ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 个人信息跨境传输认证要求

Information security technology-Certification requirements for cross-border transmission of personal information

（征求意见稿）

（本草案完成时间：2023 年 2 月 10 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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。

本文件由全国信息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、中国网络安全审查技术与认证中心、中国电子标准化研究院、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、中国科学技术大学、中央财经大学、银行卡检测中心、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、蚂蚁科技集团股份有限公司、华为技术有限公司、北京百度网讯科技有限公司、腾讯云计算（北京）有限责任公司、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京快手科技有限公司、北京同城必应科技有限公司、上海商汤智能科技有限公司、中国软件评测中心、成都卫士通信息产业股份有限公司、奇安信科技集团股份有限公司等。

本文件主要起草人：　布宁、陈世翔、王凤娇、胡影、史大为、左晓栋、张金平、王晖、段静辉等。

信息安全技术　个人信息跨境传输认证要求

1　范围

本文件规定了个人信息处理者跨境提供个人信息的基本原则、基本要求和个人信息主体权益保障要求。

本文件适用于认证机构对个人信息处理者跨境提供个人信息活动开展个人信息保护认证，也适用于主管部门、第三方评估机构等组织对个人信息处理者跨境提供个人信息进行监督、管理和评估。

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 25069-2022 信息安全技术　术语

GB/T 35273-2020 信息安全技术　个人信息安全规范

3　术语和定义

GB/T25069-2022、GB/T 35273-2020界定的以及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 35273-2020，3.1，有修改]

3.2

敏感个人信息 sensitive personal information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[来源：GB/T 35273-2020，3.2，有修改]

3.3

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

[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、处理方式的组织或个人。

3.5

境外接收方 outland receiver

位于中华人民共和国境外并自个人信息处理者处接收个人信息的组织或个人。

3.6

单独同意 separate consent

对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意。

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应满足法律法规的规定，按照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，不应违背约定和承诺损害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应满足处理规则公开、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者姓名、联系方式，个人信息跨境处理的目的、范围和处理方式，以及权利、行使权利的方式和程序等，确保个人信息主体了解自身个人信息的跨境处理情况。

4.3 信息质量保障原则

个人信息处理者和境外接收方在跨境处理个人信息时应保障个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

4.4 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应采取必要措施，保护所处理个人信息的安全，确保个人信息跨境处理活动达到《中华人民共和国个人信息保护法》等规定的个人信息保护标准。

4.5 责任明确原则

个人信息处理者和境外接收方应履行法律法规规定的责任义务，在跨境处理个人信息时应保障个人信息主体权益，并指定境内一方、多方或者境外接收方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违规处理活动承担民事法律责任。

4.6 自愿认证原则

鼓励开展个人信息跨境处理活动的个人信息处理者自愿申请个人信息保护认证，充分发挥认证在加强个人信息保护、提高个人信息跨境处理效率方面的作用。

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具有法律约束力和可执行的文件，确保个人信息主体权益得到充分的保障。文件应至少明确下列内容：

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、地址、联系人姓名、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、方式、保存期限、存储地点等；

c） 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；
d） 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；
e） 救济、合同解除、违约责任、争议解决等；
f） 境外接收方承诺并遵守同一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；
g） 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；
h） 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、行政法规管辖；
i） 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；
j） 个人信息处理者和境外接收方均承诺对侵害个人信息权益行为承担民事法律责任，并明确约定双方应承担的民事法律责任；
k） 其他应遵守的法律、行政法规规定的义务。

5.2 组织管理

5.2.1 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，由本组织的决策层成员担任。个人信息保护负责人应承担下列职责：

a） 明确个人信息保护工作的主要目标、基本要求、工作任务、保护措施；
b） 为本组织的个人信息保护工作提供人力、财力、物力保障，确保所需资源可用；
c） 指导、支持相关人员开展本组织的个人信息保护工作，确保个人信息保护工作达到预期目标；
d） 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。

5.2.2 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设立个人信息保护机构，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） 依法制定并实施个人信息跨境处理活动计划；
b） 组织开展个人信息保护影响评估；
c） 监督本组织按照约定的个人信息跨境处理规则处理跨境个人信息，保护个人信息权益；
d） 采取有效措施保证按照约定的处理目的、范围、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；
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、配合检查等。

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共同遵守同一个人信息跨境处理规则，规则应至少包括下列事项：

a） 明确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、敏感程度等；
b） 明确跨境处理个人信息的目的、方式和范围；
c） 明确个人信息境外存储的起止时间及期满后的处理方式；

d) 明确跨境处理个人信息需要中转的国家或者地区；
e) 明确保障个人信息主体权益所需资源和采取的措施；
f) 明确个人信息安全事件的赔偿、处置规则。

5.4 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，评估报告至少保存3年。评估报告应至少包括下列事项：

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、类型、敏感程度、频率，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的泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等；
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数据安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者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，及与我国个人信息保护相关法律法规、标准情况的差异；
   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。

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，有权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实现，或直接向境外接收方提出请求。个人信息处理者无法实现的，应通知并要求境外接收方协助实现。个人信息主体有权要求个人信息处理者和境外接收方对其个人信息跨境处理规则进行解释说明；
d) 个人信息主体有权拒绝个人信息处理者仅通过自动化决策方式作出的个人信息跨境处理决定；

e) 个人信息主体有权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) 个人信息权益受到损害时，个人信息主体有权向个人信息处理者、境外接收方的任何一方提出赔偿要求；
g) 个人信息主体有权依据《中华人民共和国民事诉讼法》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责任义务

人信息处理者和境外接收方应履行下列责任义务：

a) 以电子邮件、即时通信、信函、传真等方式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，以及向境外提供个人信息的目的、类型和保存时间，并取得个人信息主体的单独同意；
b) 如果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认证所提出的要求，境外接收方在知道前述变化后立即通知个人信息处理者及认证机构；
c) 按照已签署的具有法律效力文件约定的处理目的、处理方式、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；
d) 境外接收方承诺不将所接收的个人信息提供给第三方。如确需提供的，应满足中华人民共和国有关法律、行政法规要求，并采取必要措施确保第三方个人信息跨境处理活动达到《中华人民共和国个人信息保护法》规定的个人信息保护标准；
e) 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、补充或者删除其个人信息时，应及时予以响应，拒绝其请求的，应说明理由；
f) 客观记录开展的个人信息跨境处理活动，保存记录至少 3 年；按照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；
g) 当出现难以保证个人信息安全的情况时，及时停止跨境处理个人信息，并通知对方；
h) 发生或者可能发生个人信息泄露、篡改、丢失的，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，报告中华人民共和国履行个人信息保护职责的部门，按照相关法律法规要求通知个人信息主体，记录并留存所有与个人信息泄露、篡改、丢失有关的事实及其影响，包括采取的所有补救措施。通知、报告包含以下内容：
   1) 个人信息泄露、篡改、丢失的原因；
   2) 泄露的个人信息种类和可能造成的危害；
   3) 已采取的补救措施；
   4) 个人可以采取的减轻危害的措施；
   5) 负责处理个人信息泄露、篡改、丢失的负责人或负责团队的联系方式。
i) 应个人信息主体的请求，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；
j) 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；
k) 承诺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、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；
l) 承担证明相关责任义务已履行的举证责任；
m) 承诺遵守中华人民共和国个人信息保护有关法律、行政法规，接受中华人民共和国司法管辖；承诺与个人信息跨境处理有关的纠纷适用中华人民共和国相关法律法规。

参 考 文 献

[1] GB/T 35273-2020 信息安全技术　个人信息安全规范

[2] 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）

[3] 数据出境安全评估办法（国家互联网信息办公室令第11号）

[4] 国家互联网信息办公室关于《个人信息出境标准合同规定（征求意见稿）》公开征求意见的通知(国家互联网信息办公室 2022年6月30日)

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

[6] APEC Privacy Framework，APEC，2005

[7] EU General Data Protection Regulation，2015