

个人信息保护认证实施规则

1 适用范围

本规则依据《中华人民共和国认证认可条例》制定，规定了对个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等处理活动进行认证的基本原则和要求。

2 认证依据

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，还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。

上述标准、规范原则上应当执行最新版本。

3 认证模式

个人信息保护认证的认证模式为：

技术验证 + 现场审核 + 获证后监督

4 认证实施程序

4.1 认证委托

认证机构应当明确认证委托资料要求，包括但不限于认证委托人基本材料、认证委托书、相关证明文档等。

认证委托人应当按认证机构要求提交认证委托资料，认证机构在对认证委托资料审查后及时反馈是否受理。

认证机构应当根据认证委托资料确定认证方案，包括个人信息类型和数量、涉及的个人信息处理活动范围、技术验证机构信息等，并通知认证委托人。

4.2 技术验证

技术验证机构应当按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告。

4.3 现场审核

认证机构实施现场审核，并向认证委托人出具现场审核报告。

4.4 认证结果评价和批准

认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

4.5 获证后监督

4.5.1 监督的频次

认证机构应当在认证有效期内，对获得认证的个人信息处理者进行持续监督，并合理确定监督频次。

4.5.2 监督的内容

认证机构应当采取适当的方式实施获证后监督，确保获得认

证的个人信息处理者持续符合认证要求。

4.5.3 获证后监督结果的评价

认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

4.6 认证时限

认证机构应当对认证各环节的时限作出明确规定，并确保相关工作按时限要求完成。认证委托人应当对认证活动予以积极配合。

5 认证证书和认证标志

5.1 认证证书

5.1.1 认证证书的保持

认证证书有效期为 3 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。

证书到期需延续使用的，认证委托人应当在有效期届满前 6 个月内提出认证委托。认证机构应当采用获证后监督的方式，对符合认证要求的委托换发新证书。

5.1.2 认证证书的变更

认证证书有效期内，若获得认证的个人信息处理者名称、注册地址，或认证要求、认证范围等发生变化时，认证委托人应当向认证机构提出变更委托。认证机构根据变更的内容，对变更委托资料进行评价，确定是否可以批准变更。如需进行技术验证和/

或现场审核，还应当在批准变更前进行技术验证和/或现场审核。

5.1.3 认证证书的注销、暂停和撤销

当获得认证的个人信息处理者不再符合认证要求时，认证机构应当及时对认证证书予以暂停直至撤销。认证委托人在认证证书有效期内可申请认证证书暂停、注销。

5.1.4 认证证书的公布

认证机构应当采用适当方式对外公布认证证书颁发、变更、暂停、注销和撤销等相关信息。

5.2 认证标志

不含跨境处理活动的个人信息保护认证标志如下：



包含跨境处理活动的个人信息保护认证标志如下：



“ABCD”代表认证机构识别信息。

5.3 认证证书和认证标志的使用

在认证证书有效期内，获得认证的个人信息处理者应当按照

有关规定在广告等宣传中正确使用认证证书和认证标志，不得对公众产生误导。

6 认证实施细则

认证机构应当依据本规则有关要求，细化认证实施程序，制定科学、合理、可操作的认证实施细则，并对外公布实施。

7 认证责任

认证机构应当对现场审核结论、认证结论负责。

技术验证机构应当对技术验证结论负责。

认证委托人应当对认证委托资料的真实性、合法性负责。