ICS 33.030
CCS M 21

团　体　标　准

T/TAF 236—2024

个人信息保护保障能力评估规范 深度合成服务

Personal information protection and guarantee ability—Deep synthesis service

2024-09-02 发布　　2024-09-02 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、北京快手科技有限公司、华为终端有限公司、维沃移动通信有限公司、百度在线网络技术（北京）有限公司、荣耀终端有限公司、北京三星通信技术研究有限公司、北京微梦创科网络技术有限公司、OPPO广东移动通信有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：冯金金、傅山、王嘉义、魏凡星、杨萌科、刘陶、陈鑫爱、王艳红、落红卫、谷晨、李实、赵盈洁、姚一楠、郭建领、王颖华、李辰淑、吴越、任资政、邹庆、李根、李腾、刘献伦。

引　　言

近年来，随着深度合成技术不断发展，越来越多的组织、个人参与到深度合成服务的开发和使用。深度合成服务造成的个人信息泄露事件时有发生，为落实相关法律法规的要求，提出个人信息保护保障能力评估规范 深度合成服务，用于指导行业进行系统性的保障能力建设、规程建设、技术建设，落实个人信息保护工作。

个人信息保护保障能力评估规范　深度合成服务

1　范围

本文件规定电信和互联网行业深度合成服务提供者在评估提供深度合成服务时应满足的个人信息保护保障能力要求等内容。

本文件适用于深度合成服务提供者进行自评估，同时也适用于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。

T/TAF 148—2023　电信和互联网个人信息保护保障能力评估规范

3　术语和定义

3.1

深度合成技术　deep synthesis technology

利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等信息的技术，包括语音合成、人脸再现、全身合成、数字虚拟人、虚拟现实等场景。

3.2

深度合成服务　deep synthesis service

利用深度合成技术，合成出图像、视频、音频等数字化内容的服务。

3.3

深度合成服务提供者　deep synthesis service provider

提供深度合成服务的组织、个人。

3.4

深度合成服务使用者　deep synthesis service user

使用深度合成服务，制作、复制、发布、传播信息的组织、个人。

4　缩略语

下列缩略语适用于本文件。

APP：移动互联网应用程序（mobile internet application）

5 个人信息保护保障能力评估概述

5.1 评估原则

开展基于深度合成服务的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：应确保评估指标可覆盖保障能力措施实施情况。
c) 全面性原则：评估应当贯穿个人信息保护全生命周期，实现对个人信息保护全面评价。
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 评估内容

深度合成服务提供者提供的深度合成服务，在数据安全、深度合成模型、深度合成服务使用等方面提供的个人信息保护保障能力。

5.3 评估对象

本文件中的评估对象为深度合成服务提供者。

6 个人信息保护保障能力评估要求

6.1 保障功能要求

6.1.1 基本要求

深度合成服务提供者处理个人信息时，应符合T/TAF 148—2023 中6.1 个人信息处理活动、6.2.1 个人信息处理者基本要求、6.2.2 访问控制与审计中的相关要求。

6.1.2 深度合成模型安全防护能力要求

深度合成模型安全防护能力应符合如下要求：

a) 应采取加密、访问控制等技术手段保证算法模型的存储安全，防止被恶意组织或个人窃取，造成深度合成服务使用者个人信息泄露；
b) 应采取权限管控等措施保证模型设计文件的安全性，防止因设计文件被利用而导致深度合成服务使用者个人信息泄露；
c) 应采取代码审计等措施保证模型代码的安全性，防止因代码中的潜在问题和错误导致深度合成服务使用者个人信息泄露；
d) 应建立算法模型管理制度，明确算法涉及的个人信息范围、个人信息主体授权同意情况、存储位置、存储时间、测评记录、上线记录、下线记录、部署记录等信息；
e) 应建立深度合成服务使用制度，明确做好使用流程记录，包括深度合成服务使用者唯一标识、深度合成服务提供者唯一标识、生成时间、内容唯一标识、算法模型标识等。

6.1.3 深度合成服务数据安全防护能力要求

深度合成服务数据安全防护能力应符合如下要求：

a) 利用个人信息作为训练数据前，应通过用户协议、隐私声明、弹窗等方式提前告知用户，采用公开数据作为训练数据的除外；

b） 在提供深度合成服务时，涉及人脸信息等敏感个人信息编辑功能的，应通过用户协议、弹窗等形式提前告知用户相关要求；
c） 应建立分级分类的安全存储和访问机制，采取加密、访问控制等技术手段保证个人信息安全；
d） 除个人信息主体授权同意用于其他用途外，应及时删除不再使用和存储期满的个人信息；
e） 应采取技术措施保证日志的完整性。

6.1.4 深度合成服务标识要求

应根据使用场景和生成内容是否容易混淆，对使用深度合成服务生成的信息内容添加显式标识或隐式标识。

6.2 保障管理要求

6.2.1 组织

应满足以下组织要求：
a） 应建立个人信息保护组织机构，符合T/TAF 148—2023中6.2.5 组织中的相关要求；
b） 应设置人员负责深度合成服务个人信息保护工作，人员应满足以下要求：
1） 应具有相关工作经历、具备深度合成技术专业知识和深度合成技术相关法律法规知识。
2） 应具有较强独立性，不宜兼任可能有利益冲突的职位。
3） 应参与基于深度合成服务个人信息处理活动的重要决策，并直接向公司负责深度合成工作的人报告。
c） 应设立深度合成服务个人信息保护工作组，明确工作组工作职责，组内宜包括管理决策、政策支持、技术支持等部门或人员，依据法律法规和相关标准及时负责完善企业内部管理制度。

6.2.2 制度

应满足以下制度要求：
a） 应建立管理制度体系，符合T/TAF 148—2023中6.2.6 制度的相关要求。

6.2.3 管理机制

应建立健全基于深度合成服务个人信息保护的管理机制：
a） 除确不需要用户账户外，应建立用户真实身份信息验证机制，验证用户真实身份后向用户提供深度合成服务。
b） 除确不涉及用户账户外，应建立深度合成服务使用者账号管理机制，对违法制作、复制、发布、传播不良信息的，依法依约采取警示、限制功能、暂停服务、关闭账号等处置措施，保存日志记录，并上报相关部门；
c） 应建立完善用户举报投诉处置措施，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；
d） 应建立深度合成模型安全评估机制，定期审核、评估、验证生成合成类算法机制机理，确保服务无法泄露个人信息；
e） 应建立溯源机制，应支持查询利用深度合成服务制作、复制、发布、传播的处理链条数据；
f） 应建立内容审核机制，构建用于识别违法和不良信息的特征库，能对深度合成服务使用者的输入数据和合成结果进行审核；
g） 应建立训练数据管理机制，加强训练数据管理，保障训练数据安全；
h） 应建立违法违规服务处理机制，予以及时下线。

6.2.4 人员管理与考核

应满足以下人员管理与考核要求：

a) 应建立人员管理与考核机制，符合 T/TAF 148—2023 中 6.2.7 人员管理与考核的相关要求。

6.2.5 事件应急处理

应满足以下事件应急处置要求：

a) 应建立事件应急处理机制，符合T/TAF 148—2023中6.2.12 事件应急处置的相关要求。

6.2.6 第三方管理

应满足以下第三方管理要求：

a) 使用第三方提供深度合成服务或深度合成技术时，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处置措施；

b) 应通过签订合同等形式，约定双方或多方的安全责任与个人信息安全措施；

c) 宜对第三方接入工具，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) 应主动查看第三方个人信息处理活动审计情况，发现违约行为及时切断接入；

e) 使用第三方的深度合成服务时，应主动查看其备案信息、公示信息等相关资质证照。

6.2.7 安全审计

应满足以下安全审计要求：

a) 应建立全审计机制，符合T/TAF 148—2023中6.2.10 安全审计的相关要求。

7 个人信息保护保障能力评估方法

7.1 总体要求

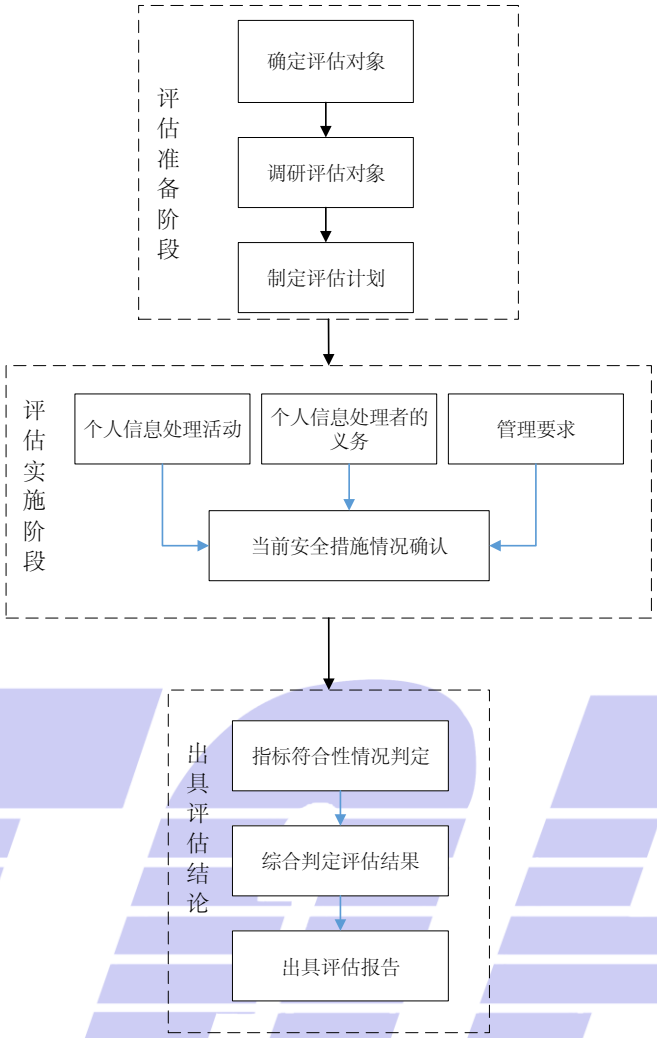

图1　个人信息保护保障能力评估流程图

深度合成服务提供具有生成或者编辑人脸、人声等生物识别信息的模型、模板等工具时，深度合成服务提供者应依法自行或者委托专业机构开展安全评估：

a）　评估包括自评估和检查评估两种形式；

b）　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1所示；

c）　评估准备阶段应实施以下步骤：

1）　第一步，评估方应协同被评估方确定评估对象，如被评估方的一种或多种产品或服务、被评估方的某个或多个关键信息系统和关键业务流程、被评估方的部分或全部系统、部门等；

2）　第二步，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；

3）　第三步，评估方应根据对评估对象的调研结果制定合理的评估计划安排。

d）　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；

e）　出具评估结论阶段，应根据评估实施内容和具体评估指标相符合情况给出评估报告和结论。

7.2　确定评估对象

应根据评估目标，评估方和被评估方共同确定评估对象：

a) 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。
b) 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。
c) 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。

7.3 调研评估对象

评估对象确认后，应对其相关的保障功能要求和保障管理要求分别进行调研：
a) 保障功能要求应至少调研以下方面：
   1) 基本信息管理能力；
   2) 主要的业务功能和个人信息处理活动规模；
   3) 相关个人信息处理系统；
   4) 相关个人信息类型和敏感程度；
   5) 相关组织结构和人员；
   6) 相关制度和流程。
b) 保障管理要求应至少调研以下方面：
   1) 相关组织结构和人员；
   2) 相关管理制度和流程。

7.4 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。

7.5 评估方法

评估方法应确定评估范围、评估指标、综合计算方法等：
a) 被评估方应提供可进行测评的深度合成服务版本或APP等；
b) 被评估方应通过自证等方式提供证明材料；
c) 评估方应通过问卷、文档审阅和访谈等方式对证明材料内容进行评估确认；
d) 评估方应依据保障功能要求及保障管理要求的评估指标进行确认；
e) 评估方可针对评估条款进行深度分析，并结合现行法律法规和相关行业标准以及市场情况，在量化的基础上制定出量标，按一定的量标实行评估，或采用数学模型方式实行评估；
f) 评估方可进行定性评估，结合专家意见征询、民意调查和公识获取综合进行评估。

7.6 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。

7.7 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；

b) 评估结论如包含未通过项，则评估报告中应包含未通过原因的具体描述；

c) 根据评估对象情况给出整改意见和建议；

d) 若有需要，宜提供整改后复查环节。

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范
[2] T/TAF 077.7—2020 APP 收集使用个人信息最小必要评估规范 人脸信息

电信终端产业协会团体标准

个人信息保护保障能力评估规范　深度合成服务

T/TAF 236—2024

*

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