ISC 35.100.70
L 79

团 体 标 准

T/CHEAA 0001.2—2019

智能家电云云互联互通
第 2 部分：信息安全能力要求

Cloud to cloud interconnection for smart household appliances—

Part 2: Requirements for the competence of information security

2019-03-15 发布 2019-03-15 实施

中国家用电器协会 发布

目　　次

前言 II
引言 III
1. 范围 1
2. 规范性引用文件 1
3. 术语和定义及缩略语 1
3.1 术语和定义 1
3.2 缩略语 3
4. 接口信息安全要求 4
4.1 通信安全 4
4.2 身份认证和授权 4
4.3 数据安全 5
4.4 错误信息处理 6
4.5 接口稳定性 6
4.6 日志审计 6
5. 安全事件协同管理要求 7
5.1 安全事件的分类和分级 7
5.2 责任模型 7
5.3 服务条款 7
5.4 明确责任部门和人员 8
5.5 应急响应 8
5.6 事件通告 8
5.7 持续改进 9
附录 A（规范性附录）对用户数据和隐私保护的特别要求 10
A.1 导则 10
A.2 数据生产和收集 10
A.3 数据传输 10
A.4 数据的使用 10
A.5 数据保存 11
A.6 数据销毁 11
附录 B（资料性附录）相关法规、标准、认证规则 12
B.1 导则 12
B.2 国内相关标准和认证规则 12
B.3 国际相关法规、标准、认证规则 12

前　言

T/CHEAA 0001《智能家电云云互联互通》分为以下 2 个部分：

——第 1 部分：基本要求及一般模型

——第 2 部分：信息安全能力要求

本部分为 T/CHEAA 0001 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由中国家用电器协会提出。

本部分由中国家用电器协会标准化委员会归口。

截至本部分正式发布之日，中国家用电器协会未收到任何有关于本部分涉及专利的报告，中国家用电器协会不负责确认本部分的某些内容是否还存在涉及专利的可能性。

本部分起草单位：中国家用电器协会、杭州涂鸦信息技术有限公司、青岛海尔科技有限公司、博西家用电器投资（中国）有限公司、广州云智易物联网有限公司、联想（北京）有限公司、青岛聚好联科技有限公司、TCL 电子控股有限公司、长虹美菱股份有限公司、创维集团有限公司、康佳集团股份有限公司、美的集团股份有限公司、奥克斯空调股份有限公司、广东格兰仕集团有限公司、苏州三星电子有限公司、惠而浦（中国）股份有限公司。

本部分主要起草人：姜风、刘龙威、王淼、苏州、李杨、张亚群、张沛、罗寿中、李昱兵、黄辰、陆军锋、陈挺、刘复鑫、李桂丰、黄圣祥、谢厂节、万春晖、邵光达、钱海峰、柯都敏、周瑞鑫、井皓、祖岩岩、黄兵、胡协斌、张瑜龙、祁树壮、罗新宇、严勇、陈嘉琦、廖杰、毕志国、张天顺、曾伟枢、张小平、王涛。

引　言

近年，随着越来越多的家用电器接入了互联网、物联网，众多家电厂商的智能云平台从私有走向开放共享，而信息安全风险也随之被扩大，所以，实施云云互联互通的厂商间达成一致的信息安全要求就势在必行。

本部分针对家电云云互联面临的信息安全风险，提出了实施云云互联的云平台接口的信息安全能力要求、出现安全事件的协同管理机制、应满足或参考的国内外标准和技术法规、用户数据和隐私的保护规定，旨在帮助云云互联的企业达成一致的信息安全规范，保障双方利益，遏制因共享而产生的安全风险。

智能家电云云互联互通

第 2 部分：信息安全能力要求

1. 范围

本部分规定了在中国开展云云互联互通业务的各关联厂商云平台（以下简称各云平台）之间云云互联互通接口及相关要素的信息安全能力要求、信息安全事件的管理要求、相关标准及技术法规以及对用户数据和隐私保护的特别要求。

本部分不涉及对各云平台上非云云互联互通业务的安全和隐私性做要求。

2. 规范性引用文件

下列文件对于本部分的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本部分。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本部分。

GB/T 16264.8 信息技术 第 8 部分：开放系统互联目录

GB/Z 20985 信息技术 安全技术 信息安全事件管理指南

GB/Z 20986 信息安全技术 信息安全分类事件分级指南

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

IETF RFC 5246 安全传输层协议 1.2 版本［The Transport Layer Security（TLS）Protocol Version 1.2］

3. 术语和定义及缩略语

3.1 术语和定义

以下术语和定义适用于本部分。

3.1.1

安全传输层协议 transport layer security

在两个通信应用程序之间提供身份认证、数据保密性和数据完整性功能的协议。

[IETF RFC 5246，The Transport Layer Security (TLS) Protocol Version 1.2]

3.1.2

证书认证机构 Certificate Authority（CA）

负责创建和分配证书，受用户信任的权威机构。用户可以选择该机构为其创建密钥。

［GB/T 16264.8-2005，定义 3.3.16］

3.1.3

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、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、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的范围和类型详见 GB/T 35273-2017 附录 A。

［GB/T 35273-2017，定义 3.1］

3.1.4

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：关于个人敏感信息的范围和类型可详见 GB/T 35273-2017 附录 B。

［GB/T 35273-2017，定义 3.2］

3.1.5

个人信息主体 personal data subject

个人信息所标识的自然人

［GB/T 35273-2017，定义 3.3］

3.1.6

收集 collect

获得对个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。

［GB/T 35273-2017，定义 3.5］

3.1.7

密钥 key

一种用于控制密码变换操作(例如加密、解密、密码校验函数计算、签名生成或签名验证)的符号序列。

［GB/T 25069-2010，定义 2.2.2.106］

3.1.8

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。

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 35273-2017，定义 3.13］

3.1.9

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，无法识别个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

［GB/T 35273-2017，定义 3.14］

3.1.10

重放攻击 replay attack

一种主动攻击方法，攻击者通过记录通信会话，并在以后某个时刻重放这个会话或者会话的一部分。

［GB/T 25069-2010，定义 2.2.1.138］

3.1.11

信息安全事件 information security incident

一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，他们具有损害业务运作和威胁信息安全的极大可能性。

［GB/T 20985-2007，定义 3.3］

3.2 缩略语

以下缩略词适用于本部分。

TLS：安全传输协议（Transport Layer Security）

AES：高级加密标准（Advanced Encryption Standard）

3DES：三重数据加密算法（Triple Data Encryption Algorithm）

CFB：密码反馈（Cipher Feedback）

OFB：输出反馈（Output Feedback）

IV：初始化向量（Initialization Vector）

HMAC：哈希消息认证码（Hash-based Message Authentication Code）

SHA：安全散列演算法（Secure Hash Algorithm）

JSON：对象标记（Java Script Object Notation）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

CDN：内容分发网络（Content Delivery Network）

API：应用程序接口（Application Programming Interface）

4. 接口信息安全要求

4.1 通信安全

4.1.1 通信两端建立 TLS 传输通道

a) 各云平台之间的通讯接口均应采用 TLS 安全机制，应使用不低于 1.2 的安全版本。同时需要通过各自的证书进行双向认证，只允许证书校验通过后，才能完成请求。
b) 各云平台均应向证书认证机构（CA）申请证书或通过特定组织统一自建证书，并在云平台上部署证书。证书有效期不超过 24 个月。

4.2 身份认证和授权

4.2.1 平台登录接口

a) 各云平台的唯一标识符 PlatID 应满足随机性。
b) 各云平台的身份令牌 AuthToken 应根据 PlatID 和时间戳、随机数等计算得出，应通过安全的哈希方式生成，长度不应低于 16 位，应使用数字和字母组成。
   注 1： PlatID 和 AuthToken，来源于 T/CHEAA 0001-2017《智能家电云云云云互联互通标准》。
   注 2： 时间戳精度毫秒级，采用东 8 区（北京时间）的网络时间。
c) 每对 PlatID 和 AuthToken 应仅适用于对接的两个平台。
   例：A 平台给 B 平台发送的 PlatID 和 AuthToken，仅适用于 B 平台对 A 平台的身份验证，其他平台需要重新协商。
d) 应采取双向身份校验。
   例：A 平台发送验证信息给 B 平台，B 平台再确认 A 平台身份正确后，也发送自己的验证信息给 A 平台。

4.2.2 访问令牌管理

a) 完成身份验证后，A 平台应通过 AuthToken 提交获取访问令牌 AccessToken 的请求，B 平台下发给 A 平台访问令牌 AccessToken、更新令牌 RefreshToken 和 AccessToken 的有效时长，A 平台所有的请求都应在有效时长内，且包含该 AccessToken 才能正常请求。
   注： AccessToken 和 RefreshToken,分别用来做请求和刷新的 token。
b) AccessToken 和 RefreshToken 应根据 PlatID 和时间戳、随机数等，通过安全的哈希方式生成，长度不应低于 32 位，应使用数字和大小字母和特殊字符组成。
c) AccessToken 有效期不应超过 2 小时，过期或登出操作后应自动销毁。RefreshToken 有效期不应超过 14 天，过期或登出操作后应自动销毁。
d) 应主动更新 AccessToken，应使用 RefreshToken 进行请求更新， RefreshToken 应仅可使用一次，更新一次 AccessToken 后，RefreshToken 也应进行更新。

4.2.3 授权

平台应使用精细粒度的访问权限控制，能够根据平台账号分配最小、仅必要的权限。

4.3 数据安全

4.3.1 个人敏感信息传输

1） 加密密钥获取要求

a) 平台认证后，各厂商之间应相互下发密钥以加密隐私数据。
例如，A 厂商的 APP 通过 A 厂商的云请求控制 B 厂商的云，需要拿到 B 厂商下发的动态密钥，进行数据加密。
b) 各商云平台之间共享的数据，如果涉及个人敏感信息，需要分发密钥，用来加密传输，密钥有效期 60 分钟。
c) 密钥应保证随机性，应结合用户 ID，以及时间戳和随机数的哈希函数生成 128 位及以上字符串。
d) 动态密钥：每次用户登录认证后，应下发最新密钥，旧密钥废弃。
e) 用户登出操作后，旧密钥应废弃。
f) 加密算法应使用 AES 或 3DES 加密算法。
g) 加密模式应使用 CFB 或 OFB 模式，IV 应通过伪随机数生成器生成。

2） 安全传输要求

a) 个人敏感信息传输前应使用动态获取的加密密钥加密。
b) 涉及个人身份信息、个人生物特征识别信息或者密码和口令的传输应通过安全的哈希方式处理，应通过 HMAC-SHA256 方式进行加盐哈希。
c) 其他个人敏感信息的传输应根据业务场景选择去标签化、匿名化等处理方式。

表 1 个人敏感信息举例

隐私类型	举例
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、 手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康 状况产生的相关信息等
网络身份标识信息	系统账号、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等
其他信息	个人电话号码、性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

注：关于个人敏感信息的范围和类型可详见 GB/T 35273-2017 附录 B。

4.3.2 消息认证

a) 所有请求应取有效手段防止重放攻击。
例：可采取时间戳均存储在缓存中，且仅一次性有效的策略，以防止重放的可能性。
b) 所有请求应携带毫秒级别时间戳标记，时间的有效期设置为前后 10 分钟内有效。
c) 应使用 HMAC-SHA256 算法对数据内容和所有接口字段进行校验。

4.3.3 数据过滤

a) 数据传输，应使用 PUT 或 POST 传输 JSON 格式的数据，请求头部应指明类型

application/json，并且使用明确恰当的字符集。

例：指定明确的字符集，比如 UTF-8。

b) 验证数据范围、长度和类型。

c) JSON 中的所有参数，均应使用强类型和固定长度的校验。

例：PlateID 使用 Long 数字类型，长度为 16。

d) 数据过滤前，将数据按照常用字符进行编码。

e) 对所有的参数进行安全过滤，应对内容包含特殊字符和注入攻击的行为应进行严格检测，丢弃任何没有通过检测的数据。

注：常见的危险字符包括，< > " ' % ( ) & + \\' \"。

f) 尽可能采用“白名单”形式，验证所有参数。

4.4 错误信息处理

各云平台在云云对接过程中请求失败的情况下，应通过错误编码来表示错误类型，不应暴露任何平台或用户的敏感信息。

4.5 接口稳定性

4.5.1 分布式拒绝服务攻击（DDoS）的防护

a) 针对流量型和系统资源型的攻击，应有完善的应急防护手段，应通过运营商或基于域名的云防护产品实现快速流量迁移和清洗、CDN 等方式实现流量的稀释。

b) 针对应用服务资源消耗类型，应通过中间件层、应用层面对访问频率和访问特征进行限制等策略进行防护。

4.5.2 应用服务的系统安全

提供 API 的平台和对应的服务器，应执行系统和服务的加固，包括开放端口的白名单严格限制和对外服务的加固。

例：使用了 Apache，需要使用安全的 Apache 版本，并进行安全的配置。系统、中间件和应用服务应使用一定强度以上的密码，使其能够抵御字典式攻击。

4.5.3 应急响应与灾备

各云平台应为云计算平台制定应急响应计划，并定期演练，确保在紧急情况下重要信息资源的可用性。厂商云平台应建立事件处理计划，包括对事件的预防、检测、分析、控制、恢复及用户响应活动等，对事件进行跟踪、记录并向相关人员报告。各云平台应具备灾难恢复能力，建立必要的备份设施，确保客户业务可持续。

4.5.4 风险评估与监控

各云平台应定期或在威胁环境发生变化时，对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。应采取第三方机构进行风险评估、服务商安全监控预警等方式加强风险评估能力。

4.6 日志审计

各云平台应具备自动化请求日志收集和审计系统，监控采集云端云云互联互通业务相关的日志及网络流量，通过离线分析和实时分析两种方式识别并发现潜在的网络攻击行为，及时预警并采取相应的应对措施。

a) 日志收集和审计系统中应包括 API 接口日志和其他相关业务的服务和流量日志。
b) 日志收集和审计系统应根据安全需求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查，还应防范对审计记录的未授权访问、篡改和删除行为，为事后调查提供支撑。
c) 日志收集和审计系统应防止非授权访问、篡改或删除审计记录。
d) 日志收集和审计系统的接口请求日志保存时间应不少于 6 个月。
e) 日志中不应记录用户敏感数据信息。
f) 针对异常日志，应自动告警到相关运维人员，并进行对应的分析和处理。

5. 安全事件协同管理要求

5.1 安全事件的分类和分级

5.1.1 安全事件分类

应根据信息安全事件产生的结果表象做分类，分为数据泄露事件、服务不可用事件和其他事件。

a) 数据泄露事件：云云互联的数据出现泄露。
b) 服务不可用事件：服务出现不稳定或者不可用情况，并且影响到云互联的其他厂商的事件。
c) 其他事件，除了上述事件以外的其他事件。

5.1.2 事件分级

安全事件应依据国标 GB/Z 20986 中的安全事件分级考虑隐私，将信息安全事件划分为四级：特别重大事件、重大事件、较大事件和一般事件。

a) 特别重大事件是指能够导致特别严重影响或破坏的信息安全事件。
b) 重大事件是指能够导致严重影响或破坏的信息安全事件。
c) 较大事件是指能够导致较严重影响或破坏的信息安全事件。
d) 一般事件是指不满足以上条件的信息安全事件。

注：事件详细说明请参考 GB/Z 20986。

5.2 责任模型

a) 针对数据泄露事件，各云平台相互间的追责，基本依据是责任归属于直接导致数据泄露的云平台或客户端所属的厂商。
b) 针对服务不可用事件，应根据导致服务不稳定或不可用的节点判断，责任应归属于该节点所有者平台。
c) 在责任未明确的时候，双方应共同协商、承担并调查原因。在双方对于数据泄露事件无法达成一致的情况下，应由独立的第三方介入调查。如调查无果，双方应共同承担责任。

5.3 服务条款

云云互联双方应签订具有法律效应的服务条款，应包含以下等内容：

a) 云云互联企业双方的服务内容。
b) 云云互联企业双方各自的权利和义务。
c) 涉及用户数据、用户隐私数据，需要明确数据的所有权，使用权限。
d) 保密条款，包括用户数据、用户隐私数据不允许主动向第三方披露等。

e) 服务期限和终止，并且终止后双方对于信息安全的义务。
f) 违约责任和免责条款。

5.3.1 平台数据所有权说明

a) 个人信息所有权应归属于信息所标识的自然人，即使用物联网服务的实际个人用户。个人信息所有者应拥有信息数据的完全访问和控制权限，并且有权利要求提供服务的厂商对其信息数据进行对应的操作。
b) 经过匿名化处理后的数据和信息，应归属于这些信息的提供者，即提供信息的云平台主体。数据归属的云平台应具有对数据的完全访问和控制权限。
c) 云平台的用户数据和归属合作平台的数据，不能执行任何未获授权的使用和披露，但是以下情形除外：在国家有关机关依法查询或调阅用户数据时，平台具有按照相关法律法规或政策文件要求提供配合，并向第三方或者行政、司法等机构披露的义务。

5.3.2 平台数据使用权限说明

1) 数据的披露

a) 未在双方书面允许下，不允许向第三方披露。
b) 只允许为提供或改进产品、服务的目的而与第三方共享。
c) 不允许为第三方的销售目的而与第三方共享数据，更不允许销售共享数据。

2) 数据的删除

a) 用户有权申请删除其在双方平台交互过程中，产生的个人数据。平台双方需要在 7 天内完成数据删除。
b) 非个人数据，数据归属平台有权利要求共享平台对数据进行删除的操作。
c) 所有数据删除的操作，需要在企业内部有明确的流程和制度保障。
d) 在服务终止后，必须安全删除通过云云互联接口同步过来的用户数据及用户隐私数据。

5.4 明确责任部门和人员

a) 应明确各云平台主要负责人对信息安全负全面领导责任，包括为信息安全工作提供人力、财力、物力保障等。
b) 应明确各云平台对接的安全接口人和备用接口人，及其职责。

5.5 应急响应

a) 各平台协同诊断，认定安全事件和确认事件的责任方。
b) 事件责任方应根据合作服务条款内的明细，在指定时间内抑制受害范围并恢复业务服务。
c) 事件责任方应负责整个事件调查，包括必要的调查记录。

5.6 事件通告

a) 云云互联任何一方应有义务和权力向各相关方通告详细的安全事件原因。
b) 如果因特别重大事件、重大事件或较大事件，而导致对业务可用性和稳定性的影响时间超过 1 个小时，应按照与各相关方的服务条款进行事件对外的通告。
c) 需要向在有关事件响应的法律、法规和/或规章中要求的地方、省、国家有关部门通告。
d) 在牵涉到法律强制的地方，事件责任方负责与法律强制部门的联络。

5.7 持续改进

云云互联各相关方应对重大事件和特别重大事件进行持续的跟踪。责任方应给出相应的改进措施，并通过管理手段或技术手段真实落地。

附 录 A

（规范性附录）

对用户数据和隐私保护的特别要求

A.1 导则

由于云云互联涉及的业务场景必然涉及用户隐私的传输，为保护用户的隐私数据，对信息收集主体及云云互联中各关联厂商（以下简称各方）特别提出以下信息安全能力要求。

A.2 数据生产和收集

A.2.1 基本原则

a) 合法性：对各方的所有行为应进行合法要求，同时，明确对应的法律责任的明确。
b) 用户授权：应通过有效的渠道获取信息主体的授权，不允许超过信息主体授权行为以外的数据收集和操作。
c) 用户权限保障：各方需要通过技术或管理流程保障用户的权限能够得到有效的保障。
d) 数据最小化：各方不应收集、存储、请求、提供、传递与服务无关的数据。
e) 数据分类：应区分个人数据和平台信息数据。
f) 匿名化：个人敏感信息在传递前应做匿名化处理。

A.2.2 用户权限

1) 知情权

a) 用户应能通过隐私条款等方式知悉信息收集主体及其所提供服务的基本信息和数据。
b) 用户应能通过隐私条款等方式知悉其将被收集到的所有数据及这些数据的全部用途。
c) 用户应能通过隐私条款等方式知悉其享有的用户数据保存、访问、迁移、删除等权力。

注：隐私条款模板应参考 GB/T 35273—2017 的附录 D。

2) 选择权

当某位用户不选择上传数据或不同意隐私条款时，不应收集该用户的数据。

3) 处置权

用户应能通过电邮或联系客服等方式履行访问、迁移、删除等权力。信息收集主体和云云互联中各关联厂商应支持用户账号注销等机制，某一用户要求删除用户数据或注销用户账号时应删除与之相关的用户数据。

A.3 数据传输

参考 4.1 通讯安全和 4.3.1 个人敏感信息传输的要求。

A.4 数据的使用

A.4.1 认证和授权

参考 4.2 身份认证和授权的要求。

A.4.2 数据展示

各方应对需展示的个人信息采取去标识化处理等措施，以降低个人信息在展示环节的泄露风险。

A.4.3 数据审计

a) 各方均应具有完备的自动化数据库操作审计记录。
b) 针对可能有风险的操作，比如 A 厂家要求删除其所有数据，需要进一步沟通和需要一定的审批流程。

A.5 数据保存

a) 各方均应对敏感数据进行集中地分布式存储，统一监控管理，通过 VPC 隔离。
b) 各方均应实施数据库加密, 对所有隐私信息进行加密或 hash 后存储。
c) 各方均应将用户数据和用户隐私数据存储在中国境内。
d) 各方均应采用分布式架构，所有业务服务器需要同时部署在多个不同的机房，数据同时存放两个以上机房，并实时备份。
e) 各方对用户隐私数据保存时间均不应超过 1 年。
f) 各方在服务期届满、服务提前终止时，需要按照平台约定的缓冲期内继续存储对方平台的用户数据，缓冲期不超过 7 天，缓冲期届满平台将在 7 天限期删除的时间后立即执行删除所有相关用户数据的操作，包括缓存或者备份的副本。

A.6 数据销毁

a) 各云平台应对平台内部的数据制定相应的安全销毁策略，包括云主机内部的数据以及实体介质的数据。应明确记录数据销毁的过程以及对销毁过程进行全程记录和监督。
b) 如果一方平台存在违约未销毁数据的行为，须依法承担违约责任。

附 录 B

（资料性附录）

相关法规、标准、认证规则

B.1 导则

以下列举当前对于云平台和个人信息保护具有重要指导作用的法规、标准、认证规则，为了保障互联双方具有能力共同保障互联业务的信息安全，云云互联双方应基于具体的业务特点，在参考以下一项或多项标准及技术法规的基础上，实现云云互联互通。

B.2 国内相关标准和认证规则

a) GB/T 18336 信息技术 安全技术 信息技术安全评估准则
b) GB/T 31167 信息安全技术 云计算服务安全指南
c) GB/T 31168 信息安全技术 云计算服务安全能力要求
d) 可信云服务认证（TRUCS）

B.3 国际相关法规、标准、认证规则

a) ISO 15408 信息技术安全评估准则
b) ISO 27001 信息安全标准
c) ISO 27017 云服务安全标准
d) ISO 27018 云服务隐私保护操作规范
e) CSA STAR 云安全保障认证
f) 欧盟一般数据保护条例（GDPR）