公有云中个人信息保护管理体系技术规范

文件编号：DNI-GZ-JS-70

技术规范编号：CTS DNI-CPII-2026

文档版本：A/0

编制：技术部　　日期：2026.5.19

审核：杨舒　　日期：2026.5.19

批准：杨舒　　日期：2026.5.19

受控状态：受控文件

发布日期：2026年05月19日　　实施日期：2026年05月19日

发布单位：数网信认证服务（北京）有限公同

变更履历

日期	变更描述	版本/版次	审核	批准
2026.05.19	初始发布	A/0	杨舒	杨舒

公有云中个人信息保护管理体系技术规范

1 范围

本技术规范为公有云计算环境中的个人身份信息 (PII)保护措施的实施制定了公认的控制目标、控制措施和指南，以符合ISO/IEC 29100中的隐私原则。

本技术规范特别要求组织已依据GB/T 22080-2025/ISO/IEC 27001:2022建立信息安全管理体系并运行，以使达到管理体系的基本特性。

本技术规范特别规定了基于ISO/IEC 27002:2022的指南，并考虑了公共云服务提供商信息安全风险环境中可能适用的个人身份信息(PII)保护监管要求，是基于ISO/IEC 27018:2025转换为对公有云中个人信息保护提出了信息安全控制要求,是我机构开展公有云中个人信息保护管理体系认证的认证依据。

本技术规范适用于所有类型和规模的组织，包括公共和私营公司、政府实体和非营利组织，这些组织通过云计算以PII处理者的身份，根据合同向其他组织提供信息处理服务。本技术规范也适用于作为PII控制者的组织。

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 22080-2025/ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 信息安全管理体系 要求

ISO/IEC 27002:2022 信息安全 网络安全和隐私保护—信息安全控制

ISO/IEC 27018:2025 信息安全、网络安全和隐私保护—个人身份信息保护指南 公有云中作为PII处理者的信息 (PII)

ISO/IEC 29100:2011 信息技术 - 安全技术 - 隐私框架

ISO/IEC 27000 信息技术—安全技术—信息安全管理体系一概述和词汇

ISO/IEC 22123-1 信息技术—云计算—第1部分：词汇

3 术语和定义

就本文件而言，ISO/IEC 22123-1、ISO/IEC 27000、ISO/IEC 27002 以及以下内容中给出的术语和定义适用。

3.1数据泄露

安全漏洞导致传输、存储或以其他方式处理的受保护数据遭到意外或非法破坏、丢失、更改、未经授权的披露或访问。

3.2个人身份信息PII

a)可用于建立信息与相关自然人之间联系的信息，此类信息涉及的，或b)直接或间接与自然人相关的信息。

3.3PII控制者

确定处理目的和方式的隐私利益相关者（或多个隐私利益相关者）；

个人身份信息 (PII) (3.2)，指除出于个人目的使用数据的自然人以外的其他人员。注1：PII控制者有时会指示其他人（例如PII处理者(3.5)）代表其处理PII，但处理责任仍由PII控制者承担。

3.4PII主体

个人身份信息 (PII)(3.2)所关联的自然人。

3.5PII处理者

代表个人身份信息 (PII) 处理个人身份信息 (PII) 的隐私利益相关方(3.2)并按照PII控制者的指示进行处理(3.3)。

3.6PII处理

对个人身份信息 (PII) 执行的操作或一组操作(3.2)。

3.7公有云服务提供商

根据公有云模型提供云服务的当事方。

4 概述

本文件遵循ISO/IEC 27002:2022中用于描述控制的结构，本文件中的条款编号与ISO/IEC 27002:2022中的相应条款编号一致。本规范包含两个主要规范性部分。

5 组织控制措施

5.1 信息安全策略

ISO/IEC 27002:2022 5.1条款中的指南原则适用。此外，以下针对公有云服务提供商的特定指导原则及相关信息也适用。

a) 公有云个人身份信息 (PII) 保护实施指南

合同协议应明确公共云个人身份信息 (PII) 处理者、其分包商和云服务客户之间的责任分配，并考虑相关云服务的类型[例如，云计算参考架构中的基础设施即服务 (IaaS)、平台即服务 (PaaS) 或软件即服务 (SaaS) 类别的服务]。例如，应用层控制的责任分配可能因公共云PII处理者提供的是 SaaS 服务，还是云服务客户可以构建或叠加其自身应用程序的 PaaS 或 IaaS 服务而有所不同。

b) 公共云PII保护的其他信息

在某些司法管辖区，公共云PII处理者直接受PII保护法规的约束。在其他司法管辖区，PII保护法规可能仅适用于PII控制者。

云服务客户与公共云PII处理者之间的合同必须包含一种机制，以确保公共云PII处理者支持并管理双方合同的履行。云服务客户和公有云PII处理者。合同可以要求进行独立审计，以确保云服务客户认可的合规性，例如通过实施本文档和 ISO/IEC 27002中的相关控制措施。

5.2 信息安全角色和职责

ISO/IEC 27002:2022 5.2条款的指南原则适用。此外，以下针对公有云服务提供商的特定指南也适用。

a)公有云PII保护实施指南

公有云PII处理者应配备一名PII专家，为云服务客户提供关于正确处理PII信息的建议。

5.3 职责分离

ISO/IEC 27002:2022中5.3条款中的指南原则适用。

5.4 管理职责

ISO/IEC 27002:2022中5.4条款中的指南原则适用。

5.5 与主管机构联系

ISO/IEC 27002:2022中5.5条款中的指南原则适用。

5.6 与特殊利益集团联系

ISO/IEC 27002:2022中5.6条款中的指南原则适用。

5.7 威胁情报

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022条款中的指南原则适用。 27002:2022中5.7 适用

5.8 项目管理中的信息安全

ISO/IEC 27002:2022中5.8条款中的指南适用。

5.9 信息及其他相关资产的清单

ISO/IEC 27002:2022中5.9条款中的指南适用。

5.10 信息及其他相关资产的合理使用

ISO/IEC 27002:2022中5.10条款中的指南适用。

5.11 资产归还

ISO/IEC 27002:2022中5.11条款中的指南适用。

5.12 信息的分类

ISO/IEC 27002:2022中5.12条款中的指南适用。 27002:2022中5.12 适用。

5.13 信息标签

ISO/IEC 27002:2022中5.13条款中的指南适用。

5.14 信息传输

ISO/IEC 27002:2022中5.14条款中的指南适用。此外，以下针对公有云服务提供商的特定指南也适用。

a) 公有云PII保护实施指南

无论何时使用物理介质进行信息传输，都应建立一个系统来记录包含PII的传入和传出物理介质，包括物理介质类型、授权的发送方/接收方、日期和时间以及物理介质数量。在适当情况下，云服务客户应实施，公有云PII处理者应支持实施以下技术能力：

其他措施（例如加密）以降低在到达目的之前，途中发生未经授权访问的可能性。在这种情况下，双方都可以采取各自的此类措施。

5.15 访问控制

ISO/IEC 27002:2022中5.15条款中的指南适用。

5.16 身份管理

ISO/IEC 27002:2022中5.16条款中的指南适用。此外，以下针对公有云服务提供商的特定指南及相关信息也适用。

a) 公有云个人身份信息 (PII) 保护实施指南

在云计算参考架构的服务类别中，云服务客户可以负责其控制下的云服务用户的部分或全部访问管理。在适当情况下，公有云PII处理程序应允许云服务客户管理其云服务下云服务用户的访问权限。客户控制。

用户注册和注销程序应涵盖用户访问控制受损的情况，例如密码或其他用户注册数据损坏或泄露（例如，由于意外泄露）。

注：各个司法管辖区可能对未使用身份验证凭据的检查频率有具体要求。在这些司法管辖区运营的组织有责任确保其遵守这些要求。

5.17 身份验证信息

ISO/IEC 27002:2022中5.17条款中的指南适用。

5.18 访问权限

ISO/IEC 27002:2022中5.18条款中的指南适用。

5.19 供应商关系中的信息安全

ISO/IEC 27002:2022中5.18条款中的指南适用。 27002:2022中5.19 适用。

5.20 供应商协议中的信息安全问题

ISO/IEC 27002:2022中5.20条款中的指南适用。

5.21 信息通信技术供应链中的信息安全管理

ISO/IEC 27002:2022中5.21条款中的指南适用。

5.22 供应商服务的监控、审查和变更管理

ISO/IEC 27002:2022中5.22条款中的指南适用。

5.23 云服务使用的信息安全

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中5.23条款中的指南适用。

5.24 信息安全事件管理规划和准备

ISO/IEC 27002:2022中5.24条款中的指南适用。

5.25 信息安全事件的评估和决策

ISO/IEC 27002:2022 5.25条款中的指南适用。

5.26 信息安全事件响应

ISO/IEC 27002:2022中5.26条款中的指南适用。

a) 公有云PII保护实施指南

信息安全事件应触发公有云PII处理者进行审查，作为其信息安全事件管理流程的一部分，以确定是否发生了涉及PII的数据泄露（参见A.10.1）。

并非所有信息安全事件都必须触发此类审查。信息安全事件可能不会导致实际的、或极有可能的、未经授权访问个人身份信息 (PII) 或任何公共云PII处理器的设备或设施（用于存储PII）的情况，并且可能包括但不限于对防火墙或边缘服务器的 ping 和其他诊断探测。

5.27 从信息安全事件中吸取教训

ISO/IEC 27002:2022中5.27条款中的指南适用。

5.28 收集证据

ISO/IEC 27002:2022中5.28条款中的指南适用。

5.29 信息安全期间中断

ISO/IEC 27002:2022中5.29条款中的指南原则适用。

5.30 信息通信技术（ICT）业务连续性准备情况

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中5.30条款中的指南原则适用。

5.31 法律、法规、规章和合同要求

ISO/IEC 27002:2022中5.31条款中的指南原则适用。

5.32 知识产权

ISO/IEC 27002:2022中5.32条款中的指南原则适用。

5.33 记录保护

ISO/IEC 27002:2022中5.33条款中的指南原则适用。

5.34 隐私和个人身份信息（PII）保护

ISO/IEC 27002:2022中5.34条款中的指南原则适用。

5.35信息安全独立审查

ISO/IEC 27002:2022中5.35条款中的指南原则适用。此外，以下针对公共云服务提供商的指南也适用。适用。

a) 公有云PII保护实施指南

在对单个云服务客户进行审计不切实际或可能增加安全风险的情况下,公有云PII处理者应在与潜在云服务客户签订合同之前以及合同有效期内，向其提供独立证据，证明信息安全已得到实施，并且

按照公有云PII处理者的政策和程序运行。由公有云PII处理者选择的相关独立审计通常应是满足云服务客户审查公有云PII处理者处理操作的合理方法，前提是具有足够的透明度。提供。

5.36 遵守信息安全政策、规则和标准

ISO/IEC 27002:2022中5.36条款中的指南适用。

5.37 文件化的操作规程

ISO/IEC 27002:2022中5.37条款中的指南适用。

6 人员控制

6.1 筛选

ISO/IEC 27002:2022中6.1条款中的指南适用。

6.2 雇佣条款和条件

ISO/IEC 27002:2022中6.2条款中的指南适用。

6.3信息安全意识、教育和培训

ISO/IEC 27002:2022 6.3条款中的指南原则适用。此外，以下针对公有云服务提供商的特定指导原则

及相关信息也适用。

a) 公有云个人身份信息（PII）保护实施指导

应采取措施，使相关人员了解违反隐私或安全规则和程序（尤其是有关PII处理的规则和程序）可能对公有云PII处理者（例如，业务损失和品牌或声誉损害）、员工（例如，纪律处分）以及PII主体（例如，身体、物质和精神后果）造成的后果。

b) 公有云PII保护的其他信息

在某些司法管辖区，公有云PII处理者可能受到法律制裁，包括当地PII保护机构直接处以的巨额罚款。

6.4纪律处分程序

ISO/IEC 27002:2022中6.4条款中的指导适用。

6.5 终止或变更雇佣关系后的责任

ISO/IEC 27002:2022中6.5条款中的指导适用。

6.6 保密协议或不披露协议

注：有关保密协议或不披露协议的其他控制措施和指导，请参见A.10.1。

ISO/IEC 27002:2022中6.6条款中的指导适用。

6.7 远程办公

ISO/IEC 27002:2022中6.7条款中的指南适用。

6.8 信息安全事件报告

ISO/IEC 27002:2022中6.8条款中的指南适用。

7 物理控制

7.1 物理安全边界

ISO/IEC 27002:2022中7.1条款中的指南适用。

7.2物理入口

ISO/IEC 27002:2022中7.1条款中的指南适用。

7.3办公室、房间和设施的安全保障

ISO/IEC 27002:2022中7.3条款中的指南适用。

7.4 物理安全监控

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中7.4条款中的指南适用。

7.5 防范物理和环境威胁

ISO/IEC 27002:2022中7.5条款中的指南适用。

7.6 在安全区域工作

ISO/IEC 27002:2022中7.6条款中的指南适用。

7.7 保持桌面和屏幕清洁

ISO/IEC 27002:2022中7.7条款中的指南适用。

7.8 设备选址和保护

ISO/IEC 27002:2022中7.8条款中的指南适用。

7.9 安全场外资产

ISO/IEC27002:2022中7.9条款中的指南适用。

7.10 存储介质

ISO/IEC 27002:2022中7.10条款中的指南适用。

7.11 支持实用程序

ISO/IEC 27002:2022中7.11条款中的指南适用。

7.12 布线安全

ISO/IEC 27002:2022中7.12条款中的指南适用。

7.13 设备维护

ISO/IEC 27002:2022中7.13条款中的指南适用。

7.14 安全处置或再利用设备

ISO/IEC 27002:2022中7.14条款中的指南适用，以下针对公有云服务提供商的特定指南也适用。

a) 公有云PII保护实施指南

为安全处置或再利用，包含可能包含PII的存储介质的设备应视为包含PII。

注：有关安全处置或再利用设备的其他控制措施和指南，请参见A.11.7。

8 技术控制

8.1 用户终端设备

ISO/IEC 27002:2022中8.1条款中的指南原则。

8.2 特权访问权限

ISO/IEC 27002:2022中8.2条款中的指南原则。

8.3信息访问限制

ISO/IEC 27002:2022中8.3条款中的指南原则。

8.4 源代码访问

ISO/IEC 27002:2022中8.4条款中的指南原则。

8.5安全认证

ISO/IEC 27002:2022中8.5条款中的指南适用，以下针对公有云服务提供商的特定指南也适用。

a) 公有云PII保护实施指南

如有需要，公有云PII处理者应为其控制下的云服务用户，为云服务客户请求的任何帐户提供安全的登录程序。

8.6 容量管理

ISO/IEC 27002:2022中8.6条款中的指南适用。

8.7恶意软件防护

ISO/IEC 27002:2022中8.7条款中的指南适用。

8.8 技术漏洞管理

ISO/IEC 27002:2022中8.8条款中的指南适用。

8.9 配置管理

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.9条款中的指南适用。

8.10 信息删除

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.10条款中的指南适用。

8.11 数据脱敏

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.11条款中的指南适用。

8.12 数据泄漏预防

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.12条款中的指南适用。

8.13 信息备份

ISO/IEC 27002:2022中8.13条款中的指南适用。以下针对公有云服务提供商的指南也适用。

a) 公有云PII保护实施指导

基于云计算模型的信息处理系统引入了除异地备份之外的额外或替代机制，以防止数据丢失，确保数据处理操作的连续性，并提供在中断事件发生后恢复数据处理操作的能力。应创建或维护多个数据副本，这些副本可以位于物理位置或逻辑位置的不同地点，或两者兼有（这些副本也可以位于信息处理系统内部），用于备份或恢复，或两者兼而有之。

在这方面，个人身份信息（PII）的特定责任可能由云服务客户承担。如果公有云PII处理者明确向云服务客户提供备份和恢复服务，则公有云PII处理者应向云服务客户提供有关云服务在备份和恢复云服务客户数据方面的能力的信息。

应制定程序，以便在中断事件发生后的特定且有记录的期限内恢复数据处理操作。

应定期审查备份和恢复程序，并制定相应的记录。

注：某些司法管辖区可能对备份和恢复程序的审查频率有具体要求。在这些司法管辖区运营的组织有责任确保其遵守这些要求。

使用分包商存储正在处理的数据的复制或备份副本，受本文件中适用于分包个人身份信息（PII）处理的控制措施A.8.1和A.11.12的约束。如果涉及物理介质传输，则也受本文件中控制措施5.14和A.11.5的约束。

公有云个人身份信息（PII）处理者应制定一项策略，以解决信息备份的要求，以及任何其他要求（例如合同要求），即删除用于备份目的的信息中所包含的PII。

8.14 信息处理设施的冗余

ISO/IEC 27002:2022中8.14条款中的指南适用。

8.15日志记录

ISO/IEC 27002:2022中8.15条款中的指南适用。以下公有云服务提供商特定指南也适用。

a) 公有云PII保护实施指南

应建立一套流程，以指定且有记录的周期审查事件日志，以识别异常情况并提出补救措施。

如有可能，事件日志应记录个人身份信息（PII）是否因事件而发生更改（例如，添加、修改或删除），以及更改者。如果多个服务提供商参与提供来自云计算参考架构不同服务类别的服务，则在实施本指南时可以有不同的角色或共享角色。

公有云PII处理者应定义关于何时、如何以及是否向云服务客户提供日志信息的标准。这些程序应提供给云服务客户。

如果允许云服务客户访问由公有云PII处理者控制的日志记录，则公有云PII处理者应确保云服务客户只能访问与其自身活动相关的记录，而不能访问任何与其他云服务客户活动相关的日志记录。服务客户。

出于安全监控和运行诊断等目的记录的日志信息可能包含个人身份信息（PII）。应采取措施（例如控制访问权限）以确保记录的信息仅用于其预期用途。

应制定程序（最好是自动程序）以确保在指定且有记录的期限内删除记录的信息。

8.16 监控活动

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.16条款中的指南适用。

8.17 时钟同步

ISO/IEC 27002:2022中8.17条款中的指南适用。

8.18 特权实用程序的使用

ISO/IEC 27002:2022中8.17条款中的指南适用。

8.19 在操作系统上安装软件

ISO/IEC 27002:2022中8.19条款中的指南适用。

8.20 网络安全

ISO/IEC 27002:2022中8.20条款中的指南适用。

8.21 网络服务安全

ISO/IEC 27002:2022中8.21条款中的指南适用。

8.22 隔离网络

ISO/IEC 27002:2022中8.22条款中的指南适用。

8.23 Web 过滤

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.23条款中的指南适用。

8.24 加密技术的应用

ISO/IEC 27002:2022中8.24条款中的指南适用，以下针对公有云服务提供商的特定指南也适用。

a) 公有云PII保护实施指南

公有云PII处理者还应向云服务客户提供信息，说明其提供的任何功能可以帮助云服务客户应用和管理

自身的加密保护和流程，例如在密钥库、密钥管理系统（KMS）和硬件中管理密钥或秘密的各种方法。安全模块（HSM）支持的服务、云HSM等。

注意：在某些司法管辖区，可能需要应用加密技术来保护特定类型的个人身份信息，例如与个人身份信息主体相关的健康数据、居民登记号码、护照号码和驾驶执照号码。

8.25 安全开发生命周期

ISO/IEC 27002:2022中8.25条款中的指南适用。

8.26 应用安全要求

ISO/IEC 27002:2022中8.26条款中的指南适用。

8.27 安全系统架构和工程原则

ISO/IEC 27002:2022中8.27条款中的指南适用。

8.28 安全编码

注：ISO/IEC 27002:2022中引入了新的控制措施。

ISO/IEC 27002:2022中8.28条款中的指南适用。

8.29 开发和验收中的安全测试

ISO/IEC 27002:2022中8.29 安全测试适用。

8.30 外包开发

ISO/IEC 27002:2022中8.30条款中的指南适用。

8.31 开发、测试和生产环境的分离

ISO/IEC 27002:2022中8.31条款中的指南适用，以下针对公有云服务提供商的特定指南也适用。

a) 公有云PII保护实施指南

如果无法避免将PII用于测试目的，则应进行风险评估。已采取。应实施技术和组织措施，以最大限度地降低已识别的风险。

8.32 变更管理

ISO/IEC 27002:2022中8.32条款中的指南适用。

8.33 测试信息

ISO/IEC 27002:2022中8.33条款中的指南适用。

8.34 审核测试期间信息系统的保护

ISO/IEC 27002:2022中8.34条款中的指南适用。

附件A

（信息性）

公有云PII处理器扩展控制集，用于PII保护

A.1 总则

本附件规定了新的控制措施和相关的实施指南，这些措施与 ISO/IEC 27002中的控制措施和指南（参见第5至8条）共同构成了一套扩展的控制措施，以满足适用于作为个人身份信息 (PII) 处理者的公共云服务提供商的PII保护要求。

这些附加控制措施根据 ISO/IEC 29100 的11项隐私原则进行分类。在许多情况下，这些控制措施可以归入多个隐私原则。在这种情况下，它们将归入最相关的原则。

A.2 同意和选择

A.2.1 关于PII主体权利的合作义务

a) 控制

公共云PII处理者应通过向云服务客户提供便利行使权利的手段，使云服务客户能够履行其义务。个人身份信息主体（PII）访问、更正和删除与其相关的PII的权利。

b) 公有云PII保护实施指南

PII控制者在这方面的义务可由法律、法规或合同规定。这些义务可以包括云服务客户使用公有云PII处理者的服务进行实施的情况。例如，这可能包括及时更正或删除PII。

如果PII控制者依赖公有云PII处理者提供信息或技术措施以方便PII主体行使权利,则相关信息或技术措施应在合同中明确规定。

A.3 目的的合法性和明确性

A.3.1 公有云PII处理者的目的

a) 控制

根据合同处理的PII不得用于任何与云服务指示无关的目的。

b)公有云个人身份信息 (PII) 保护实施指南

公共云个人身份信息 (PII) 处理者与云服务客户之间的合同中可以包含指令，例如服务要达成的目标和时间框架。

为了实现云服务客户的目标，出于技术原因，公共云PII处理者可以根据云服务客户的一般指令（即使没有云服务客户的明确指示）来确定PII处理方法。例如，为了有效利用网络或处理能力，可能需要根据PII主体的某些特征分配特定的处理资源。

处理资源。在公共云PII处理者确定处理方法涉及PII的收集和使用的情况下，公有云个人身份信息 (PII) 处理者应遵守 ISO/IEC 29100中规定的相关隐私原则以及“隐私设计”原则（参见参考文献[64]和[65]）。

公有云PII处理者应及时向云服务客户提供所有相关信息，以便云服务客户确保公有云PII处理者遵守用途规范和限制原则，并确保公有云PII处理者或其任何分包商不会将任何PII用于未经云服务客户指示的

其他用途。

A.3.2 公有云PII处理者的商业用途

a) 控制

根据合同处理的个人身份信息（PII）未经明确同意，不得由公共云PII处理者用于营销和广告目的。此类同意不应作为接受服务的条件。

注意：此控制是对A.3.1中更一般控制的补充，并不取代或凌驾于其之上。

A.4 收集限制

没有其他控制与此隐私原则相关。

A.5 数据最小化

A.5.1 安全擦除临时文件

a) 控制

临时文件和文档应在规定的、有记录的期限内擦除或销毁。b) 公共云PII保护实施指南

关于PII擦除的实施指南见 A.10.3。

信息系统在正常运行过程中会创建临时文件。此类文件特定于某个系统或应用程序，但可能包括文件系统回滚日志以及与数据库更新和其他应用程序软件运行相关的临时文件。相关信息处理任务完成后，临时文件不再需要，除非特殊情况要求保留，否则应在完成后删除。这些文件的使用时长并非总是确定的，但“垃圾回收”程序应识别相关文件并确定其上次使用至今的时间。

处理个人身份信息（PII）的信息系统应实施定期检查，确保删除超过指定期限的未使用临时文件。

A.6 使用、保留和披露限制

A.6.1PII披露通知

a) 控制

预计公有云PII处理者与云服务客户之间的合同将要求公有云PII处理者按照合同约定的任何程序和时间段，通知云服务客户有关执法机构提出的任何具有法律约束力的PII披露请求，[tg1]除非此类披露另有规定。

合同约定的时间段内，除非法律另有规定，否则应执法机构提出的任何具有法律约束力的PII披露请求，否则应通知云服务客户。

b)公有云PII保护实施指南

公有云PII处理者应提供合同保证，确保：

—拒绝任何不具有法律约束力的PII披露请求；

—在法律允许的情况下，在进行任何PII披露之前，咨询相应的云服务客户；以及

— 接受任何经相应云服务客户授权的、合同约定的PII披露请求。

示例：一项可能的禁止披露情形是，根据刑法，为了维护执法调查的机密性而禁止披露。

A.6.2 个人身份信息（PII）披露的记录

a) 控制

应记录向第三方披露PII的情况，包括已披露的PII内容、披露原因、披露对象以及披露时间。

b) 公有云PII保护实施指南

在正常运营过程中可能会披露PII。这些披露应予以记录。任何其他向第三方的披露，例如因合法调查或外部审计而产生的披露，也应予以记录。记录应包括披露来源、披露原因以及披露授权来源。

A.7准确性和质量

本隐私原则不涉及其他控制措施。

A.8 公开、透明和通知

A.8.1 分包个人身份信息处理的披露

a) 控制

如果公有云个人身份信息处理者打算使用分包商处理个人身份信息,则应事先向相关云服务客户披露。

b) 公有云个人身份信息 (PII) 保护实施指南

关于使用分包商处理PII的规定应在公有云PII处理者与云服务客户之间的合同中明确规定。

合同应明确规定，分包商只能在获得云服务客户同意的情况下才能委托处理，而云服务客户通常可以在服务开始时给予同意。公有云PII处理者应及时告知云服务客户任何此类变更，以便云服务客户能够对变更提出异议或终止合同。

披露的信息应包括使用分包的事实以及相关分包商的名称，但不包括任何特定于业务的细节。披露的信息还应包括分包商可以处理数据的国家/地区（参见 A.12.1）以及分包商履行或超越相关义务的方式。公有云PII处理器（参见 A.11.12）。

如果评估认为公开分包商信息会导致安全风险增加,则应根据保密协议和/或应云服务客户的要求进行披露。应告知云服务客户该信息可用。

A.9 I个人参与和访问

本隐私原则不涉及其他控制措施。

A.10 问责制

A.10.1 涉及个人身份信息 (PII) 的数据泄露通知

a) 控制

如果发生任何未经授权访问PII或未经授权访问处理设备或设施，导致PII丢失、泄露或更改，公有云PII处理者应立即通知相关的云服务客户。

b) 公有云PII保护实施指南

关于涉及PII的数据泄露通知的条款应构成公有云PII处理者与云服务客户之间合同的一部分。合同应明确规定公有云PII处理者将如何向云服务客户提供履行其通知相关机构义务所需的信息。此通知义务不适用于由云服务引起的数据泄露。客户或PII主体，或其负责的系统组件。合同还应明确规定涉及PII的数据泄露通知的最长延迟时间。

如果发生涉及PII的数据泄露，应保存一份记录，其中包含事件描述、时间段、事件后果、报告人姓名、事件报告对象、为解决事件而采取的步骤（包括负责人和已恢复的数据）以及事件导致PII丢失、泄露或更改的事实。

如果发生涉及PII的数据泄露，记录还应包含对泄露数据的描述（如果已知）。如果已发出通知，记录

应包含通知云服务客户或监管机构或两者所采取的步骤。

在某些司法管辖区，相关法律法规可能要求公有云个人身份信息（PII）处理者直接向相应的监管机构（例如PII保护机构）报告涉及PII的数据泄露事件。

注意：可能存在其他需要通知的泄露事件，例如未经同意或其他授权的收集、用于未经授权的目的等，但此处并未涵盖。

A.10.2 管理安全策略和指南的保留期限

a）控制

更新后的安全策略和操作规程的现有副本应保留一段指定的、有记录的更换期限。

b）公有云PII保护实施指南

可能需要审查当前和历史策略及程序，例如在客户纠纷解决和PII保护机构调查的情况下。如果没有具体的合同要求或其他要求，建议至少保留五年。适用。

A.10.3 个人身份信息（PII）的返还、转移和处置

a）控制

公有云PII处理者应制定关于这些活动的政策，并应将该政策提供给云服务客户。

b）公有云PII保护实施指南

在某些情况下，PII需要以某种方式处置。这可能包括将PII返还给云服务客户、将其转移给另一个公有云PII处理者或PII控制者（例如，由于合并）、安全地删除或以其他方式销毁、匿名化或存档。

公有云个人身份信息（PII）处理者应提供必要信息，以确保根据合同处理的PII在不再用于云服务客户的特定用途时，能够立即从其存储的任何位置（包括出于备份和业务连续性目的）被删除（由公有云PII处理者及其任何分包商删除）。处置机制（例如解除链接、覆盖、消磁、销毁或其他形式的擦除）和/或适用的商业标准应在合同中予以明确规定。

公有云PII处理者应制定并实施PII处置政策，并向云服务客户提供该政策。

该政策应涵盖合同终止后PII销毁前的保留期限，以防止云服务客户因合同意外失效而丢失PII。

注：此控制和指南也适用于“使用和保留”中的保留要素。以及披露限制原则（参见 A.6）

A.11 信息安全

A.11.1 保密或不披露协议

a）控制

受公有云PII处理者控制且能够访问PII的个人应承担保密义务。

b）公有云PII保护实施指南

公有云PII处理者、其员工和代理人之间签订的任何形式的保密协议均应确保员工和代理人不会出于与云服务客户指示无关的目的披露PII（参见 A.3.1）。保密协议的义务应在任何相关合同终止后继续有效。

A.11.2 限制创建纸质材料

a）控制

应限制创建包含个人身份信息（PII）的纸质材料。

b）公有云PII保护实施指南 纸质材料包括打印创建的材料。

A.11.3 数据恢复的控制和日志记录

a) 控制

应制定数据恢复流程并记录恢复过程。

b) 公有云PII保护实施指南

数据恢复日志应包含：负责人、恢复数据的描述以及手动恢复的数据。

A.11.4 保护离开机构场所的存储介质上的数据

a) 控制

离开机构场所的存储介质上的个人身份信息（PII）应经过授权程序，除授权人员外，任何人不得访问（例如，通过加密相关数据）。

A.11.5 使用未加密的便携式存储介质和设备

a) 控制

除非万不得已，否则不应使用不允许加密的便携式物理介质和便携式设备，并且任何此类便携式介质和设备的使用都应记录在案。

A.11.6 通过公共数据传输网络传输的个人身份信息（PII）的加密

a) 控制

通过公共数据传输网络传输的个人身份信息（PII）应事先加密。传输。

b)公有云个人身份信息（PII）保护实施指南

在某些情况下，例如电子邮件交换，公共数据传输网络系统的固有特性可能要求为了有效传输而暴露某些头部或流量数据。

当多个服务提供商参与提供来自不同服务类别的服务时

云计算参考架构，在实施本指南的过程中，角色可以多样化或共享。A.11.7 安全处置纸质材料

a) 控制

销毁纸质材料时，应使用诸如交叉切割、粉碎、焚烧、制浆等机制进行安全销毁。

A.11.8 用户 ID 的唯一性使用

a) 控制

如果多人可以访问存储的个人身份信息（PII），则每个人都应拥有一个不同的用户 ID，用于身份识别、身份验证和授权。

A.11.9 用户ID管理

a) 控制

已停用或已过期的用户ID不应授予其他个人。

b) 公有云PII保护实施指南

在整个背景下根据云计算参考架构，云服务客户可以负责其控制下的云服务用户的部分或全部用户 ID 管理工作。

A.11.10 授权用户记录

a) 控制

应维护已获得信息系统授权访问权限的用户或用户配置文件的最新记录。

b) 公有云PII保护实施指南

应为所有经公有云PII处理者授权访问的用户维护用户配置文件。用户配置文件包含有关该用户的数据集，包括用户 ID 是实施技术控制所必需的，该技术控制用于提供对信息系统的授权访问。

A.11.11合同措施

a) 控制

云服务客户与公共云PII处理者之间的合同应明确规定最低要求。

技术和组织措施，以确保合同约定的安全安排到位，并且数据不会被用于任何未经控制者指示的目的。此类措施

公共云个人身份信息处理者不得单方面减少此类措施。

b) 公共云个人身份信息保护实施指南

与公共云个人身份信息处理者相关的信息安全和个人身份信息保护义务可能直接源于适用法律。如果并非如此，则与公共云个人身份信息处理者相关的个人身份信息保护义务应在合同中予以涵盖。

本文件中的控制措施，连同 ISO/IEC 27002中的控制措施，旨在作为一项参考措施目录，以协助签订有关个人身份信息的信息处理合同。公共云个人身份信息处理者应在签订合同前，告知潜在的云服务客户其为保护个人身份信息而实施的信息安全和隐私控制措施。

公共云PII处理者在签订合同过程中应公开透明地说明其能力。然而，最终确保公有云PII处理者所采取的措施符合其义务是云服务客户的责任。

A.11.12分包PII处理

a) 控制

公有云PII处理者与任何处理PII的分包商之间的合同应明确规定满足公有云PII处理者信息安全和PII保护义务的最低技术和组织措施。分包商不得单方面降低此类措施。

b) 公有云PII保护实施指南

使用分包商存储备份副本受此控制（参见A.8.1）。

A.11.13访问已使用的数据存储空间

a) 控制

公有云PII处理者应确保，每当向云服务客户分配数据存储空间时，该存储空间上先前存在的任何数据对该云服务客户均不可见。

b) 公有云PII保护实施指南

当云服务用户删除信息系统中存储的数据时，性能问题可能导致显式擦除这些数据不切实际。这会造成其他用户可以读取数据的风险。应通过特定的技术措施来避免此类风险。

没有特别适用于所有情况的特定指南来实施此控制。但是，例如，某些云基础设施、平台或应用程序在云服务用户删除数据时会返回零或随机数。服务用户尝试读取尚未被该用户自身数据覆盖的存储空间。

A.12 隐私合规性

A.12.1 个人身份信息 (PII) 的地理位置

a） 控制

公有云PII处理者应明确并记录PII可能存储的国家/地区。

b） 公有云PII保护实施指南

应向云服务客户提供可能存储个人身份信息（PII）的国家/地区信息。应包括因使用外包PII处理而产生的国家/地区信息。如果国际数据传输适用特定合同协议（例如标准合同条款、具有约束力的公司规则或跨境隐私规则），则还应明确这些协议以及适用这些协议的国家/地区或情况。公共云PII处理者应及时告知云服务客户任何此类变更，以便云服务客户能够反对此类变更或终止合同。

A.12.2PII的预期目的

a） 控制

使用数据传输网络传输的PII应受到适当的控制，以确保数据到达其预期目的。