ICS 35.030
CCS L80

团　　体　　标　　准

T/SZBA 002—2023

基于区块链的数据资产评估实施指南

Implementation Guidelines for Data Asset Evaluation Based on Blockchain

2023-10-24

2023－10－25 发布

2023－11－01 实施

深圳市信息服务业区块链协会　　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。

本文件由深圳市信息服务业区块链协会归口。

本文件起草单位：深圳数宝数据服务股份有限公司、深圳职业技术大学、中国社会科学院信息化研究中心、中国社会科学院数量经济与技术经济研究所、中国科学院深圳先进技术研究院、中国电子技术标准化研究院、中国（天津）自由贸易试验区政策与产业创新发展局、网络空间治理与数字经济法治（长三角）研究基地、广东省投资和信用中心、京东科技信息技术有限公司、山东数据交易有限公司、深圳市国标知识产权大数据中心、中国光大银行股份有限公司深圳分行、腾讯科技（深圳）有限公司、深圳前海微众银行股份有限公司、XuperCore 开源工作组、南方电网数字平台科技（广东）有限公司、中移动信息技术有限公司、大有云钞科技（北京）有限公司、金蝶软件（中国）有限公司、中国移动通信集团设计院有限公司、广东省电信规划设计院有限公司、中国移动通信有限公司政企客户分公司、北京红枣科技有限公司、芯昇科技有限公司、天津华夏金信资产评估有限公司深圳分公司、江西开创数码科技有限公司、北京创安恒宇科技有限公司、深圳金赋科技有限公司、深圳哈希可信互联科技有限公司、深圳市智策科技有限公司、深圳市一航网络信息技术有限公司、深圳市前海数据服务有限公司、江西省霖溪科技发展有限公司、深圳竹云科技股份有限公司、北京中科华资产评估有限公司、北京国新丝路会计师事务所、广西金融职业技术学院、北京市道可特（深圳）律师事务所、中国民营科技实业家协会元宇宙工作委员会、上海靖予霖律师事务所、西牛数据科技服务（深圳）有限公司、广东财经大学数字经济学院、深圳市非凡互动网络科技有限公司、深圳链协发展集团有限公司、深圳市信息服务业区块链协会。

本文件主要起草人：易海博、王春晖、郑定向、姜奇平、李雪松、左鹏飞、王晨辉、白东国、盛长琳、曲强、谭敏、于小丽、李军、李立中、刘德远、苏毓腾、蔡玉娟、郑李梨、安琪、郝轶、任泳然、欧志、杨志武、华崇鑫、杨磊、刘永年、刘例、马占飞、卢盛羽、周宏、刘国栋、吕元宇、刘项杨、季慧丽、刘心田、李军（腾讯）、李克鹏、温尊权、王磊、赵红武、邓伟平、黄云、杨光、凌敏、张蕾、龙玺争、李琦、潘晓丰、高宏民、肖银飞、郎晓夫、曾哲君、黄旭斌、宁李艳、林梓鹏、于本江、陈炜、李欣、肖青、杨龙波、柳耀勇、魏伟、樊贤斌、江杰、佟辉、熊建晨、黄睿、李丽、韦量、彭英武、吴高斌、程文彬、周响阳、王方方、韩月、刘远骐。

基于区块链的数据资产评估实施指南

1 范围

本文件规定了基于区块链的数据资产的评估框架、评估过程以及评估内容和要求。

本文件适用于各类组织基于区块链开展数据资产评估工作。

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 25069-2022 信息安全技术 术语

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

20230235-T-469 信息安全技术 数据交易服务安全要求

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

GB/T 40685—2021 信息技术服务 数据资产 管理要求

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 42752-2023 区块链和分布式记账技术 参考架构

20213310-T-469 区块链和分布式记账技术 系统测试规范

20213307-T-469 区块链和分布式记账技术 应用程序接口 中间件技术指南

20201615-T-469 区块链和分布式记账技术 智能合约生命周期管理技术规范

20201612-T-469 区块链和分布式记账技术 存证通用服务指南

20210929-T-469 区块链和分布式记账技术 术语

GB/T 42570-2023 信息安全技术 区块链技术安全框架

GB/T 42571-2023 信息安全技术 区块链信息服务安全规范

20221465-T-469 信息技术 区块链和分布式记账技术 物流追踪服务应用指南

20214285-T-469 信息技术 大数据 数据资产价值评估

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者其他方式对信息的记录。

[GB/T 41479—2022，3.1]

3.2

数据资产 data asset

特定主体合法拥有或者控制的、能进行货币计量的、且能带来直接或者间接经济利益的数据资源。

[GB/T 40685—2021，3.1，有修改]

3.3

数据资产评估 data asset assessmuent

对组织内数据资产现状以及质量、价值等进行定量和定性评价的活动。

[GB/T 40685—2021，3.9]

3.4

数据交易 data transaction

数据供方和需方之间以数据商品作为交易对象，进行的以货币或货币等价物交换数据商品的行为。

注1:数据商品包括用于交易的原始数据或加工处理后的数据衍生产品。

注2:数据交易包括以大数据或其衍生品作为数据商品的数据交易，也包括以传统数据或其衍生品作为数据商品的数据交易。

[GB/T 37932—2019，3.1]

3.5

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

[GB/T 41479—2022，3.13]

3.6

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以识别自然人有关的各种信息。

注1：个人信息包括姓名、出生日期、公民身份证号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：不包括匿名化处理后的信息。

[GB/T 41479—2022，3.6]

3.7

重要数据 important data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

注：重要数据包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。

[GB/T 41479—2022，3.9]

3.8

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息所标识的自然人的过程。

注：去除标识符与个人信息主体（个人信息所标识的自然人）之间关联性。

[GB/T 37964—2019，3.13，有修改]

3.9

小程序 mini program

基于应用程序开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

注：应用程序通过公开其应用程序编程接口（API）或函数，使外部的程序可以增加该应用的功能或使用该应用程序的资源，而不需要更改该应用程序的源代码。

[GB/T 41391—2022，3.3]

3.10

区块链 blockchain

一种有多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致性、防篡改、防抵赖的技术。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

CIIO：关键信息基础设施运营者（Critical Information Infrastructure Operator）

5 评估过程

5.1 准备

5.1.1 评估方案制定

评估准备阶段应首先制订评估方案，评估方案的制订是一个不断确认的过程，至少应完成以下工作内容的确认：

a) 评估团队

应完成评估团队的组建，包括评估实施机构与被评估机构的人员数量、专业组成以及沟通机制的确认等。评估团队相关各方成员应具备可支撑评估开展的法律、技术、安全管理、业务规则等方面的相关专业知识和技能，如具有区块链、隐私计算等方面的专业能力，以及数据资产评估的专业知识和实践经验，可承担相关的评估和配合工作。评估团队开展数据资产评估业务，应当独立进行分析和估算并形成专业意见，拒绝委托人或者其他相关当事人的干预，不得直接以预先设定的价值作为评估结论。

b) 评估范围

应根据评估目的和评估对象来确定评估内容的边界。在某些情况下，评估对象可能不是一个特定的组织机构，而是某些数据、某个项目、某个业务、某笔交易、某个信息系统或是一个数据处理的生命周期等。例如，委托方为达到境外上市或投资收购等目的而进行的数据资产评估，可根据实际情况对评估内容进行裁剪辑或补充。

注：数据处理生命周期可能跨越组织、业务、系统等。

注：评估范围可包括组织范围、物理地域范围、项目范围、业务流程和业务活动范围、信息系统和技术工具范围、人员范围、数据范围、时间范围等维度。

c） 评估依据

应根据评估目的确定评估依据。包括适用的国家相关法律法规、监管规定、行业准则和国际条约、规则，以及相关国际、国家及行业标准等。

d） 评估工具

应明确评估过程中使用的工具。包括检查表、定价工具、基线检查工具、安全扫描及测试工具、安全审计工具等。除此之外，应运用区块链作为评估工具。

e） 评估进度

应对评估进度进行预期规划，包括准备、审核、分析阶段的时间及里程碑安排。以便参与各方预留时间和资源参与评估工作，保障评估活动的实施效率。

f） 评估风险

应对评估活动可能引入的风险及其影响进行分析，如审查活动对信息泄密的风险、测试扫描活动对业务运行和数据正确性的影响、评估工作自身的局限性及约束等，应采用最小影响原则并给出应对措施。

5.1.2 以上内容应与评估活动管理单位充分沟通，制定成文档化的评估方案并获得批准和实施授权。

5.1.3 评估对象调研

应对被评估的对象进行充分的调研，作为后续评估工作的基础。调研应包括如下内容：

a） 业务运营模式

评估对象涉及的业务范围、内容、模式以及与外部组织机构合作的情况。

b） 数据处理活动

评估对象处理数据的类型、流程、规模以及在处理过程中所处的角色和地位，评估数据收集、存储、使用、加工、传输、提供、公开、删除等全生命周期处理活动的情况。评估对象处理数据是否妥善运用区块链工具。

c） 安全管理制度及落实

评估对象的数据安全管理组织架构、管理制度、技术措施、网络安全等级保护、培训教育等情况。

d） 处罚及整改

评估对象及其所在组织涉及的数据资产的投诉、行政处罚、诉讼、仲裁，以及以往资产管理相关测评和数据资产评估的整改和纠正措施情况。

宜通过现场调查及发放调查单的形式来对评估对象进行调研。

5.1.4 评估资料收集

应根据评估目的进行对评估对象相关的数字资产资料收集，包括但不仅限于如下内容：

a） 业务介绍、分支机构及股权架构、所在组织的营业执照以及相关行业的经营许可。

b） 与数据供应商和第三方公司签订的协议、合同、文件范本和实例以及对供应商的审查文件。

c） 现有的网络安全、数据安全、数据分级分类、个人信息保护等事项的管理文件。包括制度、规范、程序文件、行业准则和承诺、指引文件、培训考核和监督要求以及近三年执行相关活动形成的技术和质量记录等。

d） 与数据资产或数据安全相关的诉讼、仲裁和被执法机关调查和处罚的相关文件，包括约谈、调查通知、处罚通知、判决书等。

e） 涉及的网络安全审查报告、等级保护的备案证明以及相关信息系统的等级保护测评报告、网络信息安全及数据安全风险评估报告等。

f） 已发生过的网络安全攻击、系统中断、信息泄露等事件的情况分析及应急响应报告。

g） 与区块链相关的业务、数据、测试报告等。

h） 收集、存储、处理数据的设备、人力成本，以及前期的研发成本等。

i） 权属资料、数据资产信息要素、财务会计信息和其他资料并进行核查验证、分析整理和记录。

j） 评估人员可通过对公开信息进行查询的方式获取评估对象的相关信息，以对收到的资料进行印证和补充。查询渠道可包括：

1） 国家企业信用信息公示系统、信息产业主管部门网站、各地行业主管部门网站、国家及地方网信部门网站以及执行和裁判信息公开网站等。

2） 可利用公共或专用网络搜索引擎对被评估对象散布在互联网或专用网络上的相关信息进行查阅整理。

必要时，可根据实际评估情况，要求被评估方补充资料。

5.2 审核

5.2.1 文档审查

评估人员应对在收集资料过程中收到的相关文件进行逐一审查，以评估相关制度、文件及落实情况是否符合评估依据的相关要求。

5.2.2 安全检测

评估人员可对相关实际运行的网络、信息系统和数据信息实施安全检测，通过查看、分析被测系统的响应和输出结果，评估被测系统的安全技术保障措施是否有效。执行此项工作时，应运用区块链工具并注意测试数据和评估工具可能对系统运行产生的影响，并尽可能减小这些影响。

5.2.3 人员访谈

必要时，作为文档审查和安全检测结果的补充，可对被评估对象涉及的相关人员进行访谈，以核实评估对象数据资产的实际情况。访谈可以采取交流、讨论、询问等形式，访谈对象可视情况包含如下人员：

a） 信息系统、区块链相关的研发人员、产品经理和业务设计人员。

b） 组织内部的业务负责人、技术负责人、数据安全负责人以及法律合规负责人。

c） 网络、应用和数据运维人员以及信息安全管理人员。

d） 系统及数据的运营人员。

5.3 分析

5.3.1 数据资产定价分析

在分析过程的执行中，应考虑到数据资产不具备实物形态，且具有非货币性，符合无形资产特性，综合运用一种或多种定价分析方式，如成本法、收益法、市场法、期权定价法，并运用区块链工具，基于无形资产的价值评估方法完成数据资产定价的分析。

5.3.2 问题和风险

在审核过程的执行中，应对审核的实际情况进行及时记录，对发现的问题形成问题记录，并对问题可能产生的风险进行分析。问题记录应包括如下内容：

a） 问题事实的描述，包括所在业务、违规事实和发生场景等。

b） 违反的内部制度名称及条款。

c） 违反的评估依据的名称及条款。

d) 问题可能引起的风险或处罚后果。
e) 必要时，问题的严重性级别。

5.3.3 整改计划

必要时，评估人员可协助评估对象所在组织针对问题进行整改计划的制定。整改计划应包括：
a) 问题的描述或识别信息。
b) 工作建议与整改措施。
c) 责任方或落实方。
d) 整改有效性的验证方。
e) 计划完成期限。

5.4 评价

5.4.1 评估报告

评估工作完成后，应形成数据资产评估报告，评估报告应包括如下内容：
a) 评估背景：描述评估的目的。
b) 评估声明：评估结果的适用范围、约束、假设以及免责声明。
c) 评估依据：评估所依赖的法律法规、相关标准或文件。
d) 评估范围：评估对象的组成和评估内容和指标的描述。
e) 评估流程：评估实施活动的过程性描述。
f) 评估结论：在充分审核的基础上，对评估对象的数据资产情况进行客观、公正的结论性总结，可包括：
   1) 数据处理业务活动的评估总结。
   2) 数据资产定价分析的评估总结。
   3) 安全管理措施及落实情况的评估总结。
   4) 技术保障措施及落实情况的评估总结。
   5) 发现问题及存在风险情况总结。
   6) 适用时，针对之前的数据资产定价、网络、区块链和数据安全审查、测评、评估、行政调查中发现问题的整改及落实情况的总结。
   7) 必要时，给予评估对象问题整改及后续持续改进的意见和建议。

5.4.2 专项意见

基于特定目的的数据资产定价评估，可按被评估对象所在组织的要求出具专项分析意见，如：
a) 数据资产的使用权。
b) 数据资产的成本。
c) 是否采用成本法、收益法、市场法、期权定价法等。

基于特定目的的数据安全评估，可按被评估对象所在组织的要求出具专项分析意见，如：
a) 是否属于关键信息基础设施运营者的专项分析意见。
b) 数据分级分类管理的专项意见。
c) 是否需要进行网络安全审查的专项意见。
d) 关于数据出境的专项意见。
e) 关于上市融资项目的专项意见。

5.4.3 备忘录

基于特定目的的数据资产评估，如发现涉及重大问题，可能对特定目的的达成产生直接影响，可以备忘录的形式进行重大问题说明和风险揭示，以供评估对象所在组织快速了解问题并引起重视，更有针对性的实施整改并提高效率。

6 评估内容

6.1 业务运营模式

6.1.1 处理模式

应对评估对象或所在组织的业务模式、业务流程进行充分识别，包括：

a) 组织与客户、供应商和其它合作方的模式（提供方、接收方、共同处理等）。

b) 组织在数据处理或是交易链中所处的角色（收集方、使用方、交易中介方等）。

c) 组织是数据处理平台的建设者还是运营者，或两者兼有。

不同的业务模式及角色对于数据资产的要求不同，评估方应根据识别的结果来选取后续的评估内容。

6.1.2 系统平台

应对评估对象数据处理所依附的信息系统和网络资产进行识别，形成系统资产清单。包括各类应用系统、网站、移动App、小程序、云平台、区块链等网络系统，以决定安全检测等评估所覆盖的范围。

6.2 数据处理主体

6.2.1 处理资质

应对评估对象所在组织的行政许可及相关证照的完备性、运营主体的一致性、授权范围、资质有效期限与实际数据处理相关活动的匹配性以及质量管理体系的健全性进行审查。如营业执照、增值电信业务经营许可证、在线数据与交易处理业务许可证、网络文化经营许可证、网络出版服务许可证、信息网络传播视听节目许可证、互联网药品信息服务资格证、质量管理体系认证等相关的许可和认证范围。

6.2.2 委托处理

6.2.2.1 委托方

评估对象委托外部机构处理数据时，应对如下内容进行审核：

a) 建立基于区块链的数据资产评估、定价分析、个人信息安全影响评估以及内外部数据安全检查与评估制度的情况。

b) 对受托方的资格审查的相关记录。包括行政许可、授权范围、质量管理体系等。

c) 与受托方签订的数据处理合同或协议的效力及内容。包括依照评估依据要求和合同约定履行数据安全要求、数据处理目的、处理期限、处理方式、信息种类、保护措施、处理地点、销毁、转委托处理、分享以及双方的权利和义务等。

d) 对受托方数据处理过程的监督记录。包括履行数据安全保护义务情况、处理方式及处理地点的正确性、是否进行超出目的处理、处理后数据的删除和销毁情况等。

e) 涉及处理个人信息的，委托前进行个人信息安全影响评估的实施记录并保存情况，个人信息安全影响评估活动应依据 GB/T 39335—2020 开展。

6.2.2.2 受托方

评估对象为数据处理的受托方时，应对如下内容进行审核：

a) 必要时，对委托方的资格审查的相关记录。包括行政许可、授权范围、质量管理体系等。
b) 委托合同或协议中委托方确保数据来源合法的承诺和违约赔偿责任。
c) 受托方依照评估依据要求和合同约定履行数据安全保护义务，不超出约定范围处理方式和处理目的承诺。
d) 相关情况下（如合同无效、中止、处理完成后等）数据的返还、删除、销毁的相关实施和确认记录。

6.2.3 共同处理

评估对象为数据的共同处理方时，应对如下内容进行审核：
a) 自主决定数据处理目的及处理方式的主体资格。
b) 共同处理数据各方的权利、义务的约定。
c) 依法承担相关法律责任的约定。

6.2.4 主体变更转移

评估对象在数据处理过程中发生合并、分立、解散、破产等变化导致数据处理的主体发生转移时，应对如下内容进行审核：
a) 通知数据来源数据（可能为组织或个人），处理方发生变化的相关信息（名称/姓名、联系方式等）。
b) 涉及处理个人信息的，若处理目的和方式发生变化，重新取得个人同意的相关证据。

6.3 数据处理活动

6.3.1 数据资源合规

应对数据资源来源的合规情况进行评估，内容包括：
a) 数据资源来源应符合合法、正当、必要、诚信原则。
b) 数据资源应获得用户授权或依法无需获得授权。
c) 数据资源的授权应覆盖拟进行的数据处理活动。

6.3.2 分类分级

应对数据分级类情况进行评估，内容包括：
a) 数据分类分级的依据对相关评估依据要求的符合性。如：
   1) 从对国家安全、公共利益或个人、组织合法权益的危害程度对数据进行分类分级；
   2) 根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等因素，采取个人信息分类管理措施；
   3) 结合对个人权益影响分析的结果（宜参照 GB/T 39335—2020 表 D3）对个人信息数据进行分类分级。
b) 对不同分级的数据分别实施不同的管理和技术保护措施的合理性。

注：在大多数情况，对不同分级的数据实施完全一致的管理和技术保护措施是不现实的。

6.3.3 处理过程

6.3.3.1 收集

应对收集数据的情况进行评估，内容包括：

a) 收集信息的合法性基础，相关资质、行政许可、授权等。是否收集与其提供的服务无关的个人信息，是否违反评估依据要求和双方的约定收集、使用个人信息。
b) 收集个人信息的授权同意情况，宜参照 GB/T 35272—2020 5.4、GB/T 41479—2022 5.2 以及评估依据要求开展。
c) 收集信息行为的正当、必要性，宜参照 GB/T 35273—2022 5.1、5.2 以及评估依据进行审核。包括：
   1) 用户授权（告知—同意）使用的展示时机、形式（显著、醒目、非默认同意）和内容的规范性。
   2) 收集内容应当与处理目的直接相关，采取对个人权益影响最小的方式，限于实现处理目的的最小范围，不过度收集个人信息。
   3) 应用系统实际收集内容与其宣称的隐私政策、用户协议等内容的一致性。

注：对 App 的个人信息收集行为进行评估，宜参照 GB/T 41391—2022 开展。

6.3.3.2 存储

应对数据的存储情况进行评估，内容包括：

a) 对数据及其副本存储所采取的安全措施，宜参照 GB/T 41479—2022 5.3 以及评估依据要求进行审核。审核项应包括：
   1) 技术保护措施的要求，如加密算法、访问控制、安全审计、个人信息的匿名化等。
   2) 存储期限，符合评估依据要求、合同和用户约定的有效期限。
   3) 对重要系统和数据库进行容灾备份。
b) 数据及其副本的存储地点满足数据本地化存储和数据跨境的评估依据要求的情况。
c) 必要时，可使用第三方机构提供的数据存证服务，保证数据的真实性和完整性。

6.3.3.3 使用、加工

应对数据的使用和加工情况进行评估，内容包括：

a) 数据的使用和加工获得相关方的授权文件并符合评估依据要求的证明。
b) 数据实际使用、加工的方式和范围符合约定。

注：对于隐蔽的、嵌入式或第三方 SDK 提供的处理过程可采用安全检测的手段予以确认。

c) 未涉及相关规定禁止的数据使用和加工，如未获得用户授权、用户已撤回同意、歧视性的营销策略、违反道德伦理等情况。

注：宜结合 GB/T 41479—2022 5.4-5.5 的要求开展。

6.3.3.4 传输、提供

应对数据的传输和提供情况进行评估，内容包括：

a) 数据提供和接收方的审核，应符合本标准 7.2.1 的要求。
b) 数据传输和提供的安全措施和协议约定，宜参照 GB/T 41479—2022 5.6-5.7 以及法律和相关行业要求进行审核。
c) 涉及第三方 SDK 或 API 的，应对 SDK 组件或 API 接口进行安全检测，评估是否存在已知的安全漏洞以及可能引起数据泄露或未授权的数据跨境的行为。
d) 利用个人信息和个性化推送算法向用户提供信息的，须对推送信息的真实性、准确性以及来源合法性负责，并符合以下要求：

1） 收集个人信息用于个性化推荐时，应取得个人单独同意；
2） 设置易于理解、便于访问和操作的一键关闭个性化推荐选项，允许用户拒绝接受定向推送信息，允许用户重置、修改、调整针对其个人特征的定向推送参数；
3） 允许个人删除定向推送信息服务收集产生的个人信息，法律、行政法规另有规定或者与用户另有约定的除外。

e）向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

f）涉及数据交易活动时：
1） 数据供方、数据需方、数据服务机构应符合 GB/T 37932—2019 5 的相关要求；
2） 交易的数据对象应符合 GB/T 37932—2019 6 的相关要求；
3） 交易的过程应符合 GB/T 37932—2019 7 的相关要求；
4） 应对数据交易中介服务的机构留存的交易双方的审查、交易记录进行审核。

6.3.3.5 公开

应对评估对象的数据公开行为进行评估，包括：
a) 公开前的影响评估情况。如是否对危害国家安全、公共安全、经济安全和社会稳定造成影响。
b) 必要时，数据公开行为和内容是否取得了相关单位的许可和授权。
c) 处理已公开的个人信息，对个人权益有重大影响的，应按评估依据要求取得个人同意。

6.3.3.6 删除、匿名化

应对评估对象删除数据和用户注销后的匿名化处理情况进行评估，内容包括：
a) 对符合 GB/T 41479—2022 5.13、GB/T 35273—2020 8.3、8.5 和评估依据要求的数据进行删除或匿名化处理的处理记录，评估方应从处理的内容、数据量、及时性等方面进行审查。
b) 适用时，APP 提供的用户注销用户的方式，宜参照 GB/T 35273—2020 8.5 的要求进行审核。
c) 处理范围包括数据本身及其全部副本。
d) 处理后的数据无法或不再继续参与数据处理与加工的证明。
e) 适用时，拒绝删除或注销用户给出反馈的情况，应包括：
1) 通知的告知渠道，如 APP 通知、短信、邮件等。
2) 拒绝理由，如依据的法律法规、行业监管要求等。
3) 投诉渠道和途径。

6.4 管理措施及落实

6.4.1 责任人与责任机构

应对评估对象所在组织的数据资产管理责任人和组织架构进行评估，内容包括：
a) 责任人，包括背景审查、工作职责、绩效考核、履行其对应的工作职能的相关工作记录等。可参照 GB/T 41479—2022 6.1、6.2 的要求进行审核。个人信息处理者应公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

注：履行个人信息保护职责的部门包括：国家网信部门和县级以上地方人民政府有关部门。国家网信部门的职责是统筹协调个人信息保护工作。

b) 责任机构，包括机构的岗职位设置、运行经费、独立性以及开展相关工作的运行记录等。

6.4.2 数据安全管理措施

应对评估对象所在组织的数据资产安全管理措施的完整性、一致性、可行性、依从性等方面进行评估，评估内容可包括：

a) 管理体系，包括总体要求、机构设置及职责、基本原则等。
b) 处理流程管理，包括数据收集、使用、传输、提供、存储、删除等管理要求。
c) 数据分类分级管理：
   1) 划分数据类别、级别的原则及对应采取管理和技术措施的要求。
   2) 适用时，个人信息按敏感程度的分类及保护措施。
d) 网络及数据安全风险评估及报送机制，按相关要求定期开展风险评估并报送或公布结果的相并规定。
e) 数据安全风险管理机制，包括开展数据安全风险评估、报告、共享、预警检测等机制。
f) 网络及数据安全应急预案，发现信息安全事件时，启动应急预案、采取补救措施、向主管部门报告、定期实施应急演练等措施。可参照 GB/T 41479—2022 6.3 的要求进行审核。
g) 投诉、举报制度，接受网络信息安全投诉、举报并及时处理、反馈的机制。
h) 数据出境管理，适用时，对数据出境条件、数据出境自评估及程序的要求。
i) 网络安全审查，适用时，制定并落实网络安全审查相关的管理制度和程序。
j) 个人信息管理，包括：
   1) 对个人信息访问和操作权的要求。
   2) 定期进行个人信息合规审计的要求。
   3) 适用时，对个人信息安全影响评估的要求。
   4) 适用时，对未成年人和儿童信息保护的管理要求。
   5) 员工个人信息保护，如对员工的简历、体检信息、生物识别信息的以及雇佣外籍员工的信息保护的规定。

6.4.3 数据安全技术措施

应对评估对象的数据资产安全保护的技术措施落实情况进行评估，内容可包括：

a) 定期的安全检测，包括网络、主机、应用等层面的安全扫描和安全配置的检测。
b) 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照评估依据要求留存相关的网络日志情况。
c) 防御措施，防范计算机病毒、网络攻击等危害网络安全行为的措施有效性检测。
d) 数据备份，包括备份的内容、范围、形式（全备份、增量备份、差分备份等）、备份地点（本地、异地）、备份及时性以及备份有效性验证等。
e) 加密，包括加密的内容、算法的强度、算法的使用（如必须使用国密算法的场景）、密钥的管理措施等。
f) 去标识化，适用时，对个人信息去标识化的情况，宜参照 GB/T 37964—2019 5、6 部分的要求进行审核。
g) 访问控制，数据访问和操作前对访问者进行鉴别与授权的记录和检测。
h) 监控和预警记录，对网络和应用运行状态、操作的监控和预警记录的完整性和保存期限的检测。
i) 应评估对象与合作伙伴之间的正式沟通所用的通信工具安全性，是否完全依赖第三方 IM 工具；有多少业务需依赖 SaaS；评估对象对于自身业务数据的控制能力；评估对象是否充分利用现有的密码等技术来充分保护自身的数据权益。

6.4.4 人员管理及安全教育

应对评估对象的人员管理及安全教育落实情况进行评估，内容应包括：

a) 人员签保密协议的情况，如保密内容、保密范围、保密期限、奖惩措施等。
b) 人员上岗前的审查情况，如工作履历、技术能力、人员资质、教育学习等。
c) 人员在岗期间的安全意识、工作技能、管理制度的培训及培训有效性考核情况。
d) 人员离岗后按照相关管理要求进行离岗交接、审计、脱密等措施执行的情况。

6.4.5 网络安全及关键信息基础设施保护

应对评估对象实施网络安全等级保护情况进行评估，内容应包括：

a) 评估对象的定级和备案情况。须按 GB/T 22240 的要求对定级结果进行复核。
b) 对于确定为二级以上的网络信息系统，须对等级保护备案情况、测评的频率进行确认。
c) 对于确定为三级及以上系统、面向社会服务的政务信息系统以及关键信息基础设施按频率开展密码评估工作的情况进行确认。
d) 处理重要数据的系统应满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关评估依据要求从严保护。
e) 必要时，网络信息系统安全保护措施和测评整改符合要求的情况，应按 GB/T 22239 对应级别的相关要求进行审核和检测。
f) 如评估对象有已被认定或可能被认定为关键信息基础设施运营者的情况，还应按 GB/T 39204 的相关要求进行审核和检测。

注：关键信息基础设施的确定参见附录 B。

6.4.6 数据出境安全合规

适用时，应对评估对象数据出境的情况进行评估，评估内容包括：

a) 向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。
b) 组织指定个人信息安全影响评估的责任部门或责任人员，自行开展或聘请外部独立第三方进行个人信息保护影响评估，个人信息保护影响评估报告和处理情况记录应当至少保存三年。
注：个人信息安全影响评估活动应依据 GB/T 39335—2020 开展。
c) 按照网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务。合同中应当至少约定数据出境的目的及方式、境外数据保存情况、境外数据再转移、不可抗力以及其他违约或侵权事宜及其解决途径与方式。
d) 评估对象的数据出境处理活动是否需向网信部门等管理机构申报数据出境安全评估，如需要申报，应开展数据出境风险自评估，并向网信部门申报数据出境安全评估。
注：自估内容应当包括处理数据的目的及范围、敏感程度、境外接收方义务及相关责任，审慎评估其出境对国家安全、公共利益等权益带来的风险，以及其他可能影响数据出境安全的事项。
e) 未达到申报数据出境安全评估条件的，是否经专业认证机构进行个人信息保护认证。
f) 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。
g) 符合境外地区相关规定和要求的情况。
h) 评估依据要求的禁止出境的情况。网信部门认定不得出境的数据，是否已停止数据出境，并采取有效措施对已出境数据的安全予以补救。
i) 适用时，使用境外的服务供应商和第三方组件（SDK）可能引起的潜在数据传输链路的数据出境风险情况。

j） 必要时，跨境传输相关的管理记录，包括传输发送方、接收方及所在区域、传输机制、信息类型、处理目的、合同条款、数据主体同意的相关记录。

6.4.7 问题整改和纠正措施

适用时，应对评估对象涉及与数据和网络安全相关的投诉、争议、诉讼、仲裁、行政处罚等情况评估，内容应包括：

a） 投诉、争议、诉讼、仲裁、行政处罚的进展情况。

b） 采取的纠正、纠正措施的适宜性和落实情况。

c） 是否可能产生潜在的被监管部门进一步调查或采取其他措施，导致更为严厉的处罚。

6.5 数据资产跟踪评估

宜对评估对象数据的管理的改进和按期执行情况进行持续跟踪监控和评估，包括：

a） 结合评估依据要求，对外部政策、用户服务协议、合同范本等内容进行定期审查和更新的情况。

b） 持续改进和完善内部数据安全管理制度以及流程优化的情况。

c） 定期开展员工数据资产管理培训和考核、开展年度安全风险与资产管理评估以及相关的问题整改落实情况。