国际标准 **ISO/IEC 27018**

第二版
2019-01

信息技术 安全技术 个人身份信息（PII）处理者在公有云中保护 PII 的实践指南。

参考号
ISO/IEC 27018:2019E

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门系统。作为 iso 或 iec 成员的国家机构通过各自组织所建立的技术委员会参与国际标准的制定。 技术活动的特定领域 ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。其他政府和非政府国际组织同 ISo 和 IEC 联络，也参加信息技术领域的工作，ISo 和 IEC 建立了联合技术委员会，ISO / IEC JTC 1。

用于开发本文档的程序和用于进一步维护的程序如下,在 ISO / IEC 指令的第 1 部分中进行了详细描述。特别要注意的是，不同类型的文档需要不同的批准标准。本文件是根据 ISo/EC 指令第 2 部分的编辑规则起草的(参见 wwwiso, org/directives)。

请注意，本文档的某些内容可能是专利权的主题。 ISo 和 IEC 对识别任何或所有此类专利权概不负责。 在文档开发过程中确定的任何专利权的详细信息将在“引言和/或收到的专利声明的独立性”上（请参见 www.iso，orglpatents）。

本文档中使用的任何商品名称都是为了方便用户而提供的信息，并不构成对本产品的认可。

对于标准的自愿性的解释，ISO 特定术语的含义和与合格评定有关的表述，以及有关 ISO 遵守、技术性贸易壁垒（TBT）中的世界贸易组织（WTO）原则，请参见 www.iso.org/iso/foreword.html。

本文档由 ISO / IEC TC 1 技术委员会准备的，信息技术、SC 27 小组委员会、IT 安全技术。

本第二版取消并替代了第一版（ISO / EC 27018：2014），对第一版仅作小修改。 与上一版本相比，主要的变化是对附件 A 中编辑错误的更正。

关于本文档的任何反馈或问题应直接发送给用户的国家标准机构。 这些机构的完整列表可以在 www.iso.org/members.html 上找到。

介绍

0.1 背景和语境

根据与客户签订的合同处理个人可识别信息（PI1）的云服务提供商需要以允许双方都满足适用法律和法规（涉及保护 PII 的要求）的方式来运营其服务。云服务提供商及其客户的要求和要求的方式因法律管辖权以及云服务提供商与客户之间的合同条款而有所不同。 有时被称为数据保护法规；有时会将 PII 称为个人数据或个人信息。PII 处理者所承担的义务因司法管辖区而异，这使得提供云计算服务的企业在跨国运营中面临挑战。

当公有云服务提供商根据云服务客户的指示处理 PII 时，它就是一个“ PII 处理者”。与公有云 PII 处理者有合同关系的云服务客户，可以从自然人(处理他或她自己在云中的 PII 的 PII 主体)到组织(处理与许多 PII 主体相关的 PII 的 PII 控制者)。云服务客户可以授权一个或多个与其关联的云服务用户使用根据其与公有云 PII 处理者的合同提供的服务。请注意，云服务客户有权处理和使用数据。与公有云 PII 处理者相比，同时也是 PII 控制者的云服务客户在管理 PII 保护方面需要承担更广泛的义务。维持 PII 控制者和 PII 处理者之间的区别依赖于公有云 PII 处理者，PII 处理者没有其他数据处理目标，不同于为实现云服务客户要求的遵守 PII 处理要求和实现云服务客户目标所必需的操作目标。

注：公有云 PII 处理者在处理云服务客户账户数据时，可以充当此目的的 PII 控制者。本文档不包括此类活动。

当与 ISo/IEC 27002 中的信息安全目标和控制结合使用时，本文档的目的是创建一套通用的安全类别和控制，可以由公有云计算服务提供商作为 PII 处理者来实现。它的目标如下:

—帮助公有云服务提供商在作为 PII 处理者时遵守适用的义务，无论这些义务是由 PII 处理者直接承担还是通过合同承担;

—使公有云 PII 处理者在相关事务上透明，以便云服务客户可以选择管理良好的基于云的 PII 处理服务；

—协助云服务客户和公有共云 PII 处理者签订合同协议

—为云服务客户提供一种机制，以在多方虚拟化服务器（云）环境中托管的单个云服务客户对托管数据进行技术审计，在技术上不切实际的情况下行使审计、合规权利和责任的机制，并可增加风险以使这些物理和逻辑网络安全控制到位。

本文件为公有云服务提供商，特别是在跨国市场运营的云服务提供商，提供了一个通用的合规框架。

0.2 公有云计算服务的 PII 保护控制

本文档的设计是用来给组织提供参考，以作为在基于 ISO / IEC 27001 的云计算信息安全管理系统的实施过程中选择 PII 保护措施的参考，或作为指导性文档，以为“公有云 PII 处理者”身份的组织实施普遍接受的 PII 保护措施。特别地，本文档基于 ISO / IEC 27002，并考虑到由此产生的特定风险环境。 PII 保护要求，适用于作为 PII 处理者的公有云计算服务提供商。

通常，一个实施 ISO/EC 27001 的组织是正在保护它自己的信息资产。但是，在对充当 PII 处理者的公有云服务提供商的 PII 保护要求的范围内，组织正在保护其客户委托给它的信息资产。由公有云 PII 处理者实施 ISo / iEC 27002 的控制措施是： 既适合于此目的，又是必要的。本文档对 Iso/IEC 27002 控制进行了扩充，以适应风险的分布式性质以及云服务客户与公有云 PII 处理者之间存在的合同关系。 本文档以两种方式对 ISo/IEC 27002 进行了扩充：

—针对某些现有的 ISO/IEC 27002 控制，提供了适用于公有云 PII 保护的实施指南，并且，

—附件 A 提供了一组旨在解决现有 ISO / IEC 27002 控制集未解决的公有云 PII 保护要求的其他控制措施和相关指南。

本文档中的大多数控制和指南也适用于 PII 控制者。然而，在大多数情况下，PII 控制者要承担此处未指定的其他义务。

0.3 PII 保护要求

对于一个组织来说，识别其保护 PII 的要求是至关重要的。下面给出了三个主要的要求来源：

a) 法律、法规、监管和合同要求：一个来源是组织、其贸易伙伴、承包商和服务提供者必须满足的法律、法规、监管和合同要求和义务，以及他们的社会文化责任和经营环境。应当指出，PII 处理者所制定的法律，法规和合同承诺可以强制选择特定的控制措施，也可能需要特定的标准来实施这些控制措施。这些要求可能因司法管辖区的不同而有所不同。

b) 风险：另一个来源来自评估与 PII 相关的组织的风险，同时考虑了组织的整体业务战略和目标。通过风险评估，可以识别威胁，评估发生的脆弱性和发生的可能性，并估计潜在的影响。ISO / IEC 27005 提供了信息安全风险管理指南，包括有关风险评估，风险接受，风险沟通，风险监视和风险评审的建议。 ISO / IEC 29134 提供了有关隐私影响评估的指南。

c)公司策略：虽然公司策略涵盖的许多方面都源于法律和社会文化义务，但组织也可以自愿选择超越源自 a)的要求的标准。

0.4 在云计算环境中选择和实施控制

可从本文件中选择控制(其中包括引用 ISO/IEC 27002 中的控制、为范围定义的部门或应用创建一个组合的参考控制集)。如果需要，还可以从其他控件集中选择控制，或者可以根据需要设计新的控制来满足特定的需要。

注：由公有云 PII 处理者提供的 PII 数据处理服务，可以看作一个云计算的应用程序，而不是其自身的一个部门。然而，在本文档中使用术语“特定行业”，因为这是 ISo / IEC 27000 系列其他标准中使用的常规术语。

控制措施的选择取决于组织的决策，这些决策基于风险接受标准、风险处理方案，以及应用于组织的一般风险管理方法，并通过合同协议，应用于其客户和供应商。如果没有选择本文件中的控制措施，则还应遵守相关的国家和国际法律法规，需要对其进行记录，以说明遗漏的理由。

此外，控制的选择和实现取决于公有云提供商在整个云计算参考体系结构背景下的实际角色(参见 ISO/IEC 17789)。许多不同的组织可以参与在云计算环境中提供基础设施和应用程序服务。在某些情况下，所选控制对于云计算参考体系结构的特定服务类别可能是唯一的。在其他情况下，实现安全控制时，可以共享角色。合同协议需要明确规定所有参与提供或使用云服务的组织的 PII 保护责任，包括公有云 PII 处理者、其分包商和云服务客户。

本文档中的控 制可以被视为指导原则，并且适用于大多数组织。下面将对它们进行详细说明，并提供实施指南。如果在公共有 PII 处理者的信息系统、服务和操作的设计中考虑了 PII 的保护要求，那么实施就可以变得简单。这种考虑是通常被称为“隐私设计”的概念的一个元素(见书目条目[9])。

0.5 开发其他指南

该文档可被视为制定 PII 保护指南的起点。可能并非该实施规程中的所有控制和指南都适用。此外，可能需要本文档未包含的其他控制和指南。当开发的文档中包含其他指南或控件时，在适用时，在本文档中包括对条款的交叉引用可能会很有用，以方便审核员和业务合作伙伴进行合规性检查。

0.6 生命周期注意事项

PII 具有自然的生命周期，从创建和起源，经过存储、处理、使用和传播，直到最终的销毁或衰变。PII 的风险在其生命周期中可能会有所不同，在某种程度上，整个阶段对 PII 的保护都仍然很重要。

由于现有信息系统和新信息系统是通过生命周期进行管理的，因此必须考虑 PII 保护要求。

信息技术-安全技术-个人身份信息（PII）处理者在公有云中保护PII的实践指南。

1 范围

本文档建立了普遍接受的控制目标、控制和指南，用于根据ISO/IEC 29100中针对公有云计算环境的隐私原则来实施保护个人身份信息（PI1）的措施。

特别地，本文档以ISO/IEC 27002为基础，考虑到公有云服务提供商的信息安全风险环境中对保护PII的监管要求，规定了指南。

本文档适用于所有类型和规模的组织，包括公共和私营公司，政府机构和不以营利为目的的组织，这些组织通过与其他组织签订合同通过云计算提供信息处理服务（作为PII处理者）。

本文件中的指南也适用于作为PII控制者的组织。但是，PII控制者可能受到不适用于PII处理者的额外的PII保护立法、法规和义务的约束。本文档无意涵盖此类额外义务。

2 引用标准

下列文件在本文档中被引用时，其部分或全部内容构成本文件的要求。凡是注日期的引用文件，仅适用所引用的版本。如引用的文件未注明日期，应采用引用文件的最新版本(包括任何修订)。

ISO / IEC 17788，信息技术-云计算-概述和词汇

ISO / IEC 27000，信息技术-安全技术-信息安全管理体系-概述和词汇

ISO / IEC 27002：2013，信息技术-安全技术-信息安全控制实践指南

3 术语和定义

本文档的术语和定义适用于ISO/IEC 17788、ISO/IEC 27000及下面的应用。

ISO和IEC在以下地址维护用于标准化的术语数据库:

—ISO Online browsing platform:available at https://www.iso.org/obp

—IEC Electropedia:available at http://www.electropedia.org/

—ISO在线浏览平台:https://www.iso.org/obp

—IEC电子百科：可在http://www.electropedia.org/获得

3.1 数据泄露 （data breach）

危及安全，导致意外或非法破坏、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的受保护数据.

[来源:ISO/IEC 27040: 2015, 3.7]

3.2 个人身份信息 PII （personally identifiable information PII）

任何信息(a)可用于建立信息与该信息相关的自然人之间的联系，或(b)是或可以直接或间接与自然人联系。

注 1：定义中的“自然人”是 PII 主体（3.4）。 为了确定 PII 主体是否可识别，应考虑持有数据的隐私利益相关者或任何其他方可以合理使用的所有手段，以在 PII 组和自然人之间建立联系。

注 2：包含此定义是为了定义本文档中使用的术语 PII。 除非云服务客户将其透明化，否则公有云 PII 处理者（3.5）通常无法明确知道其处理的信息是否属于特定的类别。

[来源：ISO / EC 29100：2011 /修正 1：2018，2.9，已修改-已在条目中添加注 2。]

3.3 PII 控制者 （PII controller）

隐私权利益相关者（或隐私权利益相关者们），其决定处理个人身份信息（PII）（3.2）的目的和方法，因个人目的使用数据的自然人不在此列。

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，但处理的责任仍由 PII 控制者承担。

[来源: ISO/EC 29100: 2011, 2.10]

3.4 PII 主体 （PII principal）

与个人身份信息（PI1）相关联的自然人。

注释 1：根据司法管辖权以及特定的 PII 保护和隐私法规，也可以使用同义词“数据主体”代替术语“ PII 主体”。（本标准翻译者注解：在 GDPR 中，称为" data subject" （“数据主体”））

[来源:ISO/IEC29100:2011,2.11]

3.5 PII 处理者 （PII processor）

代表 PII 控制者（3.3），并按照其指示对个人身份信息（PII）进行处理的隐私权利益相关者。

[来源: ISO/IEC 29100: 2011, 2.12]

3.6 PII 的处理 （processing of PII）

对个人身份信息（PI1）进行的一项或多项操作（3,2）

注 1：PII 的处理操作示例包括但不限于：PII 的收集、存储、修改、检索、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁。

[来源：ISO/IEC29100:2011.2.23]

3.7 公有云服务提供商 （public cloud service provider）

根据公有云模型提供云服务的一方

4 概述

4. 1 本文件的结构

本文件的结构与 ISO/IEC 27002 类似。如果 ISO/IEC 27002 规定的目标和控制适用而不需要任何额外信息，则只提供 ISO/IEC 27002 的参考。适用于云计算服务提供商 PII 保护的附加控制和相关实施指南见附件 A。

适用于云计算服务提供商的 PII 保护的附加指南的控制，则在“公有云 PII 保护实施指南”标题下给出。在某些情况下，在该标题下提供进一步增强额外的指南的相关信息“有关公有云 PII 保护的其他信息”。

如表 1 所示，此类特定于行业的指南和信息包含在 ISO / IEC 27002 中定义的类别中，条款编号与 ISO/IEC 27002 中相应条款编号一致，如表 1 所示。

在实施基于 ISO/IEC 27001 的信息安全管理体系过程中，应考虑采用本文件的使用、ISO/IEC 27001 和附录 A 中规定的附加控制。

表 1-用于实施 ISO / IEC 27002 中的控制的特定行业指南和其他信息的地方

条款编号	标题	备注
5	信息安全策略	提供了特定行业的实施指南和其他信息。
6	信息安全组织	提供了针对特定行业的实施指南。
7	人力资源安全	提供了特定行业的实施指南和其他信息。
8	资产管理	没有提供其他针对特定行业的实施指南或其他信息
9	访问控制	提供了针对特定行业的实施指南，并在附录 A 中交叉引用了控制措施。
10	密码	提供了针对特定行业的实施指南。
11	物理和环境安全	提供了针对特定行业的实施指南，并在附录 A 中交叉引用了控制措施。
12	运行安全	提供了针对特定行业的实施指南。
13	通信安全	提供了针对特定行业的实施指南，并在附录 A 中交叉引用了控制措施。
14	系统获取、开发和维护	没有提供其他针对特定行业的实施指南或其他信息
15	供应商关系	没有提供其他针对特定行业的实施指南或其他信息
16	信息安全事件管理	提供了针对特定行业的实施指南。
17	业务连续性管理的信息安全方面	没有提供其他针对特定行业的实施指南或其他信息
18	符合性	提供了针对特定行业的实施指南，并在附录 A 中交叉引用了控制措施。

4.2 控制类别

按照 ISO/IEC 27002，每个主要控制类别均包含：

a)控制目标，说明要实现什么;和

b)可用于实现控制目标的一个或多个控制。

控制描述的结构如下:

控制

定义特定的控制声明以满足控制目标。

公有云 PII 保护实施指南

提供更详细的信息，以支持控制的实施和达到控制目标。该指南可能并非在所有情况下都完全合适或充分的，并且可能无法满足组织的特定控制要求。因此，替代或额外的控制措施或其他形式的风险处理（避免，转移或接受风险）可能是适当的。

有关公有云 PII 保护的其他信息

提供需要考虑的进一步信息，如法律考虑事项和对其他标准的引用。

5 信息安全策略

5.1 信息安全的管理指导

ISO/IEC 27002: 2013, 5.1 规定的目标适用。

5.1.1 信息安全策略

ISO/IEC 27002 中的 5.1.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

信息安全策略还应通过以下声明予以补充：说明支持和承诺遵守适用的 PII 保护立法，以及公有云 PII 处理者与其客户(云服务客户)之间达成的合同条款。

合同协议应明确分配公有云 PII 处理者、其分包商和云服务客户之间的责任，并考虑到相关云服务的类型 (例如: 云计算参考结构的 IaaS、PaaS 或 SaaS 类别的服务)。例如，根据公有云 PII 处理者是提供 SaaS 服务还是提供 PaaS 或 laaS 服务，云服务客户可以在其上构建或分层其自己的应用程序，因此对应用层控制的责任分配可能会有所不同。

公有云 PII 保护的其他信息

在某些司法管辖区，公有云 PII 处理者直接受 Pll 保护立法的约束。在其他国家，PII 保护立法只能适用于 PII 控制者。

云服务客户和公有云 PII 处理者之间的合同提供了一种确保公有云 PII 处理者有义务支持和管理合规性的机制。合同可以要求进行云服务客户可以接受的独立审核的合规性，例如。通过实施本文件和 ISO/IEC 27002 中的相关控制。

5.1.2 审查信息安全策略的评审

ISO/IEC 27002 中的 5.1.2 控制、相关实施指南适用。

6 信息安全组织

6.1 内部组织

ISO / IEC 27002:2013 中的 6.1 条规定的目标适用。

6.1.1 信息安全角色和职责

ISO/IEC 27002 中的 6. 1.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

公有云 PII 处理者应指定一个联系点，供云服务客户关注根据合同进行的“PII 的处理”时使用。

6.1.2 职责分离

ISO/IEC 27002 中的 6.1.2 控制、相关实施指南以及其他信息适用。

6.1.3 与职能机构的联系

ISO/IEC 27002 中的 6.1.3 控制、相关实施指南以及其他信息适用。

6.1.4 与特定相关方的联系

ISO/IEC 27002 中的 6.1.4 控制、相关实施指南以及其他信息适用。

6.1.5 项目管理中的信息安全

ISO/IEC 27002 中的 6.1.5 控制、相关实施指南适用。

6.2 移动设备和远程工作

ISO / IEC 27002：2013 中 6.2 规定的目标及其内容适用。

7 人力资源安全

7.1 任用前

ISO / IEC 27002：2013 中 7.1 规定的目标及其内容适用。

7. 2 任用中

ISO / IEC 27002:2013 中 7.2 规定的目标适用。

7. 2.1 管理职责

ISO/IEC 27002 中的 7.2.1 控制、相关实施指南以及其他信息适用。

7.2.2 信息安全意识、教育和培训

ISO/IEC 27002 中的 7.2.2 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

应采取措施使相关人员了解：当违反隐私或安全规则和程序、尤其是那些针对 PII 处理的规则和程序时，对公有云 PII 处理者可能造成的后果（例如法律后果，业务和品牌的损失或声誉受损）、对员工造成的后果（例如纪律后果）以及对 PII 主体的影响 （例如，身体，物质和情感后果）。

公有云 PII 保护的其他信息

在一些司法管辖区，公有云 PII 处理者可能会受到法律制裁，包括直接来自当地 PII 保护部门的巨额罚款。在其他司法管辖区，在建立公有云 PII 处理者与云服务客户之间的合同时使用本文档等国际标准应有助于为违反安全规则和程序的合同制裁奠定基础。

7. 2.3 违纪处理过程

ISO/IEC 27002 中的 7.2.3 控制、相关实施指南以及其他信息适用。

7.3 任用职责的终止或变更

ISO/IEC 27002:2013 中 7.3 规定的目标及其内容适用。

8 资产管理

ISO/IEC 27002:2013 中 8 条款规定的目标及其内容适用。

9 访问控制

9.1 访问控制的业务要求

ISO/IEC 27002:2013 中 9.1 规定的目标及其内容适用。

9.2 用户访问管理

ISO/IEC 27002:2013 中 9.2 规定的目标适用，以下特定行业的指南也适用于本条款中所有控制的实施

公有云 PII 保护实施指南

在云计算参考体系结构的服务类别的语境中，云服务客户可以负责在其控制下的云服务用户的访问管理的某些或所有方面。 在适当的情况下，公有云 PII 处理者应使云服务客户能够在云服务客户控制下管理云服务用户的访问，例如通过提供管理权限来管理或终止访问。

9.2.1 用户注册和注销

ISO/IEC 27002 中的 9.2.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

用户注册和注销程序应处理用户访问控制受到损害的情况，例如密码或其他用户注册数据的损坏或泄露（例如，由于无意披露）。

注：别的司法管辖区可以对未使用身份验证证书的检查频率提出特定的要求。在这些辖区内运营的组织有责任确保他们遵守这些要求。

9.2.2 用户访问供给

ISO/IEC 27002 中的 9.2.2 控制、相关实施指南以及其他信息适用。

9.2.3 特权访问权限管理

ISO/IEC 27002 中的 **9.2.3** 控制、相关实施指南以及其他信息适用。

9.2.4 用户的秘密鉴别信息管理

ISO/IEC 27002 中的 9.2, 4 控制、相关实施指南以及其他信息适用。

9.2.5 用户访问权限的评审

ISO/IEC 27002 中的 9.2.5 控制、相关实施指南以及其他信息适用。

9.2.6 访问权限的移出或调整

ISO/IEC 27002 中的 9.2.6 控制、相关实施指南以及其他信息适用。

9.3 用户责任

ISO/IEC 27002:2013 中 9.3 规定的目标适用。

9.3.1 秘密鉴别信息的使用

ISO/IEC 27002 中的 9.3.1 控制、相关实施指南适用。

9.4 系统和应用访问控制

ISO/IEC 27002:2013 中 9.4 规定的目标适用。

9.4.1 信息访问限制

ISO/IEC 27002 中的 9.4.1 控制、相关实施指南适用。

注：与信息访问限制有关的其他控制和指南可以在 A.10.13 中找到。

9.4.2 安全的登录过程

ISO/IEC 27002 中的 9.4.2 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

在需要时，公有云 PII 处理者应为云服务客户在其控制下的云服务用户所请求的任何帐户提供安全的登录过程。

9.4.3 口令管理系统

ISO/IEC 27002 中的 9.4.3 控制、相关实施指南以及其他信息适用。

9.4.4 特权实用程序的使用

ISO/IEC 27002 中的 **9.4.4** 控制、相关实施指南以及其他信息适用。

9.4.5 程序源代码的访问控制

ISO/IEC 27002 中的 9.4.5 控制、相关实施指南以及其他信息适用。

10 密码

10.1 密码控制

ISO/IEC 27002:2013 中 10.1 规定的目标适用。

10.1.1 密码控制的使用政策

ISO/IEC 27002 中的 10. 1.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也

公有云 PII 保护实施指南

公有云 PII 处理者应该向云服务客户提供有关使用加密技术保护 PII 处理的情况的信息。公有云 PII 处理者还应该向云服务客户提供有关其提供的任何功能的信息，这些功能可以帮助云服务客户应用其自己的加密保护。

注：在一些司法管辖区，可能需要应用加密技术来保护特定种类的 PII，例如有关 PII 主体的健康数据，居民登记号，护照号和驾照号。

10.1.2 密钥管理

ISO/IEC 27002 中的 10. 1. 2 控制、相关实施指南以及其他信息适用。

11 物理和环境安全

11.1 安全区域

ISO/IEC 27002:2013 中 11.1 规定的目标及其内容适用。

11.2 设备

ISO/IEC 27002:2013 中 11.2 规定的目标适用。

11.2.1 设备安置和保护

ISO/IEC 27002 中的 11.2.1 控制、相关实施指南适用。

11.2.2 支持行设施

ISO/IEC 27002 中的 11.2.2 控制、相关实施指南以及其他信息适用。

11.2.3 布线安全

ISO/IEC 27002 中的 11.2.3 控制、相关实施指南适用。

11.2.4 设备维护

ISO/IEC 27002 中的 11.2.4 控制、相关实施指南适用。

11.2.5 资产的移动

ISO/IEC 27002 中的 11.2.5 控制、相关实施指南以及其他信息适用。

11.2.6 组织场外设备和资产的安全

ISO/IEC 27002 中的 11.2.6 控制、相关实施指南以及其他信息适用。

11.2.7 设备的安全处置或再利用

ISO/IEC 27002 中的 11.2.7 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

为了安全处置或重复使用， 包含可能包含 PII 的存储介质的设备应该像它一样处理。

注：与安全处置或重复使用设备有关的其他控制和指南可在 A.10.13 中找到。

11.2.8 无人值守的用户设备

ISO/IEC 27002 中的 11.2.8 控制、相关实施指南适用。

11.2.9 清空桌面和屏幕策略

ISO/IEC 27002 中的 11.2.9 控制、相关实施指南以及其他信息适用。

12 运行安全

12.1 运行规程和责任

ISO/IEC 27002:2013 中 12.1 规定的目标适用。

12.1.1 文件化的操作规程

ISO/IEC 27002 中的 12.1.1 控制、相关实施指南适用。

12.1.2 变更管理

ISO/IEC 27002 中的 12.1.2 控制、相关实施指南以及其他信息适用。

12.1.3 容量管理

ISO/IEC 27002 中的 12.1.3 控制、相关实施指南以及其他信息适用。

12.1.4 开发，测试和运行环境分离

ISO/IEC 27002 中的 12.1.4 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

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。 应采取技术和组织措施以最大程度地减少所确定的风险。

12.2 恶意软件防范

ISO/IEC 27002:2013 中 12.2 规定的目标及其内容适用。

12.3 备份

ISO/IEC 27002:2013 中 12.3 规定的目标适用。

12.3. 1 信息备份

ISO/IEC 27002 中的 5.1.1 控制、相关实施指南适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

基于云计算模型的信息处理系统引入了额外的或替代的异地备份机制，以防止数据丢失，确保数据处理操作的连续性，并提供在破坏性事件后恢复数据处理操作的能力。为了备份和/或恢复，应该在物理和或逻辑上不同的位置(可以在信息处理系统本身内)创建或维护数据的多个副本。

在这方面特定于 PII 的责任可以由云服务客户承担。当公有云 PII 处理者明确向云服务客户提供备份和恢复服务时，公有云 PII 处理者应向云服务客户提供关于云服务在备份和恢复云服务客户数据方面的能力的明确信息。

注 1：某些司法管辖区可能对备份频率提出特定要求。 在这些辖区运营的组织有责任确保它们遵守这些要求。

应制定程序以允许在破坏性事件发生后的指定记录时间内恢复数据处理操作。
备份和恢复程序应按照规定的、记录在案的频率进行审查。

注 2:有些司法管辖区可对备份和恢复程序的审查频率提出具体要求。在这些辖区内运营的组织有责任确保他们遵守这些要求。

本文档中适用于分包 PII 处理的控制，涵盖了使用分包商存储正在处理的数据的复制或备份副本的情况。 在进行物理介质发生转移的地方，这也在本文档的控制中涵盖。

公有云 PII 处理者应该有一个政策来满足信息备份的要求，以及任何进一步的要求(如合同和/或法律要求)，以删除为备份目的而保存的信息中包含的 PII。

12.4 日志和监视

ISO/IEC 27002:2013 中 12.4 规定的目标适用。

12.4.1 事态日志

ISO/IEC 27002 中的 12.4.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

应该建立一个过程以指定的、记录的周期性检查事件日志，以识别违规行为并提出补救措施。

在可能的情况下，事件日志应该记录 PII 是否因事件而被更改(添加、修改或删除)以及由谁更改。如果云计算参考体系结构的不同服务类别涉及到多个服务供应商，那么在实现本指南时，可以扮演多种角色或担当共享角色。

公有云 PII 处理者应该定义关于日志信息是否、何时以及如何可以提供给云服务客户或由云服务客户使用的标准。这些过程应该对云服务客户可用。

如果云服务客户被允许访问由公有云 PII 处理者控制的日志记录，公有云 PII 处理者应确保云服务客户只能访问与该云服务客户活动相关的记录，并且无法访问任何与其他云服务客户活动相关的日志记录。

12.4.2 日志信息的保护

ISO/IEC 27002 中的 12.4.2 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

为安全监视和操作诊断等目的而记录的日志信息可以包含 PII。应该采取措施，例如控制访问（请参阅 9.2.3），以确保记录的信息仅用于其预期目的。

应该设置一个过程（最好是自动过程）以确保在指定的和有记录的期限内删除记录的信息。

12.4.3 管理员和操作员日志

ISO/IEC 27002 中的 12.4.3 控制、相关实施指南以及其他信息适用。

12. 4.4 时钟同步

ISO/IEC 27002 中的 12.4.4 控制、相关实施指南以及其他信息适用。

12.5 运行系统的软件安装

ISO/IEC 27002:2013 中 12.5 规定的目标及其内容适用。

12.6 技术方面的脆弱性管理

ISO/IEC 27002:2013 中 12.6 规定的目标及其内容适用。

12.7 信息系统审计的考虑

ISO/IEC 27002:2013 中 12.7 规定的目标及其内容适用。

13 通讯安全

13.1 网络安全管理

ISO/IEC 27002:2013 中 13.1 规定的目标及其内容适用。

13.2 信息传递

ISO/IEC 27002:2013 中 13.2 规定的目标适用。

13.2.1 信息传输策略和规程

ISO/IEC 27002 中的 13.2.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

无论何时使用物理介质进行信息传输，都应该设置一个系统来记录包含 PII 的传入和传出的物理介质，包括物理介质的类型、授权的发送者/接收者、日期和时间，以及物理介质的数量。在可能的情况下，应该要求云服务客户采取额外的措施(如加密)，以确保数据只能在目的地点访问，而不能在途中访问。

13.2.2 信息传输协议

ISO/IEC 27002 中的 13.2.2 控制、相关实施指南以及其他信息适用。

13.2.3 电子消息发送

ISO/IEC 27002 中的 13.2.3 控制、相关实施指南以及其他信息适用。

13.2.4 保密性或不泄露协议

ISO/IEC 27002 中的 13.2.4 控制、相关实施指南以及其他信息适用。

注：与保密或不泄露协议相关的其他控制和指南可在 A10.1 中找到.

14 系统获取、开发和维护

ISO/IEC 27002:2013 中 14 条规定的目标及其内容适用。

15 供应商关系

ISO/IEC 27002:2013 第 15 条中规定的目标及其内容适用。

注：有关供应商关系管理的更多信息在 ISO / IEC 27036-4 中提供。

16 信息安全事件管理

16. 1 信息安全事件的管理和改进

ISO/IEC 27002:2013 中 16.1 规定的目标适用，以下特定行业的指南也适用于本条款中所有控制的实施

公有云 PII 保护实施指南

在整个云计算参考体系结构的语境中，可以在信息安全事件的管理和改进方面共享角色。在实施本节中的控制时，可能需要公有云 PII 处理者与云服务客户合作。

16.1.1 责任和规程

ISO/IEC 27002 中的 16. 1.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

一个信息安全事件应触发公有云 PII 处理者的审查，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（请参阅 A9.1）。

信息安全事态不一定会触发这种审查。一个信息安全事态是指不会导致实际的, 值得注意的概率、未经授权访问 PII 或任何存储 PII 的公有云 PII 处理者的设备或设施,并且可以包括但不限于 ping 和其他广播攻击在防火墙或边缘服务器上，端口扫描，不成功的登录尝试，拒绝服务攻击和数据包嗅探。

16.1.2 报告信息安全事态

ISO/IEC 27002 中的 16.1.2 控制、相关实施指南以及其他信息适用。

16.1. 3 报告信息安全弱点

ISO/IEC 27002 中的 **16.1. 3** 控制、相关实施指南以及其他信息适用。

16.1.4 信息安全事态的评估和决策

ISO/IEC 27002 中的 16.1.4 控制、相关实施指南适用。

16.1.5 信息安全事件的响应

ISO/IEC 27002 中的 16. 1.5 控制、相关实施指南以及其他信息适用。

16.1.6 从信息安全事件中学习

ISO/IEC 27002 中的 16. 1.6 控制、相关实施指南以及其他信息适用。

16. 1.7 证据收集

ISO/IEC 27002 中的 16. 1.7 控制、相关实施指南以及其他信息适用。

17 业务连续性管理的信息安全方面

ISO/IEC 27002:2013 中第 17 条规定的目标及其内容适用。

18 符合性

18.1 符合法律和合同要求

ISO/IEC 27002:2013 中 18.1 规定的目标及其内容适用。

注:与遵守法律和合同要求有关的其他控制和指南可在 A 11 中找到。

18.2 信息安全评审

ISO/IEC 27002:2013 中 18.2 规定的目标适用。

18.2.1 信息安全的独立评审

ISO/IEC 27002 中的 18.2.1 控制、相关实施指南以及其他信息适用。 以下特定行业的指南也适用。

公有云 PII 保护实施指南

如果个别云服务客户的审计不切实际或可能增加安全风险（请参阅 0.1），公有云 PII 处理者应在签订合同之前并在合同期间向潜在云服务客户提供:有独立证据证明信息安全是按照公有云 PII 处理者的策略和程序实施和操作的。如果提供了足够的透明度，由公有云 PII 处理者选择的相关独立审核通常应是一种可接受的方法，可以满足云服务客户对公有云 PII 处理者的处理操作进行审核的兴趣。

18.2.2 符合安全策略和标准

ISO/IEC 27002 中的 18.2.2 控制、相关实施指南以及其他信息适用。

18.2.3 技术符合性评审

ISO/IEC 27002 中的 18.2.3 控制、相关实施指南以及其他信息适用。

附件 A

（规范性）

用于 PII 保护的公有云 PII 处理者扩展控制集

A.1 总则

本附件规定了新的控制和相关的实施指南，与 ISo/IEC 27002(见第 5 至 18 条)中增强的控制和指南相结合，构成了一个扩展的控制集，以满足充当 PII 处理者的服务提供商对 PII 保护的要求。

这些附加的控制是根据 ISO/IEC 29100 的 11 项隐私原则分类的。在许多情况下，这些控制可以根据一种以上的隐私原则进行分类。在这种情况下，将根据最相关的原则对其进行分类。

A.2 同意和选择

A.2.1 在 PII 主体的权利方面进行合作的义务

控制

公有云 PII 处理者应向云服务客户提供使他们能够履行其义务的手段，以便利行使 PII 主体访问，更正和/或删除与他们有关的 PII 的权利。

公有云 PII 保护实施指南

在这方面，PII 控制者的义务可以通过法律、法规或合同来规定。这些义务包括云服务客户使用公有云 PII 处理者的服务来实现的事项。例如，这可以包括及时更正或删除 PII。

如果 PII 控制者依靠公有云 PII 处理者提供信息或技术措施以方便 PII 主体权利的行使，则应在合同中指定相关的信息或技术措施。

A .3 目的合法性和规范

A.3.1 公有云 PII 处理者的目的

控制

根据合同处理的 PII 不应独立于云服务客户的指示进行任何处理。

公有云 PII 保护实施指南

指令可以包含在公有云 PII 处理者和云服务客户之间的合同中，包括服务要实现的目标和时间表。

为了实现云服务客户的目的，可能有技术上的原因，使公有云 PII 处理者确定处理 PII 的方法是适当的，这与云服务客户的通用指令一致，但没有云服务客户的专业指令。例如，为了有效地利用网络或处理能力，可能有需要根据 PII 主体的某些特征来分配特定的处理资源。在公有云 PII 处理者确定的处理方法涉及 PII 的收集和使用的情况下，公有云 PII 处理者应遵守 ISO / EC 29100 中规定的相关隐私原则。

公有云 PII 处理者应及时向云服务客户提供所有相关信息，以使云服务客户能够确保公有云 PII 处理者遵守规范和目的限制原则，并确保公有云 PII 处理者或其任何分包商为了不受云服务客户指示支配的附加目的，而不处理任何 PII。

A.3.2 公有云 PII 处理者的商用

控制

未经明确同意，公有云 PII 处理者不得将根据合同处理的 PII 用于公共营销和广告目的。这种同意不应成为接受服务的条件。

注: 这个控制是对 A.3 中更通用的控制的补充。并不能取代或以其他方式取代它。

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

控制

临时文件和文档应在规定的、法定期间内删除或销毁。

公有云 PII 保护实施指南

A .10.3 中提供了有关清除 PII 的实施指南

信息系统可以在其正常运行过程中创建临时文件。此类文件是特定于系统或应用程序，但可以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的操作相关的临时文件。相关信息处理任务完成后，不需要临时文件，但是在某些情况下可能无法删除它们。这些文件保留使用的时间长度并不总是确定的，但是“垃圾回收”过程应标识相关文件，并确定从它们最后一次使用到现在已经多长时间了。

PII 处理信息系统应实施定期检查，以删除指定期限以上的未使用的临时文件。

A .6 使用，保留和披露限制

A .6.1 PII 披露通知

控制

公有云 PII 处理者与云服务客户之间的合同应要求公有云 PII 处理者根据合同中约定的任何程序和时间段，完成执法机构提出的任何具有法律约束力的披露 PII 的请求。除非此类披露是被禁止的。

公有云 PII 保护实施指南

公有云 PII 处理者应提供合同保证，以确保：

—拒绝任何不具有法律约束力的 PII 披露要求；

—在进行任何 PII 披露之前，请在法律允许的情况下商议相应的云服务客户：以及

—接受由相应的云服务客户授权的任何合同约定的 PII 披露请求。

例如：一项可能禁止披露的规定是根据刑法禁止为执法调查保密。

A.6.2 PII 披露的记录

控制

向第三方进行的 PII 披露的应被记录下来，包括哪些 PII 被披露、向谁披露、在什么时间披露。

公有云 PII 保护实施指南

可以在正常操作过程中披露 PII。这些披露应予以记录（见 12. 4.1）。还应记录对第三方的任何其他披露，例如合法调查或外部审计所产生的披露。记录应包括披露资料的来源及作出披露的当局的来源。

A .7 准确性和质量

无其他控制与此隐私原则相关。

A. 8 公开，透明和通知

A. 8.1 分包 PII 处理的披露

控制

公有云 PII 处理者使用分包商处理 PII 之前，应向相关云服务客户披露这些信息。

公有云 PII 保护实施指南

在公有云 PII 处理者和云服务客户之间的合同中，使用分包商处理 PII 的规定条款应是透明的。合同应明确规定，只有在云服务客户在服务开始时同意的基础上，才能委托分包商。公有云 PII 处理者应及时通知云服务客户关于这方面的任何预期更改，以便云服务客户能够反对这些更改或终止合同。

所披露的信息应包括使用分包商的事实和相关分包商的名称，但不包括任何具体业务的细节。所披露的信息还应包括分包商可以在其中处理数据的国家(见 A 12,1)以及分包商有义务满足或超过公有云 PII 处理者义务的方式(见 A 11.12)。

如果公开披露分包商的信息被评估为增加超过可接受限度的安全风险，则应根据保密协议和/或根据云服务客户的要求进行披露。应该让云服务客户知道这些信息是可用的。

A.9 个体参与和访问

无其他控制与此隐私原则相关。

A.10 问责制

A.10.1 涉及 PII 的数据泄露的通知

控制

如果对 PII 的任何未经授权的访问或对处理设备或设施的未经授权的访问导致 PII 的丢失、披露或更改，则公有云 PII 处理者应立即通知相关云服务客户。

公有云 PII 保护实施指南

有关涉及 PII 的数据泄露通知的规定应构成公有云 PII 处理者与云服务客户之间的合同的一部分。合同应规定公有云 PII 处理者将如何提供云服务客户履行其通知相关部门的义务的必要信息。本通知义务不适用于由云服务客户或 PII 负责人或他们负责的系统组件内引起的数据泄漏。合同还应规定在涉及 PII 的数据泄露通知中的最大延迟时间。

如果发生涉及 PII 的数据泄露事件，则应保留记录，其中包含事件的描述，时间，事件的后果，报告者的姓名，事件的报告对象以及为解决该事件所采取的步骤（包括负责人和恢复的数据）以及事件导致 PII 的丢失，披露或更改的事实。

如果发生涉及 PII 的数据泄露，则记录还应包括对数据泄露的描述（如果已知）；如果执行了通知，则要采取步骤通知云服务客户和/或监管机构。

在某些司法管辖区中，相关法律或法规可能要求公有云 PII 处理者直接将涉及 PII 的数据泄露通知相关的监管机构（例如，PII 保护机构）。

注：可能有其他违规要求通知未在此处涵盖，例如未经同意或其他授权收集，用于未经授权的目的等。

A.10.2 行政安全策略和指导方针的保留期

控制

安全策略和操作程序的副本应在更换时（包括更新）的指定记录时间内保留。

公有云 PII 保护实施指南

可能需要审查当前和历史的政策和程序，例如在客户纠纷解决和由 PII 保护机构进行调查的情况下。在没有具体法律或合同要求的情况下，建议最短保留期为五年。

A.10.3 PII 的的归还、转移和处置

控制

公有云 PII 处理者应该有关于 PII 的归还、转移和处置的策略，并且应该让云服务客户可以使用该策略。

公有云 PII 保护实施指南

在某个时间点，需要以某种方式处理 PII。这可能涉及将 PII 返回给云服务客户，将其转移到另一个公有云 PII 处理者或 PII 控制者(例如，由于合并的结果)，安全地删除或以其他方式销毁它，将其匿名化或存档。

公有云 PII 处理者应提供必要的信息，以使云服务客户能够确保根据合同处理的 PII，无论存储在何处，都会被公有云 PII 处理者及其分包商删除，包括出于备份和业务连续性的目的，一旦对于云服务客户的特定目的而言不再需要它们。合同应规定处置机制的性质（取消链接、覆盖、消磁、破坏或其他形式的擦除）和/或适用的商业标准。

公有云 PII 处理者应制定和实施有关 PII 安排的策略，并应使该策略可供云服务客户使用。

该策略应涵盖合同终止后销毁 PII 之前的保留期，以保护云服务客户不因合同的意外失效而失去 PII。

注：该控制和指南在“使用，保留和披露限制”原则的保留内容下也适用（参见 A 6）。

A .11 信息安全

A .11. 1 保密或不泄露协议

控制

在公有云 PII 处理者的控制下，有权访问 PII 的个人应承担保密义务。

公有云 PII 保护实施指南

公有云 PII 处理者、其员工及其代理商之间以任何形式签订的保密协议，应确保员工和代理商不会出于与云服务客户的指示无关的目的而披露 PII（请参阅 A.3.1）。本保密协议的义务应在任何相关合同终止后仍然有效。

A.11.2 创建硬拷贝材料的限制

控制

展示 PII 的硬拷贝材料的创建应受到限制。

公有云 PII 保护实施指南

硬拷贝材料包括通过打印产生的材料。

A .11.3 数据恢复的控制和记录

控制

应该有一个数据恢复工作的程序和记录。（a log）

公有云 PII 保护实施指南

注:上述控制使适用于某些司法管辖区的下列要求具有通用性。数据恢复工作的记录应包括:负责人、恢复数据的描述和手工恢复的数据。

A. 11.4 保护离开场所的存储介质上的数据

控制

离开组织场所的介质上的 PII 应该经过授权程序，除授权人员外，其他任何人都不能访问（例如，对有关数据进行加密）。

A .11. 5 未加密的便携式存储介质和设备的使用

控制

不应使用不允许加密的便携式存储介质和便携式设备，除非不可避免，并应记录此类便携式存储介质和设备的任何使用。

A .11.6 通过公共数据传输网络传输的 PII 的加密

控制

通过公共数据传输网络传输的 PII 应该在传输之前进行加密。

公有云 PII 保护实施指南

在某些情况下，例如 在电子邮件交换中，公共数据传输网络系统的固有特性可能要求公开一些头或流量数据以进行有效传输。

如果有多个服务提供商参与提供来自云计算参考架构的不同服务类别的服务，则在实施本指南时可能会有不同或共享的角色。

A. 11. 7 硬拷贝材料的安全处置

控制

如要销毁硬拷贝材料，应使用横切、切碎、焚烧、制浆等机制安全地销毁。

A.11.8 用户 ID 的唯一使用

控制

如果不止一个人可以访问存储的 PII，则每个人都应具有不同的用户 ID，以进行标识，身份验证和授权。

A.11.9 授权用户记录

控制

应保留已获授权访问信息系统的用户的最新记录或用户的个人资料。

公有云 PII 保护实施指南

应该为公有云 Pll 处理者授权其访问的所有用户维护用户个人资料。 用户的个人资料包括有关该用户的数据集，包括用户 ID，这对于实现提供对信息系统的授权访问的技术控制是必需的。

A.11.10 用户 ID 管理

控制

停用或过期的用户 ID 不应授予其他人。

公有云 PII 保护实施指南

在整个云计算参考体系结构的语境中，云服务客户可以负责在其控制下的云服务用户的用户 ID 管理的某些或全部方面。

A.11.11 合同措施

控制

云服务客户与公有云 PII 处理者之间的合同应规定最低限的技术和组织措施，以确保合同中的安全安排已经落实，并且数据不会出于任何独立于控制者指令的目的进行处理。 公有云 PII 处理者不应单方面减少此类措施。

公有云 PII 保护实施指南

与公有云 PII 处理者相关的信息安全和 PII 保护义务可以直接从适用法律中产生。 如果不是这种情况，与公有云 PII 处理者相关的 PII 保护义务应包含在合同中。

本文档中的控制与 ISO / IEC 27002 中的控制一起，旨在作为参考目录，以协助签订有关 PII 的信息处理合同。公有云 PII 处理者应通知未来的云服务客户：在签订合同之前，有关其服务方面的资料要保护 PII。

在签订合同的过程中，公有云 PII 处理者的功能应该是透明的。然而，确保公有云 PII 处理者实现的措施满足其义务是云服务客户的最终责任。

A.11.12 分包 PII 处理

控制

公有云 PII 处理者和任何处理 PII 的分包商之间的合同应指定满足公有云 PII 处理者信息安全和 PII 保护义务的最低技术和组织措施。这种措施不应由分包商单方面减少。

公有云 PII 保护实施指南

使用分包商储存备份副本也受此控制（请参阅 A 8.1）

A.11.13 用过的的数据存储空间的数据访问

控制

公有云 PII 处理者应确保。每当将数据存储空间分配给云服务客户时，该云服务客户就不会看到以前驻留在该存储空间上的任何数据。

公有云 PII 保护实施指南

在云服务用户删除信息系统中保存的数据时，性能问题可能意味着显式删除这些数据是不切实际的。这就产生了另一个用户能够读取数据的风险。这种风险应通过具体的技术措施加以规避。

实施这一控制时，没有特别适合处理所有情况的具体指南。但是，作为示例，如果云服务用户试图读取尚未被该用户自己的数据覆盖的存储空间，则某些云基础设施，平台或应用程序将返回零。

A .12 隐私合规性

A. 12.1 PII 的地理位置

控制

公有云 PII 处理者应说明并记录可能存储 PII 的国家。

公有云 PII 保护实施指南

应该向云服务客户提供可能存储 PII 的国家的标识。应包括使用分包的 PII 加工所产生的国家的特征。如果具体的合同协议适用于数据的国际传输，例如示范合同条款、有约束力的公司规则或跨境隐私规则，还应确定这些协议以及适用这些协议的国家或客观环境。公有云 PII 处理者应及时通知云服务客户关于这方面的任何预期更改，以便云服务客户能够反对这些更改或终止合同。

A. 12.2 PII 的预期目的地

控制

使用数据传输网络传输的 PII 应受到适当的控制，以确保数据到达预期的目的地。

参考书目

[1] ISO / IEC 17789，信息技术-云计算-参考体系结构

[2] ISO / IEC 27001，信息技术-安全技术-信息安全管理系统-要求

[3] ISO / IEC 27005，信息技术安全技术-信息安全风险管理

[4] ISO / EC 27035，信息技术-安全技术-信息安全事件管理

[5] ISO / IEC 27036-4，信息技术安全技术-信息安全供应商关系-第 4 部分：云服务安全性准则

[6] ISO / EC 27040，信息技术-安全技术-存储安全

[7] ISO / EC 29100：2011，信息技术-安全技术-隐私框架

[8] ISO / IEC 29101，信息技术安全技术-隐私体系结构框架

[9] ISO / IEC 29134，信息技术安全技术隐私影响准则评估

[10] ISO /IEC 29191，信息技术安全技术部分要求

[11] ISO/IEC JTC 1/SC 27, WG 5 Standing Document 2- Part 1: Privacy References List. Latest version,availableathttp://www.jtc1sc27.din.de/sbe/wgssd2

[12] BS 10012：2009，数据保护。个人信息管理系统规范

[13] JIS Q 15001：2006，个人信息保护管理系统-要求

[14] NIST SP 800-53rev4, Security and Privacy Controls for Federal Information Systems and OrganizationsapRil2013(http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800 53r4. pdf)

[15] NIST SP 800-122，《保护个人身份信息机密性的指南》（2010 年 4 月，pII）（http：///lcsrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[16] NIST SP 800-144，《公有云计算中的安全性和隐私准则》，2011 年 12 月（http：//csrcnistgoy/publications/nistpubs/800-144/sp800-144.pdn）

[17] ENISA。云计算报告：收益，风险和信息建议

安全性 2009 年 11 月（http：//www.enisa.europa.euactivities/risk-management/files/deliverables/cloud-computing- risk-assessment / at_download / fullReport

[18]欧洲联盟，第 29 条工作组，关于云计算的意见 05 / 2012，2012 年 7 月通过：（http：/ lec，europaeu / justice / datacprotectionarticle-29 / documentationopinion 建议/文件/ 2012 / wp196-enpdf）