TC260-PG-20222A

网络安全标准实践指南

—个人信息跨境处理活动安全认证规范

(v1.0-202206)

全国信息安全标准化技术委员会秘书处

2022 年 6 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国网络安全审查技术与认证中心、中国电子技术标准化研究院等单位的技术支持。

摘　要

本实践指南依据有关政策法规要求，为落实《个人信息保护法》建立个人信息保护认证制度提供认证依据。申请个人信息保护认证的个人信息处理者应当符合GB/T 35273《信息安全技术 个人信息安全规范》的要求；对于开展跨境处理活动的个人信息处理者，还必须符合本实践指南的要求。本实践指南从基本原则、个人信息处理者和境外接收方在跨境处理活动中应遵循的要求、个人信息主体权益保障等方面提出了要求，为认证机构实施个人信息保护认证提供跨境处理活动认证依据，也为个人信息处理者规范个人信息跨境处理活动提供参考。

目　录

1 适用情形

本文件作为认证机构对个人信息跨境处理活动进行个人信息保护认证的基本要求，适用于以下情形：

a) 跨国公司或者同一经济、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；

b) 《中华人民共和国个人信息保护法》第三条第二款适用的个人信息处理活动。

2 认证主体

跨国公司或者同一经济、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可以由境内一方申请认证，并承担法律责任。

《中华人民共和国个人信息保护法》第三条第二款规定的境外个人信息处理者，可以由其在境内设置的专门机构或指定代表申请认证，并承担法律责任。

3 基本原则

a) 合法、正当、必要和诚信原则。个人信息处理者在跨境处理个人信息时应当满足法律法规的规定，严格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，严守合同、协议等具有法律效力文件的约定和承诺，不得违背约定和承诺损害个人信息主体的合法权益。

b) 公开、透明原则。个人信息处理者在跨境处理个人信息时应当满足处理规则公开、处理过程透明要求，及时向个人信息主体告知个

人信息跨境提供的目的、范围和处理方式，确保个人信息主体了解自身个人信息的跨境处理情况。

c) 信息质量原则。个人信息处理者和境外接收方在跨境处理个人信息时应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

d) 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应当采取必要措施，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相关法律法规规定的个人信息保护标准。

e) 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应当采取必要措施，保护所处理个人信息的安全，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承担法律责任。

f) 自愿认证原则。个人信息跨境处理活动认证属于国家推荐的自愿性认证，鼓励符合条件的个人信息处理者和境外接收方在跨境处理个人信息时自愿申请个人信息跨境处理活动认证，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。

4 基本要求

4.1 有法律约束力的协议

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之间应当签订具有法律约束力和执行力的文件，确保个人信息主体权益得到充分的保障。文件应当至少明确下列内容：

a) 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；

b) 跨境处理个人信息的目的以及个人信息的类别、范围；

c) 个人信息主体权益保护措施；

d) 境外接收方承诺并遵守统一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；

e) 境外接收方承诺接受认证机构监督；

f) 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；

g) 明确在中华人民共和国境内承担法律责任的组织；

h) 其他应当遵守的法律、行政法规规定的义务。

4.2 组织管理

4.2.1 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承担。个人信息保护负责人应当承担下列职责：

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。

4.2.2 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) 监督本组织按照处理者和境外接收方约定的个人信息跨境处理规则处理跨境个人信息；

d) 接受和处理个人信息主体的请求和投诉。

4.3 个人信息跨境处理规则

开展个人信息跨境处理活动的处理者和境外接收方遵守统一的个人信息跨境处理规则，至少包括下列事项：

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、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到期后的处理方式；

d) 跨境处理个人信息需要中转的国家或者地区；

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。

4.4 个人信息保护影响评估

开展个人信息跨境活动的个人信息处理者事前评估向境外提供个人信息活动是否合法、正当、必要，所采取的保护措施是否与风险程度相适应并有效等，个人信息保护影响评估至少包括下列事项：

a) 向境外提供个人信息是否符合法律、行政法规；

b) 对个人信息主体权益产生的影响，特别是境外国家和地区的法律环境、网络安全环境等对个人信息主体权益的影响；

c) 其他维护个人信息权益所必需的事项。

5 个人信息主体权益保障

5.1 个人信息主体权利

a) 个人信息主体是个人信息处理者和境外接收方签订法律文件中涉及个人信息主体权益相关条款的受益人，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；

b) 个人信息主体对其个人信息的处理享有知情权、决定权，有权撤回对其个人信息跨境处理的同意，有权限制或者拒绝他人对其个人信息进行处理；

c) 个人信息主体有权向境外接收方查阅、复制、更正、补充、删除其个人信息；

d) 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；

e) 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的

方式作出决定；

f) 个人信息主体有权对违法个人信息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；

g) 个人信息主体有权在其经常居住地所在法院向开展个人信息跨境处理活动的处理者和境外接收方提起司法诉讼；

h) 其他法律、行政法规规定的权利等。

5.2 个人信息处理者和境外接收方的责任义务

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) 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，不得超出约定跨境处理个人信息；

c) 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，应当及时予以响应，拒绝其请求的，应当说明理由；

d) 当出现难以保证跨境个人信息安全的情况时，应当及时中止跨境处理个人信息；

e) 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；

f) 应个人信息主体的请求，提供法律文本中涉及个人信息主体权

益部分的副本；

g) 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，承担法律赔偿责任；

h) 承诺接受中华人民共和国认证机构对个人信息跨境处理活动的监督，包括答复询问、例行检查等；

i) 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。