ICS 33.030
CCS M 21

团　体　标　准

T/TAF 268.8—2025

生成式人工智能个人信息保护技术要求
第 8 部分：供应链管理

Generative artificial intelligence personal information protection technical requirements—Part 8: Supply chain management

2025-02-10 发布　　　　2025-02-10 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。

本文件是T/TAF 268《生成式人工智能个人信息保护技术要求》的第8部分。T/TAF 268已发布了以下部分：

——第1部分：总则；

——第2部分：隐私声明告知；

——第3部分：训练数据构建；

——第4部分：模型规制控制；

——第5部分：二次开发管理；

——第6部分：输出策略控制；

——第7部分：个人权利响应；

——第8部分：供应链管理。

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、阿里巴巴（中国）有限公司、中兴通讯股份有限公司、北京快手科技有限公司、新华三技术有限公司、北京微梦创科网络技术有限公司、联通华盛通信有限公司、北京卡路里科技有限公司、上海声网科技有限公司、OPPO广东移动通信有限公司、科大讯飞股份有限公司、广州视睿电子科技有限公司、蚂蚁科技集团股份有限公司、珠海魅族科技有限公司、荣耀终端股份有限公司、厦门美柚股份有限公司、维沃移动通信有限公司、北京理想汽车有限公司、广州虎牙信息科技有限公司、北京转转精神科技有限责任公司、友盟同欣（北京）科技有限公司、华为终端有限公司、北京小桔科技有限公司、北京象信智能科技有限公司、高通无线通信技术(中国)有限公司、北京智者天下科技有限公司。

本文件主要起草人：武林娜、王艳红、王淞鹤、屈蕾蕾、陈鑫爱、李可心、汪海、李京典、杨萌科、周飞、安达、李碧君、熊有竹、潘万鹏、谷晨、落红卫、李培、任资政、康宇、刘觅、王海涛、曹昉赫、张天若、陈宝金、钱雷、李根、李腾、王士进、高建清、刘胜宇、尹志超、林冠辰、石玉珍、朱玲凤、周煌凯、李辰淑、赵晓娜、黄鹏华、徐曼、贾科、刘晓杰、胡梦云、马海龙、李晨瑜、姚栋、贾紫薇、阮玲宏、董继征、孙铁、许锐、王磊、周辰、王江胜、杨弋。

引　　言

在生成式人工智能领域，第三方供应商的集成是一种战略上的必然。经济因素和海量的训练数据源是生成式人工智能服务提供者需引入供应商的主要原因，它通常超出许多组织自身的能力，同时也影响着研发成本和训练成果，从而决定生成式人工智能产品或服务在市场上的扩张与收缩。

供应链安全目前是一个世界性难题，尤其是开源项目，其维护者对安全问题的重视度和修复积极性较低。供应链中可能会产生个人信息风险，其来源可能包含供应商提供的含有明文个人信息的训练数据，也有从用户反馈中获取的个人信息。随着这些数据在供应链各个环节的传输、加工和处理，会将隐私安全暴露到供应链中，加大个人信息泄露和滥用的风险。

因此，亟待制定相关标准，来规范生成式人工智能服务在供应链安全部分的个人信息保护的要求，来保障用户的个人信息在供应链使用过程啊中的合规和安全，促进生成式人工智能合理应用和健康发展。

T/TAF 268—2025旨在对生成式人工智能的个人信息保护问题提出技术要求，拟由8部分构成。

——第1部分：总则。目的在于规定生成式人工智能服务个人信息保护的术语、总体原则和个人信息保护框架。

——第2部分：隐私声明告知。目的在于提出向服务使用者进行隐私声明告知时的个人信息保护技术要求。

——第3部分：训练数据构建。目的在于提出生成式人工智能数据集构建过程中的个人信息保护技术要求。

——第4部分：模型规制控制。目的在于提出生成式人工智能模型训练阶段个人信息保护方面的规制控制要求。

——第5部分：二次开发管理。目的在于提出面向开发者提供二次开发应用时，个人信息保护相关的管理要求。

——第6部分：输出阶段管理。目的在于提出生成式人工智能服务在内容输出时对输出阶段管理的个人信息保护要求。

——第7部分：个人权利响应。目的在于提出服务提供者对于服务使用者个人权利响应要求。

——第8部分：供应链管理。目的在于提出供应链管理中所应满足保护个人信息安全的技术要求和管理措施。

生成式人工智能个人信息保护技术要求　第8部分：供应链管理

1　范围

本文件规定了生成式人工智能服务提供者在生成式人工智能系统的设计阶段、训练阶段和应用阶段的供应链管理过程中所应满足保护个人信息安全的管理措施。

本文件适用于指导生成式人工智能服务提供者在供应链管理过程中对个人信息安全保护的管理，同时适用于监管机构、第三方测评机构对生成式人工智能个人信息保护在供应链管理方面的安全控制情况进行监督与评估。

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 25069　信息安全技术　术语

GB/T 41867—2022　信息技术　人工智能　术语

3　术语和定义

GB/T 25069—2010、GB/T 41867—2022界定的以及下列术语和定义适用于本文件。

3.1

供应链　supply chain

生成式人工智能供应链是指生成式人工智能的产品或服务从概念形成、设计、开发、训练、到达市场应用及其生命周期管理的直接关联节点，包括物理设备的生产，以及软件、算法和服务的开发和部署。

3.2

供应商　supplier

在生成式人工智能供应链网络中，向下游用户或产品提供必要的算法、数据、计算资源或其他人工智能开发组件的组织或个体。

3.3

供应链管理　supply chain management

从生成式人工智能供应链整体目标触发，对算法设计、开发、训练、测试、部署、迭代的全过程的计划、组织、协调、控制的活动或过程。

4　缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

CPU：中央处理单元（Central Processing Unit）

GPU：图形处理单元（Graphic Processing Unit）

NPU：神经网络处理单元（Neural-network Processing Uni）

SLA：服务等级协议（Service Level Agreement）

5 概述

生成式人工智能系统的高度复杂和扩展性需求，导致对生成式人工智能服务提供者的供应链要求较高。个人信息在整个生成式人工智能供应链流转过程中的安全风险也会扩大。生成式人工智能供应链框架，见图1，主要包括以下三个阶段：

a) 在设计阶段，服务提供者即应识别与记录生成式人工智能系统中涉及的第三方供应商以及数据预处理时包含的个人信息。服务提供者应对识别的供应商及时开展安全评估，并与供应商明确个人信息的使用权利与保护责任，以保障个人信息在供应链中的合规使用与风险可控；

b) 在训练阶段，服务提供者应能针对 AI 模型的预训练和调参过程中供应商可能影响个人信息安全的不良因素进行控制。这些不良因素集中在供应商提供的训练数据、AI 模型和计算环境；

c) 在应用阶段，服务提供者应关注潜在的与供应链关联的个人信息安全事件应急处置，包括应急预案制定和事件上报等。

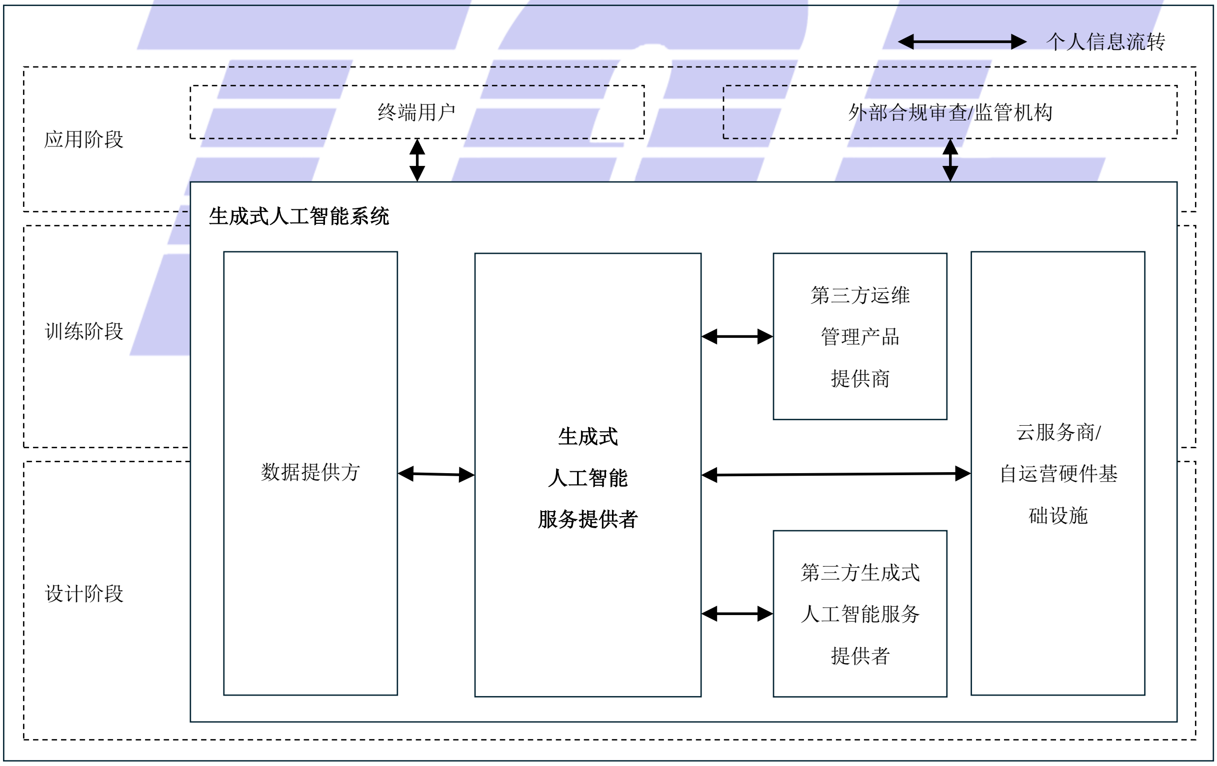

图 1 生成式人工智能供应链模型

6 供应商识别和记录

应记录第三方生成式人工智能系统及其组件是如何被集成开发或使用在系统中的，以及个人信息在相关系统和组件中流转情况，识别并记录生成式人工智能系统供应商组件中可能存在的个人信息及其数据生命周期。生成式人工智能供应链中可能包含的供应商类型包括：

a) 数据提供方：提供可能包括个人信息的原始数据的实体，这些数据将用于训练和测试 AI 模型；
b) 第三方生成式人工智能服务提供者：由服务提供者采购或使用的由第三方提供的生成式人工智能能力的实体，从而进行产品、服务的封装或二次开发、训练；
c) 云服务商：提供云计算资源的实体，为训练 AI 模型提供必要的基础设施，例如云计算环境、大数据平台、存储能力等；
d) 硬件提供商：制造和供应 AI 系统所需物理组件的实体，例如 CPU、GPU、NPU、内存和其他高性能计算和存储硬件；
e) 第三方运维管理产品提供商：可能包括提供数据清洗、标注等工具，以及身份鉴别、访问控制、日志记录等安全功能的软件或服务提供商，这些软件或服务用于人工智能系统运维管理。

注：供应链中的每个实体都有责任保护个人信息，并确保安全和合乎道德地使用生成式人工智能技术。

7 设计阶段

7.1 供应商评估机制

为了保护个人信息在生成式人工智能供应链中的安全，服务提供者在选择供应商的过程中应评估和选择具有足够安全控制能力和合规证据的供应商，并对其进行评审，以消除相关安全风险。对于不同的供应商类型，应满足相应的安全能力或获取相关证明。

7.1.1 通用评估机制

对所有类型的供应商，评估机制包括：

a) 个人信息安全风险评估：应对供应商可能带来的个人信息保护安全风险纳入风险评估范围，包括物理和逻辑访问、个人信息的获取、使用、存储、修改、删除等，以及第三方产品或服务对生成式人工智能业务的支持程度和保护能力；
b) 综合评估：应通过对供应商产品或服务的敏感性进行评估和选择供应商，例如开展市场分析、客户参考、舆论情报、合规认证、文件评审、现场评估等，确定供应商提供的产品或服务能够针对个人信息提供足够的安全控制。

7.1.2 数据提供方

对数据提供方的评估机制包括：

a) 个人信息收集来源保障：应要求数据提供方提供并证明个人信息的合法收集来源；
b) 加密能力保障：若模型训练过程涉及使用密码技术对个人信息进行保护，宜要求数据提供方具备相应的加解密能力；
c) 数据分类分级标准对齐：宜确保数据提供方提供的数据（尤其是个人信息）进行了分类分级，并映射至服务提供者自身的分类分级方案。

7.1.3 第三方运维管理产品提供商

对第三方运维管理产品提供商的评估机制包括：

日志记录内容核查：应核查第三方运维管理产品是否会记录可能包含个人信息的日志，如服务运行日志、错误日志等；对于包含个人信息日志的产品，应评估其是否具有相应的个人信息保护能力，并根据评估结果实施相应的个人信息保护措施。

7.1.4 无法开展评估的情况

当服务提供者无法对供应商开展评估（例如政府监管部门或指定供应商的情况）时，宜根据风险评估结果实施必要的补偿控制，例如加强内部监控和日志审计，以及针对员工的个人信息保护意识开展培训等。

7.2 供应商协议和权责划分

应建立供应商协议并形成文件，以确保服务提供者和供应商对双方履行相关个人信息保护要求的权利和责任有明确的理解。为满足确定的安全要求，宜考虑在协议中包含以下条款：

a) 明确界定服务提供者与供应商合作过程中关于个人信息保护的角色、关系、义务、责任和职能；
b) 依照法律、法规和监管要求，明确供应商所提供产品或服务的数据保护、个人信息处理方式，以及如何确保满足这些要求的说明；
c) 在协议中包含明确的保密条款；
d) 明确项目过程中的安全管理要求，尤其是出现个人信息安全相关问题时，对处理措施、流程的要求，如异常事件的处理流程，响应机制等；
e) 明确项目过程中供应商服务变更应遵循的流程，包括服务内容、服务人员的变更，需要对变更造成的个人信息安全影响进行评估，并就处理方式进行约定，有效控制变更带来的个人信息安全风险；
f) 明确供应商委托、分包、转包时不同的场景规则和要求，确保个人信息在流转过程中的有效管控；
g) 当供应商未能满足个人信息保护时的补救措施或赔偿方案；
h) 协议签订后的终止条款，包括个人信息的安全处置、持续的保密义务等。

8 训练阶段

8.1 个人信息安全控制

服务提供者可能在设计阶段未能充分开展供应商个人信息安全评估。在训练阶段，服务提供者应及时识别和记录生成式人工供应商系统中可能涉及的第三方供应商，并对潜在的个人信息安全风险采取相关控制措施。

8.1.1 训练数据

若训练数据含有通过数据提供方获取的个人信息：

a) 应确认供应商已征得个人信息主体的授权同意，保证个人信息具备合法性来源，具体实现形式可与供应商通过签订协议等形式进行约定，法律法规另有规定的情形除外；
b) 宜采用经加密、去标识化或匿名化等方式处理后无法定位到个人的数据，或采用基于隐私计算的方式进行训练，避免潜个人信息泄露风险和直接或间接地定位到个体；若必须使用明文个人信息进行训练，应确认供应商是否履行告知义务并获得个人信息主体的授权同意。

8.1.2 AI 模型

若AI模型来自第三方生成式人工智能服务提供者：

a) 在使用前，应对模型的个人信息保护能力进行评估；
b) 应与供应商签订数据隐私保护协议，明确双方的权利和义务；
c) 在对第三方提供用户输入数据前，宜先对个人信息进行识别，并采取去标识化或匿名化处理等安全保护措施；
d) 对外提供个人信息时，应验证第三方身份，并与第三方建立安全传输通道；
e) 宜检查 AI 模型供应商的 AI 模型数据合规处理相关证明，确保个人信息的合法处理。

8.1.3 计算环境

若计算环境涉及云服务商、硬件提供商及第三方运维管理产品提供商：

a) 应执行个人信息保护影响评估，识别和评估个人信息在整个生成式人工智能训练计算环境中可能泄露或盗窃的风险点，给出相应控制措施；
b) 应针对计算环境中涉及的供应商组件开展安全测试，包括但不限于漏洞扫描、渗透测试、第三方安全测试等，对发现的漏洞或后门程序及时修复和处置；
c) 应与供应商协商 SLA，包括数据和个人隐私保护、事件报告、法律合规义务等明确条款。

9 应用阶段

9.1 第三方服务告知

若生成式人工智能系统的应用过程涉及第三方服务：

a) 服务提供者应在生成式人工智能系统中明示告知用户涉及使用第三方 AI 模型或数据服务的情况，告知内容应包括可能对用户个人信息产生的影响；

注：无法对供应商开展评估的情况除外。

b) 生成式人工智能系统界面应设置显著标识，以清楚地表明第三方 AI 模型或数据服务的使用情况，使用户能够快速知悉，例如在系统启动时展示，并在配置相关位置持续可见。

9.2 应急处置

与生成式人工智能系统供应链相关的应急响应和事件处置的要求如下：

a) 应制定面向供应链的个人信息安全应急预案，做好应急策略和资源准备；
b) 当供应链环节发生个人信息安全事件时，应立即通知供应链对应的上下游供应商，协同启动应急处置措施，结合实际情况及时处置；
c) 当服务提供者内部发生个人信息安全事件且影响到供应链环节的，应将事件影响告知受影响的供应商，并协同应急处置。

参 考 文 献

[1] ISO/IEC 27001:2022 信息安全、网络安全与隐私保护—信息安全管理体系—要求（Information security, cybersecurity and privacy protection—Information security management systems—Requirements）

[2] ISO/IEC 27002:2022 信息安全、网络安全与隐私保护—信息安全控制（Information security, cybersecurity and privacy protection—Information security controls）

[3] ISO/IEC 27701:2019 安全技术—针对 ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理的扩展—要求和指南(Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines）

[4] ISO/IEC 42001:2023 信息技术—人工智能—管理体系（Information technology—Artificial intelligence—Management system）

电信终端产业协会团体标准

生成式人工智能个人信息保护技术要求　第8部分：供应链管理

T/TAF 268.8—2025

*

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