ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 46068—2025

数据安全技术
个人信息跨境处理活动安全认证要求

Data security technology—Security certification requirements for cross-border processing activity of personal information

2025-08-29 发布　　2026-03-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中认信安(北京)技术服务有限公司、中国网络安全审查认证和市场监管大数据中心、中央财经大学、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、国家计算机网络与信息安全管理中心北京分中心、中国软件评测中心、中电科网络安全科技股份有限公司、清华大学、中国科学技术大学、北京市经济和信息化局网络安全管理中心、北京快手科技有限公司、北京银联金卡科技有限公司、华为技术有限公司、蚂蚁科技集团股份有限公司、深信服科技股份有限公司、阿里巴巴(北京)软件服务有限公司、北京百度网讯科技有限公司、奇安信科技集团股份有限公司。

本文件主要起草人：布宁、陈世翔、王凤娇、张金平、胡影、王晖、孙晓丽、陈琦、史大为、陈特、陈亮、杨婷、晏慧、望娅露、卢磊、李海东、金涛、左晓栋、霍然、李媛、李安伦、落红卫、程瑜琦、段静辉、樊华、王惠莅、郑峥、郑云文、白晓媛、叶润国、李子涵、刘斌、于园园、董华凌、郭建领、刘前伟、吴梦婷。

数据安全技术
个人信息跨境处理活动安全认证要求

1 范围

本文件规定了跨境处理个人信息时相关方遵守的基本原则、基本要求和个人信息主体权益保障要求。

本文件适用于跨境处理个人信息的相关方规范自身个人信息跨境处理活动，也适用于主管部门、第三方机构等组织对个人信息处理者跨境处理个人信息的活动进行监督、管理、认证和评估。

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 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

个人信息 personal information

以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息。

注：不包括匿名化处理后的信息。

3.2

敏感个人信息 sensitive personal information

一旦泄露或非法使用，容易导致自然人的人格尊严受到侵害或人身、财产安全受到危害的个人信息。

注：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。

3.3

个人信息主体 personal information subject

个人信息所标识或关联的自然人。

[来源：GB/T 35273—2020，3.3]

3.4

个人信息处理者 personal information processor

在个人信息处理活动中自主决定处理目的、处理方式的组织。

3.5

境外接收方 overseas recipient

位于中华人民共和国境外并自个人信息处理者处接收、处理个人信息的组织或个人。

注：包含接收并处理、受托处理及共同处理个人信息的组织或个人。

3.6

单独同意　separate consent

个人针对其个人信息进行特定处理而专门作出具体、明确授权的行为，不包括一次性针对多种目的或方式的个人信息处理活动作出的同意。

注 1：单独同意的告知内容与取得同意的方式需与其他处理活动予以区分。

注 2：单独同意适用于以同意为合法性基础的场景。

[来源：GB/T 42574—2023，3.7]

3.7

个人信息跨境处理活动　cross-border processing activity of personal information

境外接收方自个人信息处理者处接收个人信息并在境外开展存储、使用、加工、传输、提供、公开、删除等处理活动，或境外接收方直接通过查询、调取、下载、导出的方式处理存储在境内个人信息处理者处个人信息的活动，及符合《中华人民共和国个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息的活动。

4　基本原则

4.1　合法、正当、必要和诚信原则

个人信息处理者和境外接收方在跨境处理个人信息时需遵守法律法规的规定，按约定目的并采取对个人信息权益影响最小的方式处理个人信息，遵守合同、协议等具有法律约束力文件的约定和承诺，保障个人信息主体的合法权益。

4.2　公开、透明原则

个人信息处理者和境外接收方在跨境处理个人信息时需按处理规则公开、处理过程透明要求，及时向个人信息主体告知境外接收方的名称或姓名、联系方式，个人信息跨境处理的目的、处理方式、个人信息的种类、权利以及行使权利的方式和程序等，便于个人信息主体了解自身个人信息的跨境处理情况。

4.3　同等保护原则

个人信息处理者和境外接收方在跨境处理个人信息时均需采取必要措施，保护所处理个人信息的安全，个人信息跨境处理活动需达到中华人民共和国个人信息保护相关法律法规规定的个人信息保护标准，典型个人信息跨境处理场景见附录 A。

4.4　责任明确原则

个人信息处理者和境外接收方在跨境处理个人信息时需履行法律法规规定的责任义务，保障个人信息主体权益。境外接收方需指定境内一方、多方代表或在境内设置的机构对境外接收方损害个人信息权益的个人信息处理活动承担民事法律责任。

注：境外个人信息处理者、接收方在境内设置的机构需为法人实体，设置的机构或指定代表均需具备承担法律责任的能力。

5　基本要求

5.1　具有法律约束力的文件

开展个人信息跨境处理活动的个人信息处理者和境外接收方应签订合同或其他具有法律约束力和

可执行的文件，个人信息主体权益应得到保障。文件应至少包含下列内容：

a) 个人信息处理者和境外接收方的基本信息，包括但不限于名称、注册地址、联系人姓名和联系方式等；
b) 个人信息跨境处理的目的、范围、类型、敏感程度、数量和方式，境外接收方处理个人信息的用途和方式等；
c) 个人信息在境外的保存期限、存储地点及达到保存期限、完成约定目的及法律文件终止后的处理措施等；
d) 个人信息处理者和境外接收方保护个人信息的责任与义务，以及为防范个人信息跨境处理可能带来安全风险所采取的技术和管理措施等；
e) 个人信息主体的权利，以及保障个人信息主体权利的途径和方式；
f) 救济、合同解除、违约责任和争议解决等；
g) 境外接收方承诺遵守与个人信息处理者约定的个人信息跨境处理规则，并确保个人信息保护水平不低于中华人民共和国个人信息保护相关法律、行政法规规定的标准；
h) 境外接收方承诺接受认证机构对个人信息跨境处理活动的持续监督；
i) 境外接收方承诺接受中华人民共和国个人信息保护相关法律和行政法规管辖；
j) 境外接收方应通过合同或其他具有法律效力的文件明确在中华人民共和国境内承担法律责任的组织，并承诺履行个人信息保护义务；
k) 个人信息处理者和境外接收方均承诺对损害个人信息权益行为承担民事法律责任，并明确约定双方的责任承担方式；
l) 其他应遵守的法律和行政法规规定的义务。

5.2 组织管理

5.2.1 个人信息保护机构

开展个人信息跨境处理活动的个人信息处理者和境外接收方均应具有履行个人信息保护职能的机构，履行个人信息保护义务，防止未经授权的访问以及个人信息泄露、篡改、丢失等，并在个人信息跨境处理活动中承担下列职责：

a) 制定并实施个人信息跨境处理活动保护计划；
b) 组织开展向境外提供个人信息时的个人信息保护影响评估；
c) 采取有效措施保证按约定的处理目的、范围和方式处理跨境个人信息，履行个人信息保护义务，保障个人信息安全；
d) 监督本组织按约定的个人信息跨境处理规则处理跨境个人信息，保护个人信息主体权益；
e) 定期对本组织处理个人信息遵守中华人民共和国个人信息保护相关法律、行政法规的情况进行合规审计；
f) 接受和处理个人信息主体的请求和投诉；
g) 接受认证机构对个人信息跨境处理活动的持续监督，包括答复询问和配合检查等。

5.2.2 个人信息保护负责人

开展个人信息跨境处理活动的个人信息处理者和境外接收方均应指定个人信息保护负责人。个人信息保护负责人应具备个人信息保护专业知识和相关管理工作经历，参与有关个人信息跨境处理的重要决策。个人信息保护负责人应承担下列职责：

a) 确定个人信息保护工作的主要目标、基本要求、工作任务和保护措施；
b) 为本组织的个人信息保护工作提供人力、财力和物力等资源保障；

c） 指导、支持相关人员开展本组织的个人信息保护工作，个人信息保护工作应达到预期目标；
d） 直接向本组织的主要负责人汇报个人信息保护工作情况，推动个人信息保护工作持续改进；
e） 领导个人信息保护机构开展工作。

5.3 个人信息跨境处理规则

开展个人信息跨境处理活动的个人信息处理者和境外接收方应约定并遵守共同的个人信息跨境处理规则，规则应至少包括下列内容：

a） 跨境处理个人信息的基本情况，包括个人信息数量、范围、种类和敏感程度等；
b） 跨境处理个人信息的目的、方式和范围；
c） 个人信息境外存储的起止时间及期满后的处理方式；
d） 跨境处理个人信息需要中转的国家或地区；

注：“中转的国家或地区”是指数据跨境传输过程中暂时存储、处理或转发所经过的第三国或地区。

e） 保障个人信息主体权益所需资源和采取的措施；
f） 个人信息安全事件的赔偿、处置规则。

5.4 向境外提供个人信息时的个人信息保护影响评估

个人信息处理者应对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估，并形成个人信息保护影响评估报告，个人信息保护影响评估报告模板见附录B，评估报告至少保存3年。评估报告应至少包括下列内容。

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） 跨境处理个人信息的规模、范围、种类和敏感程度，个人信息跨境处理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、能力等能否保障跨境处理个人信息的安全。
d） 个人信息跨境处理存在泄露、损毁、篡改和滥用等的风险，个人信息主体维护个人信息权益的渠道是否畅通。
e） 境外接收方所在国家或地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响，包括但不限于：
   1） 境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效的处置、境外接收方是否曾收到其所在国家或地区公共机关要求其提供个人信息的请求及境外接收方应对的情况；
   2） 该国家或地区现行的个人信息保护法律法规、普遍适用的标准情况，与我国个人信息保护相关法律法规、标准的差异，及是否达到我国个人信息保护法确定的保护标准；
   3） 该国家或地区加入的区域或全球性的个人信息保护方面的组织，以及所做出的具有约束力的国际承诺；
   4） 该国家或地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。
f） 其他可能影响个人信息跨境处理安全的事项。

5.5 个人信息处理要求

个人信息处理者、境外接收方的个人信息处理活动应符合GB/T 35273—2020的要求。

6 个人信息主体权益保障要求

6.1 个人信息主体权利

个人信息处理者和境外接收方应承认个人信息主体享有下列权利，并为个人信息主体行使权利提供便利条件：

a) 个人信息主体是个人信息处理者和境外接收方签订具有法律约束力文件中的第三方受益人，可要求个人信息处理者和境外接收方提供法律文本中涉及个人信息主体权益部分的副本，并向个人信息处理者和境外接收方主张权利；

b) 个人信息主体对其个人信息的处理拥有知情权、决定权、限制或拒绝他人对其个人信息进行处理的权利、查阅权、复制权、更正与补充的权利、删除权，有权撤回对其个人信息跨境处理的同意；

c) 个人信息主体行使上述权利时，个人信息主体可请求个人信息处理者采取适当措施予以实现，或直接向境外接收方提出请求；

d) 个人信息主体可要求个人信息处理者或境外接收方对其个人信息跨境处理规则进行解释说明；

e) 个人信息主体可对违法个人信息跨境处理活动向中华人民共和国履行个人信息保护职责的部门进行投诉、举报；

f) 个人信息主体权益受到损害时，个人信息主体可向个人信息处理者、境外接收方的任何一方主张法律责任；

g) 个人信息主体可依据中华人民共和国民事诉讼相关法律确定的管辖法院向开展个人信息跨境处理活动的个人信息处理者和境外接收方提起司法诉讼；

h) 法律、行政法规规定的其他权利等。

6.2 个人信息处理者和境外接收方的义务和责任

个人信息处理者和境外接收方履行下列义务和责任。

a) 个人信息处理者应告知个人信息主体开展个人信息跨境处理活动的个人信息处理者和境外接收方的基本情况，包括名称或姓名、联系方式、向境外提供个人信息的目的、类型、处理方式和保存期限，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，个人信息处理者应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，应取得未成年人的父母或其他监护人的单独同意。法律、行政法规规定需取得书面同意的，应取得书面同意。

b) 因境外接收方在实际控制权或经营范围发生实质性变化、境外接收方所在国家或地区法律或政策发生变化，导致境外接收方无法履行本文件所提出的要求，境外接收方应在知道变化后立即通知个人信息处理者；个人信息处理者应暂停向境外接收方提供个人信息并通知认证机构，采取相应保护措施，直到个人信息处理者和认证机构重新评估通过后方可恢复。

c) 境外接收方在意识到其所在国家立法妨碍其履行本文件规定义务，包括接到所在国家或地区的政府部门、司法机构关于提供或访问所接收的个人信息的要求时，应立即通知个人信息处理者，并采取进一步的适宜保护措施，包括审查请求的合法性等。

d) 双方应按已签署的具有法律效力文件约定的处理目的、处理方式和保护措施等跨境处理个人信息，不应超出约定处理个人信息。个人信息处理过程中凡涉及采用密码技术的应符合密码相关国家标准和行业标准。

e) 境外接收方不应将所接收的个人信息提供给位于中华人民共和国境外的第三方。确需向第三

方提供的，需同时符合以下要求：

1） 确有业务需要，且境外接收方为受托人时已事先征得个人信息处理者同意；

2） 已告知个人信息主体该第三方的名称或姓名、联系方式、处理目的、处理方式、个人信息类型、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。向第三方提供敏感个人信息的，还应向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响，但是法律、行政法规规定不需要告知的除外；

3） 基于个人同意处理个人信息的，应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，应取得未成年人的父母或其他监护人的单独同意。法律、行政法规规定需取得书面同意的，应取得书面同意；

4） 与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任；

5） 根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。

f） 双方应为个人信息主体提供查阅其个人信息的途径，个人信息主体要求查阅、复制、更正、补充或删除其个人信息时，应及时予以响应，拒绝其请求的，应说明正当理由。个人信息处理者无法实现的，个人信息处理者应通知并要求境外接收方协助实现。

g） 双方应客观记录开展的个人信息跨境处理活动，保存记录至少三年；按相关法律法规要求向中华人民共和国履行个人信息保护职责的部门提供相关记录文件。

h） 当出现难以保证个人信息安全的情况时，应及时停止跨境处理个人信息，并通知对方。

i） 发生或可能发生个人信息篡改、破坏、泄露、丢失、非法利用、未经授权提供或访问，个人信息处理者及境外接收方应立即采取补救措施并通知对方，按《国家网络安全事件应急预案》等有关规定及时报告中华人民共和国履行个人信息保护职责的部门。相关法律法规要求通知个人信息主体的应由个人信息处理者通知。记录并留存所有与个人信息篡改、破坏、泄露、丢失、非法利用、未经授权提供或访问有关的事实及其影响，包括采取的补救措施。通知、报告包含以下内容：

1） 发生或可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或访问的个人信息种类、原因和可能造成的危害；

2） 已采取的补救措施；

3） 个人信息主体可采取的减轻危害的措施；

4） 负责处理相关情况的负责人或负责团队的联系方式。

j） 应个人信息主体的请求，应为个人信息主体提供双方有法律约束力文件中涉及个人信息主体权益部分的副本。如涉及商业秘密或保密商务信息，在不影响个人信息主体理解的前提下，可对文件副本相关内容进行适当处理。

k） 境外接收方的境内法律责任承担方承诺为个人信息主体行使权利提供便利条件，当发生个人信息跨境处理活动损害个人信息主体权益时，为境外接收方承担相应的民事法律责任。

l） 境外接收方承诺接受认证机构对个人信息跨境处理活动的持续监督和监管机构的监督、管理，包括答复询问、配合检查、服从采取的措施或做出的决定等，并提供已采取必要行动的书面证明。

m） 承担证明相关责任义务已履行的举证责任。

n） 当境外接收方为受托人时，按双方签订的具有法律约束力文件约定，个人信息处理者应按5.1的要求，与境外接收方约定受托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。未经个人信息处理者同意，受托人不应转委托他人处理个人信息。

附 录 A
（资料性）
典型个人信息跨境处理场景

A.1 跨国公司或同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动

跨国公司总部位于境外：基于跨国公司总部对分支机构集中管理的需要，从境内向境外提供其在境内处理的客户个人信息、涉及个人信息的业务信息等。

跨国公司总部位于境内：境外分支机构出于业务需要调用总部数据，从境外访问存储在境内的客户个人信息、涉及个人信息的业务信息等。

该场景见图 A.1。

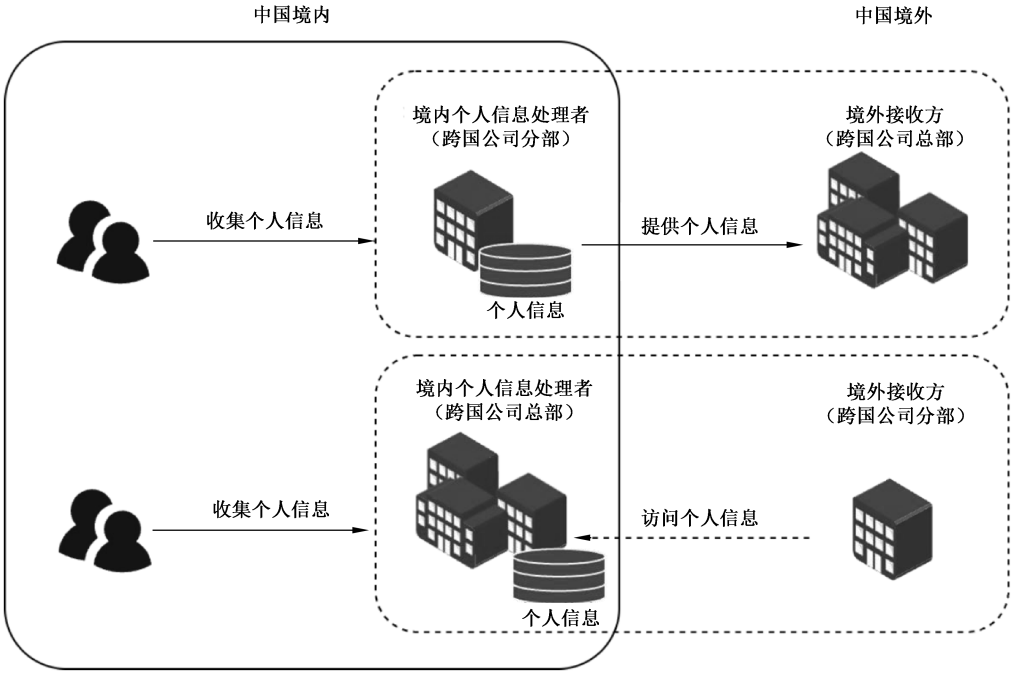

图 A.1 跨国公司或同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动

A.2 境内个人信息处理者委托境外服务提供商处理数据

境外服务提供商不实际处理数据：境内个人信息处理者利用境外云服务、备份服务等开展个人信息处理活动。

境外服务提供商实际处理数据：境外服务提供商通过网络远程接入境内个人信息处理者的信息系统进行技术支持、故障处理等，其中会涉及个人信息的处理；境内个人信息处理者委托境外律所、会计师事务所或出口管制筛查机构提供合规服务，向境外传输境内自然人的个人信息。

该场景见图 A.2。

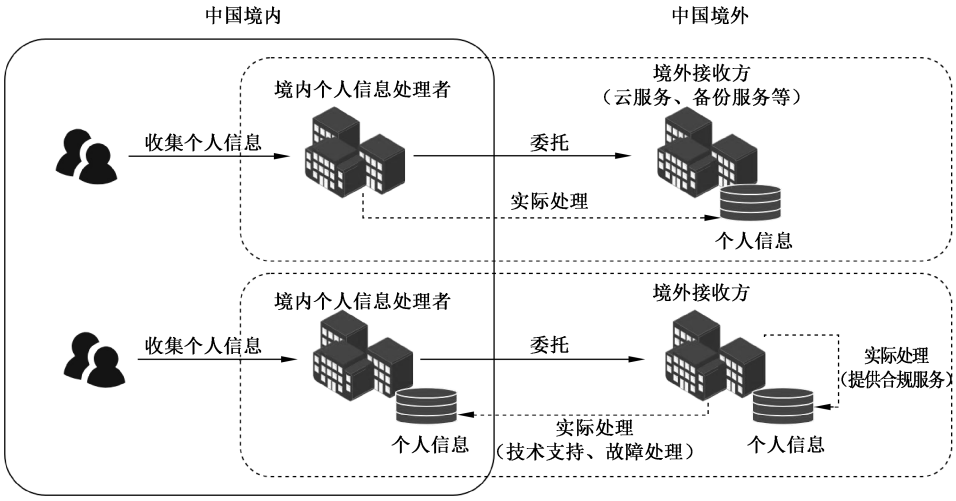

图 A.2　境内个人信息处理者委托境外服务提供商处理数据

A.3　境内个人信息处理者向境外接收方提供个人信息

境内个人信息处理者向境外接收方提供个人信息。例如，跨境电商向一个或多个境外接收方提供用户的购物记录和浏览行为等个人购买行为数据。

该场景见图 A.3。

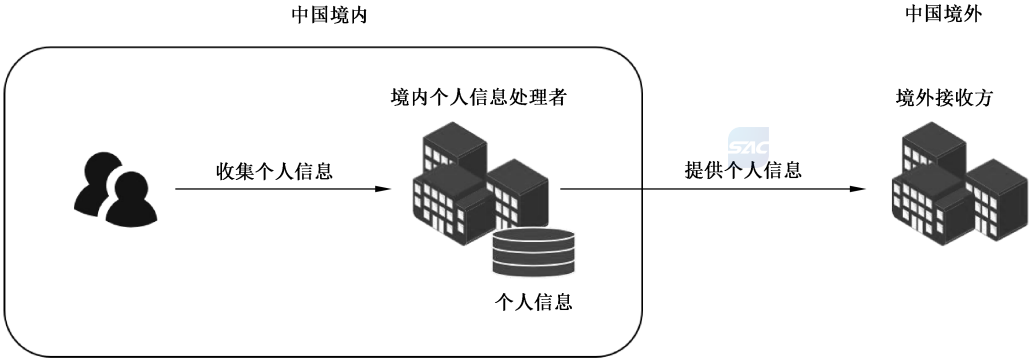

图 A.3　境内个人信息处理者向境外接收方提供个人信息

A.4　境内个人信息处理者与境外接收方共同处理个人信息

境内个人信息处理者与境外接收方共同处理个人信息。例如，境内个人信息处理者与境外接收方进行科研项目合作，将境内自然人的个人信息传输至境外接收方的研发中心；与境外接收方合作推广联名产品或共同提供服务，将境内自然人的个人信息传输至境外接收方的营销中心。

该场景见图 A.4。

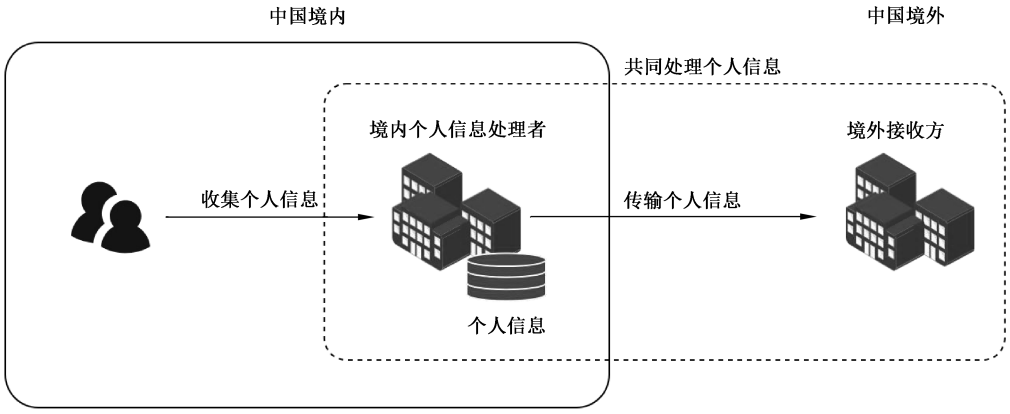

图 A.4　境内个人信息处理者与境外接收方共同处理个人信息

A.5　境外个人信息处理者在境外收集分析境内自然人个人信息

符合《中华人民共和国个人信息保护法》第三条第二款规定，在中华人民共和国境外处理境内自然人个人信息的情形。例如，境外电商平台面向境内自然人提供服务，收集分析境内自然人身份、住址、电话号码等个人信息，及购买记录、购买行为等信息。

该场景见图 A.5。

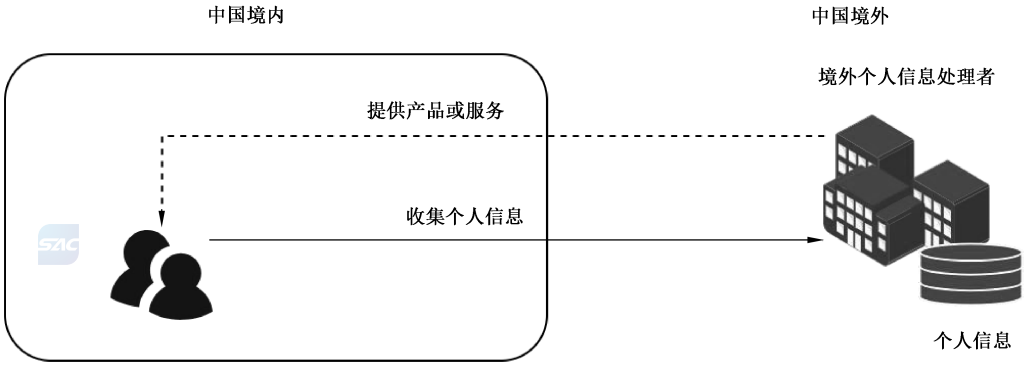

图 A.5　境外个人信息处理者在境外收集分析境内自然人个人信息

附 录 B
（资料性）
个人信息保护影响评估报告模板

B.1 概述

本文件要求的个人信息保护影响评估参考 GB/T 39335—2020 给出的评估原理和实施流程，并重点考虑个人信息跨境处理的场景，补足跨境风险因素。

B.2 评估说明

对评估涉及的如下方面进行说明：

a） 审批页面；
b） 评估起止时间；
c） 实施评估和撰写报告的人员信息；
d） 参考的法律、法规和标准；
e） 实施过程；
f） 实施方式。

B.3 跨境处理个人信息活动整体情况

说明个人信息处理者基本情况、个人信息出境涉及的业务和信息系统、出境个人信息情况、个人信息处理者安全保障能力情况、境外接收方情况和第三方基本情况。包括但不限于以下内容。

a） 个人信息处理者基本情况：
   1） 组织基本信息；
   2） 股权结构和实际控制人信息；
   3） 组织结构信息；
   4） 个人信息保护职责部门信息；
   5） 整体业务与个人信息情况；
   6） 境内外投资情况。
b） 个人信息出境涉及业务和信息系统情况：
   1） 个人信息出境涉及业务的基本情况；
   2） 个人信息出境涉及业务的个人信息资产情况；
   3） 个人信息出境涉及业务的信息系统情况；
   4） 个人信息出境涉及的数据中心（包含云服务）情况；
   5） 个人信息出境链路相关情况。
c） 拟出境个人信息情况：
   1） 说明个人信息处理者和境外接收方处理个人信息的目的、范围和方式等的合法性、正当性和必要性；
   2） 说明出境个人信息的规模、范围、种类和敏感程度，处理敏感个人信息和利用个人信息进行自动化决策情况；
   3） 拟出境个人信息在境内存储的信息系统平台和数据中心等情况，计划出境后存储的信息系统平台和数据中心等。

d) 个人信息处理者数据安全保障能力情况：
   1) 数据安全管理能力，包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估和个人信息主体权益保护等制度及落实情况；
   2) 数据安全技术能力，包括个人信息收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等；
   3) 数据安全保障措施有效性证明，例如开展的个人信息保护认证、数据安全管理认证、数据安全合规审计和网络安全等级保护测评等情况；
   4) 遵守境内外数据和网络安全相关法律法规的情况；
   5) 收到个人信息主体的投诉或诉讼、被监管部门约谈、处罚等情况；
   6) 对个人信息主体权益有重大影响的个人信息处理活动的保障能力。
e) 境外接收方情况：
   1) 境外接收方基本情况；
   2) 境外接收方处理个人信息的用途和方式等；
   3) 境外接收方的数据安全保障能力；
   4) 境外接收方处理个人信息的全生存周期过程描述。
f) 第三方基本情况：
   1) 组织或个人基本信息；
   2) 处理个人信息的目的、方式、种类和保存期限等；
   3) 境外接收方和第三方的关系或合作模式等基本信息；
   4) 第三方所在国家或地区的个人信息保护政策和法规对履行认证规则和标准的影响。
g) 个人信息处理者认为需要说明的其他情况。

B.4 风险分析

B.4.1 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、正当性和必要性

合法性、正当性和必要性风险评估如下。

a) 合法性可重点评估如下方面：
   1) 履行我国政府与其他国家和地区、国际组织签署的条约或协议所规定的情况；
   2) 不属于国家网信部门、公安部门和安全部门等有关部门认定不能出境的情况；
   3) 已取得个人信息主体同意或具有其他处理个人信息的合法性基础，符合国家规定的数据出境前置性程序要求；
   4) 不属于法律法规明令禁止的情况；
   5) 其他可能影响个人信息跨境处理合法性的方面。
b) 正当性可重点评估如下方面：
   1) 个人信息出境及境外接收方处理个人信息具有明确、特定和合理的目的，且使用形式和程序正当；
   2) 不存在故意隐瞒收集使用个人信息真实目的或向相关个人信息主体披露的收集目的与个人信息处理者和境外接收方真实目的不一致的情况；
   3) 处理个人信息所采用的方式方法符合社会公众对个人信息处理者所属行业的一般期待以及公序良俗要求；
   4) 其他可能影响个人信息跨境处理正当性的方面。
c) 必要性可重点评估如下方面：

1） 个人信息跨境处理活动为履行合同义务所必需，或履行法定义务所必需，或同一机构、组织内部开展业务所必需；
2） 向境外传输及出境后处理的个人信息与相关业务功能有直接关联，即没有该等信息的参与，相应功能及业务目的无法实现；
3） 向境外传输及出境后处理数据的频率为实现相关业务功能所必需的最低频率；
4） 向境外传输的个人信息数量为实现相关业务功能所必需的最少数量，企业在评估个人信息处理活动时关注出境的个人信息类型和数量与企业相关业务之间的必要性；
5） 其他可能影响个人信息跨境处理必要性的方面。

B.4.2 跨境处理个人信息的规模、范围、种类和敏感程度，个人信息跨境处理可能对个人信息权益带来的风险

评估个人信息权益受影响等级时，需参考个人信息权益影响常见情形，初步判定影响等级，见表B.1；根据个人信息的规模、范围、种类、敏感程度和技术处理情况等要素对影响等级进行进一步修正，修正要素见表B.2。除以上修正要素外，评估时还可根据实际情形加入相应的修正要素，如某个特定年龄、职业的群体个人信息，是否对个人权益形成额外影响等。

表B.1 个人信息权益影响程度初步判定等级

个人权益影响类别	个人信息权益影响常见情形	影响程度参考	是否存在该影响	个人权益影响程度
影响个人自主决定权	1） 直接导致个人人身自由受限； 2） 遭受人肉搜索、网络暴力、网络攻击、网络霸凌等（涉及未成年人个人信息时需着重考虑）； 3） 被迫执行不合法、不合规的操作	严重		
	1） 被迫执行违反个人意愿的操作； 2） 推送消息影响个人价值观判断； 3） 欺诈、诱骗、误导用户决定	高		
	1） 未提供行使个人权利的途径和方法； 2） 个人维权成本高； 3） 为使用产品或服务而付出额外的、不成比例的资金、时间成本	中		
	被占用额外时间	低		
引发差别性待遇	1） 被用人单位解除劳动关系； 2） 被歧视性对待、打上标签、区别对待	严重		
	1） 遭受歧视性待遇； 2） 无法全部或部分使用应提供的产品或服务	高		
	1） 为使用产品或服务而付出额外的、不成比例的资金、时间成本； 2） 产生害怕和紧张的情绪、导致心理或生理疾病等	中		
	耗费额外的时间获取公平的服务或取得相应的资格	低		

表 B.1　个人信息权益影响程度初步判定等级（续）

个人权益影响类别	个人信息权益影响常见情形	影响程度参考	是否存在该影响	个人权益影响程度
个人名誉受损和遭受精神压力	1）　导致长期无法获得财务收入、导致长期的心理或生理疾病以至于失去工作能力、导致死亡； 2）　信息泄露导致个人社交活动遇到困难，被社会歧视，遭受精神压力，产生心理压力或自闭等疾病	严重		
	1）　被用人单位解除劳务关系、导致心理或生理疾病以致健康遭受不可逆的损害等； 2）　面部识别特征被篡改或嫁接到其他视频，给个人形象造成损坏	高		
	1）　造成误解、名誉受损、产生害怕和紧张的情绪、导致心理或生理疾病等； 2）　指纹被泄露后，不法分子使用指纹进行犯罪，影响个人的生活	中		
	可能导致被频繁打扰、产生厌烦和恼怒情绪等	低		
人身财产受损	遭受金融诈骗、资金被盗用、征信信息受损等	严重		
	造成轻伤、金融诈骗、资金被盗用、征信信息受损等	高		
	1）　造成轻微伤、社会信用受损； 2）　为获取金融产品或服务，或挽回损失付出额外的成本等	中		
	为个人信息更正执行额外的流程	低		

表 B.2　个人信息权益影响程度修正要素

关键要素 个人权益影响类别	个人权益影响程度	修正要素				修正后影响程度
		敏感程度	规模	范围	技术处理措施	
影响个人自主决定权		大部分为敏感个人信息，影响程度可升一级	一年内涉及出境的个人信息大于 50 万人，影响程度可升一级	如果出境个人信息超出满足出境目的最小元素集，则影响程度可升一级	使用技术措施对涉及出境的个人信息进行去标识化处理，能有效防止识别出个人的，影响程度可降一级	
引发差别性待遇						
个人名誉受损和遭受精神压力						
人身财产受损						

B.4.3　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、能力等能否保障跨境处理个人信息的安全

根据境外接收方承诺承担的责任义务，以及对管理和技术措施、能力要求的实施情况，将保障能力等级划分为高、中、低三个等级，见表 B.3。

表 B.3　境外接收方安全保障能力等级

类别	具体描述	保障能力等级参考	保障能力说明及差距分析	结论
技术保障能力	接收方采用了个人信息传输保护、边界防护等总体安全防护技术手段，并建立个人信息出境日志留存机制，能够有效保护个人信息安全，如果被威胁利用，造成的损害可忽略；安全事件还未被证实发生过	高		
	接收方采用的个人信息传输保护、边界防护等技术手段存在可被利用的低等级缺陷，或日志留存机制不够完善，如果被威胁利用，将造成一般损害。 安全事件在同行业、领域被证实发生过	中		
	接收方采用的个人信息传输保护、边界防护等技术手段存在较高等级缺陷，或未建立日志留存机制，无法有效保护数据安全，如果被威胁利用，将造成完全损害。 安全事件曾经发生过或在类似场景下被证实发生过	低		
管理保障能力	接收方具备完备的管理制度、应急机制、审计机制、投诉与处置策略、安全事件上报机制等管理机制，能够有效保护数据安全，如果被威胁利用，造成的损害可忽略。 安全事件还未被证实发生过	高		
	接收方具备基本的管理制度、应急机制、审计机制等管理机制，管理方式有待提升，如果被威胁利用，将造成一般损害。 安全事件在同行业、领域被证实发生过	中		
	接收方不具备有效的管理制度、应急机制、审计机制等管理机制，管理手段缺失严重，数据泄露可能性极大，如果被威胁利用，将造成完全损害。 安全事件曾经发生过或在类似场景下被证实发生过	低		

B.4.4　个人信息跨境处理后泄露、损毁、篡改和滥用等的风险，个人维护个人信息权益的渠道

维护个人信息权益的渠道畅通的影响因素：

a) 在验证个人信息主体身份后，及时响应个人信息主体基于相关法律法规提出的请求，在法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径；
b) 采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使相关权利；
c) 对合理的请求原则上不收取费用，一定时期内多次重复的请求除外；
d) 直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，向个人信息主体提供替代方法，以保障个人信息主体的合法权益；
e) 如决定不响应个人信息主体的请求，向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。

B.4.5　境外接收方所在国家或地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响

境外接收方所在国家/地区个人信息保护政策法规影响等级判定见表 B.4，影响因素包括但不

限于：

a) 境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方曾发生数据安全相关事件及处置情况、境外接收方收到其所在国家或地区公共机关要求其提供个人信息请求及境外接收方应对的情况；

b) 该国家或地区现行的个人信息保护法律法规、普遍适用的标准情况，及与我国个人信息保护相关法律法规、标准的差异；

c) 该国家或地区加入的区域或全球性的个人信息保护方面的组织，以及所做出的具有约束力的国际承诺；

d) 该国家或地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

表 B.4 境外接收方所在国家/地区个人信息保护政策法规影响等级判定

具体描述	保障能力等级参考	保障能力说明及差距分析	结论
境外接收方个人信息跨境传输和处理相关经验丰富，可及时有效处置数据安全相关事件，可有效应对所在国家或地区公共机关要求其提供个人信息的请求。 个人信息保护方面的法律法规标准较为成熟且已形成体系化，与我国相比几乎不存在差异。 加入了区域或全球性的个人信息保护方面的组织。做出了具有约束力的国际承诺。 保障了个人在个人信息方面的各项权利，具备个人信息保护的监督执法机构和相关司法机构，同时具备完备、有效、多层次的救济渠道	高		
境外接收方有个人信息跨境传输和处理相关经验，可处置数据安全相关事件，可应对所在国家或地区公共机关要求其提供个人信息的请求。 个人信息保护方面的法律法规标准基本齐备，与我国相比不存在重大差异。 保障了个人在个人信息方面的部分权利，具备个人信息保护的监督执法机构和相关司法机构，具备相应的行政、司法救济渠道	中		
境外接收方没有个人信息跨境传输和处理相关经验，难以及处置数据安全相关事件，难以应对所在国家或地区公共机关要求其提供个人信息的请求。 个人信息保护方面的法律法规标准欠缺或不完备，与我国相比存在重大差异。 不具备个人信息保护的监督执法机构，个人仅能通过司法救济渠道维护权利	低		

B.4.6 其他可能影响个人信息跨境处理安全的事项

结合具体的个人信息跨境处理场景，分析其他可能影响个人信息跨境处理安全的事项。

B.5 风险综合评估

风险综合评估是根据 B.4.1～B.4.6 的六个方面进行综合评估，分析个人信息跨境处理活动整体的安全风险级别。

B.6 风险处置建议

根据风险综合评估结果，可选取并实施相应的安全控制措施进行风险处置。通常情况下，可根据风险的等级，采取立即处置、限期处置、权衡影响和成本后处置，接受风险等处置方式。相关部门还需持续跟踪风险处置的落实情况，评估剩余风险，将风险控制在可接受的范围内。

参 考 文 献

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

[2] 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

[3] GM/Y 5001—2021 密码标准应用指南(密码行业标准化技术委员会)

[4] ISO/IEC 27701 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines

[5] 国家网络安全事件应急预案(2017 年 1 月 10 日中央网络安全和信息化领导小组办公室发布)

[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)

[7] 数据出境安全评估办法(2022 年 7 月 7 日国家互联网信息办公室令第 11 号发布)

[8] 数据出境安全评估申报指南(第二版)(2022 年 8 月 31 日国家互联网信息办公室发布)

[9] 个人信息出境标准合同办法(2023 年 2 月 22 日国家互联网信息办公室令第 13 号发布)

[10] 促进和规范数据跨境流动规定(2024 年 3 月 22 日国家互联网信息办公室令第 16 号发布)

[11] Guidelines 07/2022 on certification as a tool for transfers,EDPB,2022.6

[12] EU General Data Protection Regulation,2015