ICS 35.020
CCS A 20

团　　体　　标　　准

T/ISC XXXX—XXXX

数据确权风险控制通则

General rules for risk control of data rights confirmation

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中　国　互　联　网　协　会　　发 布

目　　次

目次 I
前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 数据确权风险控制框架 2
5 数据采集存储环节确权风险控制通则 2
5.1 采集存储个人数据确权风险控制要求 2
5.2 采集存储非个人数据确权风险控制要求 3
6 数据加工分析环节确权风险控制通则 4
6.1 加工分析个人数据确权风险控制要求 4
6.2 加工分析非个人数据确权风险控制要求 5
7 数据使用环节确权风险控制通则 6
7.1 使用个人数据确权风险控制要求 6
7.2 使用非个人数据确权风险控制要求 7
8 数据交互/交易环节确权风险控制通则 7
8.1 交互/交易个人数据确权风险控制要求 7
8.2 交互/交易非个人数据确权风险控制要求 8
参考文献 10

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。

本文件由中国互联网协会归口。

本文件起草单位：上海邮电设计咨询研究院等。

本文件主要起草人：王德东、李儒耕等。

引　言

随着网络、电子商务的发展，民众的生活、学习、工作、企业的商业行为、政府的社会治理和互联网紧密地融为一体。随之而来的数据的生产、加工、流通和分析利用成为了整个互联网发展的核心，数据也成为推动经济发展的新要素，但是由于数据的虚拟性、多样性和可复制性，使数据的各类权属的确定、保障存在一定的困难，出现了大量数据错误地挪用给他人加工、处理、使用甚至买卖等问题。需要构建数据权属确定、保护、管理等一系列安全准则，以保障个人隐私安全、保护企业竞争利益以及国家数据主权的安全。

本文件的研制将为各类数据企业在数据生命周期各环节确定数据权属、行使数据权利提供控制风险的方法和工作指引，能够有效的保障数据处理、流通、交易的各环节的数据安全及个人隐私保护，推动数据要素价值发挥，促进数据经济发展。

数据确权风险控制通则

1 范围

本文件确立了数据确权风险控制框架，规定了数据采集存储、加工分析、使用和交互/交易环节确权风险控制要求。

本文件适用于企业内部处理个人数据和非个人数据时的确权安全。也适用于数据交易过程中的确权安全。

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 37973-2019 信息安全技术 大数据安全管理指南

GB/T 37932-2019 信息安全技术 数据交易服务安全要求

GB/T 40094（所有部分）电子商务数据交易

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据财产权 data property rights

民事主体对其持有的数据进行利用（处理）、收益以及依法占有、处分的对世性财产权利。

3.2

数据人格权 data personality rights

以主体依法固有的人格利益为客体的，以维护和实现人格平等、人格尊严、人身自由为目标的权利据。

注：数据人格权包括数据知情同意权、数据修改删除权、数据被遗忘权。

3.3

数据处理权 data processing rights

对各种数据进行收集、存储、整理、分类、统计、加工等操作的权利。

3.4

数据使用权 data usage rights

使用指定数据的权利，在所有权确定的情况下，数据所有人可以将数据的使用权授予数据使用人。

3.5

数据确权 data authentication

确定数据的权利属性，确定数据的权利主体和权利的内容，设置确定和行使数据权利的规则和程序架构。

4 数据确权风险控制框架

本文件从数据生命周期四大环节确立不同类型数据的权属风险控制通用规则。

表1 数据确权风险控制框架

数据类型	确权环节			
	数据采集存储	数据加工分析	数据使用	数据交互/交易
个人数据	规范类数据财产权、数据人格权、数据处理权、数据使用权风险控制通则	规范类数据财产权、数据人格权、数据处理权风险控制通则	规范类数据财产权、数据人格权、数据使用权风险控制通则	规范类数据财产权、数据人格权、数据使用权风险控制通则
	技术类风险控制通则	技术类风险控制通则	技术类风险控制通则	技术类风险控制通则
非个人数据	规范类数据财产权、数据处理权、数据使用权风险控制通则	规范类数据财产权、数据处理权风险控制通则	规范类数据财产权、数据使用权风险控制通则	规范类数据财产权、数据使用权风险控制通则
	技术类风险控制通则	技术类风险控制通则	技术类风险控制通则	技术类风险控制通则

5 数据采集存储环节确权风险控制通则

5.1 采集存储个人数据确权风险控制要求

5.1.1 概述

个人数据权属在数据采集环节主要涉及到财产权的转移、人格权的授权和保护、处理权和使用权的获取。针对不同权属的转移、保护和获取，企业或组织应遵循规范类和技术类准则进行风险控制。

5.1.2 规范类风险控制通则

个人数据采集存储环节确权风险控制规范类通则，应包括以下四类权属风险控制要求。

a) 数据财产权风险控制要求：
   1) 数据的财产权天然属于个人拥有，企业或组织取得个人数据的财产权应与个人签署数据所有权转让/转移协议，明确约定双方权益分配方式、数据处理和使用方式、数据保护责任、个人权益受损时的惩罚和赔偿等内容；
   2) 个人数据财产权涉及个人、企业或组织、第三方的经济收益，为确保收益有效分配、保护各方利益，企业或组织应制定相关的管理规范，明确个人数据利益保护的责任人，制定个人数据财产权保护工作内容和流程，制定个人数据财产权侵害惩处机制。企业或组织应做好员工培训，确保各层级员工遵循管理规范，保障个人数据财产权有效行使。
b) 数据人格权风险控制要求：
   1) 企业或组织在采集和存储个人数据时应对数据人格权属进行保护，应与个人签署隐私协议，告知个人采集的数据范围、使用目的、共享的第三方；

2） 企业或组织应制定明确的制度，规范个人信息的采集和存储。应制定明确的惩罚措施，避免非法、超最小必要原则采集个人数据。

c） 数据处理权风险控制要求：

1） 企业或组织应合法的取得个人数据的处理权，应通过协议或隐私条款来明确处理数据的范围、处理数据的方式等；

2） 针对个人数据交由第三方处理的，还应明确取得个人同意。

d） 数据使用权风险控制要求：

1） 企业或组织在使用个人数据时应通过协议或隐私条款取得个人同意，应与个人明确约定使用数据的范围、使用的目的、期限等；

2） 企业或组织应定期检查数据使用协议和隐私条款，确保协议和隐私条款满足要求。

5.1.3 技术类风险控制通则

个人数据采集存储环节确权风险控制技术类通则，应包括以下两类风险控制技术要求。

a） 数据采集端技术要求：

1） 企业或组织应建立个人数据授权管理平台，实现个人数据使用场景的标注，明确每项个人数据能够用于的场景，避免出现个人数据超权属处理和使用的情况；

注 1：个人数据使用场景包括但不限于经营统计分析、用户分析、客户画像、精准营销、AI 建模、数据挖掘、风险控制、信用评估等类型。

2） 企业或组织应通过日志平台记录个人数据采集阶段的授权过程，保留个人点击/签署协议的痕迹、个人改变或撤销授权的痕迹，同时点击、变更授权的操作记录或日志应进行长期保留，保留期限不低于 3 年；

注 1：参照《中华人民共和国电子商务法》第三十一条　电子商务平台经营者应当记录、保存平台上发布的商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年。

3） 企业或组织应建立授权追溯技术，准确的记录个人数据授权不同时序的状态，实现不同时间点个人数据权属的查询，实现根据个人客用户的要求进行权属增加、删除、变更等操作。

b） 数据存储端技术要求：

1） 个人数据存储应做好个人敏感信息的加密或者脱敏，确保个人信息的安全，避免出现因敏感字段泄漏而造成的人格权属侵害；

2） 数据存储应做好数据的血缘管理，通过数据血缘关系，明确定义数据字段、数据表之间的变换关系，避免因在不同系统/数据库中存储变换字段名和表名而出现权属标注信息丢失。

5.2 采集存储非个人数据确权风险控制要求

5.2.1 概述

非个人数据权属在数据采集环节主要涉及权属的转移和共享，以及在权属转移或共享之后转让方和受让方各自享有权属的界定和双方的责任义务。针对不同的权属应遵循规范类和技术类准则进行风险控制。

5.2.2 规范风险控制通则

非个人数据采集存储环节确权风险控制规范类通则，应包括以下三类权属风险控制要求。

a） 数据财产权风险控制要求：

1） 非个人数据一般为企业或组织拥有，部分也可能由个人拥有。企业或组织取得非个人数据的财产权应与数据拥有人签署数据所有权转让/转移协议，明确约定双方权益分配方式、

数据的复制和转售权利、数据处理和使用权、数据保护责任、双方权益受损时的惩罚和赔偿等内容；

2) 数据财产权涉及到数据提供方、企业或组织和第三方的利益，在获取和存储非个人数据时企业或者组织应制定非个人数据财产权保护机制，明确该数据的责任人、保护数据权益的工作要求，制定非个人数据利益侵害的惩处办法，确保企业或组织内部人员遵循相应规范，规避非个人数据财产权受侵害风险。

b) 数据处理权风险控制要求：

1) 企业或组织应合法的取得非个人数据的处理权，应签订协议来明确处理数据的范围、处理数据的方式、处理的要求、处理后数据的归属、处理后双方的责任、权属受到侵害后的惩处等；

2) 企业或组织需要引入第三方协作进行数据处理，应与第三方签署数据委托处理协议，约定双方的数据保护责任及违约惩处。同时告知非个人数据提供方，说明数据委托第三方处理的流程、各方的保护责任和机制，避免第三方处理所产生的风险。

c) 数据使用权风险控制要求：

1) 企业或组织在使用非个人数据时应通过协议取得数据的使用权，明确数据的知识产权。双方应约定数据的使用场景，并对于超范围、超场景使用等违法行为明确惩处和赔偿条款。

5.2.3 技术风险控制通则

非个人数据采集存储环节确权风险控制技术类通则，应包括以下两类风险控制技术要求。

a) 数据采集端技术要求：

1) 企业或组织应建立权属管理平台，在采集/接收外部非个人数据时做好数据权属的标注，明确该数据的来源方、数据的权属范围、数据的处理和使用范围等信息，便于在数据加工、数据使用、数据交互、数据价值分配等环节进行权属的查询与审核；

2) 企业或组织应构建数据权属变化跟踪技术，在归集整合多源内外部非个人数据时做好数据权属变化的时序化登记，确保数据归集前和数据归集后权属信息的一致性和连贯性，应避免多源数据整合后出现数据权属模糊。

b) 数据存储端技术要求：

1) 数据存储端应做好非个人数据的血缘管理，通过数据的血缘关系，明确定义数据字段、数据表之间的变换关系，避免因在不同系统/数据库中存储变换字段名和表名而出现权属标注信息丢失情况。

6 数据加工分析环节确权风险控制通则

6.1 加工分析个人数据确权风险控制要求

6.1.1 概述

个人数据权属在数据加工和分析环节主要涉及数据开发人员是否超权限、超范围、超场景进行数据加工和分析，是否侵害个人的数据人格权、数据处理权，企业或组织应遵循规范类和技术类准则进行风险控制。

6.1.2 规范类风险控制通则

个人数据加工分析环节确权风险控制规范类通则，应包括以下三类权属风险控制要求。

a) 数据财产权风险控制要求：
   1) 个人数据加工和分析之后数据财产权会发生改变，企业或组织应建立数据加工规范，约束数据分析人员对数据加工和分析的方式，确保个人数据的财产权按协议约定进行保护和保留，避免个人数据加工和分析后源数据方财产权受到侵害；
   2) 个人数据加工和分析后应对数据财产权进行更新，明确加工后数据各相关方的财产权属，确保各方在数据财产权约束之下利益分配清晰。
b) 数据人格权风险控制要求：
   1) 企业或组织加工和分析个人数据应对数据人格权属进行保护，应制定明确的制度来规范个人数据的加工和分析，应制定明确的惩罚措施，避免超权加工和分析；
   2) 企业或者组织加工和分析个人数据应进行事前、事中、事后全流程管控。数据开发人员事前应说明加工数据的目标、范围、使用的技术等，数据管理员应进行合规性审核，确保个人数据加工分析符合规范。事中和事后应对数据开发人员的加工过程进行审计，确保数据加工和分析符合数据人格权保护要求。
c) 数据处理权风险控制要求：
   1) 企业和组织在行使个人数据处理权时应制定数据权限体系，管理不同类型人员的数据权限，规范数据需求人员、数据开发人员、数据分析人员的行为，约束人员权限，管控数据开发和分析过程。

6.1.3 技术类风险控制通则

个人数据加工分析环节确权风险控制技术类通则，应包括以下两类风险控制技术要求。

a) 数据加工技术要求：
   1) 企业或组织应建立数据加工分析日志管控平台，记录全过程操作日志，包括但不限于数据来源的系统信息、数据输出/调用的系统信息、数据访问记录、数据加工记录等内容；
   2) 企业或组织应通过平台对数据加工过程进行管理，对个人数据加工需求进行事前审批、事中开发过程监控、事后个人授权合规审计；
   3) 数据权限控制应通过平台实现对不同数据进行人员数据权限的分配与管控，确保人员、数据、权限三者合理配置。
b) 数据分析技术要求：
   1) 个人数据分析和挖掘过程应进行算法监控，避免在处理过程中实现带有歧视性、不正当性算法和模型。

6.2 加工分析非个人数据确权风险控制要求

6.2.1 概述

非个人数据权属在数据加工和分析环节主要是要控制数据处理人员不按协议、不按业务要求、不按权限要求进行数据加工和分析。企业或组织应遵循规范类和技术类准则进行风险控制。

6.2.2 规范类风险控制通则

非个人数据加工分析环节确权风险控制规范类通则，包括以下两类权属控制要求。

a) 数据财产权风险控制要求：
   1) 非个人数据加工和分析后数据财产权会发生改变，企业应建立数据加工规范，约束数据分析人员数据加工和分析方式，确保非个人数据的财产权按协议约定进行保护和保留；

2) 非个人数据加工和分析后应对数据财产权进行更新，明确加工后数据各相关方的财产权属，确保各方在数据财产权约束之下利益分配清晰。

b) 数据处理权风险控制要求：

1) 企业或组织在行使非个人数据处理权时应规范数据开发和分析人员的行为，约束人员权限，管控数据开发和分析过程。

6.2.3 技术类风险控制通则

非个人数据加工分析环节确权风险控制技术类通则，包括以下两类风险控制技术要求。

a) 数据加工技术要求：

1) 企业或组织应通过平台对数据加工过程进行管控，事前应对非个人数据加工需求进行审批，确保数据加工需求不超出合作协议范围，事后应进行需求实现审计，确保需求按事前审批范围进行开发；

2) 企业或组织应通过平台对人员数据权限进行分配与管控，确保给人员的数据权限合理配置。

b) 数据分析技术要求：

1) 数据分析和挖掘过程应进行算法监控，避免在处理过程中实现带有歧视性、不正当性算法和模型。

7 数据使用环节确权风险控制通则

7.1 使用个人数据确权风险控制要求

7.1.1 概述

个人数据权属在数据使用环节主要是涉及财产权的保护、人格权的保护和数据使用权的正确行使。针对不同权属的保护和行使，企业或组织应遵循规范类和技术类准则进行风险控制。

7.1.2 规范类风险控制通则

个人数据使用环节确权风险控制规范类通则，包括以下三类权属控制要求。

a) 数据财产权风险控制要求：

1) 在数据使用环节企业和组织应保护好数据的财产权，制定数据使用阶段个人数据财产保护规范和行为准则，限定数据使用人员范围，管控数据使用场合。

b) 数据人格权风险控制要求：

1) 企业或组织在使用个人数据时应对数据人格权属进行保护，应有清晰的个人隐私协议告知个人数据使用的目的、使用的范围、使用的方式等，针对敏感个人数据使用应取得个人单独同意；

2) 企业或组织应制定明确的规范来约束个人数据的使用，应制定明确的惩罚措施，制止非法使用个人数据。

c) 数据使用权风险控制要求：

1) 企业或组织在行使数据使用权时应保障按隐私协议、授权协议、个人单独同意条款要求进行；

2) 企业或组织应建立个人数据使用的事前授权审批、事后鉴权审查机制，确保部门和人员合规使用个人数据。

7.1.3 技术类风险控制通则

个人数据使用环节确权风险控制技术类通则，包括以下风险控制技术要求。

a） 企业或组织应通过技术平台对个人数据使用进行授权管理，实现个人数据使用事前审批、事中鉴权，确保每一项个人数据的使用场景与个人信息授权范围相一致。

b） 个人数据使用和调用应有技术平台对数据 API 接口、数据文件输出、数据抽取、数据下载/导出等进行监控，确保数据使用流向可查询、可追踪。

7.2 使用非个人数据确权风险控制要求

7.2.1 概述

非个人数据权属在数据使用环节主要是涉及财产权的保护和数据使用权的正确行使。针对这两类权属应遵循规范类和技术类准则进行风险控制。

7.2.2 规范类风险控制通则

非个人数据使用环节确权风险控制规范类通则，包括以下两类权属控制要求。

a) 数据财产权风险控制要求：
   1) 在数据使用环节企业或组织应保护好数据的财产权，制定数据使用阶段非个人数据财产保护机制；
   2) 企业或组织应管控数据使用人员及使用场合，防止在数据使用过程中数据泄露，造成财产权受到损失。
b) 数据使用权风险控制要求：
   1) 企业或组织应建立数据使用事前审批、事后审查机制，确保部门和人员合理使用非个人数据。

7.2.3 技术类风险控制通则

非个人数据使用环节确权风险控制技术类通则，包括以下风险控制技术要求：

a) 非个人数据使用应通过技术平台进行事前的需求审批管理和事后的数据使用审计，确保非个人数据合理的使用。
b) 非个人数据使用和调用应有技术平台对数据 API 接口、数据文件输出、数据抽取、数据下载/导出等进行监控，确保数据使用流向可查询、可追踪。

8 数据交互/交易环节确权风险控制通则

8.1 交互/交易个人数据确权风险控制要求

8.1.1 概述

个人数据权属在数据交互/交易环节主要涉及财产权的合法交易、人格权的保护和使用权的合规转移。企业或组织在进行权属的交互、转移时应遵循规范类和技术类准则进行风险控制。

8.1.2 规范类风险控制通则

个人数据交互/交易环节确权风险控制规范类通则，包括以下三类权属控制要求。

a) 数据财产权风险控制要求：
   1) 在数据交互/交易过程中，企业或组织应与交易方签订数据委托处理协议或数据转让协议，约定双方的收益、责任和义务，以及对个人数据的保护责任；
   2) 企业或组织应制定交易处理人员的行为规范，避免交易人员私自复制、转卖个人数据，侵害各方数据财产权益；
   3) 针对数据采集阶段与个人约定的财产权条款，企业或组织应按要求履约，保障个人权益。
b) 数据人格权风险控制要求：
   1) 企业或组织在交互/交易个人数据时应对数据人格权属进行保护，应有清晰的隐私协议告知个人，数据的交易方、交易数据的范围、交易后的用途、交易方加工数据的方式等，针对敏感个人数据的交易应取得个人单独同意；
   2) 企业或组织应制定明确的制度来规范交易过程中的人格权保护，应制定明确的惩罚措施，制止非法交易个人数据。
c) 数据使用权风险控制要求：
   1) 企业或组织交易数据使用权时应与使用权受让方签订协议，确保按隐私协议、授权协议、个人单独同意条款的要求进行交易，约束受让方在授权范围内使用个人数据；
   2) 企业或组织应建立数据使用授权事前审批、事后审查机制，确保数据交易/交互过程合规。

8.1.3 技术类风险控制通则

个人数据交互/交易环节确权风险控制技术类通则，包括以下两类风险控制技术要求。

a) 数据交互技术要求：
   1) 企业或组织进行个人数据交互宜使用隐私计算技术，确保多方数据在不可见数据环境下进行联合建模，实现数据交互；
   2) 个人数据交互/交易应建立管控平台，实现交互申请管理、数据对外输出管控。
b) 数据交互安全技术要求包括但不限于不可逆数据库技术、数据水印、权限控制、日志审计、交易过程加密等。

8.2 交互/交易非个人数据确权风险控制要求

8.2.1 概述

非个人数据权属在数据交易环节主要是涉及财产权和使用权的交易，企业或组织在此过程中应遵循规范类和技术类准则进行风险控制。

8.2.2 规范类风险控制通则

非个人数据交互/交易环节确权风险控制规范类通则，包括以下两大类权属控制要求。

a) 数据财产权风险控制要求：
   1) 在数据交互/交易过程中，企业或组织应与交易方签订数据委托处理协议或数据转让协议约定双方的收益、责任和义务；
   2) 企业或组织应制定交易处理人员的行为规范，避免交易人员私自复制、转卖数据，侵害各方数据财产权益。
b) 数据使用权风险控制要求：
   1) 企业或组织交易数据使用权时应签署转移协议，约定数据使用的场景和范围；
   2) 企业或组织应建立数据使用授权事前审批、事后审查机制，确保数据在第三方合理使用。

8.2.3 技术类风险控制通则

非个人数据交互/交易环节确权风险控制技术类通则，分别从数据交互技术和安全技术来制定控制要求。

a) 数据交互技术要求：
   1) 非个人数据交互宜使用隐私计算技术，确保多方数据在不可见数据环境下进行联合建模，实现数据交互；
   2) 非个人数据交互/交易应建立管控平台，实现交互申请管理、数据对外输出管控。
b) 数据交互安全技术要求包括但不限于不可逆数据库技术、数据水印、权限控制、日志审计、交易过程加密等。

参 考 文 献

[1] GB/T 37932-2019 信息安全技术-数据交易服务安全要求
[2] GB/T 37973-2019 信息安全技术-大数据安全管理指南
[3] GB/T 40094　电子商务数据交易（所有部分）
[4]《中华人民共和国个人信息保护法》
[5]《中华人民共和国数据安全法》
[6]《中华人民共和国网络安全法》
[7]肖冬梅，文禹衡. 数据权谱系论纲. 湘潭大学学报（哲学社会科学版），2015（6）
[8]祝梦迪. 大数据时代数据确权问题研究. 科学导报·学术，2020（20）
[9]张钦润，傅晓媚. 数据权利属性法律问题研究. 燕山大学学报(哲学社会科学版)，2020（1）
[10]丁晓东.数据到底属于谁? 从网络爬虫看平台数据权属与数据保护.华东政法大学学报，2019（5）
[11]付熙雯，王新泽. 我国数据交易研究进展：系统性文献综述. 情报杂志,2022（11）
[12]卫球. 数据新型财产权构建及其体系研究. 政法论坛，2017（4）
[13]费方域. 数字 经济时代数据性质、产权和竞争. 财经问题研究，2018 （2）
[14]程啸. 论大数据时代的个人数据权利. 中国社会科学，2018 （3）
[15]郭明军、安小米、洪学海.关于规范大数据交易充分释放大数据价值的研究.电子政务 2018 (1)