。

聚合效应的评估，须有技术支撑。网信部门可以要求企业提供数据字段、关联关系、分析模型的说明，必要时组织专家论证。这一环节，是评估中最具专业性的部分。

评估结论的说理，也须加强。实践中，不通过的决定往往只说风险不可控，不说明具体理由。说理不足，企业无从整改，救济也无从展开。

五、评估的程序

安全评估的程序，分为申报、受理、评估、决定四个环节。程序的设计，体现了事前许可的性质，也体现了风险管理的思路。

申报的主体，是数据处理者。申报的材料，包括申报书、数据出境的风险自评估报告、与境外接收方订立的法律文件、安全评估要求的其他材料。材料的核心，是风险自评估报告。

风险自评估，是评估的前置。办法要求数据处理者在申报前开展自评估，重点评估：数据出境的目的、范围、方式的合法性、正当性、必要性；出境数据对国家安全、公共利益、个人或者组织合法权益的影响；接收方的保障能力；风险防范措施。

自评估的性质，是企业内部的合规审查，不是行政机关的评估。但自评估的报告，是行政机关评估的基础。自评估不实的，企业须承担相应的责任。

受理的环节，网信部门对材料进行形式审查。材料齐全的，予以受理；材料不齐的，一次性告知补正。受理的期限，办法规定为七个工作日。

评估的环节，网信部门组织评估。评估的方式，包括书面审查、现场核查、专家论证。评估的期限，一般为四十五个工作日，情况复杂的可以延长十五个工作日。

评估的内容，包括三项：数据出境是否合法、正当、必要；境外接收方的保障能力；数据出境的风险是否可控。三项内容，对应了合法性、安全性与风险控制三个维度。

合法性的审查，关注出境的目的与范围。目的是否特定、明确；范围是否限于实现目的所必需；是否取得了个人的单独同意；是否履行了告知义务。

安全性的审查，关注接收方的能力。接收方的所在国家或者地区的法律环境、数据保护水平；接收方的技术与管理措施；双方合同中的保障条款。

风险控制的审查，关注救济的途径。数据主体能否行使权利；发生泄露时的通知与补救；争议的解决方式与管辖。

决定的环节，网信部门作出通过或者不通过的决定。通过的，发给书面通知，有效期一般为二年；不通过的，说明理由。有效期内情况发生变化的，须重新申报。

有效期的设计，体现了动态管理。二年期满，或者出境目的、方式、种类发生变化，或者接收方所在法律环境发生变化的，须重新评估。这一设计，避免了评估的一劳永逸。

程序的救济，须予明确。企业对不通过的决定不服的，能否申请行政复议或者提起行政诉讼？办法未明确规定。本文认为，应可以。评估决定是行政行为，属于行政复议与行政诉讼的受案范围。

救济的意义，在于约束裁量。评估的标准较为抽象，裁量的空间较大。若无救济，企业只能被动接受；有救济，裁量才能受到审查，标准才能逐步明确。

综上，评估的程序包括申报、受理、评估、决定四个环节，核心是风险自评估与实质审查。程序的公开与救济的通畅，是评估正当性的保障。

需要补充的是举证责任的分配。行政机关认定未评估出境，应证明企业属于应当申报的情形；企业主张已申报或者无需申报的，应提供相应证据。

在民事案件中，数据主体主张损害的，应证明损害的存在与因果关系；企业主张已尽合规义务的，应提供评估文件、合同、监督记录。这一分配，符合证据的接近性。

责任的追究，还涉及管辖。数据出境的违法行为，由何地机关管辖？本文认为，应由数据处理者所在地的网信部门管辖，必要时由上级机关指定。

境外接收方违反约定的，我国机关能否处罚？依效果原则，若其行为对境内产生影响，可以管辖；但实际执行，须靠国际协作。这是当前的难题。

六、未评估出境的后果

未评估出境，是指依法应当申报评估而未申报，或者评估未通过仍出境的行为。此类行为的后果，涉及行政、民事、刑事三个层面。三个层面的规范，尚缺乏衔接。

行政层面，数据安全法第四十六条规定，违反规定向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

个人信息保护法第六十六条规定，违反规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，拒不改正的，并处一百万元以下罚款；情节严重的，处五千万元以下或者上一年度营业额百分之五以下罚款。

两部法律的处罚，存在竞合。同一行为既违反数据安全法又违反个人信息保护法的，如何处罚？本文认为，应依行政处罚法第二十九条的一事不再罚原则，按罚款数额较高的规定处罚。

一事不再罚的适用，须注意两点：一是同一行为，即同一出境行为；二是同一性质，即都是罚款。若一处为罚款、一处为吊销执照，则不属于重复处罚，可以并用。

民事层面，未评估出境的合同效力如何？这一问题，实践中有三种观点：无效说、可撤销说、有效说。三种观点，各有理由。

无效说的理由，是违反法律的强制性规定。数据安全法、个人信息保护法的评估规定，属于效力性强制性规定，违反的合同无效。这一观点的依据，是民法典第一百五十三条。

可撤销说的理由，是违反公序良俗或者显失公平。未评估出境，可能损害数据主体的权益，受损害方可以请求撤销。这一观点的依据，是民法典第一百四十七条至第一百五十一条。

有效说的理由，是评估规定属于管理性强制性规定，违反的不影响合同效力，只产生

行政责任。这一观点的依据，是最高人民法院关于合同编的司法解释，该解释区分了效力性规定与管理性规定。

本文倾向于有效说，但须补充。理由是：评估规定的内容，是行政管理的要求，其目的不在于否定合同的效力，而在于维护数据安全；若一概认定无效，将使跨境交易陷入不确定，反而损害当事人的利益。

但有效不等于无责。未评估出境的，相对方可以解除合同，理由是合同的目的不能实现，或者一方违反附随义务。数据主体也可以主张侵权，要求赔偿损失。

还有一种情形，是评估未通过仍出境。此时合同不仅违反管理规定，而且违反了行政机关的决定，性质更为严重。本文认为，此时应认定合同无效，理由是标的违法。

刑事层面，可能涉及侵犯公民个人信息罪、非法获取计算机信息系统数据罪、危害国家安全的相关罪名。入罪的关键，是行为是否造成了法益侵害，而非是否履行了评估程序。

未评估本身，不构成犯罪。评估是行政管理的程序，不履行程序不等于犯罪。但未评估出境，若同时造成了大量个人信息泄露，可能构成侵犯公民个人信息罪。

三个层面的衔接，须注意顺序。行政责任是基础，民事责任是补充，刑事责任是例外。三者并用时，应遵循过罚相当、责任自负的原则，避免重复评价。

综上，未评估出境的后果，行政上应受处罚，民事上合同不当然无效但可解除，刑事上须以法益侵害为前提。三个层面的界限，须由立法或者司法解释明确。

标准合同的适用范围，由《个人信息出境标准合同办法》规定。适用前提是未达到评估标准的一般个人信息出境，且不含重要数据。

保护认证的适用范围，与标准合同相近，但认证的审查更为专业，适合数据量大、接收方多的企业。认证的有效期与监督，另有规定。

三条路径的成本，差异明显。评估耗时最长、成本最高；标准合同的成本最低；认证居中。企业应依自身情形选择，不宜盲目追求低成本。

七、与另两条路径的关系

标准合同与保护认证，是安全评估之外的两条路径。三条路径的关系，是适用上的选择关系，还是层级上的递进关系？这一问题，直接影响企业的合规策略。

从条文看，个人信息保护法第三十八条列举的四类条件，是并列的，企业可以选择。这意味着，符合条件的企业，可以选择订立标准合同，而不申报评估。

但选择受适用范围的限制。属于应当申报评估情形的，不能以标准合同替代。例如，处理重要数据的企业，必须申报评估，不能以标准合同规避。

据此，三条路径的关系，是原则上的选择关系，例外情形下的强制关系。强制的情形，即办法第四条列举的四种。四种之外的，企业可以选择。

实践中，有一种误解，认为标准合同是评估的简化版，可以先签合同、后补评估。这一误解，须纠正。标准合同与评估是两条独立的路径，不能互相替代，也不能先后补正。

未经评估而订立标准合同的，合同的效力如何？本文认为，合同有效，但企业仍须承担未评估的责任。理由是：合同是民事行为，评估是行政程序，二者独立。

但合同的履行，可能受阻。行政机关责令停止出境的，合同无法履行，当事人可以解除。这一后果，是行政责任向民事的传导，不是合同本身的无效。

标准合同的性质，也须明确。标准合同是网信部门制定的格式条款，当事人不得修改实质内容。其性质，是行政指导下的民事合同，兼具自治与管制。

保护认证，是第三条路径。认证由专业机构进行，标准是国家标准。认证的效力，是证明企业的数据保护水平达到要求，可以作为出境的依据。

认证与评估的关系，类似于标准合同与评估的关系：原则上可以选择，法定情形下强制评估。认证的优势，在于一次认证可以覆盖多个接收方，适合集团企业的全球业务。

三条路径的转换，也须允许。企业原选择标准合同，后因业务扩大达到评估标准，应转为申报评估。转换的衔接，须有过渡期，避免业务中断。

综上，三条路径是选择与强制的结合。法定情形强制评估，其他情形可以自选。路径之间不得互相替代，但可以转换，转换须有过渡安排。

合规的成本，须有合理的预期。若规则频繁变动、标准模糊不清，企业只能过度合规，成本最终转嫁给消费者，社会总福利下降。

合规的外部性，也须考虑。单个企业的合规，可能使整个供应链受益；反之，单个企业的违规，可能使整个行业受累。行业协会的自律，因此有其价值。

八、企业的合规义务

安全评估的适用，最终落到企业的合规义务上。义务的内容，包括识别、申报、履行、监督四个方面。四个方面，构成合规的闭环。

识别的义务，是判断自身是否属于应当申报的情形。判断的依据，是数据的性质、主体的身份、传输的数量。判断的方法，是前文所述的四步法。

识别的义务，须有组织保障。企业应设立数据保护的负责人或者机构，建立数据的分类分级制度，定期开展数据资产的梳理。这些工作，是识别的基础。

申报的义务，是在识别的基础上，向网信部门申报。申报的材料须真实、完整。虚假申报的，须承担相应的责任，包括撤销许可、行政处罚。

履行的义务，是按评估通过的条件出境。出境的目的、范围、方式，不得超出评估的范围；接收方变更的，须重新评估；出境的目的完成或者终止的，须停止出境。

监督的义务，是对接收方的持续监督。监督的内容，包括接收方是否按约定使用数据、是否采取约定的保护措施、是否发生数据泄露。监督的方式，可以是审计、检查、定

期报告。

四项义务之外，还有一项附随义务，是记录与留存。企业应记录出境的台账，保存评估的文件、合同、监督记录，保存期限一般不少于三年。记录的留存，是合规的证明。

违反义务的责任，须区分层次。未识别、未申报的，承担行政责任；申报不实的，加重处罚；履行不到位的，责令改正；监督不力的，承担连带责任。层次的区分，体现过罚相当。

企业合规的激励机制，也须建立。主动申报、主动整改的，可以从轻或者减轻处罚；建立有效合规体系的，可以作为减免责任的情节。这一机制，符合行政法上的激励相容原理。

从司法角度看，合规体系的意义在于证明过错的有无。企业已建立合规体系、尽到注意义务的，可以主张无过错，免除或者减轻赔偿责任。这一抗辩，在民事案件中尤为重要。

综上，企业的合规义务，包括识别、申报、履行、监督与记录五个方面。义务的履行，须有组织、制度与技术的支撑。合规不仅是成本，也是竞争力。

还有一点须强调，是制度的时间维度。数据出境的规则仍在快速演进，企业须持续跟踪，及时调整合规策略。一次合规不等于永久合规。

监管沙盒的探索，值得关注。在特定区域、特定行业先行试点，积累经验后再推广，可以降低制度试错的成本，也可以为企业提供可预期的试验空间。

区域协作的机制，也须建立。粤港澳大湾区、自贸试验区等区域，存在跨境数据流动的现实需求，可探索白名单、负面清单等差异化管理方式。

国际互认的路径，更有长远意义。与贸易伙伴就数据保护水平达成互认，可以避免企业重复合规，也可以提升我国规则的国际影响力。

最后须指出，安全评估不是万能的。事前许可只能过滤部分风险，事中的监督与事后的追责同样重要。三者结合，才是完整的治理链条。

技术的进步，也会改变规制的形态。隐私计算、联邦学习等技术的应用，使数据可用不可见，出境的形态随之变化。规则须留出适应的空间。

本文的讨论，以现行规范为限。规范的变动，可能使部分结论需要修正。但方法论上的立场，即限缩解释与比例原则，应具持久的价值。

数据治理的本质，是规则的治理。规则清晰，市场主体才能形成稳定的预期；预期稳定，创新才有可能。这是本文最想强调的一点。

九、结语

数据出境安全评估，是我国数据治理体系中的重要一环。它的适用范围，关系到数据安全的保障，也关系到跨境业务的开展。范围过宽，企业不堪重负；范围过窄，风险难以

控制。

本文的基本结论是：安全评估的适用范围应作限缩解释，以重要数据与法定情形为限；重要数据的识别，应采取目录加自主识别相结合的模式，并引入事前沟通；触发条件的计算，一般个人信息按人、敏感个人信息按条，同一自然人去重，以自然年为周期；未评估出境的，行政上应受处罚，民事上合同不当然无效但可解除。

这些结论，须以立法的完善为支撑。建议加快重要数据目录的制定，明确触发条件的计算口径，规定评估决定的救济途径，厘清三条路径的适用关系。

这些结论，也须以执法的一致为保障。同一行为，在不同地区受到不同处理，会损害制度的权威。执法的统一，须靠细则的明确与案例的指导。

从长远看，数据出境的管理，须在安全与发展之间寻找动态平衡。技术在变，业务在变，风险也在变。制度须有适应性，才能既守住底线，又不窒息活力。

让数据安全得到保障，让跨境业务得以开展，让企业合规有章可循，这是数据出境制度的价值所在，也是法治的责任所在。

参考文献

- [1] 张新宝：《个人信息保护法释义》，中国人民大学出版社2021年版。
- [2] 周汉华主编：《数据安全法释义》，法律出版社2021年版。
- [3] 程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版。
- [4] 丁晓东：《数据出境的法律规制》，载《中国法学》2022年第3期。
- [5] 洪延青：《重要数据的识别与保护》，载《中外法学》2022年第1期。
- [6] 许可：《数据跨境流动的三种路径》，载《法学研究》2021年第6期。
- [7] 彭鐔：《数据出境安全评估的制度逻辑》，载《比较法研究》2022年第4期。
- [8] 王锡锌：《数据治理的公法维度》，载《中国法学》2021年第5期。
- [9] 高富平：《数据经济的法律基础》，法律出版社2020年版。
- [10] 姜明安：《行政法与行政诉讼法》，北京大学出版社2019年版。