ICS 35.030
CCS L 78

T/CSAS

团 体 标 准

T/CSAS 0021—2025

数据跨境安全要求

Security requirements for data cross-border

2025-11-28 发布 2025-12-29 实施

四川省网络空间安全协会 发 布

全国团体标准信息平台

目　　次

全国团体标准信息平台

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由四川省网络空间安全协会提出并归口。

本文件起草单位：成都信息工程大学、成都久信信息技术股份有限公司、全域数据信息安全重点联合实验室西南实验室、四川善嘉律师事务所。

本文件主要起草人：白杨、张倩、罗杰、段惺惺、毛伟力、李瑞、赖一阳、杨心一（排名不分先后）。

全国团体标准信息平台

引　言

数据跨境安全要求是明确数据跨境传输、存储和处理全生命周期中的核心安全要求，为组织机构提供可操作的技术与管理规范。通过建立统一的安全基线，有助于平衡数据自由流动与安全保障之间的关系，构建可信、可控、可追溯的跨境数据治理体系。为此，本文件规范了数据跨境的安全框架与原则、法律规制要求、安全流程、安全保障和应急处置要求。

全国团体标准信息平台

数据跨境安全要求

1 范围

本文件给出了个人信息和重要数据出境的安全评估流程、要点和方法。

本文件适用于网络运营者开展的个人信息和一般数据、重要数据出境安全防护以及国家网信部门、行业主管部门组织开展的个人信息和重要数据出境安全管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估方法

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 35273—2020和GB/T 20984—2022中的术语和定义，以及下列术语和定义适用于本文件。

3.1

网络运营者 network operator

网络的所有者、管理者和网络服务提供者。

3.2

境内运营 domestic operation

网络运营者在中华人民共和国境内开展业务，提供产品或服务的活动。

注1：未在中华人民共和国境内注册的网络运营者，但在中华人民共和国境内开展业务，或向中华人民共和国境内提供产品或服务的，属于境内运营。判断网络运营者是否在中华人民共和国境内开展业务，或向中华人民共和国境内提供产品或服务的参考因素包括但不限于：使用中文；以人民币作为结算货币；向中国境内配送物流等；

注2：中华人民共和国境内的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务，且不涉及境内公民个人信息和重要数据的，不视为境内运营。

3.3

个人信息 personal data

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。

注1：个人信息包括姓名、出生日期、公民身份证号、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等；

注2：不包括匿名化处理后的信息。

[来源：GB/T 43697—2024，3.5，有修改]

3.4

敏感个人信息 sensitive personal information

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。

注：敏感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14周岁未成年人的个人信息。

[来源：GB/T 43697—2024，3.6，有修改]

3.5

重要数据　important data

特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

[来源：GB/T 43697—2024，3.2]

3.6

加工处理　data processing

针对个人信息和重要数据实施的操作，包括个人信息和重要数据的收集、存储、访问、修改、转让、披露、匿名化、去标识化、恢复、删除、销毁等。

3.7

数据出境　data cross-border transfer

网络运营者通过网络等方式，将其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，通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。

注1：以下情形属于数据出境：

a）向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据；

b）数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（对境外公开访问的公开信息、网页内容除外）；

c）网络运营者集团内部数据由境内转移至境外，涉及其在境内运营中收集和产生的个人信息和重要数据的；

d）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；

e）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；

f）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。

注2：非在境内运营中收集和产生的个人信息和重要数据经由本国出境，未经任何变动或加工处理的，不属于数据出境；

注3：非在境内运营中收集和产生的个人信息和重要数据在境内存储、加工处理后出境，不涉及境内运营中收集和产生的个人信息和重要数据的，不属于数据出境。

3.8

数据出境安全风险　security risk of data cross-border transfer

数据出境可能对国家安全、经济发展、社会公共利益和个人合法利益带来的风险。

3.9

安全自评估　security self-assessment

网络运营者依照国家相关法律法规和标准的规定，自行组织或委托网络安全服务机构对数据出境开展安全评估。

3.10

主管部门评估　competent authority assessment

国家网信部门、行业主管部门依照国家相关法律法规和标准的规定组织对数据出境开展主管部门评估。

3.11

个人信息主体同意　consent of personal information subject

个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息出境做出明确授权的行为。

4　数据跨境概述

4.1　数据跨境活动

以下情况可视作数据跨境活动的范围：

a）　通过“线上”或“线下”方式将数据传输至境外，或以其他方式使数据“物理”转移到境外的活动；

b）　从境外直接或间接访问位于中国境内的服务器查阅、调取数据；

c）　跨境企业内部数据流动；

d）　向境外关联机构提供数据跨境企业内部数据流动情况。

4.2 数据跨境模型

数据跨境活动的参与方包括：

a) 数据发送方：数据跨境活动的发起者，在境内收集、产生数据的机构，又称境内数据发送方；
b) 数据接收方：境外运营的数据机构、电子商务平台等接收并进行数据处理的机构，包含境外数据接收方；
c) 数据安全管理部门：网络安全、数据治理和信息化发展的核心监管机构。

5 数据跨境安全框架与原则

5.1 数据跨境安全框架

数据跨境活动从境内数据发送方到境外数据接收方，经过安全申报、安全评估、跨境传输、合规监测四个流程，在遵循数据跨境原则基础上，组织数据跨境安全人员进行跨境活动。数据跨境的典型模式如图1所示。

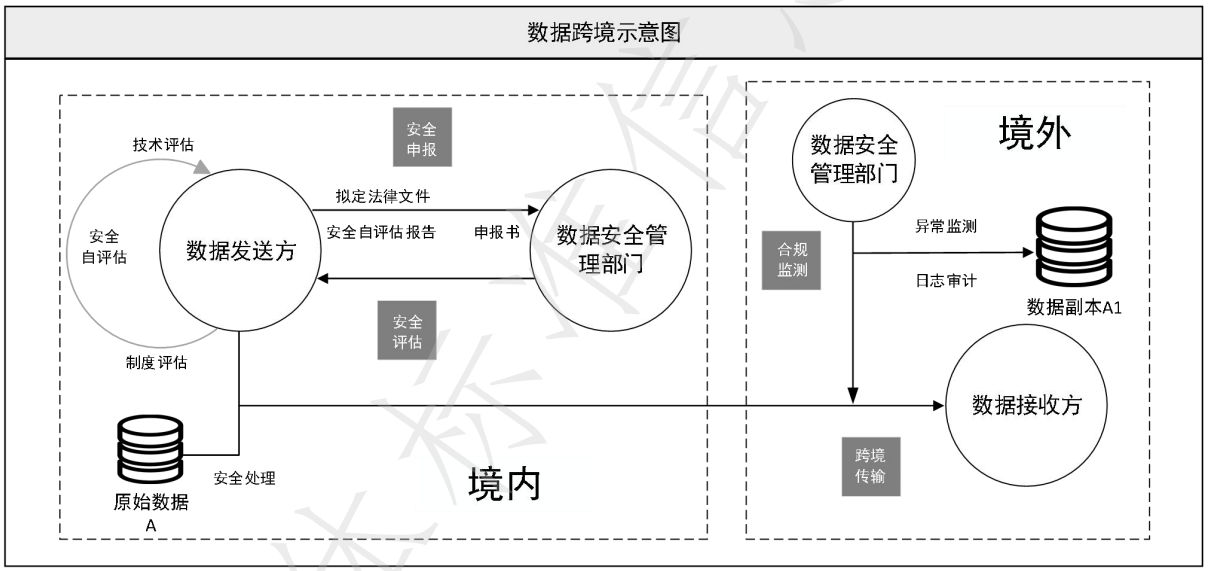

图 1 数据跨境示意图

5.2 数据跨境安全组织人员要求

应在组织内部建立数据跨境安全管理组织，包括数据跨境管理员、数据跨境评估员、数据跨境操作员、数据跨境审计员等岗位角色：

a) 数据跨境管理员应负责数据跨境活动的统筹管理工作；
b) 数据跨境评估员应负责对数据跨境合法性、正当性、安全性、必要性开展评估工作；
c) 数据跨境操作员应负责实际执行数据跨境安全方案编制、数据准备等活动；
d) 数据跨境审计员应负责对数据跨境活动的执行情况进行监督审核；
e) 应设立专业的内部合规团队或聘请外部专业机构，制定数据安全合规相关的制度、规范和流程，并重点管理以下事项：
   1) 应识别需要合规保护的数据资产、拟定隐私相关声明/协议，落实环境检测与合规评估；
   2) 应部署数据流转监测、数据访问管控、数据操作审计等产品；
   3) 应对数据管理流程和控制措施进行全面评估与检查，及时发现潜在的合规风险点，并根据审查结果做出相应调整；
   4) 应在组织内部建立数据跨境相关岗位的持续培训和考核机制且应设立专门的法务团队，负责跟踪法律动态，及时调整数据跨境策略；
   5) 应建立合规性评估机制，定期对数据跨境活动进行全面审查，确保合规性。

5.3 数据跨境原则

5.3.1 合法合规

按照国家级行业相关法律法规要求及数据跨境参与方的有关合同约定开展数据跨境活动。

5.3.2 目的明确

数据跨境活动应具有明确、清晰、具体的数据跨境目的。

5.3.3 分级分类

出境数据按照重要数据、个人信息、一般数据的出境管理要求包括如下：

a) 重要数据出境：经过安全评估认为不会危害国家安全和社会公共利益的，可以出境；
b) 个人信息出境：个人信息处理者可以选择申报数据出境安全评估，通过个人信息保护认证、与境外数据接收方订立个人信息出境标准合同等方式；
c) 不涉及重要数据或者个人信息的一般数据：在履行法律规定的一般性合规义务下，可以依法依规进行跨境流动。

5.3.4 安全可控

数据跨境活动各参与方应具备与所面临的安全风险相匹配的安全保障能力，并采取足够的管理措施和技术手段，保护跨境数据的保密性、完整性及可用性。

5.3.5 权责一致

数据跨境活动各参与方应采取安全技术等必要措施保障跨境数据的安全，并承担因数据跨境造成的数据主体合法权益损害责任。

5.3.6 国别差异化

数据跨境应考虑各国实际数据流通相关法案法规或文化和信仰差异，适情采取相应的安全方案对数据流通进行管控，避免因国别差异导致的违规违法情况。

注：中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供数据的条件等有规定的，可以按照其规定执行。

6 数据跨境法律规制要求

6.1 数据发送方法律规制

因业务需要确需向境外提供数据的，应按照数据安全部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。具体如下：

a) 中华人民共和国境内，关键信息基础设施的运营者在运营中收集和产生的重要数据出境安全管理，适用《中华人民共和国网络安全法》规定；
b) 中华人民共和国境内，其他数据接收方在运营中收集和产生的重要数据出境安全管理办法由国家网信部门会同国务院有关部门制定；
c) 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，可以通过安全评估、个人信息保护认证、与境外数据接收方订立标准合同等多种合规途径实现。

6.2 数据接收方法律规制

数据接收方法律规制要求如下：

a) 应时刻关注数据接收方所在国家或地区的数据安全方面现行的法律法规和标准情况；
b) 应明确数据接收方国家或地区落实数据安全的机制、该国家或地区政府在执法、国防、国家安全等部门调取数据的法律权力；
c) 涉及个人信息及数据出境时，应对数据接收方所在国家或地区的政治法律环境进行评估，并完善内部的数据合规体系。

7 数据跨境安全流程

7.1 数据跨境基本流程

数据跨境应包含数据跨境自评估、数据跨境准备、数据跨境评估、数据跨境传输、跨境数据使用五个关键环节，如图2所示。

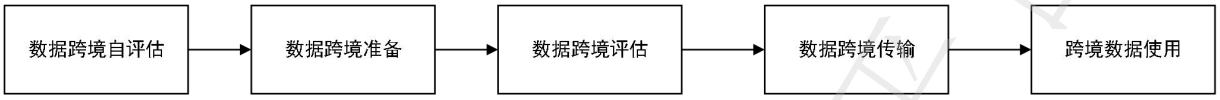

图 2 数据跨境流程图

a) 数据跨境工作流程应覆盖跨境数据发送方、数据接收方、数据安全管理部门；
b) 数据发送方与数据接收方应遵循流程要求，保存各流程产生的文件和记录。

7.2 数据跨境自评估

7.2.1 数据跨境自评估要求

数据跨境自评估要求如下：

a) 数据处理者应明确数据出境及数据接收方处理数据的目的、范围、方式，重点论证是否符合法律要求；
b) 应核查数据接收方所在国家或地区的数据保护政策、网络安全环境，评估其是否达到我国法律和强制性国标要求；
c) 自评估应按照国标对数据进行分类和分级，结合数据规模、敏感程度评估出境风险，分类分级可参考《网络安全等级保护基本要求》《数据分类分级规则》等相关标准；
d) 自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内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），经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。自由贸易试验区内数据处理者向境外提供数据分类分级可参考当地自由贸易试验区印发的负面清单。

注 1：自由贸易试验区内数据处理者向境外提供负面清单外的数据，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。

注 2：自由贸易试验区数据处理者应根据当前政策及法律法规实时调整数据分类分级方法并谨防因政策及法律法规调整而失效的情况。

注 3：一些特殊行业如医疗、测绘、交通等数据跨境应查询行业相关法律规范，部分行业可参考附录A。

7.2.2 一般数据安全评估要求

数据发送方在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：

a) 境内数据接收方和境外数据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、安全性；
b) 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；
c) 境外数据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；
d) 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；
e) 与境外数据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等是否充分约定了数据安全保护责任义务；
f) 其他可能影响数据出境安全的事项。

7.2.3 重要数据安全评估要求

数据出境安全评估应当重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：

a) 数据出境的目的、方式和数据范围，境外数据接收方处理数据的用途、方式等；

b） 数据在境外的保存地点、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；
c） 对于境外数据接收方将出境数据再转移给其他组织、个人的约束性要求；
d） 境外数据接收方因所在国家、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，应采取的安全措施；
e） 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；
f） 其他可能影响数据出境安全的事项。

7.2.4 个人信息安全评估要求

境内数据发送方向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：
a） 境内数据发送方和境外数据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、安全性；
b） 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；
c） 境外数据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；
d） 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；
e） 境外数据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；
f） 其他可能影响个人信息出境安全的事项。

7.3 数据跨境准备

数据处理者向境外提供数据，符合下列条件之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：
a） 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；
b） 关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 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。

7.3.1 数据跨境申报

数据跨境申报要求如下：
a） 数据发送方应按照国家有关规定识别、申报重要数据；
b） 未被相关地区、部门告知或者公开发布为重要数据的，无须将其作为重要数据申报数据出境安全评估；
c） 数据发送方应提前向数据安全管理部门提交相关材料进行申报查验；
d） 申报数据出境安全评估应当提交以下材料：申报书、数据出境风险自评估报告、数据处理者与境外数据接收方拟订立的法律文件、安全评估工作需要的其他材料。

注：安全评估申报材料可参考附录D。

7.3.2 拟出境数据要求

拟出境数要求如下：
a） 应明确数据出境涉及业务、数据资产等情况，并提供数据出境业务说明文档及数据资产清单（包括数据类型、敏感程度、出境范围及关联业务系统）；
b） 应明确数据出境及境外数据接收方处理数据的目的、范围、方式，提供数据出境合同/协议副本及合法性证明文件，说明业务需求合法性、用户同意依据及安全措施有效性；
c） 应明确境外数据接收方所在国家或地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响，提交境外国家/地区数据安全法规风险评估报告及网络安全环境分析，涵盖政治稳定性、执法机构调取风险及数据本地化要求；
d） 应明确境外数据接收方的数据保护水平是否符合中国法律及强制性国家标准，提供境外数据接收方数据保护认证文件（如ISO 27001、GDPR合规声明）及与国内标准的对比分析报告；
e） 应明确拟出境数据在境内存储的系统平台、数据中心（包含云服务）等情况，数据出境链路相关情况，计划出境后存储的系统平台、数据中心等；

f） 应明确数据处理者与境外数据接收方拟订立的法律文件中是否充分约定了数据安全争议解决条款和法律文件安全保护责任义务。

7.3.3 境外接收方要求

境外接收方要求如下：

a） 应明确境外数据接收方基本情况及境外数据接收方处理数据的用途、方式等；
b） 应明确境外数据接收方履行责任义务的管理和技术措施、能力等；
c） 应明确数据出境的目的、方式和数据范围，境外数据接收方处理数据的用途、方式等；
d） 应确保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；
e） 应明确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。

7.4 数据跨境评估

数据安全管理部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。符合下列条件之一的，境内数据发送方可以向境外提供个人信息：

a） 通过数据安全管理部门组织的数据出境安全评估；
b） 按照数据安全管理部门的规定经专业机构进行个人信息保护认证；
c） 按照数据安全管理部门制定的关于企业数据出境标准合同规定；
d） 为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；
e） 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；
f） 为履行法定职责或者法定义务，确需向境外提供个人信息。

注 1：安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估；

注 2：数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

7.5 数据跨境传输

通过数据出境安全评估后，数据发送方向境外提供个人信息和重要数据执行过程中，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等，并严格遵循下列执行要求：

a） 境内数据发送方和境外数据接收方应按照跨境安全方案执行数据跨境操作；
a） 应利用通道加密、数据加密、专线通道等机制保护数据传输过程的安全性，应依据《中华人民共和国密码法》《商用密码管理条例》等对技术应当采取的最低要求进行说明（如对称密码算法采用高级加密标准-128（Advanced Encryption Standard-128, AES-128）及以上强度，非对称密码算法采用李维斯特-沙米尔-阿德曼-2048 （Rivest-Shamir-Adleman, RSA-2048）及以上强度或SM2 算法，密码杂凑算法采用安全Hash算法-256（Secure Hash Algorithm-256, SHA-256）及以上强度或SM3 算法等，密码技术的应用应符合国家密码管理主管部门的要求，确保数据传输过程的安全性、保密性、完整性和不可否认性；
b） 应采用数据加密、数据完整性校验等方式，保证数据传输存储过程中所有数据保密性、完整性；
c） 应在数据传输完成后及时关闭通信接口，并更改或删除接口开放、使用等管控权限；
d） 数据发送方如无需保留原始数据，应及时进行数据删除、销毁，同时采取有效措施防止被删除、销毁的数据复原，并及时清理缓存数据。

7.6 数据跨境使用

数据跨境使用应至少遵循以下要求：

a） 应持续监督接收方的资质、数据安全保障能力及合法合规性，定期通过技术检验、安全审计等方式审查跨境活动及参与方；
b） 数据接收方应依据有关法律法规要求及与数据发送方的合同约定进行数据使用；
c） 接收方数据因使用范围、处理方式或场景变更，需重新获得发送方授权，并应根据情况决定是否重启跨境评估；

d) 数据接收方确保数据安全保护水平不低于约定标准，并配合发送方的监督、审计及合规检查；
e) 通过数据出境安全评估的结果有效期为 3 年，有效期届满前 60 个工作日，可向属地数据安全管理部门申请延期，经批准后延长 3 年。

8 数据跨境安全保障

8.1 技术手段要求

数据安全保障技术手段应包括加密、访问控制、数据脱敏等，且应满足以下要求：

a) 网络安全防护能力应满足GB/T 22239 相应要求或实现同等能力要求；
b) 应对数据跨境的目标地址、流量、内容等开展监控，发现攻击、流量异常、内容违规等情况；
c) 应保留数据出境安全管理全过程的操作行为记录，留存数据跨境流程各环节日志记录，记录粒度细化到操作指令、数据内容变更、访问路径等详细信息，日志仅用于合规审查、审计、调查及法律纠纷应对等用途，采用数字签名、区块链等技术确保不可篡改，实现操作可追溯与责任认定；
d) 应采取有效措施保障数据跨境日志的完整性；
e) 有条件时应采用国家批准的国产密码算法进行加密保护，以增强数据保密性和完整性。

8.2 管理政策要求

管理政策要求如下：

a) 数据发送方应遵循数据分类分级管理制度，按照“一般数据自由流动，重要数据经安全评估后方可出境”的原则开展数据出境管理；
b) 数据发送方应开展风险自评估，重点审查合法性、正当性、安全性、必要性及境外数据接收方安全保障能力，提交自评估报告，并配合数据安全管理部门审查；
c) 数据发送方应结合负面清单及数据安全技术手段构建风险防范、持续监督机制，保障数据安全。

8.3 合规监测要求

数据发送方应建立数据跨境活动的合规监测机制，且至少每年开展一次数据跨境安全审计。数据跨境安全审计工作重点审查数据跨境安全流程的执行情况：

a) 应结合相关法律法规，明确机构自身的业务性质、主体性质和数据性质；
b) 应通过建立数据跨境技术管理措施构建安全保障能力，清晰掌握数据跨境流动详情；
c) 应建立对数据跨境流转过程的监控机制；
d) 应根据威胁情报、结合异常流量分析模型针对加密出境流量进行检测；
e) 应重点对敏感数据进行分析并对重点事件进行留存取证。

注：数据跨境流动合规要点可参考附录B。

8.4 风险评估要求

重要数据的处理者应每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。风险评估报告应当包括下列内容：

a) 网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式，包括数据出境业务类型、境外数据接收方所在国家/地区及联系人信息；
b) 处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点及数据出境链路详情，明确数据出境后是否涉及二次传输及对应风险；
c) 网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性，包括数据出境链路加密方案与境外数据接收方保护措施对比分析；
d) 发现的网络数据安全风险、发生的安全事件及处置情况，涵盖数据出境后发生的风险事件、法律追责依据及合同约定的赔偿责任条款；
e) 提供委托处理、共同处理重要数据的风险评估情况及有关主管部门规定的其他报告内容，包含数据出境后剩余风险分析、数据主权承诺书签署状态及境内数据副本留存方案。

9 数据跨境应急处置要求

9.1 应急预案

应急预案要求如下：

a) 制定数据跨境安全事件应急预案，应包含对数据接收方发生数据泄露、损毁、滥用等安全事件的应急处置、安全事件告知和上报等相关内容；
b) 应根据相关法律法规、安全技术、事件处置经验等及时更新应急响应预案；
c) 应定期组织内部相关人员进行应急响应培训和应急演练。

9.2 应急通告

处理的个人信息发生或者任何可能发生如篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问等情况，数据发送方应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

a) 发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
b) 数据发送方采取的补救措施和个人可以采取的减轻危害的措施；
c) 数据发送方的联系方式；
d) 履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

9.3 应急处理

履行个人信息保护职责的部门应建立跨境应急响应协同机制，包括但不限于与境外监管机构签署合作备忘录、约定数据泄露事件通报流程等，以应对全球化风险场景，履行部门可以采取下列措施：

a) 询问有关当事人，调查与个人信息处理活动有关的情况；
b) 查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；
c) 实施现场检查，对涉嫌违法的个人信息处理活动进行调查；
d) 检查与个人信息处理活动有关的设备、物品。

全国团体标准信息平台

附 录 A
（规范性）
中国特殊行业数据跨境法律规范清单

表A. 1参考自中国一些特殊行业数据跨境法律规范。

表A. 1 中国特殊行业数据跨境法律规范清单

行业	法律规范名称	发布机构	具体要求
金融	《JR/T0171—2020 个人金融信息保护技术规范》	中国人民银行	因业务需要，确需向境外机构提供个人金融信息的，具体要求如下：应符合国家法律法规及行业主管部门有关规定；应获得个人金融信息主体明示同意；应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与数据专业机构的安全要求；应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务
	《中国人民银行数据消费者权益保护实施办法》	中国人民银行	在中国境内收集的消费者金融信息的存储、处理和分析应当在中国境内进行。因业务需要，确需向境外提供消费者金融信息的，应当同时符合以下条件：为处理跨境业务所必需；经金融消费者书面授权；信息接收方为完成该业务所必需的关联机构（含总公司、母公司或者分公司、子公司等）；通过签订协议、现场核查等有效措施，要求境外机构为所获得的消费者金融信息保密；符合法律法规和其他相关监管部门的规定
	《征信业管理条例》	国务院	征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行
交通	《网络预约出租汽车经营服务管理暂行办法》	交通部、工信部等七部委	网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流
医疗	《人口健康信息管理办法（试行）》	卫健委	不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器
出版	《网络出版服务管理规定》	国家新闻出版局、广电总局、工业和信息化部	图书、音像、电子、报纸、期刊出版单位从事网络出版服务，应当具备以下条件：有从事网络出版服务所需的必要的技术设备，相关服务器和存储设备必须存放在中华人民共和国境内
测绘	《地图管理条例》	国务院	互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施

附 录 B
（规范性）
数据跨境合规管控要点清单

表B.1整理了数据跨境合规管控要点清单。

表B.1 数据跨境合规管控要点清单

适用范围	阶段	合规管控要点
数据跨境合规管控关键控制点	跨境前：评估	1.1 数据字段清单梳理
		1.2 数据跨境流转路径识别
		1.3 境外数据接收方识别和能力评估
		1.4 跨境目的的合法性、正当性、安全性、必要性评估
		1.5 跨境字段最小化评估
		1.6 特殊类型数据筛查、拦截（国家秘密、核心数据、个人信息等）
	跨境中：执行	1.7 约定数据发送方与境外数据接收方的数据安全保护责任义务
		1.8 企业内部相关方会签审批
		1.9 向监管机构备案/获得授权
		1.10 相关人员培训
		2.1 加固跨境保障机制（签署跨境转移协议、隐私告知书等）
		2.2 保障传输安全性
		2.3 记录数据处理过程
		2.4 严格管控访问权限
		2.5 监控和防范数据泄漏风险
		2.6 保障数据主体权利响应通道
	跨境后：管理	3.1 目的完成后及时删除/销毁数据
		3.2 如超出目的范围跨境，重新进行合规评估
		3.3 开展数据跨境合规审计

全国团体标准信息平台

附 录 C
（规范性）
需要定期跟踪和反馈的信息表

表C. 1是需要定期跟踪和反馈的信息表。

表C. 1 需要定期跟踪和反馈的信息表

跟踪内容	跟踪频率	负责部门	反馈形式	风险预警触发条件
境外数据接收方数据保护合规状态变更	季度	法务部+数据安全团队	书面报告+会议纪要	收到境外数据接收方监管处罚或违规通知
境外国家/地区数据安全法规政策变化	月度	合规部门	风险提示函	新增数据本地化限制或跨境传输禁令
数据出境链路异常事件	实时	运维部+安全团队	应急响应报告	数据传输中断、未授权访问或加密失效
境外数据接收方数据处理活动审计结果	半年度	第三方审计机构	审计报告	发现数据滥用、泄露或不符合合同约定
境内存储系统备案状态更新	年度	网络安全部	备案状态确认函	云服务商资质到期或数据中心迁移

全国团体标准信息平台

附 录 D
（规范性）
数据出境安全评估申报材料要求表

表D.1是数据出境安全评估申报材料要求表。

表D.1 数据出境安全评估申报材料要求表

序号	材料名称	要求	备注
1	统一社会信用代码证件	影印件加盖公章	
2	法定代表人身份证件	影印件加盖公章	
3	经办人身份证件	影印件加盖公章	
4	经办人授权委托书		
5	数据出境安全评估申报表		使用中文填写
6	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		对数据出境相关约定条款作高亮、线框等显著标识。法律文件以中文版本为准，若仅有非中文版本，须同步提交准确的中文译本
7	数据出境风险自评估报告		使用中文撰写
8	其他相关证明材料		
注：采用线下方式提交申报材料的数据处理者，需同步通过光盘提交相应电子版材料			

全国团体标准信息平台

参 考 文 献

[1] GB/T 22239 信息安全技术 网络安全等级保护基本要求
[2] GB/T 43697—2024 数据安全技术 数据分类分级规则
[3] 《中华人民共和国网络安全法》（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过，自2017年6月1日起施行）
[4] 《中华人民共和国密码法》（2019年10月26日第十三届全国人民代表大会常务委员会第十四次会议通过，自2020年1月1日起施行）
[5] 《中华人民共和国数据安全法》（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过，自2021年9月1日起施行）
[6] 《中华人民共和国个人信息保护法》（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过，自2021年11月1日起施行）
[7] 《促进和规范数据跨境流动规定》（2023年11月28日国家互联网信息办公室2023年第26次室务会议审议通过，自公布之日起施行）

全国团体标准信息平台

四 川 省 网 络 空 间 安 全 协 会

团 体 标 准

数据跨境安全要求

T/CSAS 0021—2025

*

中国轻工业出版社出版

地址：北京鲁谷东街 5 号

邮政编码：100040

发行电话：(010)85119832

网址：http://www.chlip.com.cn

Email：club@chlip.com.cn

*

版权所有　侵权必究

书号：155019·7159

印数：1—200 册　　定价：64.00 元

全国团体标准信息平台