

团 体 标 准

T/ISC 0046—2024

数据跨境流通安全技术要求

Technical requirements for security of cross-border data flow

2024-06-12 发布

2024-07-12 实施

中 国 互 联 网 协 会 发 布

目次

前言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 缩略语..... 1

5 数据跨境流通概述..... 2

 5.1 数据跨境流通活动..... 2

 5.2 数据跨境流通模式..... 2

 5.3 数据跨境流通风险..... 2

6 数据跨境安全原则..... 2

 6.1 合法合规..... 2

 6.2 目的明确..... 2

 6.3 最小必要..... 2

 6.4 安全可控..... 2

 6.5 权责一致..... 2

7 数据跨境流通安全流程..... 3

 7.1 基本流程..... 3

 7.2 数据跨境流通安全评估..... 3

 7.3 数据跨境流通准备..... 4

 7.4 数据跨境执行..... 4

 7.5 跨境数据存储..... 4

 7.6 跨境数据使用..... 5

 7.7 跨境数据销毁..... 5

8 数据跨境安全保障..... 5

 8.1 外部环境..... 5

 8.2 制度体系..... 6

 8.3 组织人员..... 6

 8.4 技术能力..... 6

 8.5 监督检查..... 6

 8.6 应急处置..... 6

参考文献..... 8

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。

本文件由奇安信科技集团股份有限公司提出。

本文件由中国互联网协会归口。

本文件起草单位：奇安信科技集团股份有限公司、桂林电子科技大学、智研高科（北京）信息技术有限公司、国科华创认证有限责任公司、上海计算机软件技术开发中心、运易通科技有限公司、北京万里红科技有限公司、北京大学长沙计算与数字经济研究院、联通数字科技有限公司、东软集团股份有限公司、清华大学丘成桐数学科学中心、数力聚（北京）科技有限公司、中科信息安全共性技术国家工程研究中心有限公司、北京政务信息安全保障中心（北京信息安全测评中心）、中国电信数据发展中心。

本文件主要起草人：安锦程、孔坚、李春海、杨昌松、梁海、张礼、杨小琴、刘振宇、张孟、刘海峰、刘利、江海昇、王巧丽、周昌令、唐源、刘建国、李冰、李凡、杨硕、丁津泰、李乐平、杨晨光、付昆、曹国华、刘元、李媛、高琦、姜晨、刘前伟、黄亮、刘洋、胡建勋、许宏伟。

数据跨境流通安全技术要求

1 范围

本文件规定了数据跨境的模式、基本原则、基本流程，以及跨境过程中相关方的行为准则与信息安全保障措施。

本文件适用于开展数据跨境活动的相关机构参考使用，并为数据跨境活动的相关机构信息安全控制措施的部署提供指导。

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 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者其他方式对信息的记录。

3.2

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，不包括匿名化处理后的信息。

[来源：GB/T 35273—2020，3.6]

3.3

重要数据 important data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

[来源：GB/T 41479—2022，3.9]

3.4

数据跨境活动 data cross-border activities

将境内收集或产生的数据通过网络传输方式提供给境外机构的一次性或连续性活动。

3.5

数据跨境评估 data cross-border transmission assessment

对数据和数据处理活动的安全风险和违法违规问题进行检测评估的过程。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

5 数据跨境流通概述

5.1 数据跨境流通活动

本文件所述数据跨境活动是指在中华人民共和国境内（不含香港、澳门）收集或产生的数据通过网络传输方式提供给境外机构的一次性或连续性活动。

5.2 数据跨境流通模式

数据跨境活动的参与方包括：

- 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；
- 数据接收方：境外运营的接收并进行数据处理的机构；
- 境外数据处理相关方：通过数据接收方间接参与跨境数据处理的境外机构。

5.3 数据跨境流通风险

数据跨境流通风险是指数据跨境活动可能对国家安全、社会利益、个人权益等造成的不良影响，包括但不限于：

- a) 数据提供风险：数据发送方提供数据的行为可能损害自身、客户及相关方权益等，包括行为造成的风险和数据内容造成的风险；
- b) 数据传输风险：数据传输过程中存在数据损坏、篡改、泄露等风险；
- c) 数据存储风险：数据出境后，存在接收方、数据处理相关方因数据存储不当或数据安全保障措施落实不到位等造成的数据泄露风险；
- d) 数据使用风险：数据出境后，存在未经授权的访问、修改、转让、共享等安全风险。

6 数据跨境安全原则

6.1 合法合规

数据跨境活动的开展按照国家及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。

6.2 目的明确

数据跨境活动具有明确、清晰、具体的数据跨境目的。

6.3 最小必要

数据跨境活动所使用的数据为完成当前跨境业务所需要的最少数据类型和数据量。

6.4 安全可控

数据跨境活动各参与方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。

6.5 权责一致

数据跨境流通活动各参与方采取安全技术等必要措施跨境数据的安全，并承担因数据跨境造成的数据主体合法权益损害责任。

7 数据跨境流通安全流程

7.1 基本流程

数据跨境流通包含数据跨境评估、数据跨境准备、数据跨境执行、数据跨境完成、跨境数据使用五个关键环节，见图 1。工作流程覆盖跨境数据发送方、数据接收方及数据处理相关方。

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。

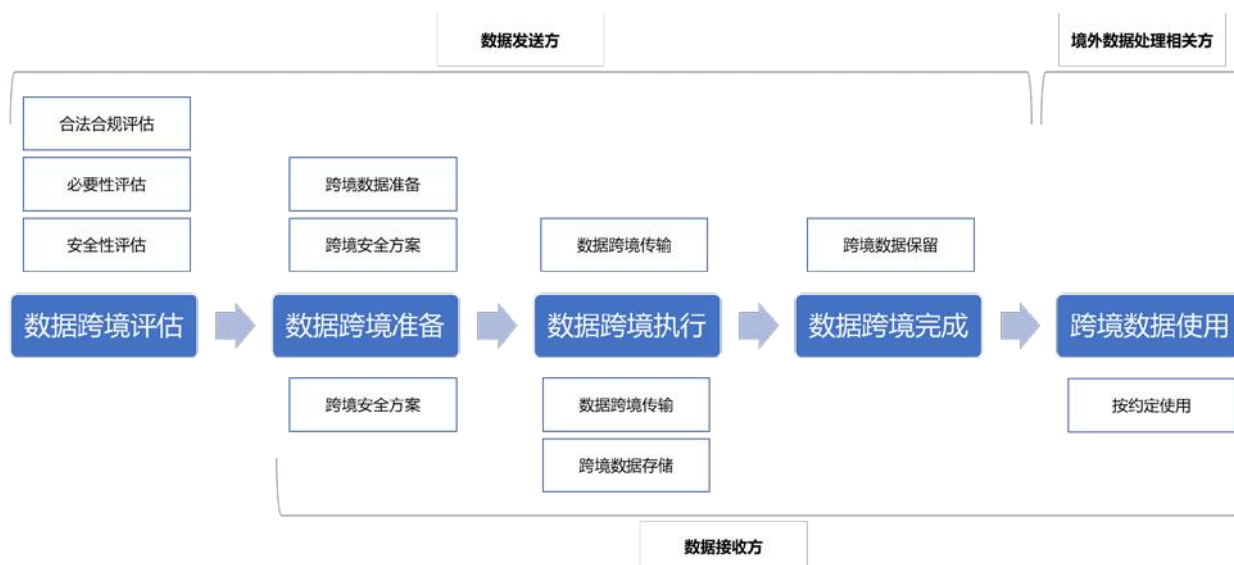


图 1 数据跨境流程

7.2 数据跨境流通安全评估

数据跨境需求是数据跨境流程启动的条件。跨境流程启动后，应首先开展数据跨境评估，为后续数据跨境活动是否能够开展提供必要的判断依据。

- 数据跨境评估流程参考《数据出境安全评估办法》执行。
- 数据跨境评估应在数据跨境活动开始前，或数据跨境目的、业务、数据范围、数据类型、数据量等发生较大变化、数据接收方变更或发生重大安全事件时开展。数据跨境评估的内容包括但不限于：
 - 合法合规评估。根据数据跨境中所涉及的业务、数据、数据处理机构及相关数据处理活动，识别该数据跨境活动相关法律法规和监管部门要求并开展评估。
 - 必要性评估。数据跨境必要性包括但不限于：业务开展的必要性；所提供数据类型、数量的必要性；履行机构合同义务所必需；履行我国与其他国家和地区、国际组织等签署的条约、协议所必需；其他维护网络空间主权和国家安全、经济发展、社会公共利益和保护公民合法权益所需。
 - 安全性评估。根据数据跨境中所涉及的数据类型、重要/敏感程度、数量、频率、范围以及数据接收方安全保障能力等开展数据跨境安全性评估。应从国家安全、经济稳定，以及数据一旦泄露将对社会稳定与公众利益造成损害的等方面评价数据跨境安全。
- 应根据数据跨境评估结果，对数据跨境活动的开展进行调整：

- 1) 数据跨境各项评估均通过后，可开展数据跨境准备活动；
- 2) 合法合规或必要性评估不通过的，禁止开展数据跨境活动；
- 3) 安全性评估不通过的，应进行安全策略检查或更正，并重新开展数据安全性评估。

7.3 数据跨境流通准备

数据发送方和数据接收方应协同制定安全、合理、可操作的数据跨境安全方案。

- a) 数据跨境安全方案包括但不限于：
 - 数据出境的原因、目的、时间；
 - 跨境数据的类型、数量、频率、范围等信息；
 - 数据的跨境传输及使用方式、范围、场景、注意事项等；
 - 数据发送方、接收方的安全保障能力和安全责任；
 - 跨境数据安全相关保障措施。
- b) 数据发送方应依据数据跨境安全方案开展数据准备。应对准备的数据和相关信息系统采取有效安全措施，防止数据泄露等风险。宜采取双人控制的方式开展数据准备和结果确认。
- c) 数据发送方在跨境传输个人信息时，应告知个人信息主体开展个人信息跨境活动的数据发送方和数据接收方的基本情况，包括名称或者姓名、联系方式、向境外提供个人信息的目的、类型、处理方式、保存期限，以及行使个人信息主体权利的方式和程序等事项，但是法律、行政法规规定不需要告知的除外；基于个人同意向境外提供个人信息的，数据接收方应当取得个人信息主体的单独同意，涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律行政法规规定应当取得书面同意的，应当取得书面同意。

7.4 数据跨境执行

数据发送方和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；
- b) 应对通信双方（包括机构、接口、设备、系统等）进行身份验证，并通过数字签名等方式保证数据传输抗抵赖性；
- c) 应采用数据加密、数据完整性校验等方式，保证数据存储过程中所的数据保密性、完整性；
- d) 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；
- e) 应对跨境数据建立有效的访问控制机制，宜进行字段级访问控制；
- f) 数据发送方采用 API 方式进行跨境数据传输的，应当对传输数据的 API 进行风险监测，包括对信息采集、信息预处理、信息识别策略配置、分析告警等进行监测。

7.5 跨境数据存储

跨境数据存储符合以下要求：

- a) 数据接收方存储数据时，应按要求采取安全措施并以合同进行约定；
- b) 数据接收方存储重要数据和个人信息等敏感网络数据，应采用加密、安全存储、访问控制、安全审计等安全措施；
- c) 数据接收方存储重要数据和个人信息，不应超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期；
- d) 数据接收方存储个人生物特征识别信息的，应采取不低于 GB/T 35273—2020 中 6.3b) 和 c) 的要求及生物特征识别信息保护相关国家标准的技术要求。

7.6 跨境数据使用

跨境数据使用应符合以下要求：

- a) 数据发送方应对数据接收方的资质、数据安全保障能力、数据使用合法合规等进行持续的监督和检查；
- b) 数据发送方应采用技术检验、安全审计等方式定期对数据跨境活动及各参与方进行数据安全审查；
- c) 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；
- d) 数据接收方数据使用超出约定使用范围、处理方式及使用场景等发生变化时，应事先获得数据发送方的二次授权，数据发送方应根据数据使用方式的变化情况确定是否重新开展数据跨境评估；
- e) 数据接收方应确保同一数据始终处于与事先约定同等或更高的安全保障能力，数据跨境安全保障能力见第7章要求；
- f) 数据接收方应接受和配合数据发送方进行数据安全合规使用、审计等监督和审核工作；
- g) 数据接收方应履行数据保护义务，并采取合约协议、技术检验等方式，对数据处理相关方进行约束和管理，防止数据泄露、滥用等风险；
- h) 数据接收方应采用合约协议、安全检查、安全评估等方式对数据处理相关方进行约束和管理，并明确有关数据安全保护责任和义务。

7.7 跨境数据销毁

跨境数据销毁应符合以下要求：

- a) 数据发送方应在达到数据安全方案约定的保存期限、约定目的完成或者法律文件终止后，要求数据接收方销毁跨境数据；
- b) 数据接收方应建立数据销毁安全管理制度和数据销毁审批机制，设置销毁相关监督角色，监督操作过程；
- c) 如无特殊情况，数据传输相关终端设备、移动应用、前端业务系统等，不应留存跨境数据（特别是重要/敏感信息相关数据），并应及时对缓存数据进行清理；
- d) 数据接收方对软件系统层数据进行销毁时，应采用将数据库中存储的结构化数据删除或置空，或通过操作系统的图形操作界面、命令或者调用接口对数据所在的文件执行删除操作等技术方式；
- e) 数据接收方对闪存、硬盘、磁带、光盘等存储介质中的数据进行销毁时，采用消磁、粉碎等方法和技术；
- f) 数据接收方对重要数据进行销毁时，应采取重复消除与消磁、粉碎等相结合的数据销毁方法，防止被重标识、重关联或非授权使用和泄露等；
- g) 数据接收方应保留销毁过程的有关记录，并提交给数据发送方。

8 数据跨境安全保障

8.1 外部环境

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，该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，该国家或地区与其

他国家或地区之间有关数据流通、共享等方面的双边或多边协定进行评估。涉及个人信息及业务数据出境时，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。

8.2 制度体系

应建立数据跨境安全管理体系，包括但不限于：

- a) 安全策略：应包含数据跨境总体原则、框架等；
- b) 安全管理制度：应包含数据跨境安全流程、组织人员、网络环境安全等；
- c) 数据跨境记录：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，建立数据跨境活动清单。

8.3 组织人员

应建立组织人员保障体系，包括但不限于：

- a) 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，并至少承担以下工作：
 - 数据跨境管理员负责数据跨境活动的统筹管理工作；
 - 数据跨境评估员负责对数据跨境合法合规、必要性、安全性开展评估工作；
 - 数据跨境操作员负责实际执行数据跨境安全方案编制、数据准备等活动；
 - 数据跨境审计员负责对数据跨境活动的执行情况进行监督审核。
- b) 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。

8.4 技术能力

应建立数据跨境的技术能力体系，包括但不限于：

- 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) 应采取有效措施保障数据跨境日志的完整性；
- d) 在满足当地法律法规要求基础上，数据跨境业务系统日志应保存 6 个月以上；
- e) 应依据本行业数据安全有关标准建立数据全生存周期防护机制。

8.5 监督检查

应建立数据跨境活动的监督检查机制，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。

8.6 应急处置

8.6.1 应急预案

应建立数据安全跨境风险的应急预案体系，包括但不限于：

- a) 应制定数据跨境安全事件应急预案，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。

8.6.2 应急响应

发生数据跨境安全事件时，应及时采取有关措施，包括但不限于：

- a) 将数据跨境安全事件告知受影响的相关方；
- b) 按照国家有关规定向行业主管部门上报；
- c) 临时中断数据跨境或其他减缓损失的措施；
- d) 应详细记录数据跨境安全事件发生的时间、数据类型、数量、范围、可能造成的影响、已采取的处置措施、事件处置相关人员的联系方式等信息；
- e) 应采用相关数据安全追溯溯源技术，及时发现并截断攻击路径。

参 考 文 献

- [1]GB/T 20984 信息安全技术 信息安全风险评估方法
 - [2]GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
 - [3]GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
 - [4]GB/T 41479—2022 信息安全技术 网络数据处理安全要求
 - [5]JR/T 0071.2—2020 金融行业网络安全等级保护实施指引 第2部分：基本要求
 - [6]JR/T 0223—2021 金融数据安全 数据生命周期安全规范
 - [7]YD/T 3801—2020 电信网和互联网数据安全风险评估实施方法
 - [8]中华人民共和国数据安全法（2021年6月10日 中华人民共和国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）
 - [9]中华人民共和国个人信息保护法（2021年8月20日 中华人民共和国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）
 - [10]中华人民共和国个人信息保护法（2016年11月7日 中华人民共和国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）
-