ICS
CCS

团　　体　　标　　准

T/CGCC XX—20XX

大宗商品电子交易
敏感数据存储和使用　规范

Electronic trading of bulk commodities—

Storage and use of sensitive data—Specification

（征求意见稿）

（本稿完成日期：2021 年 6 月 21 日）

20XX－XX－XX 发布　　20XX－XX－XX 实施

中国商业联合会　　发布

目　　次

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 总体原则 2
4.1 授权原则 2
4.2 安全原则 2
4.3 最小必要原则 2
5 敏感数据存储和使用要求 2
5.1 数据授权 2
5.2 敏感数据的存储要求 2
5.3 敏感数据的使用及分享 3
5.4 数据更正 4
5.5 数据移除 4
6 证实方法 4
6.1 交易平台授权的证实方法 4
6.2 敏感数据存储的证实方法 4
6.3 敏感数据使用及分享的证实方法 4
6.4 数据更正的证实方法 5
6.5 数据移除的证实方法 5
参考文献 6

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。

本文件由北京金网安泰信息技术有限公司提出。

本文件由中国商业联合会归口。

本文件起草单位：北京金网安泰信息技术有限公司、商业科技质量中心、江西省联交运登记结算中心有限公司、包头稀土产品交易所有限公司、国能互通内蒙古网络科技有限公司、牡丹国际商品交易中心有限公司、临沂国际商品交易中心有限公司、南方小麦交易市场有限公司。

本文件主要起草人：关键、肖燕林、唐泽宇、刘晓东、薛计涛、祁永星、刘祖国、李汉武、陈秀昆、刘月廷、谢永军、付元虎、王兰军、宋宪余、包银锋、王立荣、王轲菲。

引　　言

对于涉及大宗商品交易平台敏感信息的应用项目，除了需要对敏感信息做好脱敏和加密外，对原始敏感数据以及脱敏和加密数据的存储、使用是否合理，也是影响敏感信息安全的重要因素。数据存储不当，可能造成信息安全面临威胁、原有数据关联关系丢失、系统性能下降等问题；数据使用不当，交易参与各方和交易平台合法权益可能受到侵害。因此，敏感数据的存储和使用，在保证信息安全的同时，还需要保持原有信息数据的关联关系及数据的可用性，在需要时可识别出对应的信息主体。

本文件针对大宗商品交易平台敏感数据的存储和使用问题，规范在涉及交易平台敏感信息的行业应用项目中对敏感数据的存储和使用工作，在保证交易平台敏感数据安全的同时保证数据的可用性，在满足行业应用需求的同时最大程度地保障交易参与各方和交易平台合法权益。

大宗商品电子交易　敏感数据存储和使用　规范

1　范围

本文件确立了大宗商品交易平台敏感数据存储和使用的总体原则，规定了敏感数据存储和使用的要求，描述了对应的证实方法。

本文件适用于在涉及大宗商品交易平台敏感信息的行业应用项目中对敏感数据的存储和使用。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

交易平台　trading platform

为企业及个人提供交易、资金结算以及交收等相关服务的电子商务平台。

注：在本文件中专指大宗商品交易平台。

3.2

交易用户　customer

在交易平台（3.1）参与交易或其他相关业务，并接受相关服务的企业用户或个人用户。

3.3

信息主体　information subject

信息所标识的交易用户（3.2）。

3.4

敏感信息　sensitive information

能够单独或者与其他信息结合识别信息主体（3.3）身份，一旦泄露、非法提供或滥用可能危害信息主体（3.3）安全，泄露信息主体（3.3）隐私或商业机密的交易用户（3.2）信息。

3.5

敏感数据　sensitive data

敏感信息（3.4）所对应的计算机信息系统中的数据项或数字化文件。

3.6

脱敏　desensitization

为实现敏感信息（3.4）的可靠保护而对敏感信息（3.4）按照一定规则进行的信息变形处理。

3.7

原始信息标识　original information identification

为保证内容一致的原始敏感信息（3.4）在脱敏（3.6）后其一致性仍能被识别，而为脱敏（3.6）后信息分配的一个标识性编码。

3.8

项目运营者　project operator

实际管理行业应用项目信息系统的组织或机构。

3.9

敏感数据库 database for sensitive data

用于存储敏感数据（3.5）的数据库。

3.10

业务数据库 database for business data

用于存储业务数据的数据库。

3.11

敏感数据管理者 administrator of sensitive data

决定敏感数据（3.5）处理的目的和方式，实际管理敏感数据（3.5）并利用信息系统处理敏感数据（3.5）的组织或机构。

3.12

敏感数据获得者 receiver of sensitive data

从信息系统获取敏感数据（3.5），并对获得的敏感数据（3.5）进行处理的组织或机构。

4 总体原则

4.1 授权原则

从交易平台获取、存储、使用敏感数据前，得到交易平台的授权；敏感数据采用分级授权管理，以保证在没有得到授权的情况下无法使用或修改。

4.2 安全原则

采取足够的管理措施和技术手段，保护敏感数据的保密性、完整性、可用性。

4.3 最小必要原则

只获取、存储、使用项目所需的最少敏感数据类型和数量，使用后及时删除无保留必要的数据。

5 敏感数据存储和使用要求

5.1 数据授权

5.1.1 交易平台授权

项目运营者作为敏感数据获得者通过信息系统从交易平台获取、存储、使用敏感数据前，应得到交易平台的授权并签署授权协议，原则上只获取、存储、使用项目所需的最少敏感数据类型和数量。项目运营者从交易平台获得敏感数据后，成为敏感数据管理者。

5.1.2 授权协议的保管

项目运营者应妥善保管交易平台的授权协议。

5.2 敏感数据的存储要求

5.2.1 敏感信息的脱敏和加密

在使用从交易平台获取的敏感数据前，应先对敏感信息进行脱敏；在存储从交易平台获取的敏感数据前应对敏感信息进行加密。

在脱敏或加密前应声明所采用的脱敏或加密方法。所采用的脱敏方法应为脱敏后信息分配一个原始信息标识，并保证原始信息标识与原始数据具有一一对应关系。

5.2.2 敏感数据的加密形式

为保证敏感数据的安全性，防止数据泄露，针对敏感数据的存储应至少采取以下一种加密形式：

——数据级加密：在存储数据之前，先将数据加密后再存入数据库；

——文件级加密：将用于存储敏感数据的数据库启用透明数据加密特性。

注：透明数据加密是针对企业文件保密需求的一种文件加密技术。指对使用者来说是未知的，当使用者在打开或编辑指定文件时，系统将自动对未加密的文件进行加密，对已加密的文件自动解密；文件在硬盘上是密文，在内存中是明文；一旦离开使用环境，由于应用程序无法得到自动解密的服务而无法打开，从而起到保护文件内容的效果。

5.2.3 敏感数据的存储方式

存储敏感数据时，应将敏感数据和业务数据分开存储，不应存储在同一个数据库中，并为敏感数据和业务数据分配不同的访问控制权限。

应将原始敏感数据使用5.2.2规定的加密形式进行加密，并与已脱敏数据和原始信息标识一并存储在同一敏感数据库中，同时建立三者之间的关联关系。

应将已脱敏数据、原始信息标识、业务数据存储在业务数据库中，并建立三者之间的关联关系。

为保证数据安全，存储敏感数据时，还应采取以下措施：

——数据冗余存储：为避免数据损毁，应将同一敏感数据重复存储在至少三台不同的服务器上，若条件允许，宜将存储服务器异地部署；

——数据校验：应具有定期及使用前数据校验机制，以发现数据是否被篡改；

——数据备份：为了在数据损毁、丟失等情况发生时能够保证数据恢复，应定期对敏感信息数据库进行备份。

5.3 敏感数据的使用及分享

5.3.1 多重身份

项目运营者既作为敏感数据获得者从交易平台获取敏感数据，又可能作为敏感数据管理者使用或向其他敏感数据获得者分享敏感数据和业务数据。

5.3.2 敏感数据的使用

敏感数据管理者应针对敏感数据的使用建立严格的管理制度，科学划分管理角色和管理权限，制定严格的管理流程。

敏感数据用于对外展示时，应只展示脱敏后的数据信息。

在使用原始敏感数据时，应由敏感数据管理者授权，获得授权后才可取得相应数据的访问权限。

一般情况下，基于敏感数据进行的数据分析不需要明确信息主体身份，这样的数据分析应在已经脱敏的数据基础上进行。

若需要明确敏感信息主体及其原始敏感信息时，应严格按照管理制度要求执行。

5.3.3 敏感数据的分享

敏感数据管理者在向其他敏感数据获得者分享敏感数据前，应先开展信息安全影响评估，并依评估结果，采取有效的保护信息主体的措施。

评估通过后，敏感数据管理者应与敏感数据获得者签署对接使用协议，协议内容应包括敏感数据使用的授权方式、获取数据的方法和范围、数据保密责任、使用方法和范围等。

敏感数据获得者在使用原始敏感数据时，应由敏感数据管理者授权，获得授权后才可取得相应数据的访问权限。

若需要明确敏感信息主体及其原始敏感信息时，应严格按照双方协议约定执行，只允许在协议授权范围内进行展示。

5.4 数据更正

当信息主体的敏感信息发生变更后，敏感数据管理者应对该变更后的敏感信息重新进行脱敏或加密，并更新替换已存储的相应旧数据。

5.5 数据移除

敏感数据获得者应按照与敏感数据管理者签署的授权协议约定，对无保留必要的敏感数据及冗余存储数据及时进行移除。

6 证实方法

6.1 交易平台授权的证实方法

检查确认项目运营者保存有与交易平台签署的授权协议，并确认协议在有效期内。

6.2 敏感数据存储的证实方法

对敏感数据的存储，采取以下步骤进行证实：

——检查从交易平台获取的已存储至敏感数据库的数据，确认已按照所申明采用的脱敏或加密方法进行了脱敏或加密，并确认业务数据库中不包含敏感数据；

——检查存储在敏感数据库中的敏感数据，确认已经采用了 5.2.2 规定的至少一种加密形式：

- 数据级加密检查方法：查看数据库中存储的敏感数据，确认已经过加密；
- 文件级加密检查方法：确认数据库已启用了透明数据加密特性。

——检查确认已将敏感数据和业务数据存储在不同的数据库中，并具有不同的访问用户和访问控制权限；确认可以通过原始信息标识和已脱敏数据复原原始敏感数据，并且复原的过程中需要数据授权；

——检查确认敏感数据已经采用了冗余存储，即在至少三台不同的服务器上均有存储；确认具有数据校验机制，能够实现定期校验和使用数据前校验，确保能够发现数据被篡改；确认存在定期备份机制，并确认备份文件可以还原，确认具有数据还原的技术方案以及技术方案的验证测试方法。

6.3 敏感数据使用及分享的证实方法

对敏感数据的使用及分享，采取以下步骤进行证实：

——检查敏感数据管理者的管理制度，确认已经建立了严格的管理制度，管理角色和权限划分科学合理，制定了严格的管理流程；

——检查对外展示的敏感数据，确认展示的是脱敏后的数据信息；

——确认敏感数据获得者在获取原始敏感数据时遵守了管理流程，并确认必须经过数据授权以后才能获得数据的访问权限；

——检查记录文件和协议，确认敏感数据管理者在分享敏感数据前已经开展过信息安全影响评估，并具有详尽的评估报告，采取了可以有效保护信息主体的措施；确认敏感数据管理者与敏感数据获得者按照 5.3.3 的要求签署了对接使用协议；确认敏感数据获得者在使用敏感数据时，必须在获得了数据授权才能取得相应数据的访问权限。

6.4 数据更正的证实方法

在信息主体的敏感信息发生变更后，检查敏感数据管理者系统中敏感数据库和业务数据库里存储的数据以及冗余存储的数据，确认对应的数据已经同步更正，时间可以有延迟，但需要在合理的时间内完成。

6.5 数据移除的证实方法

确认数据移除的操作符合敏感数据获得者与敏感数据管理者签署的授权协议里相关条款的约定，系统内的敏感数据库、业务数据库及冗余存储数据库中均不存在无保留必要的敏感数据。

参 考 文 献

[1] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范