ICS 67.040

X01

团　　体　　标　　准

T/ GDFCA 059—2021

粤港澳食品追溯 数据安全及隐私保护通用要求

Food Tractability of Guangdong-Hong Kong-Macao Greater Bay Area

General Requirements for Data Security and Privacy Protection

（公开征求意见稿）

2021 - XX - XX 发布　　2021 - XX - XX 实施

广东省食品流通协会　　发 布

目　次

前　言

本标准按照GB/T 1.1—2020给出的规则起草。

本标准归口单位：广东省食品流通协会。

本标准主要起草单位：

本标准主要起草人：

粤港澳食品追溯 数据安全及隐私保护通用要求

1 范围

本文件规定了食品追溯服务可以采集、传输、存储、处理、共享、出境的数据种类、范围、方式、条件等，以及数据安全保护要求。

本文件适用于食品追溯服务提供者规范数据活动，也适用于主管监管部门、第三方评估机构对食品追溯服务数据活动进行监督、管理、评估时参考。

2 术语和定义

GB/T 25069—2010、GB/T 35273—2020界定的术语和定义适用于本文件。

3 概述

3.1 食品追溯数据类型

食品追溯服务涉及的数据类别为：用户数据、企业经营数据，具体数据类别及对应示例参见附录表A.1。

a）用户数据：指食品追溯过程当中涉及到的个人用户及企业用户相关数据。

1）个人用户数据：指食品追溯过程中涉及的个人用户数据。

2）企业用户数据：指食品追溯过程中涉及的企业客户数据、供应商数据等企业用户相关数据。

b）企业经营数据：指经营活动中产生的各类业务经营相关的数据，包括但不限于采购信息、库存信息、出入库信息、销售信息、配送信息、财务信息等。

3.2 隐私范畴

本文的隐私范畴应包括但不限于以下内容：

a）供应链渠道信息（上下游企业主体）；

b）财务信息；

c）进销存明细信息；

d）客户个人信息；

e）国家法律法规规定的其他信息。

4 数据采集安全

数据采集安全要求包括：

a)明确数据采集原则、采集目的与用途、采集范围与方式、采集周期和频率和保存期限，确保数据采集的合法性、必要性、正当性；

b)对数据源、数据采集的环境、设施、技术采取必要的安全机制和管控措施，对产生数据的数据源进行身份鉴别和记录，确保采集数据的机密性、完整性和真实性；

c)采用技术措施保护加载、清洗和转换过程中数据的安全性。

5 数据传输安全

数据传输安全要求包括：

a) 应明确需要进行传输加密的业务场景，支持对个人信息和重要数据的加密传输；

b) 应提供对传输通道两端进行主体身份鉴别和认证的技术方案和工具；

c) 应提供对传输数据的完整性进行检测并执行恢复控制的技术方案和工具；

d) 应提供对数据传输安全策略的变更进行审核和监控的技术方案和工具，对通道安全策略配置、密码算法配置、密钥管理等保护措施进行审核及监控。

6 数据存储安全

6.1 数据逻辑存储

数据逻辑存储安全要求包括：

a) 应建立各类数据存储系统的安全配置规则，采取技术手段和工具支撑数据存储系统的安全管理；

b) 应具备多租户数据存储安全隔离能力；

c) 应定期检查数据存储系统安全配置以符合基线的一致性要求；

d) 应定期探查存储系统的数据是否符合相关合规性的要求；

e) 应采用碎片化分布式离散存储技术保存数据资源，并具有完整性验证机制；

f) 应支持采用符合国家认定的密码算法对高敏感数据进行加密存储，平台服务商不得掌握密钥。

6.2 数据备份与恢复

数据备份与恢复安全要求包括：

a) 应建立数据存储冗余策略、管理制度与规程，明确定义数据复制、备份和恢复的范围、频率、工具、过程、日志记录规范、数据保存时长等；

b) 应建立用于数据备份、恢复的统一技术工具，并将具体的备份的策略固化到工具中，保证相关工作的自动化执行；

c) 应建立数据复制、数据备份与恢复的定期检查和更新工作程序，包括数据副本更新频率、保存期限等，确保数据副本或备份数据的有效性。

6.3 数据访问控制

数据访问控制安全要求包括：

a）应建立数据资源安全访问策略，由授权主体进行访问策略配置，授予数据使用者为完成各自任务所需要的最小权限。访问控制的范围应包括与数据资源访问相关的主体、客体以及它们之间的操作；

b）应采用基于用户组或角色的方法，保障数据使用者访问数据资源时权限明确；

c）应采用多种方式对数据资源访问主体的身份进行鉴别；

d）应采用必要的措施使数据使用者的访问和修改等行为具有不可抵赖性。

7 数据处理安全

7.1 数据脱敏

数据脱敏安全要求包括：

a）应建立数据脱敏规范，明确需要脱敏处理的应用场景和处理方法；

b）应支持基于规则的数据静态脱敏；

c）应提供面向使用者的定制化数据脱敏功能，可基于场景需求自定义脱敏规则；

d）应提供数据脱敏处理过程日志记录,满足数据脱敏处理安全审计要求。

7.2 数据分析

数据分析安全要求包括：

a）应对数据分析结果进行二次风险评估，确保衍生数据不超过原始数据的授权范围和安全使用要求；

b）应对利用多源数据进行大数据分析的过程进行日志记录，以备对分析结果质量、真实性和合规性进行数据溯源；

c）应对利用数据分析算法输出的结果进行风险评估,避免分析结果输出中包含可恢复的个人信息、重要数据等数据和结构标识，从而防止个人信息、重要数据等敏感信息的泄漏；

d）应对平台数据分析算法的变更进行风险评估。

7.3 数据使用

数据使用安全要求包括：

a）应制定整体的数据权限管理制度，规定了各参与方身份及访问权限的授予、变更、撤销等流程，以及数据全生命周期的管理要求和责任制；

b）应定义并执行了统一的身份及访问管理流程，各系统均遵循规范的身份及访问管理流程对用户访问数据资源进行管理，并定期审核当前的数据资源访问权限是否符合身份及访问管理的规范

要求，身份及访问管理应遵循最少够用和职责分离的原则；

c）应建立数据使用正当性的监督审核机制，保证在数据使用声明的目的和范围内对受保护的个人信息、重要数据等数据进行使用和分析处理；

d）应建立统一的身份及访问管理平台，对各系统的用户和数据资源进行权限管理，遵循做小够用的原则，并依据数据使用目的建立相应强度或粒度的访问控制机制；

e）应针对关键的系统采用多因素认证的方式进行身份认证，如可信的数字证书、生物识别方式等。

7.4 数据处理

数据处理环境安全要求包括：

a）数据处理系统或平台应与身份及访问管理平台实现联动，用户在使用数据处理系统或平台前已获得了授权；

b）应保证对不同数据使用者在数据处理平台中的数据、系统功能、会话、调度和运营环境等资源实现隔离控制；

c）应建立数据处理日志管理工具，记录用户在数据处理平台上的加工操作，以备后期追溯；

d）应对用户在数据处理平台上对数据的操作开展定期审计，确定用户对数据的加工未超出前期申请数据时的目的。

8 数据共享安全

数据共享安全要求包括：

a）应建立数据获取和使用安全规范，明确数据使用者的数据获取方式、服务接口、授权机制和数据使用的权限范围等；

b）应建立规范的数据共享审核流程，确保没有超出数据提供者所允许的数据授权使用范围；

c）数据使用者应采用数据服务接口方式获取共享数据资源；

d）应建立数据服务接口调用的安全规范，包括接口名称、接口参数、接口安全要求等；

e）应制定数据服务接口安全控制策略,提供对数据服务接口的安全限制和安全控制措施,如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等，并对数据服务接口调用的参数进行限制或过滤，一旦发现异常会触发告警机制；

f）应统一收集数据服务接口调用的相关记录日志，并建立相应针对数据接口调用的审计工具，对数据接口调用情况进行定期审计。

9 数据出境

追溯服务提供者开展跨境食品追溯时，将食品追溯相关信息传输给港澳的关联公司、组织、业务合作伙伴，构成数据出境。数据出境时应遵循以下要求：

a）事先开展数据出境安全评估，并依评估结果采取有效的保护个人信息主体权利及数据安全的措施。数据出境安全评估应包括但不限于以下内容：

1）数据出境的合法性及必要性评估；

2）涉及个人信息或重要数据的情况，包括数据类型、数量、范围、敏感程度、境外存储期限、出境目的以及接收方处理数据的目的、方式、范围等；

3）个人信息主体合法权益保障能力评估；

4）数据接收方是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件，其安全保护措施、能力和水平，以及所在国家和地区的网络安全环境、数据保护法律体系的完善性等。

5）数据出境及再转移后被泄露、毁损、篡改、滥用等风险。

6）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险。

b）具有以下情形者，还应在数据出境前报请行业主管或监管部门组织安全评估：

1）含有或累计含有50万人以上的个人信息；
2）数据量超过1000GB；
3）包含人口健康等领域数据以及敏感地理信息数据等；
4）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

附 录 A

（资料性）

食品追溯数据分类分级示例

A.1 数据定级规则

依据数据定级要素及数据重要程度对快递物流服务的数据进行分级，从低到高依次划分为 4 级，1 级是最低级，4 级是最高级。

a）1 级数据：已披露或通过公开渠道可以获取的数据，数据一旦丢失、泄露、篡改、受到破坏后对企业不会造成不利后果。

b）2 级数据：数据一旦丢失、泄露、篡改、受到破坏后，对企业合法权益造成轻微影响，不会产生商誉损害、经济损失或法律责任。

c）3 级数据：数据一旦丢失、泄露、篡改、受到破坏后，对公众权益或个人合法权益造成中等或轻微影响，或对企业合法权益造成中等影响。

d）4 级数据：数据一旦丢失、泄露、篡改、受到破坏后，对国家安全造成影响，或对公众权益、企业合法权益、个人合法权益造成严重影响。

综上所述，数据安全级别划定规则见表 A.4 所示。

A.2 数据定级示例

数据类型	子类	内容	安全级别参考
个人用户数据	个人基础信息	姓名、生日、性别等	2
	个人身份信息	身份证信息、驾驶证信息、军官证信息、护照信息等	4
	个人联系信息	个人电话号码、详细地址、电子邮箱等	3
	个人财产信息	银行卡号、支付账号等	4
	个人鉴权信息	账户登录密码、支付密码、密保答案、用户个人数字证书 等	4
	网络身份识别信息	IMEI 号、IP 地址、MAC 地址等设备唯一标识	2
	个人位置信息	精准定位信息、经纬度等	3
	个人账户信息	账号、昵称等	1
企业用户数据	企业基础信息	企业名称、营业执照、法人信息、注册地址等	2
	企业鉴权信息	账号登陆密码、支付密码、密保答案等	4
	企业通信信息	企业电话、联系人姓名、联系邮箱、企业地址等	2

	企业账户信息	企业账户信息、银行信息等	3
企业经营数据	进销信息	企业进货单、销售单，包括供应商/客户、日期、商品、数量、金额等	3
	库存信息	企业实时库存，以及出入库记录	3
	财务信息	财务运营数据、成本利润数据等	3
	渠道信息	企业上游供应商信息、下游客户信息	3
	产品信息	企业生产或经营的产品品种信息	2