ICS 33.050
CCS M 30

团　体　标　准

T/TAF 148—2023

电信和互联网个人信息保护保障能力评估规范

Telecommunications and internet evaluation specification of personal information protection and guarantee ability

2023-02-08 发布　　2023-02-08 实施

电信终端产业协会　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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、OPPO广东移动通信有限公司、泰尔认证中心有限公司、维沃移动通信有限公司、北京快手科技有限公司、南昌黑鲨科技有限公司、荣耀终端有限公司、小米通讯技术有限公司、北京奇虎科技有限公司、蚂蚁科技集团股份有限公司、阿里巴巴（中国）有限公司、北京三星通信技术研究有限公司、华为技术有限公司、上海兆言网络科技有限公司、北京抖音信息服务有限公司、广州视源电子科技股份有限公司、联想（北京）有限公司、北京微梦创科网络技术有限公司、北京三快在线科技有限公司、珠海市魅族科技有限公司。

本文件主要起草人：魏凡星、王嘉义、傅山、李可心、陈鑫爱、李京典、姜慧格、王浩仟、刘陶、王艳红、杜云、王宇晓、李腾、付艳艳、宁华、凌大兵、常琳、贾科、赵盈洁、落红卫、王昕、沈彭军、赵之成、赵晓娜、顾泽宇、杜文博、姚一楠、彭晋、林冠辰、黄天宁、吴越、衣强、李实、严涵、钱雷、杨骁涵、肖洋、李洁、李汝鑫、刘俊、邹庆、任资政、刘瑾、祖岩岩、沈玲、毕烽。

引　　言

随着《网络安全法》、《个人信息保护法》的落地和实施，个人信息保护已经成为广大人民群众最关心最直接最现实的利益问题之一，对个人信息处理者的个人信息保障能力要求也日益凸显。如何保障个人在个人信息处理活动中的权利，如何约束个人信息处理者的义务成为当前急需解决的问题之一。本文件将落实法律法规的要求，提出电信和互联网行业对个人信息保护能力的评估规范，指导行业进行系统性的评估人员建设、能力建设、规程建设，落实个人信息保护工作。

电信和互联网个人信息保护保障能力评估规范

1 范围

本文规定电信和互联网行业个人信息处理者在处理个人信息时应具备的相关保障能力，包含个人信息处理活动，个人信息处理者的义务等内容。

本文件适用于个人信息处理者自评估及第三方评估机构开展评估工作。

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

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：个人信息保护法]

3.2

敏感个人信息 personal sensitive information

一旦泄露、非法提供或者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者歧视性待遇等的个人信息。

注：敏感个人信息包括公民身份号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

[来源：GB/T 35273—2020，3.2，有修改]

3.3

个人信息主体 personal information subject

个人信息已识别或者可识别的自然人。

[来源：GB/T 35273—2020，3.3，有修改]

3.4

收集 collect

获得个人信息的控制权的行为。

[来源：GB/T 35273—2020，3.5，有修改]

3.5

第三方应用 third party application

由第三方提供的产品或者服务，以及被接入或者嵌入网络运营者产品或者服务中的自动化工具，包括但不限于软件开发工具包（SDK）、第三方代码、组件、脚本、接口、算法模型、小程序等。

3.6

删除 delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.7

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

[来源：GB/T 35273—2020，3.14]

4 缩略语

下列缩略语适用于本文件。

SIM：用户身份模块（Subscriber Identity Module）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

5 个人信息保护保障能力评估基本要求

5.1 评估原则

开展个人信息保护保障能力评估应遵循以下原则：

a) 目的性原则：评估目的应明确具体，评估范围应与评估目的相适应；

b) 可用性原则：应确保保障能力措施实施情况可被准确评测，并能和具体评估指标对应进行评估；

c) 全面性原则：评估应当贯穿个人信息全周期，实现对个人信息保护流程的全面控制；

d) 可调性原则：评估方应确保能够根据评估对象及应用场景不同进行调整，以适应多种情况的评估。

5.2 评估架构

个人信息保护保障能力评估内容是电信和互联网行业个人信息处理者在处理个人信息时应具备的相关保障能力，包含个人信息处理活动，个人信息处理者的义务等方面。评估架构如图1所示。

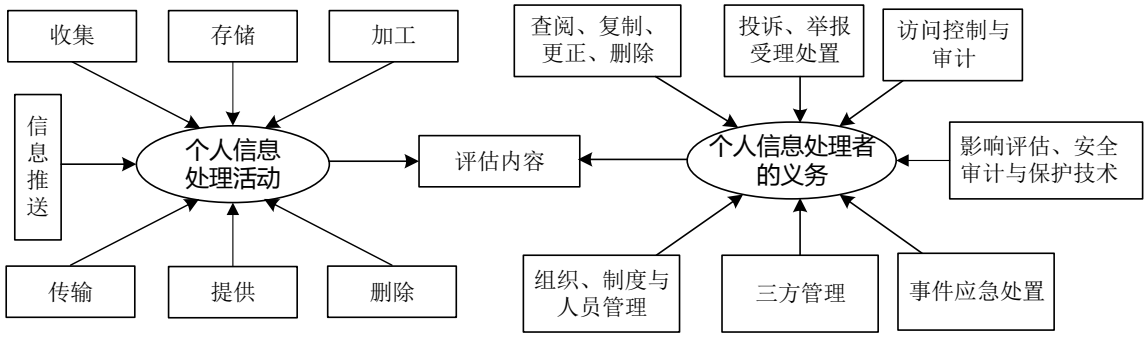

图1　个人信息保护保障能力评估架构图

6　个人信息保护保障能力评估指标

6.1　个人信息处理活动

6.1.1　收集

个人信息处理者为提供服务而必需处理个人信息的，应遵循合法、正当、必要的原则，不应收集与其提供的服务无直接或无合理关联的个人信息，且应符合以下要求：

a）　应制定和公开个人信息保护政策并严格遵守，个人信息保护政策应满足 GB/T 35273-2020 5.5 有关个人信息保护政策的要求；

b）　以取得个人同意为合法基础收集个人信息的，应在收集个人信息前明示个人信息保护政策，并征得个人信息主体同意；

c）　改变处理个人信息的目的、类型、范围、用途的，应及时告知个人信息主体，修改个人信息保护政策，并重新征得个人信息主体同意，涉及个人信息保护政策变动的应修改个人信息保护政策；

d）　明示所提供产品和服务类型，以及该类产品和服务所必需的个人信息，不应因用户拒绝提供该类产品和服务所必需的个人信息以外的信息，而拒绝提供该核心业务功能服务；不应仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为目的，强制要求、误导用户同意收集个人信息；

e）　不应存在强制授权、过度授权、超范围收集个人信息等行为；

f）　收集敏感个人信息前，应征得个人信息主体的单独同意，确保同意是在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

g）　收集不满14周岁未成年人个人信息前，应征得其监护人的单独同意；

h）　从个人信息主体以外的其他途径获得个人信息的，应了解个人信息来源、个人信息提供方已获得的个人信息处理的授权同意范围，并按照本文件的要求履行安全保护义务。数据提供方应在确保其个人信息安全的基础上提供数据。

6.1.2　存储

存储个人信息应满足以下要求：

a）　存储个人信息时，应采用加密、访问控制、安全审计等安全措施；

b）　存储和处理敏感个人信息的服务器应采取隔离措施；

c） 存储个人信息时，不应超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期，法律法规另有规定的除外；
d） 存储个人生物识别信息，应满足 GB/T 35273-2020 6.3 b）和c）的要求；
e） 数据接收方存储个人信息时，应按合同约定要求采取安全措施。

6.1.3 加工

加工个人信息应满足以下要求：
a） 在使用未明确分类分级的个人信息时，应在处理前确定个人信息级别，如无法确认则按照最高等级进行保护；
b） 应仅在具有特定目的和充分必要性，并采取严格保护措施情形下处理敏感个人信息，处理敏感个人信息应取得个人的单独同意；
c） 应确保个人信息处理应用系统、中间件、服务器等基础设施满足企业信息安全基线要求，并持续评估安全风险。

6.1.4 信息推送

个人信息推送应满足以下要求：
a） 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式，如拒绝接受信息推送，或停止、退出、关闭相应功能的机制。当用户退出或关闭信息推送模式时，应及时停止继续收集仅用于信息推送服务的个人信息，并宜向用户提供删除或匿名化信息推送功能所基于的个人信息的选项；
b） 利用个人信息进行自动化决策，应保证决策的透明度和结果公平合理；
c） 不应强制用户使用定向推送功能，包括未标明定推、未明示第三方个人信息来源、未标识定推、未提供关闭选项。

6.1.5 传输

传输个人信息应满足以下要求：
a） 个人信息的传输应按照约定目的和用途进行，传输前应对双方进行身份认证和授权，如设计敏感个人信息应明确跨安全域之间数据传输控制策略；
b） 若通过公共网络传输账户设置、传感采集、金融支付等服务相关的敏感个人信息时，应采用数字签名等技术手段保证数据的完整性和抗抵赖性，同时应采用密文方式传输。宜先对个人信息进行匿名化，消除能够识别特定个体的所有数据字段后再进行转移；
c） 传输敏感个人信息时，应采用加密等安全措施，如使用安全的HTTPS传输协议。

6.1.6 提供

提供个人信息应满足以下要求：
a） 向其他个人信息处理者提供其处理的个人信息的，应告知向他人提供的目的、类型、方式、范围、用途、存储期限，并征得个人信息主体同意；
b） 向其他个人信息处理者提供其处理的个人信息的，应与数据接收方通过合同等形式明确双方的个人信息安全保护责任和义务，采取加密、脱敏等措施保障重要个人信息安全；
c） 个人信息处理者对嵌入的第三方自动化工具，如软件开发工具包（SDK）、第三方代码、组件、脚本、接口、算法模型等，宜开展技术检测确保其个人信息处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入；

d) 应督促和监督第三方应用运营者加强个人信息安全管理，发现第三方应用没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；
e) 个人信息处理者知道或者应知道第三方应用利用其平台侵害用户权益的，应采取必要措施保障用户权益免受侵害；
f) 发生兼并、重组、破产时，数据接收方应继续履行相关个人信息安全保护义务；没有数据接收方的，应对数据作删除处理。

6.1.7 删除

删除个人信息应满足以下要求：
a) 当个人信息超出法律法规规定或者双方约定的存储期限，或者网络产品和服务停止运营，或者个人信息主体注销账号，或者当用户撤销同意后，个人信息处理者应及时对个人信息做删除或者匿名化处理，法律法规、部门规章另有规定的除外；
b) 在开发测试等生产活动完成后，应及时清除相关存储空间个人信息；
c) 存储个人信息的介质进行更换、下线、报废前，应在介质离开安全区域前及时清除数据，个人信息处理者应采用物理损毁等方式进行销毁，确保介质上数据不可恢复。

6.2 个人信息处理者的义务

6.2.1 个人信息处理者基本要求

个人信息处理者应满足以下基本要求：
a) 应全面识别组织涉及的个人信息；
b) 应对个人信息实行分类分级管理：分类分级维度包括但不限于法律法规要求、自身业务特性、行业要求；
c) 通过软件、系统或平台收集个人信息的，个人信息处理者应符合安全设计规范和安全审计要求；
d) 应采取加密、脱敏、去标识化、备份、访问控制、审计等技术或者其他必要措施，防止个人信息的泄露、篡改、损毁、不正当使用等。

6.2.2 访问控制与审计

应满足以下访问控制与审计要求：
a) 个人信息处理者开展个人信息处理活动时，应基于分类分级采取安全管理措施，明确相关人员的访问权限，防止非授权访问；
b) 个人信息处理者开展个人信息处理活动时，对个人信息的关键操作，如批量修改、拷贝、删除、下载等，应设置内部审批和审计流程，并严格执行；
c) 应按照审批流程授权个人信息接触岗人员，不应出现未授权的信息类型新增；
d) 访问控制应做到职责分离、最小化授权和可溯源审计；
e) 应保证个人信息处理过程中的安全性，在整个过程中个人信息不应被第三方无关人员或组织获知，过程数据和结果数据都应进行保护；
f) 对个人信息进行分析处理时，应保证处理系统稳定安全运行，不造成个人信息的损毁、泄露和丢失等。

6.2.3 查阅、复制、更正、删除

应满足以下查阅、复制、更正、删除的要求：

a) 应建立渠道和机制，及时响应和处理个人信息主体查阅、复制、更正、删除其个人信息的请求，不应对请求设置不合理条件；
b) 应满足 GB/T 35273 8.7 有关响应个人信息主体请求的要求。

6.2.4 投诉、举报受理处置

个人信息处理者应建立投诉、举报受理处置制度，收到相关投诉、举报的，应及时查实，并依法采取停止传输、消除等处置措施。

6.2.5 组织

应满足以下组织要求：

a) 处理个人信息达到国家网信部门规定数量的个人信息处理者应任命专门的个人信息保护负责人，负责人应具备以下要求：
   1) 应具有相关管理工作经历和专业知识；
   2) 具有较强独立性，负责人不宜兼任有利益冲突的职位；
   3) 应参与个人信息处理活动的重要决策，并直接向公司主要负责人报告。
b) 应明确企业个人信息保护责任人，负责有关个人信息处理活动的重要决策，履行相关职责，并提供资源保障，包括但不限于人力、财力、物力保障。
c) 应设立专门的企业级个人信息保护工作机构支持个人信息保护负责人工作，明确机构工作职责，机构内宜包括管理决策、政策支持、技术支持等部门或人员。
d) 个人信息保护机构主要负责统筹个人信息安全工作，具体职责可包括：
   1) 制订工作计划并督促落实；
   2) 制订、签发、实施、更新个人信息保护政策和规程；
   3) 建立、维护、更新个人信息清单和授权访问策略；
   4) 组织开展个人信息保护影响分析和风险评估，督促整改；
   5) 组织开展个人信息安全培训；
   6) 组织产品上线前个人信息安全检测；
   7) 组织个人信息安全审计；
   8) 处理、通报、报告个人信息保护相关工作或事件情况；
   9) 组织受理和处置个人信息保护相关投诉、举报。

6.2.6 制度

应满足以下制度要求：

a) 应建立个人信息管理制度体系，包括但不限于安全策略、管理制度、操作规程、记录表单等；
b) 应制订个人信息保护总体方针和安全策略等相关制度文件，文件内容包括但不限于公司个人信息保护工作目标、范围、原则和安全框架等说明；
c) 应制订个人信息管理规范等制度文件，明确对于个人信息保护的指引和要求，突出个人信息接触岗对个人信息日常管理的操作规程和要求；
d) 个人信息管理制度应由个人信息保护负责人或机构制订，明确制订程序和发布方式；
e) 应对相关制度执行情况进行记录，确保实际工作流程正确执行；
f) 个人信息对外披露或共享时，应按照企业个人信息保护机构制订的流程进行审批，审批通过后才可执行。

6.2.7 人员管理与考核

应满足以下人员管理与考核要求：

a) 应与个人信息处理岗员工签订保密协议，明确保密要求；
b) 应明确个人信息处理不同岗位安全职责，明确个人信息安全管理考核指标和问责机制，对相关人员特别是重要岗位人员的履职情况进行考核；出现个人信息安全重大事件时，对直接负责的主管人员和其他直接责任人员进行问责；
c) 应定期进行安全培训、考核，确保人员掌握个人信息安全管理相关流程；
d) 应采用最小权限原则设置人员权限和审批流程，对于批量修改、复制、下载个人信息等行为进行严格审核；
e) 对于超权限操作应经个人信息保护负责人或机构授权并存档记录；
f) 人员工作变动时，应及时调整相应信息访问和使用权限；
g) 应与个人信息接触外部人员或外部组织签订保密协议，明确保密要求；
h) 应建立外部人员访问企业安全措施，规定外部人员可访问区域、访问权限、访问内容和操作记录等要求。

6.2.8 第三方管理

应满足以下第三方管理要求：

a) 应建立第三方接入管理机制和工作流程，明确必要的风险评估等机制设置接入条件；
b) 应通过签订合同等形式约定双方或多方的安全责任与实施的个人信息安全措施；
c) 宜对于第三方接入工具，如代码、脚本、SDK、小程序等开展技术检测，确保其个人信息收集使用行为符合要求；
d) 应对第三方个人信息处理活动进行审计，发现违约行为应及时处理纠正，对于重大违约行为应及时切断接入。

6.2.9 影响评估

应满足以下影响评估要求：

a) 应建立个人信息保护影响评估制度，并定期进行评估。
b) 组织的个人信息保护机构应配置评估所需资源，评估团队成员应包括技术部门、业务部门、法律部门、标准部门等代表。
c) 个人信息处理者在以下几种场景下，应当事前进行个人信息保护影响评估并对处理情况进行记录：
    1) 处理敏感个人信息；
    2) 利用个人信息进行自动化决策；
    3) 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
    4) 向境外提供个人信息；
    5) 其他对个人权益有重大影响的个人信息处理活动。
d) 应在适当的场景和时机进行评估，包括但不限于以下场景：
    1) 新产品/服务设计阶段、初次上线评估；
    2) 新功能/业务发生重大变化时；
    3) 法律法规、政策、标准有重大变化时重新评估；
    4) 企业内外部环境发生重大变化时重新评估；
    5) IT基础设施发生重大变化；
e) 应形成个人信息保护影响评估报告并妥善留存，报告内容包括但不限于：
    1) 个人信息的处理目的、处理方式等是否合法、正当、必要；

2） 对个人权益的影响及安全风险；
3） 所采取的保护措施是否合法、有效并与风险程度相适应；
4） 适用范围；
5） 相关人员信息；
6） 依据法律、法规和标准；
7） 评估对象、评估内容；
8） 风险分析结果；
9） 风险处置建议。

6.2.10 安全审计

应满足以下安全审计要求：

a） 应监测记录组织的个人信息处理活动，宜建立自动化审计系统，审计过程记录应能对安全事件处置、应急响应和事后调差提供支撑；
b） 应防止非授权访问、篡改或删除审计记录；
c） 应及时处理审计过程中发现的违规使用、滥用等情况。

6.2.11 保护技术

应满足以下保护技术要求：

a） 应具备足够的技术措施确保个人信息的保密性、完整性，防止篡改、损毁、窃取、丢失、泄露等情况；
b） 宜部署个人信息或数据安全监测系统，针对个人信息处理过程安全风险进行分析，并采取不同处置策略；
c） 应确保技术措施有效性、并根据合规情况持续改进。

6.2.12 事件应急处置

应满足以下事件应急处置要求：

a） 应制订个人信息安全事件应急预案，包括应急处理流程、事件上报流程等。
b） 应建立个人信息安全事件应急响应机制，并根据个人信息安全计划的变化而及时调整，确保个人信息安全事件得到及时有效处置，应急响应机制应包括：
1） 个人信息安全事件分级；
2） 启动条件；
3） 启动所需的资源，如人员、设备、场所、工具、资金等；
4） 流程、人员安排和操作手册。
c） 应定期举行个人信息应急培训和应急演练，并定期对原应急预案进行重新评估、完善。
d） 应配备应急响应所需的资源，确保应急响应机制能够有效实施。
e） 应制定应急演练计划，按计划或者在应急响应机制发生变化后，组织开展应急演练，检验和完善应急响应机制，提高实战能力。
f） 发生个人信息安全事件时，个人信息处理者应立即启动应急响应机制，采取相应的补救和防范措施，可能造成危害的，应及时以电话、短信、邮件或者信函等方式告知个人信息主体，同时对可能危害国家安全、公共安全、经济安全和社会稳定的应按相关要求向有关部门报告。

7 个人信息保护保障能力评估方法

7.1 评估框架

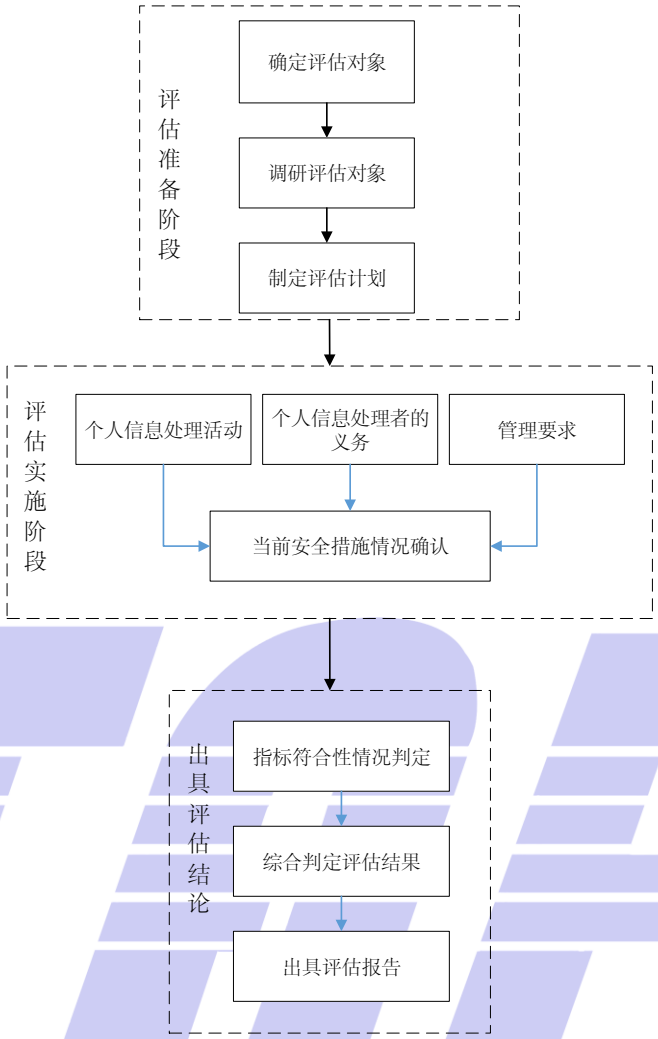

图2 个人信息保护保障能力评估框架

个人信息保护保障能力评估包括自评估和第三方评估两种形式。评估流程分为评估准备、评估实施和出具评估结论三个部分，如图2所示。评估准备阶段应实施以下步骤：

a) 确定评估对象：评估对象可以是被评估方的一种或多种产品或服务，可以是被评估方的某个或多个关键信息系统和关键业务流程，也可以是被评估方的部分或全部系统、部门等；

b) 调研评估对象：评估方应组建相应的评估团队，对评估对象进行充分调研，了解评估对象相关信息，准备相应辅助评估工具等；

c) 制定评估计划：评估方应根据评估对象调研结果制定合理的评估计划安排。

评估实施阶段评估方应根据不同评估内容采用相应的评估方法进行评估，通过问卷、文档审阅和访谈等方法确认评估内容的实际保护措施或要求落实情况等。

出具评估结论阶段应包括评估报告和结论，根据评估实施内容和具体评估指标相符合情况给出说明。

7.2 自评估流程

7.2.1 确定评估对象

根据评估目标，评估方和被评估方应共同确定评估对象。若评估形式为自评估且由评估方自行实施时，应由评估方自行确定评估对象。若评估形式为自评估且由评估方委托第三方实施时，应由评估方和受委托方协商确定，以评估方意见为主，受委托方提供建议。若评估形式为检查评估时，被评估方应配合评估方或评估方委托的第三方确认评估对象。

7.2.2 调研评估对象

评估对象确认后，应对其相关的个人信息处理活动和个人信息处理者的义务分别进行调研。

个人信息处理调研应至少包括以下方面：

a) 主要的业务功能和个人信息处理活动规模；
b) 相关个人信息处理系统；
c) 相关个人信息类型和敏感程度；
d) 相关组织结构和人员；
e) 相关制度和流程。

个人信息处理者的义务调研应至少包括以下方面：

a) 相关组织结构和人员；
b) 相关管理制度和流程。

保障管理要求调研应至少包括以下方面：

a) 相关组织结构和人员；
b) 相关管理制度和流程。

7.2.3 制定评估计划

评估方应合理预估评估工作复杂度和工作量，合理制定评估计划。评估计划中应包括以下内容：

a) 评估对象和范围、评估依据、评估环境、评估工具；
b) 评估团队人员角色分工等；
c) 评估工作计划，包括工作内容、输出结果等；
d) 时间进度安排。

7.2.4 实施评估

应考虑以下方面，实施评估工作：

a) 依据对应的评估规范标准开展实施评估活动；
b) 各部分实施评估工作可顺序开展也可并行开展，无完整的顺序关系；
c) 评估过程中均需输出评估过程文档，其内容至少应包括评估对象、评估所选择的评估指标及针对评估指标的评估结果。

7.2.5 出具评估结论

应考虑以下方面，给出评估结论：

a) 在评估报告中，应包含评估的环境、评估基本要素和每一项评估的结果，同时还应具体描述评估过程中的步骤，如包含未通过项则评估报告中应包含未通过原因的具体描述；
b) 根据评估对象情况给出整改意见和建议；
c) 若有需要，宜提供整改后复查环节；
d) 自评估方法。

7.3 自评估方法

7.3.1 个人信息处理活动

如被评估产品或服务已正常发布运营，由评估方根据被评估产品或服务的个人信息保护政策以及实际产品表现等和被评估方确定其个人信息处理活动的范围，然后对照相应评估指标进行评估。

如被评估产品或服务尚未发布或已停止服务，应按照产品和服务所处的不同生命周期阶段进行评估，并覆盖之前阶段的评估内容。各个阶段评估的主要内容可包括：

需求分析阶段：

a) 具有需求说明书，并包括个人信息清单和专门的个人信息保护需求分析内容；

b) 进行需求评审，部分场景还应进行专门的个人信息保护影响评估。

设计阶段：

a) 采用的技术路线和算法等对需求分析中的个人信息进行了充分保护，并满足个人信息保护影响评估要求；

b) 个人信息保护政策设计、个人信息保护功能设计、个人信息主体权益保护设计满足相应指标要求；

c) 第三方SDK通过安全检测，符合个人信息处理活动指标要求，第三方SDK提供者满足个人信息处理者的义务和相应管理要求；

d) 进行个人信息保护评审。

开发阶段：

a) 与设计文档中的个人信息保护要求相符合；

b) 满足业界公认的安全编码规范要求；

c) 避免将个人信息直接硬编码写入程序。

测试审核阶段：

a) 创建并维护个人信息保护测试用例，覆盖个人信息处理活动、个人信息处理者义务等指标；

b) 对个人信息保护影响评估报告中的内容进行测试，并设置阻塞项；

c) 业务团队进行整改后需再次进行测试，如整改涉及到设计文档中的个人信息保护方案设计的更改，需重新组织相关方案的评审；

d) 测试环境与生产环境隔离。

发布部署阶段：

a) 进行发布前基准测试；

b) 确认个人信息保护评审通过，个人信息保护测试审核通过。

运行维护阶段：

a) 适时进行个人信息保护保障能力评估，尤其是产品上线前和个人信息处理过程发生重大变更时；

b) 当个人信息保护保障能力评估指标更新或发生重大个人信息安全事件后重新进行个人信息保护保障能力评估。

停止服务阶段：

a) 及时通知用户并预留充分处理时间，提供个人信息处理的合理选项，包括数据复制、删除等，协助用户完成个人信息处理；

b) 在通知截止日期后及时删除用户个人信息。

7.3.2 个人信息处理者的义务

被评估方通过自证等方式提供证明材料，评估方通过问卷、文档审阅和访谈等方式对证明材料内容进行评估确认。

7.4 检查评估

检查评估的流程参考本文件7.2，评估方法参考本文件7.3。个人信息处理者满足本标准及附录A所有要求时，有关符合本标准的第三方认证结果才可被出具。

附 录 A
（资料性）
个人信息保护保障能力认证要求

A.1 总则

本附录所给出的信息适用于个人信息处理者申请并获得符合本标准的认证结果时的要求，要求参考了ISO/IEC 导则 第1部分 ISO补充规定的附件SL中给出的高层结构。

A.2 规范性引用

除了第2章给出的规范性引用文件外，本附录补充以下文件对于本附录的应用是必不可少的。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 1900-2016 质量管理体系 基础和术语（ISO 9000:2015,IDT）

A.3 术语和定义

除了第3章给出的术语和定义外，GB/T 1900-2016界定的术语和定义适用于本附录。

A.4 组织环境

A.4.1 理解个人信息处理者及其环境

个人信息处理者应确定影响其实现个人信息保护预期结果能力的各种外部和内部因素。

A.4.2 理解相关方需求和期望

个人信息处理者应确定：

a） 个人信息保护保障能力的相关方；

b） 这些相关方与个人信息保护相关的要求。

注：相关方的要求可包括法律、法规要求和合同要求，应至少包括6.2.1内容。

A.4.3 确定个人信息保障能力范围

个人信息处理者应确定个人信息保护保障能力的边界及适用性，以确定其保障范围。

在确定范围时，组织应考虑：

a） A.4.1 提到的外部和内部因素；

b） A.4.2 提到的要求；

c） 个人信息处理者实施的活动之间的及其余其他组织实施的活动之间的接口和依赖关系。

个人信息处理者应保留关于能力范围的成文信息。

A.4.4 个人信息保护保障能力范围

个人信息处理者应按照本标准及本附录的要求，建立、实施、保持和改进个人信息保护的保障能力。

A.5 领导

A.5.1 领导作用和承诺

参照6.2.5 b）。

A.5.2 个人信息保护保障能力方针

参照6.2.6 b）。

A.5.3 个人信息保护岗位、职责和权限

参照6.2.5 a）、c）、d）。

A.6 策划

A.6.1 策划输入

在策划个人信息保障能力所需实现的预期水平时，个人信息处理者应考虑A.4.1所描述的因素、A.4.2所提及的要求，以及6.2.9所获得评估结果。

A.6.2 策划输出

个人信息处理者应策划所需实现的个人信息保障能力水平，并提出具体目标，目标应与个人信息保护方针一致，可测量，予以沟通，适时更新。个人信息处理者应保留具体目标成文信息。

A.7 支持

A.7.1 资源

个人信息处理者应确定并提供个人信息保障能力所需的资源。

A.7.2 技术

参照6.2.11。

A.7.3 意识与能力

参照6.2.7。

A.7.4 沟通

个人信息处理者应确定与个人信息保护保障能力相关的内部和外部沟通，包括：

a) 与个人信息主体的沟通，参照：6.1.1 b)、c)、f)、g)、h)，6.1.7 b)，6.2.3，6.2.12 f)
b) 与公众沟通，包括：6.2.4，以及定期发布个人信息保护社会责任报告
c) 个人信息处理者内部的沟通

A.7.5 形成文件的信息

参照6.2.6。

A.8 运行

A.8.1 收集

参照6.1.1、6.2.3。

A.8.2 存储

参照6.1.2。

A.8.3 加工

参照6.1.3。

A.8.4 信息推送

参照6.1.4。

A.8.5 传输

参照6.1.5。

A.8.6 提供

参照6.1.6。

A.8.7 删除

参照6.1.7。

A.8.8 访问控制与审计

参照6.2.2。

A.8.9 第三方管理

参照6.2.8。

A.8.10 风险及应急处置

参照6.2.12。

A.9 评价

A.9.1 影响评估

参照6.2.9。

A.9.2 安全审计

参照6.2.10。

A.9.3 自评估

参照7.2和7.3。

A.9.4 管理评审

企业个人信息保护责任人应按策划的时间间隔对企业的个人信息保护保障能力进行评审，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑下列内容：

a） 以往管理评审所采取措施的情况；

b） 与个人信息保护保障能力相关的各种外部和内部因素的变化，包括：相关方需求和期望的变化、法律法规要求的变化等；

c） 个人信息保护保障能力方针和目标的实现程度；

d） 不符合及纠正措施；

e） 影响评估、安全审计、自评估、相关认证等结果；

f） 资源的充分性；

g） 改进的机会。

管理评审的输出应包括与下列事项相关的决定和措施：

a） 改进的机会；

b） 资源需求；

c） 个人信息保护保证能力所需的变更。

个人信息处理者应保留成文信息，作为管理评审结果的证据。

A.10 改进

A.10.1 不符合和纠正措施

当发生不符合时，个人信息处理者应：

a） 对不符合做出响应，适用时：

- 采取措施控制并纠正不符合；
- 处理后果；

b） 通过以下方式评价消除不符合原因的措施需求，以防止不符合再次发生或在其他地方发生：

- 评审不符合；
- 确定不符合的原因；
- 确定是否存在或是否可能发生类似的不符合。

c） 实施任何所需的措施，并评审其有效性；

d） 必要时，对个人信息保护制度或相关要求进行变更。

纠正措施应与所发生的不符合造成影响的重要程度相适应。

组织应保留对不符合、所采取措施以及有效性的文件化信息。

注：不符合包括但不限于：影响评估、安全审计、自评估、监管检查等所发现的问题，以及个人信息安全事件等。

A.10.2 持续改进

个人信息处理者应持续改进个人信息保护保障能力的适宜性、充分性和有效性。

电信终端产业协会团体标准

电信和互联网个人信息保护保障能力评估规范

T/TAF 148—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn