

# 《律师办理数据出境法律业务操作指引（2024）》

第十二届北京市律师协会  
数字经济与人工智能领域法律专业委员会

2024年10月27日



# 律师办理数据出境法律业务操作指引 (2024)

## 第一章 总则

第一条【指引目的】为明确数据出境法律业务的操作规范，提高律师办理数据出境法律业务的服务质量和水平，降低委托人在向境外提供数据过程中的法律风险，北京市律师协会特编制本指引。

第二条【适用范围】本指引适用于北京市执业律师（以下简称律师）办理数据出境法律业务，包括但不限于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证和其他与数据出境相关的活动。

第三条【重要定义】除非上下文另有所指，本指引中下列用语的定义为：

- （一）“数据”是指任何以电子或者其他方式对信息的记录。
- （二）“重要数据”是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的的数据。
- （三）“个人信息”是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
- （四）“敏感个人信息”是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及

不满十四周岁未成年人的个人信息。

(五) “数据处理”是指数据的收集、存储、使用、加工、传输、提供、公开等。

第四条【法律依据】本指引编写者全面梳理了现行有效的数据出境相关法律、规章、管理清单、标准，并将其作为本指引的附件，以供律师参考。

## 第二章 数据出境法律要求概述

第一条【数据出境行为】以下行为属于数据出境行为：

(一) 数据处理者将在境内运营中收集和产生的数据传输至境外；

(二) 数据处理者收集和产生的数据存储在境内，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数据处理活动。

第二条【向境外提供重要数据的合规路径】数据处理者向境外提供重要数据的，应当申报数据出境安全评估。

数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要将其作为重要数据申报数据出境安全评估。

第三条【向境外提供个人信息的合规路径】属于关键信息基础设施运营者的数据处理者向境外提供个人信息的，应当申报数据出境安全评估。

不属于关键信息基础设施运营者的数据处理者自当年1月1日起累计

向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息的，应当申报数据出境安全评估。

不属于关键信息基础设施运营者的数据处理者自当年 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 万人敏感个人信息的，应当选择订立个人信息出境标准合同或者通过个人信息保护认证。

**第四条【数据出境合规路径的豁免情形】**数据处理者符合以下情形之一的，免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

（一）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收集和产生的数据向境外提供，不包含个人信息或者重要数据的；

（二）在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；

（三）为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的；

（四）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；

（五）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

（六）关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的。

第五条【负面清单管理】《促进和规范数据跨境流动规定》第六条规定，自由贸易试验区内数据处理者向境外提供需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（以下简称“负面清单”）外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。截至本指引发布之日，已有北京和天津自由贸易区制定负面清单。

需要注意的是，使用负面清单出境数据虽然免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证，但不意味着无需履行任何合规手续。以北京自由贸易区为例，数据处理者向境外提供负面清单以外的数据的，需要提交负面清单使用申请并备案。

### **第三章 数据出境法律业务通用操作指引**

第一条【业务流程】律师可以按照以下流程开展数据出境法律业务：

- （一）协助数据处理者识别数据出境行为，梳理数据出境场景；
- （二）明确开展数据处理活动的法律主体，并判断该主体是否属于关键信息基础设施运营者；
- （三）根据数据处理者统计的出境数据类型和规模，判断出境数据是否包括重要数据或个人信息；
- （四）根据数据出境的场景、数据处理者的身份、出境数据的类型和

规模等因素，为数据处理器提供数据出境合规路径的选择建议；

（五）协助数据处理器开展数据安全风险评估或个人信息保护影响评估，并针对评估中发现的法律风险提出整改建议；

（六）拟定或审查合同等相关法律文件；

（七）协助数据处理器申报数据出境安全评估、备案个人信息出境标准合同或开展个人信息保护认证。

**第二条【重点评估事项】** 律师在开展数据安全风险评估或个人信息保护影响评估时，应重点评估以下事项：

（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件是否充分约定了数据安全保护责任义务（适用于数据安全风险评估），或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影响（适用于个人信息保护影响评估）；

(六) 其他可能影响数据出境安全的事项。

第三条【数据出境“三性”审查要点】律师在审查数据出境的合法性、正当性、必要性时，应重点审查以下事项：

向境外提供个人信息的，是否取得个人单独同意或存在其他合法性基础；向境外提供数据的，该等数据是否为法律、行政法规禁止出境的数据；

向境外提供数据的目的和行为是否违背公序良俗；

向境外提供的数据是否是开展业务所必需的，或者是履行法律、行政法规规定的义务所必需的。

第四条【出境数据类型审查要点】律师在审查出境数据类型时，可以参考《个人信息保护法》第四条和第二十八条的规定，以及 GB/T 35273-2020《信息安全技术 个人信息安全规范》的要求，判断出境数据是否包括个人信息、敏感个人信息。

第五条【出境数据规模审查要点】律师在审查出境数据规模时，应重点审查数据处理者是否采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

第六条【法律文件审查要点】律师在审查合同或者其他具有法律效力的文件时，应重点审查以下法律条款：

(一) 数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

(二) 数据在境外保存地点、期限，以及达到保存期限、完成约定目

的或者法律文件终止后出境数据的处理措施；

（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第七条【材料真实性、合法性、有效性审查】律师应对数据处理者提供的材料的真实性、合法性、有效性进行审查，包括但不限于：

（一）审查管理文件是否经过正当的起草或批准程序并生效实施；

（二）审查协议文件是否获得协议各方的有效同意并实际生效和执行；

（三）审查纸质或者电子记录的工作档案是否能够反映真实情况；

（四）审查网络安全等级保护、个人信息保护认证、数据安全管理体系等证明是否在有效期内；

（五）审查相关检测机构是否具有资质，是否在出具的检测报告上加盖公章并对内容真实性做出负责任承诺。

## 第四章 数据出境安全评估申报法律业务操作指引

第一条【申报方式】申报数据出境安全评估的，应当通过数据出境申报系统提交申报材料，系统网址为 <https://sjcj.cac.gov.cn>。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的，采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估。

第二条【申报材料】申报数据出境安全评估，应当提交统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、数据出境安全评估申报书、与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件、数据出境风险自评估报告、其他相关证明材料。

第三条【评估结果】对评估结果无异议的，数据处理者须按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范相关数据出境活动；对评估结果有异议的，数据处理者可在收到评估结果通知书 15 个工作日内向国家网信办申请复评，复评结果为最终结论。

通过数据出境安全评估的结果有效期为 3 年，自评估结果出具之日起计算。

第四条【重新申报】在有效期内出现以下情形之一的，数据处理者应当重新申报评估：

（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要

数据境外保存期限的；

(二) 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

(三) 出现影响出境数据安全的其他情形。

有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满 60 个工作日前提出延长评估结果有效期申请。经国家网信办批准，可以延长评估结果有效期 3 年。

## **第五章 个人信息出境标准合同备案法律业务操作指引**

**第一条【备案方式】**个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过数据出境申报系统备案，系统网址为 <https://sjcj.cac.gov.cn>。

**第二条【备案材料】**备案个人信息出境标准合同，应当提交统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、承诺书、标准合同、个人信息保护影响评估报告。

**第三条【备案结果】**备案结果分为通过、不通过。通过备案的，省网信办向个人信息处理者发放备案编号；未通过备案的，个人信息处理者将收到备案未成功通知及原因；要求补充完善材料的，个人信息处理者应当补充完善材料并于 10 个工作日内再次提交。

**第四条【重新备案】**在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

（一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；

（二）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发生变化等可能影响个人信息权益的；

（三）可能影响个人信息权益的其他情形。

个人信息处理者在标准合同有效期内补充订立标准合同的，应当提交补充材料；重新订立标准合同的，应当重新备案。补充或者重新备案的材料查验时间为 15 个工作日。

## **第六章 个人信息保护认证法律业务操作指引**

**第一条【申请主体】**申请认证的企业应取得合法的法人资格，正常经营且具有良好的信誉、商誉。

**第二条【认证依据】**对于开展跨境处理活动的企业，应当符合 GB/T 35273《信息安全技术 个人信息安全规范》和 TC260-PG-20222A《网络安全标准实践指南——个人信息跨境处理活动安全认证规范（V2.0-202212）》的要求。

**第三条【认证机构】**目前有权开展个人信息保护认证的机构为中国网

络安全审查技术与认证中心。

**第四条【认证结果】** 认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

认证证书有效期为 3 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。

**第五条【认证证书的变更和续期】** 认证证书有效期内，若获得认证的企业名称、注册地址，或认证要求、认证范围等发生变化时，认证委托人应当向认证机构提出变更委托。认证机构根据变更的内容，对变更委托资料进行评价，确定是否可以批准变更。如需进行技术验证和 / 或现场审核，还应当在批准变更前进行技术验证和 / 或现场审核。

证书到期需延续使用的，认证委托人应当在有效期届满前 6 个月内提出认证委托。认证机构应当采用获证后监督的方式，对符合认证要求的委托换发新证书。

## **第七章 附则**

**第一条【指引效力】** 本指引旨在向律师提供办理数据出境法律业务方面的一般实务操作指引，而非强制性规定或服务标准，亦不作为律师出具法

律意见或报告的法律依据，仅供律师在实践中参考。

第二条【发布日期】本指引发布于2024年10月27日。

附件 数据出境相关法律、规章、管理清单、标准汇编

1. 《中华人民共和国网络安全法》
2. 《中华人民共和国数据安全法》
3. 《中华人民共和国个人信息保护法》
4. 《促进和规范数据跨境流动规定》
5. 《数据出境安全评估办法》
6. 《数据出境安全评估申报指南（第二版）》
7. 《个人信息出境标准合同办法》
8. 《个人信息出境标准合同备案指南（第二版）》
9. 《关于实施个人信息保护认证的公告》
10. 《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》
11. 《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024年版）》
12. 《中国（上海）自由贸易试验区临港新片区智能网联汽车领域数据跨境场景化一般数据清单（试行）》
13. 《中国（上海）自由贸易试验区临港新片区生物医药领域数据跨境

场景化一般数据清单（试行）》

14.《中国（上海）自由贸易试验区临港新片区公募基金领域数据跨境场景化一般数据清单（试行）》

15.GB/T 43697-2024 《数据安全技术 数据分类分级规则》

16.GB/T 35273-2020 《信息安全技术 个人信息安全规范》

17.GB/T 42574-2023 《信息安全技术 个人信息处理中告知和同意的实施指南》

18.GB/T 39335-2020 《信息安全技术 个人信息安全影响评估指南》

19.TC260-PG-20222A 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范（V2.0-202212）》

20.TC260-PG-20231A 《网络安全标准实践指南—网络数据安全风险评估实施指引（V1.0-202305）》