

TC260-PG-2022XX

---

# 网络安全标准实践指南

## —个人信息跨境处理活动认证技术规范

---

(征求意见稿 v1.0-202204)

全国信息安全标准化技术委员会秘书处

2022年4月

本文档可从以下网址获得：

[www.tc260.org.cn/](http://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

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。



## 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》第38条建立个人信息保护认证制度提供认证依据。本实践指南从基本原则、相关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跨境处理活动认证提供认证依据，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

摘 要 .....	III
1 适用情形 .....	1
2 认证方式 .....	1
3 基本原则 .....	1
4 基本要求 .....	2
4.1 法律约束 .....	3
4.2 组织管理 .....	3
4.3 个人信息跨境处理规则 .....	4
4.4 个人信息保护影响评估 .....	5
5 个人信息主体权益保障 .....	5
5.1 个人信息主体权利 .....	5
5.2 相关方的责任义务 .....	6





## 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、事业实体内部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》第三条第二款规定的境外个人信息处理者，在境外处理境内自然人个人信息的活动。

按照法律、行政法规、部门规章有关规定，需要通过国家网信部门组织的安全评估的个人信息跨境处理活动，应当向国家网信部门申报安全评估。

中华人民共和国缔结或者参加的国际条约、协定，对向中华人民共和国境外提供个人信息的条件有规定的，按照其规定执行。

## 2 认证方式

跨国公司或者同一经济、事业实体内部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，可以由境外组织机构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。个人信息直接关系到信息主体的人格尊严，跨境个人信息处理应当满足法律法规的规定，严格按照

法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，不随意违背约定、承诺损害个人信息主体的合法权益。

b) 公开、透明原则。跨境处理个人信息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己的个人信息的处理全过程。

c) 信息质量原则。参与跨境处理个人信息活动的相关方应当保证跨境个人信息的准确性、完整性，避免个人信息处理活动出现偏差，对个人信息主体权益造成不利影响。

d) 同等保护原则。参与个人信息跨境处理活动的相关方应当采取必要措施，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。参与个人信息跨境处理活动的相关方应当采取必要措施，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、多方或者境外相关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跨境活动相关方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的作用。

## 4 基本要求



## 4.1 法律约束

参与个人信息跨境处理活动的相关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) 参与个人信息跨境处理活动的相关方；
- 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) 各相关方承诺并遵守统一的个人信息处理规则，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) 各相关方承诺接受认证机构监督；
- f) 各相关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机构；
- 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

参与个人信息跨境处理活动的相关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，由本组织机构的决策层成员承担。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) 为本组织机构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机构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) 向本组织机构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**

参与个人信息跨境处理活动的相关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，并在个人信息跨境处理活动中承担下列职责：

a) 制定并实施各相关方均认可的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) 监督本组织机构按照相关方约定的个人信息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**

参与个人信息处理的相关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，包括个人信息类型、敏感程度、数量等；

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

参照 GB/T 39335 《信息安全技术 个人信息安全影响评估指南》的最新版本,参与个人信息跨境活动的相关方事先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有效并与风险程度相适用等,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;
- c) 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;
- d) 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跨境处理活动相关方签订法律文件中个人信息权益相关条款的受益人,有权要求个人信息跨境处理相关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,有权限制或者拒绝他人对其个人信息进行处理;



- c) 有权向境外接收方查阅、复制、更正、补充、删除其个人信息；
- d) 有权要求个人信息跨境处理活动相关方对其个人信息处理规则进行解释说明；
- e) 有权拒绝仅通过自动化决策的方式作出决定；
- f) 有权向中华人民共和国监管机构进行投诉、举报；
- g) 有权在其经常居住地所在法院向参与个人信息跨境处理的相关方提起司法诉讼；
- h) 其他法律、行政法规规定的权利等。

## 5.2 相关方的责任义务

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参与个人信息跨境处理活动相关方的基本情况，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跨境提供个人信息的处理目的、处理方式、保护措施等处理跨境个人信息，不得超出约定处理个人信息；

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，应当说明理由和救济途径；

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

e) 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；



f) 境内法律负责承担方承诺为个人信息主体行使权力提供便利条件，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；

g) 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管，包括答复询问、例行检查等；

h) 承诺遵守中华人民共和国个人信息保护有关法律法规，接受中华人民共和国司法管辖。

