

企业数据出境安全合规管理指南

Enterprise outbound data transfer security compliance management guidelines

（征求意见稿）

XXXX – XX – XX 发布

XXXX – XX – XX 实施

目 次

前 言..... I

引 言..... III

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 总体流程..... 2

5 适用主体要求..... 3

 5.1 企业范围..... 3

 5.2 出境行为..... 3

6 数据出境工作准备..... 3

 6.1 出境数据基本情况分析..... 4

 6.2 豁免情形分析..... 4

 6.3 成立数据出境安全合规工作组..... 4

7 数据出境路径选择..... 4

 7.1 概述..... 4

 7.2 数据出境安全评估情形..... 6

 7.3 个人信息出境标准合同情形、个人信息出境个人信息保护认证情形..... 6

8 数据出境合规实施..... 6

 8.1 申报数据出境安全评估..... 6

 8.2 订立个人信息出境标准合同备案..... 8

 8.3 通过个人信息出境个人信息保护认证..... 8

 8.4 申报负面清单备案..... 9

 8.5 便利化措施..... 10

9 企业数据安全能力建设..... 10

 9.1 管理制度和操作规程..... 10

 9.2 安全技术措施..... 10

 9.3 人员管理措施..... 10

 9.4 安全事件应急处理..... 10

10 数据出境事后管理..... 11

 10.1 境外接收方安全防护承诺..... 11

 10.2 境外接收方合同履行情况..... 11

 10.3 认证持续监督..... 11

附 录 A （资料性） 数据安全评估要点..... 12

附 录 B （资料性） 跨境业务场景所涉个人信息示例表..... 14

附 录 C （资料性） 中国（天津）自由贸易试验区分类分级参考规则..... 15

附 录 D （资料性） 敏感个人信息类别表..... 21

参 考 文 献..... 22

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。

本文件由天津市互联网信息办公室提出并归口。

本文件起草单位：

本文件主要起草人：

引 言

国家高度重视数据跨境流动工作，《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全条例》在法律、行政法规层面对数据处理者向境外提供重要数据和个人信息作出了明确规定，国家互联网信息办公室也相继出台了《数据出境安全评估》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》等相关政策文件，为数据跨境流动安全管理提供具体的实施路径。同时，中国（天津）自由贸易试验区（以下简称“天津自贸试验区”）按照《促进和规范数据跨境流动规定》有关要求，研制并发布了《中国（天津）自由贸易试验区数据出境管理清单（负面清单）》（以下简称“《负面清单》”），为天津自贸试验区企业数据跨境流动提供便利性。

本文件结合国家有关部门发布的政策文件，针对企业数据出境场景，提出数据出境安全合规流程，将数据出境安全评估、个人信息出境标准合同、个人信息保护认证，以及《负面清单》等内容进行了汇聚融合，提供了统一指引。结合企业数据出境安全合规实际情况，给出强化事前事中事后全链条安全管理要求。

企业数据出境安全合规管理指南

1 范围

本文件给出了企业数据出境安全合规的实施流程，数据出境情形下企业的安全能力要求。

本文件适用于天津企业数据出境安全合规活动，也适用于有关主管部门实施数据出境安全检查评估时参考。

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 22239	信息安全技术	网络安全等级保护基本要求
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 39204	信息安全技术	关键信息基础设施安全保护要求
GB/T 39335	信息安全技术	个人信息安全影响评估指南
GB/T 43697	数据安全技术	数据分类分级规则
GB/T 45389	数据安全技术	数据安全评估机构能力要求
GB/T 45574	数据安全技术	敏感个人信息处理安全要求
GB/T 45577	数据安全技术	数据安全风险评估方法

3 术语和定义

GB/T 25069-2022界定的以及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

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

[来源：GB/T 45577—2025, 3.2]

3.3

重要数据 key data

特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，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。

[来源：GB/T 43697—2024, 3.2，有修改]

3.4

一般数据 general data

核心数据、重要数据之外的其他数据。

[来源：GB/T 43697—2024, 3.4]

3.5

数据安全风险 data security risk

数据安全事件的发生可能性及其对国家安全、公共利益或者组织、个人合法权益造成的损害。

[来源：GB/T 45577—2025, 3.6]

3.6

个人信息 personal information

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。

[来源：GB/T 45574—2025, 3.1]

3.7

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、不满十四周岁的未成年人的个人信息以及其他敏感个人信息。

[来源：GB/T 45574—2025, 3.2]

3.8

业务 business

组织为实现某项发展规划而开展的运营活动。

注：该活动具有明确的目标，并延续一段时间。

[来源：GB/T 20984—2022, 3.1.4]

3.9

数据出境 outbound data transfer

企业向境外提供在中华人民共和国境内运营中收集和产生的数据。

3.10

数据出境风险自评估 outbound data transfer self-assessment

由评估对象所有者自身发起，组成机构内部评估小组或委托第三方机构参与，依据国家有关法规与标准，对评估对象的数据出境情况进行风险评估的活动。

3.11

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022, 3.1]

4 总体流程

企业数据出境安全合规流程，主要包括数据出境工作准备、数据出境合规路径选择、数据出境合规实施、企业安全能力建设、数据出境安全监督等阶段，图1明确了各阶段包括的内容和关系：

- a) 数据出境工作准备：包括开展数据出境行为分析、豁免情形分析、成立数据出境安全合规工作组，详细内容见第 6 章；
- b) 数据出境路径选择：包括申报数据出境安全评估情形、订立个人信息出境标准合同情形、申请个人信息出境个人信息保护认证情形，详细内容见第 7 章；
- c) 数据出境合规实施：包括申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息出境个人信息保护认证，以及便利化措施等，详细内容见第 8 章；
- d) 企业安全能力建设：包括管理制度和操作规程、安全技术措施、人员管理措施、安全事件应急处理等，详细内容见第 9 章；
- e) 数据出境安全监督：包括境外接收方安全防护承诺、境外接收方合同履行情况、安全认证持续监督，详细内容见第 10 章，企业安全能力评估和数据出境安全管理评估可参考附录 A。

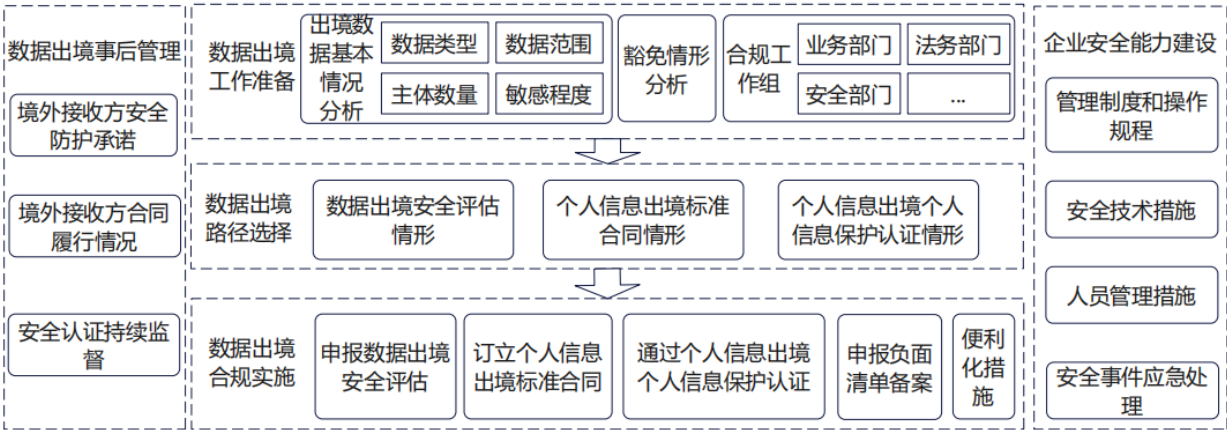


图1 企业数据出境安全合规总体框架

5 适用主体要求

5.1 企业范围

企业按照本文件开展数据出境活动的，应满足以下要求：

- a) 在天津市内登记注册、开展数据跨境流动等相关活动的企业；
- b) 若适用《负面清单》，应在天津市自由贸易试验区内登记注册、开展数据跨境流动等相关活动的企业，事业单位、机构、团体或其他组织可参照执行；
- c) 未被相关部门、地区告知为关键信息基础设施运营者的，企业不需要作为关键信息基础设施运营者申报数据出境安全评估；
- d) 未被相关部门、地区告知或者公开发布为重要数据的，企业不需要作为重要数据申报数据出境安全评估。

5.2 出境行为

企业按照本文件开展数据出境活动的，数据出境活动应属于以下情形：

- a) 企业将在境内运营中收集和产生的数据传输至境外；
- b) 企业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；
- c) 在境外分析、评估境内自然人的行为等数据处理活动。

6 数据出境工作准备

6.1 出境数据基本情况分析

有数据出境需求的企业应进行出境数据基本情况分析，以便在开展数据出境合规工作前明确数据出境合规路径，分析内容包括但不限于：

- a) 涉及的个人信息情况，包括个人信息的类型、数量、范围和敏感程度等；
- b) 按照 GB/T 45574—2025 的要求判定是否存在敏感个人信息，明确敏感个人信息数量；
- c) 涉及的重要数据情况，包括重要数据的类型、数量和范围等。重要数据的判定参考相关行业领域政策法规标准，如《工业领域重要数据识别指南》《电信领域重要数据识别指南》《汽车数据安全 安全管理若干规定（试行）》和 GB/T 43697—2024 附录 G 等。

6.2 豁免情形分析

符合以下条件之一的，可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，企业数据可直接出境：

- a) 向境外提供的数据中不包含个人信息或者重要数据的；
- b) 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；
- c) 属于天津自贸试验区企业，且出境数据不在《负面清单》所列领域的出境数据范围内的；
- d) 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；
- e) 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，所涉个人信息示例参照附录 B；
- f) 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；
- g) 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；
- h) 国家和天津市其他法律法规另有规定的。

6.3 成立数据出境安全合规工作组

若企业符合 6.2 节条件的，企业可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等；若企业不符合 6.2 节条件的，企业在数据出境前，应建立数据出境安全合规工作组（临时工作组），主要负责数据出境路径选择、数据出境合规实施以及数据出境安全监督等工作，工作组应满足以下要求：

- a) 工作组组长应为企业数据安全负责人或个人信息保护负责人，能有效协调业务、技术和安全部门；
- b) 工作组成员应包括企业法务、安全、技术、业务等相关部门人员；
- c) 工作组可委托第三方机构，第三方机构选择标准可参考 GB/T 45389—2025 中的相关要求。

7 数据出境路径选择

7.1 概述

数据出境安全合规工作组应针对数据的类型、数量、范围、敏感程度，根据《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》，参考《中国（天津）自由贸易试验区分级参考规则》（附录 C），选择数据出境方式。

针对同一领域，如果已经有其他自贸试验区发布负面清单，天津自贸试验区可参照执行，其他自贸试验区负面清单包括：《中国（北京）自由贸易试验区数据出境管理清单（负面清单）》《中国（上海）自由贸易试验区及临港新片区数据出境管理清单（负面清单）》《海南自由贸易港数据出境管理清单（负面清单）》《中国（浙江）自由贸易试验区数据出境管理清单（负面清单）》等。

企业应按照数据出境情况，参考图 2 判定流程选择数据出境路径，包括以下步骤判定：

- a) 豁免情形判定：企业应按照 6.2 确定是否属于直接出境情形；
- b) 自贸试验区判定：企业应明确申报主体是否注册在已发布《负面清单》天津自贸试验区范围内；
- c) 关键信息基础设施运营者判定：企业应明确是否被行业主管部门划分为关键信息基础设施运营者；
- d) 重要数据判定：企业应明确拟出境数据是否被行业主管部门或地区划分为重要数据；
- e) 敏感个人信息判定：企业应明确拟出境数据中是否涉及敏感个人信息，敏感个人信息范围可参考附录 D；
- f) 个人信息数量判定：企业若出境的数据包含个人信息，应明确拟出境个人信息规模，该规模按照自然人（去重）统计。

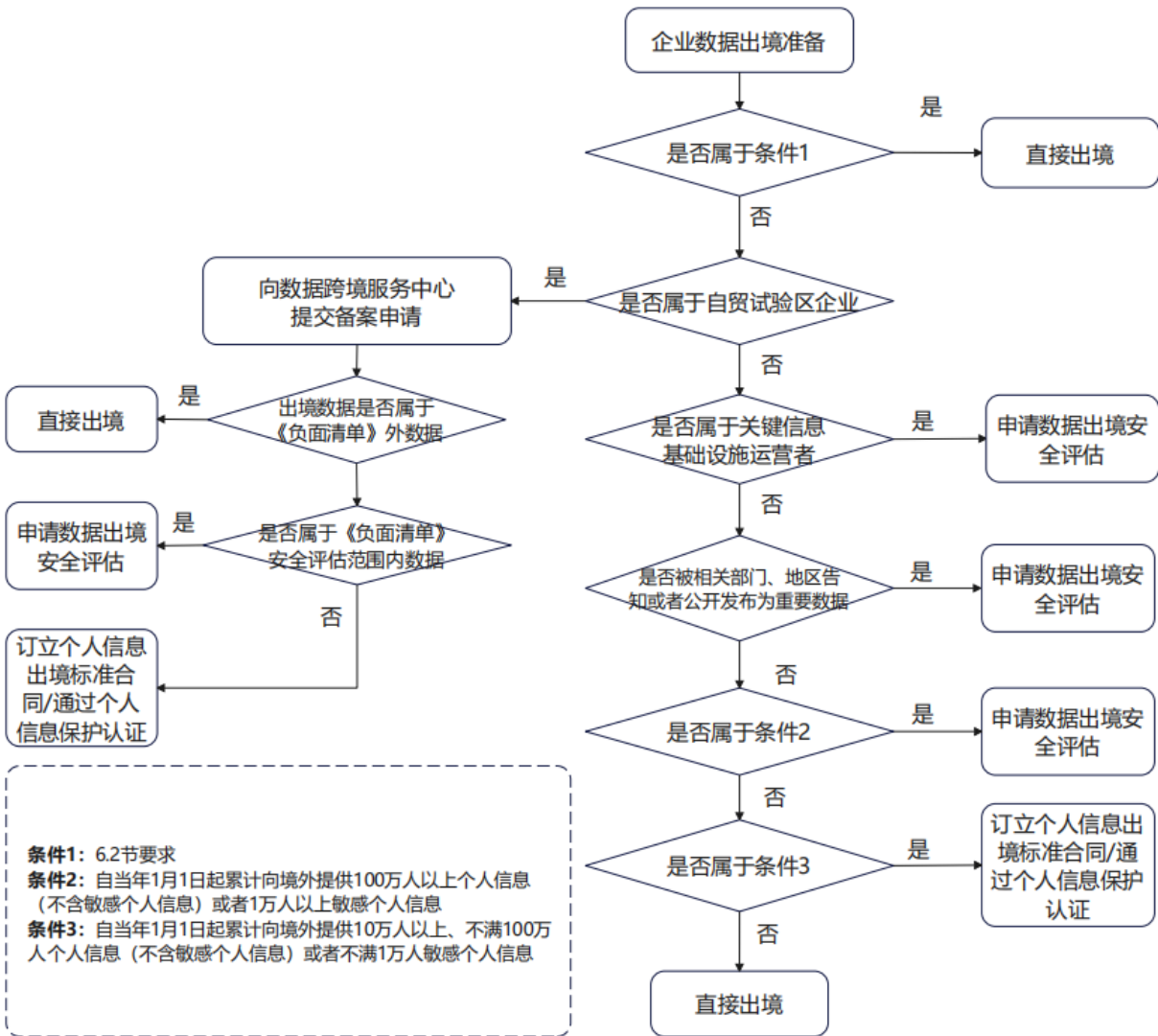


图2 数据出境路径判定流程

7.2 数据出境安全评估情形

7.2.1 非自贸试验区企业

非自贸试验区企业应符合以下要求之一：

- 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企业向境外提供重要数据；
- c) 关键信息基础设施运营者以外的企业自当年 1 月 1 日起累计向境外提供 100 万以上个人信息（不含敏感个人信息）或者 1 万人敏感个人信息。

7.2.2 自贸试验区企业

自贸试验区企业出境数据属于《负面清单》中需要通过数据出境安全评估数据清单的，应通过数据出境安全评估，以下情况除外：

- a) 战略物资和大宗商品类数据中企业在商务谈判、进出口贸易等商业活动中产生的数据；
- b) 已由气象、水利、自然资源等相关部门公开发布的数据；
- c) 工业类数据中企业在商务谈判、进出口贸易等商业活动中产生的数据；
- d) 已由统计等相关部门公开发布的数据；
- e) 已由广电等相关部门公开发布的行业管理数据；
- f) 已依法公开的知识产权数据；
- g) 属于 6.2 情形的。

7.3 个人信息出境标准合同情形、个人信息出境个人信息保护认证情形

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 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，企业订立个人信息出境标准合同或者通过个人信息保护认证。

注：属于 6.2 情形的除外。

8 数据出境合规实施

8.1 申报数据出境安全评估

8.1.1 评估实施流程

申报数据出境安全评估实施流程包括开展数据出境风险自评估、材料提交、材料查验及反馈评估结果、重新申报数据出境安全评估、延长评估结果有效期等环节，具体流程包括：

- a) 风险自评估：企业在申报数据出境安全评估前，应开展数据出境风险自评估；
- b) 线上申报：企业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>；
注：系统网址为国家互联网信息办公室官网“全国网信政务办事大厅”专栏的“数据出境申报系统”，如系统网址存在变更，可参考“全国网信政务办公大厅”专栏或国家网信部门的有关通知。
- c) 线下申报：企业属于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，采用线下方式通过天津市网信部门向国家网信部门申报数据出境安全评估；
- d) 材料查验：需要补充或者更正申报材料的，企业应当按照告知要求及时补充或者更正材料；
- e) 评审结果：企业应当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；
- f) 申请复评：企业对评估结果有异议的，可以在收到评估结果通知书 15 个工作日内向国家网信

部门申请复评，复评结果为最终结论；

- g) 延长评估结果：企业通过数据出境安全评估结果有效期届满，满足 8.1.5 条件的企业，可提出延长评估结果有效期申请。

8.1.2 数据出境风险自评估

数据出境风险自评估应重点评估以下事项：

- a) 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；
- 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（以下统称法律文件）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。

8.1.3 材料提交

企业申报数据出境安全评估，应当按照国家网信部门最新发布的《数据出境安全评估申报指南》提交材料。

8.1.4 重新申报数据出境安全评估

通过数据出境安全评估的企业，在有效期内出现以下情形之一的，应当重新申报数据出境安全评估：

- a) 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；
- b) 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；
- c) 出现影响出境数据安全的其他情形。

8.1.5 延长评估结果有效期

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。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，企业可以在有效期届满前60个工作日内通过天津市网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期3年。

满足以下条件的企业，可认为未发生需要重新申报数据出境安全评估情形：

- a) 数据出境的目的、范围等未发生变化；
- b) 数据处理者和境外接收方等未发生变化；
- c) 出境个人信息的，未来三年涉及自然人数量增幅不超过原评估结果准予过去三年出境数量的20%；
- d) 出境重要数据的，未来三年出境数据规模（MB/GB/TB）增幅不超过原评估结果准予过去三年出境数据规模的20%；
- e) 与境外接收方订立的法律文件符合《数据出境安全评估办法》第九条规定；

f) 过去三年数据出境活动严格按照评估结果通知书合规开展，且未发生重大数据安全事件。

8.2 订立个人信息出境标准合同备案

8.2.1 备案实施流程

个人信息出境标准合同备案流程包括个人信息保护影响评估、材料提交、材料查验及反馈备案结果、补充或者重新备案等环节，具体流程包括：

- a) 个人信息保护影响评估：企业在提交个人信息出境标准合同备案材料前，应开展个人信息保护影响评估，并形成影响评估报告；
- b) 线上申报：企业通过数据出境申报系统提交备案材料，系统网址为 <https://sjcj.cac.gov.cn>；
- c) 材料查验：需要补充完善材料的，企业应按要求提交补充完善材料；
- d) 备案结果：企业获取备案通知书，并按照签署合同的要求开展个人信息出境活动。

8.2.2 个人信息保护影响评估

个人信息保护影响评估应评估以下内容：

- a) 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；
- 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。

8.2.3 材料提交

企业备案标准合同，应按照国家网信部门最新发布的《个人信息出境标准合同备案指南》提交材料。

8.2.4 材料查验及反馈备案结果

需要补充完善材料的，企业应当在10个工作日内提交补充完善材料。

8.2.5 补充或者重新备案

在标准合同有效期内出现下列情形之一的，企业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：

- a) 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；
- b) 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；
- c) 可能影响个人信息权益的其他情形。

企业在标准合同有效期内补充订立标准合同的，应当向天津市网信部门提交补充材料；重新订立标准合同的，应当重新备案。

8.3 通过个人信息出境个人信息保护认证

个人信息出境个人信息保护认证作为个人信息出境的三条路径之一，同时由国家互联网信息办公室和国家市场监督管理总局联合发布公告。企业向中国网络安全审查认证和市场监管大数据中心、中央网

信办（国家网信办）数据与技术保障中心等拥有个人信息保护认证资质的单位申请个人信息保护认证，应准备以下材料：

- a) 明确认证主体和认证对象，提供相关基本信息；
- b) 认证主体的营业执照/法人证书复印件；
- c) 按照 GB/T 35273《信息安全技术 个人信息安全规范》、TC260-PG-20222A《个人信息跨境处理活动安全认证规范》等文件准备自我评价表及相关证据材料；
注：《数据安全技术 个人信息跨境处理活动安全认证要求》正式实施后，将正式代替 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》。
- d) 认证的业务流程、数据流图及描述；
- e) 认证主体的组织架构相关信息；
- f) 个人信息目录。

8.4 申报负面清单备案

8.4.1 备案流程

在天津数据跨境服务中心提交备案的实施流程包括编写情况说明表、材料提交、材料查验及反馈评估结果、重新备案等环节，具体流程包括：

- a) 编写情况说明表：企业在提交备案前，应填写好数据出境负面清单使用情况说明表；
- b) 材料提交：企业通过注册地所在片区数据跨境服务中心备案；
- c) 组织研判：天津自贸试验区管委会收到备案材料之日起 10 个工作日内，会同其他市级管理部门、相关市级行业主管部门和专家进行研判，并形成备案结果通知书；
- d) 重新备案：企业数据出境情况发生重大变更的，需要重新备案。

8.4.2 情况说明表

企业编写数据出境负面清单使用情况说明表，应包括以下内容：

- a) 企业基本情况，包括单位名称、单位注册地、单位办公所在地等；
- b) 法定代表人信息，包括姓名、职务、国籍、联系方式、证件类型和证件号码等；
- c) 经办人信息，包括姓名、职务、国籍、联系方式、证件类型和证件号码等；
- d) 企业遵守国内法律、行政法规、部门规章的情况；
- e) 数据出境场景信息，包括数据出境业务场景简述、拟出境数据类型、涉及行业/领域、拟出境数据项名称、内容描述及示例、涉及自然人（去重）数量、适用负面清单情况、境外接收方情况等。

8.4.3 材料提交

企业申报数据出境负面清单备案，应当按照天津网信部门最新发布的《中国（天津）自由贸易试验区数据出境负面清单管理办法（试行）》提交材料。

8.4.4 重新备案

企业出现如下情形的，应重新申请负面清单备案：

- a) 数据出境目的、方式或范围发生重大变化；
- b) 出境数据量级大幅度增加；
- c) 境外接收方发生重大变化或数据处理者与境外接收方法律文件变更；
- d) 其他可能导致影响出境数据安全的情形。

8.5 便利化措施

对企业申报数据出境安全评估、申请个人信息出境个人信息保护认证等，涉及以下情形的，可采取相关便利化措施。

- a) 若企业需申请数据出境安全评估的，符合以下条件之一的，可采取合并申报的方式：
 - 1) 多家具有独立法人的境内子公司同属于一家集团公司，且子公司数据出境业务场景相似；
 - 2) 一家控股公司控股多家具有独立法人资格的公司，且被控股公司数据出境业务场景相似，被控股公司通过书面或电子等形式授权控股公司进行申报；
 - 3) 属于集团公司的无独立法人资格的分公司，涉及数据出境业务场景。
- b) 若企业需通过个人信息出境个人信息保护认证的，符合以下情形的，无需签订个人信息出境标准合同，可直接进行个人信息出境活动：
 - 1) 集团公司获得个人信息出境个人信息保护认证；
 - 2) 开展个人信息出境活动的公司同属于该集团公司的多家子公司、分公司、控股公司。

9 企业数据安全能力建设

9.1 管理制度和操作规程

企业开展数据处理活动，制定的相关管理制度和操作规程应包括但不限于以下内容：

- a) 明确数据安全和个人信息保护总体策略、方针、组织体系和责任部门；
- b) 明确数据安全和个人信息保护全流程管理内容，包括收集、存储、使用、加工、传输、提供、公开、删除等流程；
- c) 明确数据分类分级要求，形成企业数据分类分级清单或重要数据目录；
- d) 明确数据安全风险评估要求，包括责任部门、评估周期和评估内容等；
- e) 明确个人信息权益保护相关要求，包括告知义务、取得个人的单独同意，以及查阅、复制、更正、补充、删除、撤回同意等相关权利。

9.2 安全技术措施

企业开展数据处理活动，应采取的安全技术措施包括但不限于以下内容：

- a) 依据 GB/T 22239 进行定级备案，采取和级别相匹配的安全防护技术措施，对涉及重要数据的信息系统，应满足网络安全等级保护三级要求；
- b) 采用数据加密、去标识等安全技术；
- c) 建设数据备份恢复策略及相关的技术措施；
- d) 建立与数据类别级别相适应的访问控制机制，限定用户可访问数据范围；
- e) 对数据安全缺陷、漏洞等风险的监测预警能力建设。

9.3 人员管理措施

企业开展数据处理活动，应对人员进行安全管理，包括但不限于以下内容：

- a) 涉及重要数据和 100 万以上个人信息的企业，应明确数据安全和个人信息保护负责人，按照国家有关规定报送负责人有关信息；
- b) 对相关人员开展数据安全意识教育培训，明确培训周期、培训计划和技能考核要求等。

9.4 安全事件应急处理

企业开展数据处理活动，针对数据安全事件应急处理，包括但不限于以下内容：

- a) 制定数据安全事件应急预案，定义数据安全事件类型，明确不同事件的处理流程和方法；
- b) 发生数据安全事件时，是否立即采取处置措施，并按照规定及时告知用户并向有关主管部门报告；
- c) 是否开展数据安全事件应急演练。

10 数据出境事后管理

10.1 境外接收方安全防护承诺

企业申请的数据出境安全评估所涉境外接收方，企业应重点监督以下安全防护措施的有效性：

- a) 境外接收方处理数据的目的、方式、范围是否发生变化；
- b) 境外接收方保存数据的地点、期限是否按照约定，数据保存地点的安全防护措施是否有效；
- c) 境外接收方所在国家、地区最新的数据安全保护政策法规和网络安全环境，是否对接收方的安全防护措施有影响，安全应急处置措施是否有效；
- d) 若出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用时，承诺的应急处置措施是否有效，是否进行过安全事件应急演练；
- e) 个人维护其个人信息权益的途径和方式是否有效。

10.2 境外接收方合同履行情况

企业订立个人信息出境标准合同，应重点监督以下情况：

- a) 境外接收方处理个人信息的目的、方式、范围是否发生变化；
- b) 境外接收方按照标准合同的要求承诺承担的义务，以及履行义务的管理和技术措施、能力等是否有效；
- c) 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是否有影响；
- d) 个人维护其个人信息权益的途径和方式是否有效。

10.3 认证持续监督

企业申请个人信息保护认证，应重点监督以下情况：

- a) 境外接收方处理个人信息的目的、方式、范围是否发生变化；
- b) 境外接收方所在国家或者地区最新的个人信息保护相关政策和法规对个人信息保护认证提出的要求是否有影响；
- c) 境外接收方对个人信息的安全防护措施是否持续有效；
- d) 若出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用时，承诺的应急处置措施是否有效，是否进行过安全事件应急演练；
- e) 境外接收方是否未向第三方提供所接收的个人信息；
- f) 个人维护其个人信息权益的途径和方式是否有效。

附 录 A
(资料性)
数据安全评估要点

主管部门和企业开展数据安全评估所涉要点见表 A. 1。

表 A. 1 数据安全评估要点

序号	检查项	检查要求	检查要点
1	安全能力 要求	管理制度 和操作规程	1. 是否在制度中明确数据安全和个人信息保护总体策略、方针、组织体系和责任部门
2			2. 是否明确数据安全管理机构、管理岗位及相关职责，是否定期开展数据安全自查工作
3			3. 是否明确了数据全生命周期管理制度
4			4. 涉及个人信息的，是否明确个人信息管理的审批制度、流程、管理范围、安全策略和管控措施，是否明确指定个人信息保护负责人
5			5. 涉及重要数据的，是否明确数据安全风险评估要求，明确风险评估的周期、评估对象和评估范围、报告报送机制等
6			6. 涉及重要数据的，是否明确了数据安全负责人、联系方式和管理部门
7			7. 是否建立数据分类分级制度、规程、操作指南
8			8. 是否有明确的数据分类分级清单或重要数据目录，明确不同级别数据的安全保障措施
9			9. 涉及个人信息的，是否明确用户个人信息权益保护相关要求，包括哪些情形进行告知，哪些情形取得个人的单独同意及如何操作，以及怎么实现用户的查阅、复制、更正、补充、删除、撤回同意等相关权利
10		安全技术 措施	1. 是否定期开展网络安全等级保护测评工作，并形成等保测评报告，是否按照测评报告要求，开展整改工作
11			2. 涉及重要数据的，承载的相关系统是否每年进行了网络安全等级保护 3 级测评，形成报告并完成整改工作
12			3. 是否采用数据加密、去标识等安全技术防范数据泄露
13			4. 是否建设数据备份恢复策略和操作规程，明确数据备份的方式、频次、保存期限、存储介质等
14			5. 定期采取必要的技术措施查验备份和归档数据完整性和可用性情况
15			6. 是否建立与数据类别级别相适应的访问控制机制情况，限定用户可访问数据范围
16			7. 是否按照以满足业务实际需要的最小权限原则进行授权，访问授权申请、审批机制明确
17		人员管理 能力	1. 是否明确数据安全和个人信息保护负责人，按照国家有关规定报送负责人有关信息
18			2. 是否明确了人员录用、保密协议、转岗离岗等相关要求
19			3. 是否制定了数据安全培训计划，明确了数据安全培训内容和培训对象，是否覆盖了关键岗位人员
20			4. 是否有数据安全培训相关记录，包括人员考核记录情况等

21		安全事件 应急处理	1. 数据安全事件应急预案制定和修订情况，是否定义数据安全事件类型，明确不同类别级别事件的处置流程和方法
22			2. 数据安全应急响应及处置机制建设情况，发生数据安全事件时是否立即采取处置措施，是否按照规定及时告知用户并向有关主管部门报告
23			3. 数据安全事件应急演练情况
24			4. 数据处理活动安全风险监测情况，发现数据安全缺陷、漏洞等风险时，是否立即采取补救措施
25			5. 安全事件对个人、其他组织造成危害的，是否将安全事件和风险情况、危害后果、已经采取的补救措施等通知利害关系人，无法通知的是否采取公告等其他方式
26			6. 面向社会提供服务的数据处理者是否建立便捷的数据安全相关投诉举报渠道，以及近 3 年的数据安全投诉举报处置、记录和整改情况，是否存在侵害用户个人信息合法权益的情况
27	数据出境 管理要求	接收方安 全防护承 诺	1. 境外接收方是否发生变化
28			2. 个人信息出境数量增幅是否超过原规划的 20%
29			3. 境外接收方处理数据的目的、方式、范围是否发生变化
30			4. 境外接收方是否将个人信息再转移给其他第三方
31			5. 数据处理者和境外接收方是否按照申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息出境个人信息保护认证等材料中要求的同等安全防护措施
32			6. 境外接收方所在国家/地区的数据安全保护政策和网络环境，是否对现有的安全防护措施有影响，数据处理者是否进行定期监督
33			7. 数据处理者和境外接收方的数据安全事件应急响应机制是否有效，是否有应急演练记录
34			8. 数据出境场景中，数据处理者是否履行了告知义务和取得个人的单独同意
35			9. 数据处理者和境外接收方保障个人信息权益的途径是否畅通，方式是否有效
36		合同履行 情形	1. 涉及数据出境安全评估的，数据处理者和境外接收方的合同有效期是否在数据出境安全评估有效期范围内
37			2. 数据处理者和境外接收方最终签订的标准合同是否和备案的个人信息出境标准合同一致
38			3. 合同中明确的数据出境目的、方式、范围是否和实际出境的一致，是否发生变化
39			4. 检测境外接收方的安全保障措施是否按照签订合同中所明确的管理和技术措施执行，是否达到同等的安全保护水平，包括加密、匿名化、去标识化、访问控制等技术和措施
40			5. 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是否有影响
41			6. 数据处理者是否开展了个人信息保护影响评估，并形成评估报告
42			7. 当前个人信息出境情况是否和个人信息影响评估报告内容保持一致
43			8. 境外接收方的个人信息权益途径是否和合同中约定的一致，途径和方式是否有效

附 录 B
(资料性)

跨境业务场景所涉个人信息示例表

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的，跨境业务场景，场景和数据示例见表B. 1。

表 B. 1 跨境业务场景所涉个人信息示例表

跨境业务场景分类	适用场景示例	数据示例
跨境购物	包括但不限于B2C跨境电商零售进口、C2C个人海淘代购平台、跨境直邮商品订购等场景	姓名、联系方式、身份证件信息（身份证）、商品偏好（产品类型、消费习惯、语言设置）、交易和消费记录（含订单编号、购买时间、商品名称、交易金额、交易状态）等
跨境寄递	包括但不限于国际快递业务、跨境保税仓直发物流、出境邮件寄递等场景	姓名、联系方式、身份证件信息（身份证）、地址信息（寄件地址、收件地址）、交易和消费记录（订单编号、商品名称、交易金额）等
跨境汇款	包括但不限于对私跨境汇出、留学缴费汇出、职工报酬和赡养款汇入、银行卡跨境汇款等场景	姓名、联系方式、身份证件信息（身份证）、银行账户信息（仅限跨境汇款必要支付）等
跨境支付	包括但不限于跨境电商付款、跨境理财通、客户服务、跨境贸易审核等场景	姓名、联系方式、支付标记、脱敏地址、证件号码等
跨境开户	包括但不限于跨境贸易结算账户设立、留学预存保证金账户开立、转介开户、见证开户等场景	姓名、联系方式、国家/地区、出生日期、证件类型、证件有效期、身份证件信息（身份证/护照号码）、证件影像、合同协议影像等
机票酒店预订	包括但不限于国际航班机票预订、境外酒店住宿预约、跨境租车服务等场景	姓名、联系方式、身份证件信息（身份证、护照号码）、行踪轨迹（住宿信息、航班信息）、交易和消费记录（预订时间、订单编号、交易状态）等
签证办理	包括但不限于因私出国签证申请、商务访问签证代办、留学签证材料审核等场景	姓名、身份证件信息（身份证、护照号码）、联系方式、行踪轨迹（出入境记录、住宿信息）、生物识别信息（人脸图像）等
考试服务	包括但不限于国际语言能力考试报名、海外院校入学申请材料提交、职业资格认证成绩核验等场景	姓名、身份证件信息（身份证、护照号码）、联系方式、交易和消费记录（报名信息、缴费记录）、设备信息（MAC地址和设备识别码）等

附 录 C
(资料性)
中国（天津）自由贸易试验区分类分级参考规则

重要数据参考规则示例见表 C.1。

表C.1 中国（天津）自由贸易试验区分类分级参考规则

一级类别	二级类别	数据基本信息描述	重要数据识别参考规则（示例）
一、战略物资和大宗商品类	1. 石油、石化、天然气	包括存储与交易数据、国际贸易数据、战略储备数据等	可能推算出涉及国家重大战略的重要领域运行状况、发展态势、增长速度等的产品产量数据、国际贸易数据等。如存储与交易数据、国际贸易数据、战略储备数据等
	2. 农产品	包括种质资源数据、国际合作数据、国际贸易数据、战略储备数据等	粮食、棉花、食用植物油、食糖、肉类、乳制品等大宗农产品战略储备数据以及未公开的国际合作数据、国际贸易数据，涉及农作物、畜禽、水产珍稀濒危种质资源（含基因）类别、数量等方面的可能影响生物安全的数据，未公开的农业农村统计数据、检验监测数据、防疫检疫数据，达到一定精度或者未公开的地理信息数据。如农作物及其野生近缘种的遗传资源数据、畜禽和水产养殖种质资源，种质资源收集、保存、鉴定评价过程中产生的分析数据等
二、自然资源和环境类	3. 地理信息	包括基础地理信息数据，可细分为定位基础数据、地名地址数据、地形地貌数据、其他基础地理信息数据；专题地理信息数据，可细分为自然资源、生态环境等领域的专题地理信息	达到国家规定的覆盖度、精度和尺度等，或表现敏感区域和目标的基础地理信息数据。如定位基础数据、地名地址数据、地形地貌数据等
	4 遥感影像	包括遥感影像数据，可细分为原始影像数据、影像产品数据和其他遥感影像数据等	达到国家规定的覆盖度、精度和尺度等，或表现敏感区域和目标的遥感影像数据、数字孪生水利地理空间数据。如原始影像数据、影像产品数据等
	5. 气象	包括气象监测数据、空间大气监测数据、气象保障数据、区域气象数据、雷达基数据、气象台站元数据等	服务军事、国防科研、高科技领域的各类气象监测数据、灾害防御数据等。如重大活动气象保障数据、重要敏感区数据、应对气候变化和农作物产量预报预测数据，风云卫星L0级数据和遥测数据、雷达基数据、人影地面作业点数据、历史气象档案及衍生数据、气象政务服务数据、气象关键信息基础设施数据等
	6. 海洋	包括海洋环境数据、海洋资源数据	不宜公开发布的具有军事价值的海洋环境监测数据。如未公开的海洋水体数据、海底矿产资源分布图、国内专属经济区资源调查数据、深海三维水文要素观测数据、海域环流动力学数据、水体温盐精细结构数据、水

			体化学成分数据、海洋气象监测数据、生态系统调查数据、环境要素监测数据、深海环流数值模型、海底光缆精确铺设路径、水声通信网络布局方案、深海导航定位系统设施分布、海洋观测网关键节点数据、通信导航设备工作参数等
	7. 环保	包括反映污染物排放水平的自行监测、接受行政处罚或其他污染物排放等数据	关系公共安全或者外交事务的环保未公开数据。如环保监测情况、执法情况或者环境影响情况等
	8. 水利	包括水利业务数据、水利工程建筑信息模型等水利基础数据，水旱灾害灾情综合分析评价等数据	关系公共安全的水利数据，能够反映水旱灾情、工程险情、综合分析评价等水旱灾害防御业务数据，重点水利工程物理安全保护情况。如险工险段、重点水利工程建筑信息模型、水旱灾害灾情、综合分析评价数据等
三、工业类	9. 钢铁、有色金属	包括储量、产量、冶炼装备、采购量等数据，国际合作数据、国际贸易数据等	具有重要军用、民用价值的有色金属储量、产量、采购量等数据，国家钢铁、有色金属战略储备数据或战略性有色金属矿床的重要地质数据，富含重要伴生矿资源的矿区数据。如特钢的生产能力数据、工艺技术路线、产能数据、储备信息、消费去向情况等，在国防军工、国民经济重点行业有重要应用价值的有色金属储量统计数据、产能数据、采购量及与相关国家的国际合作情况等
	10. 稀土	包括储量与开采数据、行业使用数据、出口数据等	我国独特掌握的稀土开采、冶炼等生产技术数据。如稀土资源储存开发情况、国际合作情况等
	11. 其他矿产	包括储量数据、国际合作数据、国际贸易谈判数据、与矿产有关的产业发展布局情况	反映国家重要资源储备能力，影响相关国际合作的数据，大宗原材料信息，以及能够左右原材料采购定价权的数据。如储量统计数据（不包括放射性矿产）、国际合作情况、国际贸易谈判情况、与矿产有关的产业发展布局情况等
	12. 化学工业	包括生产作业场所和运输信息、生产销售信息、制作方法信息，民用爆炸物品行业相关数据信息	重点危险化学品检测监控、关键工艺、设备运行、产量储量等数据。如危化品生产作业场所信息和运输路线规划、生产销售情况、制作方法等
	13. 电力	包括发电厂生产数据、输配电数据、建设运维数据	大型水电站，大型抽水蓄能电站，核电站，单机（套）容量在100万千瓦及以上、装机总容量300万千瓦及以上火力发电站，500千伏（不含）以上变电站（开关站）、换流站等电力基础设施以及远程调度控制中心的设计施工图纸资料（含精度100米内位置坐标）；特级电力用户电力消费的原始数据等
	14. 电子信息	包括基础电子信息产品（关键芯片、操作系统、大型软件等）参数，源代码、集成电路布图等数据，产品测试数据，产品面向国防军工、政务等领域销售和服务情况	电子信息行业先进技术、集成电路先进设计和制造技术、重大计算装备设计数据、算法和软硬件架构以及重要电子元器件设备国产化率等数据。如关键芯片、操作系统、大型软件等基础电子信息产品参数，源代码，集成电路布图，产品测试数据，产品面向国防军工、政务等领域销售和服务情况等

	15. 民 用 核设施	包括民用核设施科研中的试验或测试数据，核设施相关设计和制造工艺信息，核设施运行监控数据	一旦遭到篡改、泄露或者非法利用，可能影响核材料或者核设施安全的数据。如民用核设施科研中的试验或者测试数据，核设施相关设计和制造工艺，核设施运行监控数据等
	16. 工 业 装备	包括工业装备研发、应用、生产、销售、运维、管理数据	反映国家高端制造水平，体现国家在工业领域核心竞争力的数据。如应用于军事、航空航天等领域的高技术装备研发和生产情况，大型装备或者具有核心技术的重要装备的研发、生产情况等
	17. 智 能 汽车	包括智能汽车运行过程中获取的地理信息、人员流量、车辆流量等数据，智能汽车用户用车数据	反映重要敏感区域的地理位置、作业状况，以及10万以上智能汽车消费者相关敏感个人信息的数据。如智能汽车运行过程中获取的军事管理区、国防军工单位、县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量数据，OTA数据，车身稳定控制系统、主动减震器系统相关研发数据，用于研发生产的智能网联汽车自动驾驶模型训练数据等
	18. 其他	包括工业互联网的网络、平台、安全保障相关数据，工业控制系统的参数、控制、运行维护、测试数据	规模以上工业企业使用的工业互联网或工业控制系统安全运行保障数据。如年产值4亿元以上工业企业使用的工业互联网或者工业控制系统的参数及运行、维护、测试数据；城市供水、供气、供热自动控制系统的参数及运行、维护、测试数据等
四、 国防 科技 工业 类	19. 国 防 科技工业 类	包括经营管理、研发设计、生产制造、试验验证、维修保障等数据	综合反映国防科技工业重要企事业单位科研与生产能力的的数据，汇总后能反映国防科技工业整体情况的数据，国防科技工业领域相关特色重要数据。如军工科研生产单位内部名称、地理位置信息、建设计划、安防规划、警卫保护布置、生产经营情况、产品交易情况等
五、 电信 类	20. 电信	包括网络规划运维数据、安全保障数据、经济运行和业务发展数据、关键技术成果数据、用户注册信息等	基础电信骨干网络、应急通信部署类数据。如骨干网规划建设情况、运行维护数据、关键资源数据（如IP地址、接入网资源等）、应急通信部署，以及重要网络设施和信息系统的建设规划数据、性能参数数据、监测分析数据、运行维护数据、统计分析数据等
六、 广电 视听 传媒 类	21. 广 播 电视	包括广电网络规划建设类数据，广电安全播出运维、应急保障、调度指挥等信息，广电监测监管系统数据，用户注册信息等	广电网络的规划建设、运行维护、关键资源（如IP地址、接入网资源等）以及被滥用可能导致意识形态安全、公共安全的媒体数据。如未公开的视听创作内容，被滥用可能导致意识形态安全、公共安全的视听内容，视听业务省级及以上机构传输覆盖情况、视听监测监管数据，以及广播电视行业关键信息基础设施、网络安全等级保护三级及以上的重要网络和信息系统的用户总量1亿以上视听机构的重要网络和信息系统的规划情况、建设情况、资源部署及安全保障情况等
	22. 新 媒 体	包括未公开或限制公开媒体资源类文件，用户数字画像、推送地址等数据	可用于社会动员，一旦被非法利用，影响文化安全、公共安全的数据。如未公开或者限制公开的媒体资源文件，10万人以上用户上网行为数据等

七、金融类	23. 银行	包括银行客户数据、业务数据、经营管理数据、系统运行和安全管理数据等	一旦遭到泄露,可能会威胁国家安全或者银行机构自身安全,或者100万以上客户安全的数据。如银行安保数据,重要企事业单位账户信息、贷款数据、交易数据等
	24. 保险	包括保险机构客户数据、业务数据、经营管理数据、系统运行和安全管理数据等	一旦遭到泄露,可能会威胁100万以上客户安全,或者威胁国家安全或者重要单位、设施运行安全的数据。如涉及国家安全的重要设施、装备、人员的保险和理赔数据,保险机构处理的承担国家重大工程或者国民经济社会发展重要领域建设项目的企事业单位投保或者理赔数据等
	25. 证券期货	包括投资者类数据、技术类数据、业务类数据等	一旦遭到泄露,可能会威胁大量客户金融资金安全的数据。如一定规模以上个人证券账户数据、个人期货账户数据等
	26. 融资租赁	包括客户数据、企业交易数据、经营管理数据等	一旦遭到泄露或者被他国利用,可能会威胁100万以上客户安全,或者影响相关企业运营的数据。如涉及党政机关、国防军工企业的融资租赁数据等
八、交通运输类	27. 交通	包括铁路交通、公路交通、道路运输、城市交通、水路交通、民用航空、综合管理等数据	铁路交通、公路交通、道路运输、城市交通、水路交通、民用航空等领域影响生产安全的控制类数据、施工建设过程中获取的自然资源类数据、未公开的线路图、关键站点等数据,以及被泄露、篡改可能造成重大交通事故的数据等
	28. 邮政	包括邮政运输管理及其挖掘分析类数据	一旦遭到篡改、泄露,可能造成10万人以上敏感个人信息泄露,或者导致电信诈骗等活动发生的数据,以及邮政管理领域影响生产安全的控制类数据。如对运单数据进行大数据挖掘分析的结果等
九、住房建设类	29. 住房公积金	包括住房公积金缴存人和单位信息,统计分析数据	可能造成10万人以上敏感个人信息泄露,影响企业日常经营,或者汇聚后可被用于分析房地产市场状况的数据。如住房公积金缴存人和缴存单位的基本信息、账户信息及公积金缴存、提取、使用数据等
十、卫生健康和食品药品类	30. 遗传资源	包括自然人基因数据、人类遗传资源信息等与种族、群体健康相关的数据	反映种族整体情况或关系生物安全的遗传资源数据。如含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料及其开发利用结果数据等
	31. 健康医疗	包括医疗服务、电子病历、电子健康档案、医学研究等各类数据,健康数据、医疗救援保障数据、特定药品实验数据等,或对患者健康医疗数据的开发利用结果	关系国家安全、生命安全、人类自身安全的生物安全和疾控数据。如导致10万人以上敏感个人信息泄露,侵害公民隐私的个体诊疗或者健康管理数据;电子病历、检查检测结果、健康档案数据等及其开发利用结果
	32. 食品	包括食品安全溯源标识数据,食品生产中自动控制系统的参数和控制类数据	一旦遭到篡改、泄露,可能造成重大食品安全事件,影响食品安全溯源的数据。如食品安全溯源标识信息、食品生产中自动控制系统的参数和控制数据等
	33. 药品	包括药品供应、药品审批过程中提交的实验数据,以及与药品生产流程、生产设施	关系人民群众用药安全,影响生物安全、公共安全的数据。如重要疫苗、战略重要基础药物等重大医疗物资生产、供应、保障等数据;涉及国家战略安全的药品

		有关的试验数据	实验数据, 以及与药品生产流程、生产设施有关的试验数据等
	34. 生物安全	包括病毒研究或生物实验室相关数据	关系国家安全、公共安全和生物安全, 反映生物科学研究重大进展, 具有军事价值、重大经济价值的数。如病毒研究情况、生物实验室相关数据等
	35. 疾控数据	包括突发公共卫生事件及与传染病相关的疫情、治疗、疫苗、死因等数据	反映某一地区传染病防控情况, 关系公共安全和生物安全的数据。如突发公共卫生事件及与传染病相关的疫情、治疗、疫苗、死因情况等
十一、公共安全类	36. 物理安全	包括建筑基础数据、安保装备数据等	一旦遭到非法利用, 可能对物理目标发动攻击, 危害核材料与核设施安全, 威胁公民生命安全, 影响国家安全、公共安全的数据。如重要目标和场所的基本信息、安保装备数据、安保部署数据等
	37. 网络安全	包括自贸试验区企业信息系统设计运行数据、网络设施拓扑架构数据、安全保障数据等	天津市网络安全态势数据, 关键信息基础设施、网络安全等级保护三级及以上的重要网络和信息系统的建设布局规划、供应链管理, 以及未公开的网络安全漏洞等
	38. 应急管理	包括应急救援过程数据、应急物资数据、救援装备数据等	可能对突发事件应对、防灾救灾、安全生产等产生重大影响的数据。如重点目标精准位置和关键参数数据, 达到一定精度、覆盖一定范围的特定区域监测数据, 达到一定规模的应急物资、救援装备数据, 以及重大及以上等级灾害事故救援过程数据等
十二、互联网服务和电子商务类	39. 服务外包	包括境外客户委托境内企业提供服务过程中收集、产生的数据或与重要服务客户有关的数据。开展数字贸易、跨境电商业务中收集、产生的数据或与重要服务客户有关的数据	在处理境外数据过程中引入境内重要数据或者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产生的结果数据; 利用我独特掌握的技术处理境外数据产生的结果数据
	40. 互联网平台服务	包括提供互联网服务过程中产生的各类数据	互联网平台掌握的具有舆论属性或者社会动员能力的的数据。如政府官员、退伍军人等敏感人群的行为分析数据, 涉及军工、党政机关、关键信息基础设施客户的服务记录数据等
	41. 人工智能服务	包括人工智能训练数据、算法源代码、关键组件数据、控制程序等数据	可能影响国家安全和公共利益的人工智能训练数据、算法源代码、关键组件数据、控制程序等数据。
十三、统计类	42. 经济统计	包括宏观经济数据、产业统计数据、样本数据	反映某方面宏观经济运行情况, 影响一定数量的企业和个人合法权益的数据。如天津市基层数据和公开发布前的综合数据, 能够推测天津市及以上总量数据的抽样调查样本数据, 以及重要工农业产品分品种产量产能统计数据等
	43. 社会统计	包括历史特征数据、风俗习惯数据、语言文字数据等	一旦被非法利用, 可能影响国家安全或者社会稳定的数据。如反映我国语言文字、历史、风俗习惯、民族价值观念等特质的数据

十四、科学技术类	44. 属于出口管制法管制的相关数据	包括列入国家出口管制清单的相关物项数据	属于《中华人民共和国出口管制法》管制的相关数据
	45. 知识产权和重大发现	包括涉及国防、国家安全或其他非公开的知识产权，其他能显著提升国家安全能力或直接影响国家安全的科研论文、观测数据、产业化成果等	涉及国家安全的知识产权数据。如能显著提升国家安全能力或者直接影响国家安全的科研论文、观测数据、产业化成果等
十五、其他数据类	46. 禁止出口限制出口技术	包括列入《中国禁止出口限制出口技术目录》所列技术有关的数据	《中国禁止出口限制出口技术目录》所列技术的有关数据
	47. 其他数据	可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、生物等安全的数据	其他可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、生物等安全，符合重要数据定义的数据
重要数据统一识别参考规则： 1. 所在行业的重要数据识别参考规则（示例）中，由相关部门公开发布的数据除外。 2. 本参考规则适用于非涉密数据，涉密数据按相关规定执行。 3. 天津自贸试验区企业掌握的1000万人以上个人信息（不含敏感个人信息）；100万人以上敏感个人信息；10万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息。 4. 被国家认定为关键信息基础设施的运营者掌握的10万人以上个人信息。 5. 天津自贸试验区企业在研发设计过程、生产制造过程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据；涉及国家安全的企业供应链相关数据。 6. 天津自贸试验区企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。			

附 录 D
(资料性)
敏感个人信息类别表

敏感个人信息类别见表 D.1。

表 D.1 敏感个人信息类别

类别	描述
生物识别信息	个人基因、人脸、声纹、步态、指纹、掌纹、眼纹、耳廓和虹膜等生物识别信息
宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教习俗等个人信息
特定身份信息	残障人士身份信息、不适宜公开的职业身份信息等个人信息
医疗健康信息	1. 与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息，如病症、既往病史、家族病史、传染病史、体检报告和生育信息等； 2. 在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录（如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录）、检验检查数据（如检验报告和检查报告）等
金融账户信息	个人的银行、证券、基金、保险和公积金等账户的账号及密码，公积金联名账号、支付账号银行卡磁道数据（或芯片等效信息）和基于账户信息产生的支付标记信息和个人收入明细等个人信息
行踪轨迹信息	连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息
未成年个人信息	不满十四周岁未成年的个人信息
其他敏感个人信息	精准定位信息、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息和显示个人身体私密部位的照片或视频信息等个人信息
备注： 1. 个人基因，可参考 GB/T 41806。 2. 人脸，可参考 GB/T 41819。 3. 声纹，可参考 GB/T 41807。 4. 步态，可参考 GB/T 41773。 5. 医疗健康信息中，若个人的体重、身高、血型、血压和肺活量等基本体质信息，如与个人的疾病和医疗就诊无关，则可认为不属于敏感个人信息范畴。 6. 精准定位信息，通过调用个人移动通信终端精准位置权限采集的位置信息是精准定位信息，通过网络地址等测算的粗略位置信息不是精准定位信息，连续采集的精准定位信息可用于生成行踪轨迹。 7. 犯罪记录信息，指我国国家专门机关对犯罪人员的客观记载，如罪名和刑罚等记录信息。	

参 考 文 献

[1] GB/T 20000.1—2014 标准化工作指南 第1部分：标准化和相关活动的通用术语

[2] GB/T 35273—2020 信息安全技术 个人信息安全规范

[3] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[4] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[5] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[6] GB/T 43697—2024 数据安全技术 数据分类分级规则

[7] GB/T 41806—2022 信息安全技术 基因识别数据安全要求

[8] GB/T 41819—2022 信息安全技术 人脸识别数据安全要求

[9] GB/T 41807—2022 信息安全技术 声纹识别数据安全要求

[10] GB/T 41773—2022 信息安全技术 步态识别数据安全要求

[11] YD/T 4981—2024 工业领域重要数据识别指南

[12] TD/T 3867—2024 电信领域重要数据识别指南

[13] 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）

[14] 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）

[15] 中华人民共和国网络安全法（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）

[16] 网络数据安全条例（2024年8月30日国务院第40次常务会议通过）

[17] 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）

[18] 汽车数据安全若干规定（试行）（2021年7月5日国家互联网信息办公室2021年第10次室务会审议通过）

[19] 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）（2024年5月9日中国（天津）自由贸易试验区管理委员会、天津市商务局正式印发）

[20] 中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）（2024年8月26日北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局正式印发）

[21] 中国（浙江）自由贸易试验区数据出境负面清单管理办法（试行）（2025年3月31日浙江省互联网信息办公室、浙江省商务厅、浙江省数据局正式印发）

[22] 海南自由贸易港数据出境管理清单（负面清单）（2024年版）（2025年2月8日中共海南省委自贸港工作委员会办公室、海南省互联网信息办公室、海南省发展和改革委员会（海南省数据局）正式印发）

[23] 《中国（上海）自由贸易试验区及临港新片区数据出境管理清单（负面清单）（2024版）》（2025年2月8日上海市互联网信息办公室、上海市数据局、上海市发展和改革委员会、中国（上海）自由贸易试验区管委会、中国（上海）自由贸易试验区临港新片区管委会正式印发）