ICS 33.240.01
L 70

团　　体　　标　　准

T/ISC 0031—2023

个人数据云存储应用技术要求和测试方法

Technical Requirements and Evaluation Methods of Personal Data Cloud Storage Application

（发布稿）

2023-06-12 发布　　2023-07-12 实施

中　国　互　联　网　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。

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这些专利的责任。

本文件由中国互联网协会归口。

本文件主要起草单位：中国信息通信研究院、泰尔认证中心有限公司、OPPO广东移动通信有限公司、郑州信大捷安信息技术股份有限公司、北京小米移动软件有限公司、北京滴普科技有限公司、维沃移动通信有限公司。

本文件主要起草人：杨萌科、刘陶、宁华、王宇晓、钱康、薛刚、李腾、刘献伦、贾科、刘为华、徐曼、郭英男、王莲、 张鹏。

引　言

随着5G信息时代的到来，个人信息呈爆炸式增长，面对海量数据存储的需求，云存储应用得以迅速发展，并成为未来存储发展的一种趋势。另一方面，《数据安全法》和《个人信息保护法》的颁布实施，使有关云存储应用的个人信息问题受到了广泛关注。亟需一套针对个人数据云存储应用技术要求且行业统一遵循的规范。

个人数据云存储应用技术要求和测试方法

1 范围

本文件规定了个人数据云存储应用的技术要求，包括存储技术处理能力要求、用户体验保障要求和安全保障要求等，并描述了相应的测试评价方法。

本文件适用于规范个人数据云存储应用的技术要求及相关测试评价方法，指导云存储应用对个人信息的安全防护。

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 35273-2020 信息安全技术 个人信息安全规范

GB/T 41479-2022 网络数据处理安全要求

GB/T 39680-2020 信息安全技术 服务器安全技术要求和测评准则

GB/T 29765-2021 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

3 术语和定义

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。

［来源：GB/T 41479-2022，3.1］

3.2

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。

［来源：GB/T 35273-2020，3.1］

3.3

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。

［来源：GB/T 35273-2020，3.2］

3.4

云存储 cloud storage

通过集群应用、网络技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备，通过应用软件集合起来协同工作，形成云存储资源池，共同对外提供数据存储和业务访问功能的一种存储使用方式。

3.5

个人网盘服务业务运营者 personal online disk service business operator

运用特定的计算机程序向自然人消费者提供的数据存储、备份、传输及其他信息服务业务的系列服务和产品的业务运营者。

4 个人数据云存储应用技术要求

4.1 个人信息保护要求

个人信息云存储应用在收集使用用户个人信息时，满足以下要求：

a）收集使用个人信息及收集过程应严格按照GB/T 35273-2020《个人信息安全规范》中5.1和5.2的有关要求执行。

b）收集个人信息时，应当遵循合法、正当、必要的原则，向个人信息主体公开收集、使用规则，明示收集、使用信息的方式和范围，并获得个人信息主体的授权同意。

c）收集年满14周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意。

d）个人网盘服务业务运营者应建立沟通渠道和反馈机制,及时响应个人信息主体查阅、更正、删除其个人信息及注销账号的请求,不应对请求设置不合理条件,应遵守GB/T 35273—2020中 8.7有关响应个人信息主体请求的要求。

4.2 用户权益保障要求

4.2.1 传输速率要求

应用的传输速率满足以下要求：

a）在同一网络条件下，个人网盘服务业务经营者应为用户提供无差别的上传/下载速率服务。

b）确因自身服务能力、业务发展和商业模式等因素，不能提供4.2.1 a）条服务时，向免费用户提供的上传和下载的最低速率应确保满足基本的业务使用需求。

4.2.2 服务资费要求

应用的服务资费满足以下要求：

a）应优化产品服务资费介绍，向用户清晰明示存储空间、传输速率、功能权益及资费水平等内容。

b）对于包含“限速”、“极速”等相关描述的，应向用户清晰明示提供的服务速率。

4.3 安全保障要求

4.3.1 数据存储安全

对数据的存储安全满足以下要求：

a）应支持将个人信息进行匿名化或去标识化处理。

b）存储个人信息等敏感网络数据时,应采用加密、安全存储、访问控制、安全审计等安全措施，提供机密性（加密算法、密钥管理符合密码应用安全要求）和完整性（算法符合密码应用安全要求）保护。

c）对个人信息的存储应具备异地冗余容灾的数据备份机制，并保证个人信息的完整可用性。

d）存储个人信息,不应超过与和个人信息主体约定的存储期限或个人信息主体授权同意有效期。

e）存储个人生物特征识别信息的,应遵守GB/T 35273—2020中6.3 b)和c)的要求及生物特征识别信息保护相关国家标准要求。

f）进行数据存储的服务器应满足GB/T 39680-2020中5.1和5.2的安全技术要求。

4.3.2 数据传输安全

对数据的传输安全满足以下要求：

a）在数据传输过程中，应使用安全通信协议或者应用层数据加密及完整性保护措施，保护用户的数据传输安全。

b）云端应明确数据上传来源、上传方式、上传范围等内容，并记录存档。

c）在数据上传前后应采用校验技术对数据完整性进行校验。

d）应保证上传的数据不被篡改或者伪造。

4.3.3 数据备份安全

对数据的备份安全满足以下要求：

a）应在对用户进行明示并获得用户的同意后才可进行自动备份，不应在未经用户同意的情况下自动开启备份。

b）应提供方便易操作的自动备份关闭选项。

c）应用在进行自动备份时，宜采用用户可感知的方式进行。

d）应支持用户对自主备份的数据进行更新、删除等操作。

e）应提供完整性校验机制，保证备份数据完整性，一旦发现完整性破坏应及时告警。

g）进行数据备份时与恢复时，应满足GB/T 29765-2021中6.2和6.3的技术要求。

4.3.4 数据删除安全

对数据的删除安全满足以下要求：

a） 对个人云存储数据符合以下情形时，个人网盘服务业务运营者应及时告知用户转移数据，并对个人信息进行删除：

1）个人信息超出双方约定的存储期限；

2）网络产品和服务停止运营；

3）个人信息主体注销账号。

4.3.5 数据访问安全

对数据的访问安全满足以下要求：

a）个人网盘服务业务运营者开展数据处理活动时，应明确相关人员的访问权限，防止非授权访问。

b）个人网盘服务业务运营者对个人信息、个人敏感信息的关键操作（例如批量修改、拷贝、删除、下载等），应设置内部审批和审计流程，并严格执行。

5 测试评价方法

5.1 个人信息保护要求测试评价方法

测试编号：5.1.1
测试项目：个人信息保护要求
项目要求：见第 4.1 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查应用软件收集使用的个人信息及收集过程； 步骤2：检查应用软件收集使用信息的方式和范围，并核实个人信息主体知情同意的情况； 步骤3：检查应用软件收集未成年人的个人信息的相关约定； 步骤4：检查应用软件是否建立沟通渠道和反馈机制。
预期结果： 在步骤 1 后，支持收集使用的个人信息及收集过程严格按照 GB/T 35273-2020《个人信息安全规范》中 5.1 和 5.2 执行； 在步骤 2 后，支持在收集个人信息时，向个人信息主体公开收集、使用规则，明示收集、使用信息的方式和范围，并获得个人信息主体的授权同意； 在步骤 3 后，支持在收集年满 14 周岁未成年人的个人信息前，征得未成年人或其监护人的明示同意；不满 14 周岁的，征得其监护人的明示同意； 在步骤 4 后，支持及时响应个人信息主体查阅、更正、删除其个人信息及注销账号的请求。 如上述步骤 1、2、3、4 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

5.2 用户权益保障要求测试评价方法

测试编号：5.2.1
测试项目：传输速率
项目要求：见第 4.2.1 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查在同一网络条件下，为不同类别的用户提供的上传下载速率服务。
预期结果： 在步骤 1 后，未发现为不同类别的用户提供有差别的上传下载速率服务。不能提供无差别的上传下载速率服务时，向免费用户提供的上传和下载的最低速率应确保满足基本的下载需求。 如上述步骤 1 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

测试编号：5.2.2

测试项目：服务资费
项目要求：见第 4.2.2 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查云存储应用的产品服务资费介绍，并核实向用户明示的存储空间、传输速率、功能权益及资费水平等内容； 步骤2：检查包含“限速”、“极速”等相关描述的云存储应用，核实是否向用户清晰明示提供的服务速率。
预期结果： 在步骤 1 后，未发现产品服务资费介绍与实际向用户明示的内容不一致； 在步骤 2 后，支持向用户清晰明示所提供的服务速率。 如上述步骤 1、2 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

5.3 安全保障要求测试评价方法

测试编号：5.3.1
测试项目：数据存储安全
项目要求：见第 4.3.1 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查是否支持个人信息匿名化、去标识化处理的能力，并核实个人信息实际处理情况； 步骤2：检查对个人信息存储的机密性保护、完整性保护能力，并核实保护算法和密钥的安全； 步骤3：检查对个人信息的异地数据备份机制，并核实可用性； 步骤4：检查对个人信息的存储期限，并核实个人信息主体授权同意有效期； 步骤5：检查对个人生物特征信息的存储，并核实相关要求； 步骤6：检查数据存储服务器的安全规范要求。
预期结果： 在步骤 1 后，支持个人信息匿名化或去标识化处理，并对个人信息按需进行了处理； 在步骤 2 后，支持个人信息存储的机密性保护、完整性保护，采用的密码算法安全有效同时对涉及的密钥进行了安全管理； 在步骤 3 后，支持个人信息的异地数据备份机制，并且有效可用； 在步骤 4 后，支持在约定期限对个人信息进行存储； 在步骤 5 后，支持存储的个人生物特征识别信息严格按照 GB/T 35273—2020《个人信息安全规范》中 6.3 b)和 c)执行； 在步骤6后，支持数据存储的服务器安全规范严格按照GB/T 39680-2020《服务器安全技术要求和测

评准则》中5.1和5.2执行。 如上述步骤 1、2、3、4、5、6 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

测试编号：5.3.2
测试项目：数据传输安全
项目要求：见第 4.3.2 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤 1：检查传输中个人敏感信息的机密性和完整性保护措施，并核实保护实施细节（协议版本、密码算法、密钥等的安全）； 步骤 2：检查云端上传数据的来源、方式、范围等内容，并核实存档记录； 步骤 3：检查数据上传前后的校验技术，并核实数据完整性； 步骤 4：检查上传的数据的真实准确性。
预期结果： 在步骤 1 后，支持传输中个人敏感信息的机密性和完整性保护，并采用安全的通信协议或应用层数据安全加密算法进行了有效保护，同时对涉及的密钥进行了安全管理； 在步骤 2 后，支持明确数据的上传来源、上传方式、上传范围等内容，同时记录存档； 在步骤 3 后，支持在数据上传前后采用校验技术对数据完整性进行校验； 在步骤 4 后，未发现上传的数据被篡改或者伪造。 如上述步骤 1、2、3、4 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

测试编号：5.3.3
测试项目：数据备份安全
项目要求：见第 4.3.3 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查对个人信息进行自动备份的明示告知内容； 步骤2：检查进行自动备份的操作步骤； 步骤3：检查应用进行自动备份的方式； 步骤4：检查用户对自主备份的数据可进行的操作； 步骤5：检查备份系统的数据完整性校验功能。 步骤6：检查数据备份与恢复的安全规范要求。
预期结果： 在步骤 1 后，支持在应用进行自动备份前对用户进行明示，并在获得用户同意后进行自动备份； 在步骤 2 后，支持提供方便易操作的自动备份关闭选项；

在步骤 3 后，支持以用户可感知的方式进行自动备份； 在步骤 4 后，支持用户对自主备份的数据进行更新、删除等操作； 在步骤 5 后，支持数据完整性校验，能检验出备份数据的完整性已被破坏，并能给出相应的警示。 在步骤 6 后，支持按照 GB/T 29765-2021 中 6.2 和 6.3 的技术要求进行数据备份与恢复。 如上述步骤 1、2、3、4、5、6 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

测试编号：5.3.4
测试项目：数据删除安全
项目要求：见第 4.3.4 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查个人云存储数据双方约定的存储期限，并核实网络产品和服务停止运营、个人信息主体注销账号等情况。
预期结果： 在步骤1后，支持个人云存储数据符合情形时，个人网盘服务业务运营者及时告知用户转移数据，并对个人信息进行删除。 如上述步骤 1 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

测试编号：5.3.5
测试项目：数据访问安全
项目要求：见第 4.3.5 节
预置条件：1、被测应用软件处于正常工作状态
测试步骤： 步骤1：检查个人网盘服务业务运营者的数据访问控制机制； 步骤2：检测个人网盘服务业务运营者的内部审批和审计流程。
预期结果： 在步骤1后，支持数据处理活动相关人员的访问权限，防止非授权访问； 在步骤2后，支持设置内部审批和审计流程，并严格执行。 如上述步骤 1、2 无异常，则该项目评测结果为“未见异常”，否则为“不符合要求”。

附 录 A
（规范性附录/资料性附录）

《个人网盘服务业务用户体验保障自律公约》
《关于开展信息通信服务感知提升行动的通知》