个人身份信息保护管理体系技术规范

文件编号：DNI-GZ-JS-67

技术规范编号：CTS DNI-PIIP-2026

文档版本：A/0

编制：技术部　　日期：2026.04.30

审核：杨舒　　日期：2026.04.30

批准：杨舒　　日期：2026.04.30

受控状态：受控文件

发布日期：2026年04月30日　　实施日期：2026年04月30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
2026.04.30	初始发布	A/0	杨舒	杨舒

个人身份信息保护管理体系技术规范

1 范围

本技术规范适用于所有类型和规模的作为PII控制者的组织，包括公共和私营公同，政府实体和处理PII的非营利组织。其基于ISO/IEC 27951:2017，结合ISO/IEC 27002:2022进行编制，对个人身份信息保护提出了信息安全控制要求，以满足与保护个人身份信息(PII)有关的风险评估和隐私影响评估所确定的要求，是我机构开展个人身份信息保护管理体系认证的认证依据。

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。

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 29151:2017 个人身份信息保护实践指南

ISO/IEC 29100:2011 信息技术 - 安全技术 - 隐私框架

3 定义和缩写词

3.1定义

3.1.1首席隐私官 (CPO)：负责组织内个人身份信息 (PII) 保护的高级管理人员。

3.1.2去标识化过程：使用去标识化技术，消除一组识别数据与数据主体之间关联的过程。

3.2 缩写词

为便于理解，以下缩写词适用。

BCR 约束性公同规则

CCTV 闭路电视

CPO 首席隐私官

PBD 隐私设计

PDA 个人数字助理

PET 隐私增强技术

PIA 隐私影响评估

PII 个人身份信息

RFID 射频识别

USB 通用串行总线

4 概述

4.1 保护PII目标

PII保护的目标是使组织能够实施一套控制措施，作为其整体PII保护计划的一部分。根据ISO/IEC 29100中描述的隐私原则，可以用于维护和改进：

1)遵守隐私相关法律法规；

2)管理隐私风险；

3)满足PII主要负责人、监管机构、客户期望。

4.2PII的保护要求

PII保护要求有三个主要来源：

1）与保护个人身份信息有关的法律，法定，监管当局和合同要求。包括：组织、贸易伙伴、承包商、服务提供商必须遵守的PII要求。

2）风险评估

组织的总体业务战略和目标，对组织和PII主体的风险(即安全风险和隐私风险)进行评估。

3）公同策略

组织也可以自愿选择超越以前要求所产生的制度。

组织还应该考虑为支持其运营而开发的PII的目标和业务需求的原则(即ISO/IEC 29100中定义的隐私原则)。

应根据风险评估选择PII保护控制措施(包括安全控制措施)。

隐私影响评估(PIA)的结果(ISO/IEC 29134中规定的)有助于指导和确定适当的纠正措施和优先级，以管理PII的风险，并实施所选择的控制以防范这些风险。

ISO/IEC 29134可提供PIA指导，包括：风险评估、风险处理计划、风险接受的建议。

4.3PII的控制

隐私影响评估可帮助组织识别：

由于非法处理导致的隐私泄露的特定风险；

削减参与操作的PII主体权利的风险。

组织应确定并实施控制措施，以处理隐私影响评估流程所识别的风险。然后将控制和纠正结果记录在案。

某些类型的PII处理可以保证特定的控制效果，只有仔细分析了预估的操作后才能使需要变得明显。

4.4选择控制措施

可以从本规范中选择控制措施（本规范引用ISO/IEC 27002中的控制措施）。

控制措施的选择取决于组织基于风险处理方案标准和适用于该组织及其客户和供应商的一般风险管理方法而做出的决策，并且还应遵守所有适用的国家和国际法律法规。

控制措施的选择和实施还取决于组织在提供基础设施或服务中的角色。许多不同的组织可能参与提供基础设施或服务。在某些情况下，所选控制措施可能仅适用于特定组织。在其他情况下，实施控制措施可能存在共享角色。合同协议应明确规定所有参与提供或使用服务的组织的PII保护责任。

本规范中的控制措施可作为处理PII的组织的参考，并适用于所有作为PII控制者的组织。作为PII处理者的组织应按照PII控制者的指示执行。PII控制者应确保其PII处理者能够根据PII处理的目的，实施其PII处理协议中包含的所有必要控制措施。使用云服务作为PII处理者的PII控制者可以参考ISO/IEC 27018，以确定需要实施的相关控制措施。

4.5 制定组织特定要求

并非本规范中的所有控制措施都适用于所有组织。此外，可能还需要本规范中未包含的其他控制措施和要求。

4.6 生命周期考虑因素

PII具有自然的生命周期，从……开始从创建或生成、收集、存储、使用和传输，直至最终处置（例如，安全销毁），个人身份信息 (PII)都处于生命周期之中。PII的价值和风险在其生命周期中可能发生变化，但无论在生命周期的各个阶段还是在所有情况下，保护PII都至关重要。

信息系统也具有生命周期，包括构思、规范、设计、开发、测试、实施、使用、维护，最终退役并处置。在所有这些阶段，都应考虑PII保护。新系统的开发和现有系统的变更为组织提供了更新和改进安全控制以及PII保护控制的机会，同时应考虑实际发生的事件以及当前和预测的信息安全和隐私风险。

4.7 本规范的结构

本规范包含两个主要规范性部分。

本规范的第一部分（第5至18条）包含针对ISO/IEC 27002中描述的某些相关现有控制措施的补充实施要求。

第二部分包含附件A中规定的用于保护个人身份信息（PII）的特定控制集。

5 信息安全政策

5.1 信息安全管理指导

5.1.1 简介

同ISO/IEC 27002:2022中5.1依据业务要求和相关法律法规，为信息安全提供管理指导和支持。

5.1.2 信息安全策略

同ISO/IEC 27002:2022中5.1

控制

信息安全策略集宜被定义，由管理者批准，并发布、传达给所有员工和外部相关方。

保护PII的实施要求

信息安全策略应包括适当的保护PII安全措施声明。ISO/IEC 27002:2022的5.34中提供了有关PII保护的详细信息。

在设计，实施和审查信息安全策略时，组织应考虑 ISO 29100中描述的隐私保护要求。组织应制定与信息安全无关的PII保护要素，作为单独的隐私策略。

5.1.3 信息安全策略的评审

同ISO/IEC 27002:2022中5.1

控制

宜按计划的时间间隔或当重大变化发生时进行信息安全策略评审，以确保其持续的适宜性、充分性和有效性。

保护PII的实施要求

无。

6 信息安全的组织

6.1 内部组织

6.1.1 简介

ISO/IEC 27002:2022的5.2

6.1.2 信息安全角色和责任

同ISO/IEC 27002:2022中5.2

控制

所有的信息安全责任宜予以定义和分配。

保护PII的实施要求

需要明确规定保护个人身份信息的角色和责任，并妥善记录并传达。特别：

a)组织应分配高级管理成员 [有时称为首席隐私官(CPO)]对PII承担保护的责任；

b)应明确指明，每个角色担当的PII保护职能，负责与组织内的信息安全职能进行协调；

c)参与PII处理的所有人(包括用户和支持人员)应在其工作中包含适当的PII保护要求。

已建立的PII保护功能应与处理PII的其他功能(信息安全功能)密切协作，信息要求包括：由PII保护相关法规法引起的安全要求；协助解释法律法规和合同条款的功能；处理数据泄露。

该组织应审查是否需要并酌情建立跨职能的委员会，或由处理PII职能的高级成员组成的委员会。

PII的保护是一个多学科的职能，这样的委员会可以帮助主动发现改进机会，识别PIA的新风险和领域，制定预防措施，检测违规行为并采取纠正措施等。建议这样的小组应定期开会，并由a)中确定的负责PII保护的人担任主席。

PII控制者应要求其PII处理者指定一个联系点，以解决合同下有关PII的处理问题。

负有PII保护职能的人应向CPO报告，以确保他们有足够的权力履行其职责。

6.1.3 职责分离

控制

同ISO/IEC 27002:2022中5.3

保护PII的实施要求

PII保护的责任和职责范围应独立于信息安全领域。虽然认识到信息安全对保护个人识别信息的重要性，但安全和个人身份信息保护的责任和责任区域应尽可能彼此独立，这一点很重要。

如果有必要或有帮助，应该为负责信息安全的人员和负责PII保护的人员之间的协调和合作提供便利。

在为PII分配访问权时，组织应采用职责分离原则，特别是任何被确定为高风险的处理。

访问PII的权限与记录该访问的日志的访问权，不相兼容。为了回应PII主体的请求，收集PII权限应与

PII的其他所有形式的访问权分离。

访问应限于其职责要求，包括限于响应PII主要的请求。

6.1.4 与主管部门联系

控制

同ISO/IEC 27002:2022中5.5

保护PII的实施要求

在适用的情况下，组织应制定程序，规定何时和由谁联系权威机构(包括数据保护机构)，例如报告隐私违规或报告处理细节。

6.1.5 与特殊利益集团联系

控制

同ISO/IEC 27002:2022中5.6

保护PII的实施要求

无。

6.1.6 项目管理中的信息安全

控制

同ISO/IEC 27002:2022中5.8

保护PII的实施要求

任何新的项目启动都应至少触发阈值分析，以确定是否需要进行PIA。

请注意项目涵盖：组织实施新的或变更现有的技术，产品，服务，程序，信息系统，流程或项目的所有事件。进一步的指导可以在ISO 29134中规定的PIA中找到。

6.2 移动设备和远程工作

6.2.1 介绍

ISO/IEC 27002:2022的8.1中规定的目标适用。

6.2.2 移动设备政策

控制

同ISO/IEC 27002:2022中8.1

保护PII的实施要求

组织应严格限制便携式和移动设备(如笔记本电脑，手机，通用串行总线(USB)设备和个人数字助理(PDA))访问PII，这些设备通常比非便携式设备，组织设施中的台式计算机)，这取决于风险评估。

组织应严格限制对PII的远程访问,并且在远程访问不可避免的情况下,确保远程访问的通信是加密的,消息认证和完整性保护。

6.2.3 远程工作

控制

同ISO/IEC 27002:2022中6.7

7 人力资源安全

7.1 聘用前

7.1.1 介绍

同 ISO/IEC 27002:2022中6.1

确保员工和合同方理解其责任，并适合其角色。

7.1.2 审查

控制

同 ISO/IEC 27002:2022中6.1

7.1.3 任用条款和条件

控制

同 ISO/IEC 27002:2022中6.2

保护PII的实施要求

无。

7.2 在任职期间

7.2.1 介绍

同ISO/IEC 27002:2022中5.4

确保员工和合同方意识到并履行其信息安全责任。

7.2.2 管理责任

控制

同ISO/IEC 27002:2022中5.4

保护PII的实施要求

无

7.2.3 信息安全意识，教育和培训

控制

同ISO/IEC 27002:2022中6.3

保护PII的实施要求

应采取措施使相关工作人员了解PII控制者可能产生的后果(例如，法律后果，业务损失，品牌或声誉损害)，工作人员(例如，惩戒的后果)和违反隐私或安全规则、程序的主要后果(隐私主体的身体，物质和情感伤害)，尤其是涉及PII处理的规则和程序。

正如信息安全意识，教育和培训一样，组织也应提供有关保护和处理PII的适当培训，教育和意识。

7.2.4 违规处理过程

控制

同ISO/IEC 27002:2022中6.4

保护PII的实施要求

组织应该制定正式的纪律策略。

应该向受影响的个人明确告知这种隐私保护政策。在所有隐私侵犯中，组织都应该严格执行这项策略。

7.3 任用的终止或变更

7.3.1 介绍

同ISO/IEC 27002:2022中6.5在任用变更或终止过程中保护组织的利益。

7.3.2 审查

控制

同ISO/IEC 27002:2022中6.5

保护PII的实施要求

无。

8资产管理

8.1有关资产的责任

8.1.1介绍

同ISO/IEC 27002:2022中5.9-5.11识别组织资产并定义适当的保护责任。

8.1.2资产清单

组织应使用ISO29134的PIA报告所提供的信息，建立、维护和更新资产清单。

应包括PII资产和处理PII的所有系统。当开发和维护库存时，组织应该从PIAS中提取关于信息系统处理PII的下列信息元素：

PII识别系统的名称、首字母缩略词；

这些系统处理的PII类型；

个人身份信息的分类(见8.2.2),既作为单独的信息元素，又被组合在这些信息系统中；

任何违反PII的潜在影响，对PII主体和组织造成的影响；

收集PII的目的；

PII处理是否外包；

PII是否传送给其他PII控制者，如果是，向谁(或向哪组接受者)传送；

PII的保存期限；

收集或处理PII的地理区域；

是否涉及跨境数据传输。

组织应定期向PII责任者更新PII清单,以支持新的或变更的信息系统处理PII建立适当的安全控制措施。

8.1.3资产的所有权

控制

同ISO/IEC 27002:2022中5.10

8.1.4资产的可接受使用

控制

同ISO/IEC 27002:2022中5.10

保护PII的实施要求

组织应保护支持PII的资产免遭未经授权的访问，未经授权的修改，未经授权的移除，丢失或破坏，或

者错误和非法的处理等。

8.1.5资产归还

控制

同ISO/IEC 27002:2022中5.11

8.2信息分类

8.2.1介绍

同ISO/IEC 27002:2022 中5.12、5.13、5.10确保信息依据其对组织的重要程度受到适当水平的保护。

8.2.2 信息分类

控制

同ISO/IEC 27002:2022中5.12

保护PII的实施要求

组织应使用现有的或新创建的分类类别，对包含PII的所有信息进行分类。新的分类类别应包括但不限于常规的分类，如敏感和不敏感的PIII。分类方案还可以包括更具体的类别，例如个人健康信息(PHI),个人财务信息(PFI)。如果组织创建新的分类类别，那么应该定义对这些分类的保护级别。实际使用的类别还应取决于相关数据保护立法和法规中规定的要求，合同的义务，信息的性质和敏感性以及可能出现的危害风险、违规事件。

根据适用的数据保护法律，PII可能在某个国家被分类为不敏感而在其他地方可能被视为敏感。

当与一个或多个附加属性相关联时，应制定适当的指导方针和程序重新评估和修改PII元素的分类。

8.2.3信息标记

控制

同ISO/IEC 27002:2022中5.13

保护PII的实施要求

如果组织不将PII按照类别分类，组织应确保其控制下的人员了解PII的定义以及如何识别PII。

8.2.4资产处置

控制

同ISO/IEC 27002:2022中5.10

保护PII的实施要求

如果组织与PII相关的分类信息标签未采用，组织应让其控制的人员处理包含PII的所有类别的信息。

8.3介质处置

8.3.1介绍

同ISO27002:2022 中7.10防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。

8.3.2移动介质的管理

某些国家地区可能要求对包含PII的可移动介质进行加密。无论法律是否要求，建议使用加密措施来降低PII泄漏的风险。如果数据机密性或完整性是重要考虑因素，则应使用加密技术来保护可移动介质上的PII。

应该进行风险评估以确定所需的保护水平，这反过来将有助于确定所使用的密码算法的必要类型，强度和质量。

10.1中提供了有关使用加密控件的其他指导。

8.3.3介质处理

控制

同ISO/IEC 27002:2022中7.10

保护PII的实施要求

安全处置含PII介质的程序应与信息的敏感度以及不适当处理该信息的影响程度成正比。

一些国家地区可能会对用于处置含有PII的介质或特定类型的PII(例如健康数据，财务数据)的程序制定相关的标准。

8.3.4物理介质的转移

控制

同ISO/IEC 27002:2022中7.10

保护PII的实施要求

当使用物理介质传输个人身份信息时，应制定保护的实施要求，包含PII的物理介质的传入和传出信息要被登记，包括：物理介质的类型，识别码(例如序列号或清单标签号码)，授权的发件人/收件人，日期和时间，物理介质的数量以及它们包含的PII的类型，并检测物理介质的丢失。

转移的目的和范围，负责授权的人员以及转移的法律/合同依据也应该形成文件。应该额外考虑对数据最小化原则的明确引用。

9访问控制

9.1访问控制的业务需求

9.1.1简介

ISO/IEC 27002:2022 5.15中规定的目标适用。

9.1.2访问控制策略

控制

同ISO/IEC 27002:2022中5.15

9.1.3接入网络和网络服务。

控制

同ISO/IEC 27002:2022中5.15

9.2用户访问管理

9.2.1简介

同ISO/IEC 27002:2022 中5.16、5.17、5.18、8.2确保授权用户对系统和服务的访问，个人身份信息保护并防止未授权的访问。

9.2.2用户注册和注销

控制

同ISO/IEC 27002:2022中5.16

保护PII的实施要求

用户注册和注销过程以及用户生命周期管理过程，应提供相应措施来解决访问控制威胁，如：密码存储、其他用户注册数据的泄露(例如，无意泄露)。

9.2.3用户访问权供给

控制

同ISO/IEC 27002:2022中5.18

保护PII的实施要求

根据ISO29100中描述的数据最小化原则，组织应该为用户提供处理PII的适当权利。

根据ISO29100中描述的数据最小化原则,组织应将对处理PII的访问限制在满足目的的基础上人数最少。

组织应针对特定的PII和PII处理(即健康数据)采用强认证方法。

9.2.4特殊访问权的管理

控制

同ISO/IEC 27002:2022中8.2

保护PII的实施要求

PII的大规模处理(例如，批里查询，批量修改，批量导出，批里删除)增加了大规模违规的风险。为这些特权操作分配访问权时，组织应特别小心。

为了防止PII的滥用，PII处理(特别是高风险PII处理)的特权访问应在严格有限的基础上分配。还应该以有助于降低两个或两个以上个人之间共谋风险的方式进行分配。这些权利的授予和使用应记录在相关的日志文件中。所有的访问批准应该在指定的时间内完成。组织应定期审查所有此类批准，并视情况适时更新，撤销或终止审批。

9.2.5用户的秘密鉴别信息的管理

控制

同ISO/IEC 27002:2022中5.17

9.2.6用户访问权管理

控制

同ISO/IEC 27002:2022中5.18

9.2.7访问权的移除或调整

控制

同ISO/IEC 27002:2022中5.18

保护PII的实施要求

无。

9.3用户责任

9.3.1介绍

同ISO/IEC 27002:2022中5.17

让用户承担保护其鉴别信息的责任。

9.3.2秘密鉴别信息的使用

控制

同ISO/IEC 27002:2022中5.17

保护PII的实施要求

无。

9.4用户责任

9.4.1简介

同ISO/IEC 27002:2022中 5.17、8.3、8.4、8.5、8.18防止对系统和应用的未授权访问。

9.4.2信息访问限制

控制

同ISO/IEC 27002:2022中8.3

保护PII的实施要求

在允许操作员和管理员等使用能够从包含PII的数据库自动大量检索PII的查询语言之前，组织应审查其使用此类语言的必要性。

在使用查询语言符合保护要求的情况下，组织应提供技术措施，将这些语言的使用限制在满足特定目的所需的最低限度。例如，这可能意味着:在定义的敏感字段中限制使用查询语言。当需要访问未被授权的区域时(例如物理操作区域)，应实施严格的审批机制。组织应该保留所有这些批准的记录。

9.4.3安全登录规程

控制

同ISO/IEC 27002:2022中8.5

保护PII的实施要求

在PII主体可以向PII控制者请求帐户的情况下,PII控制者应根据风险分析的结果为这些帐户提供安全的登录规程(宜使用如密码手段、智能卡、令牌或生物特征识别方法等替代口令的鉴别方法。)

9.4.4用户的秘密鉴别信息的管理

控制

同ISO/IEC 27002:2022中5.17

9.4.5用户访问权管理

控制

同ISO/IEC 27002:2022中8.18

9.4.6访问权的移除或调整

控制

同ISO/IEC 27002:2022中8.4

10密码学

10.1密码控制

10.1.1介绍

同ISO/IEC 27002:2022中8.24确保适当和有效地使用密码技术以保护信息的保密性、真实性和(或)完整性。

10.1.2密码控制的使用策略

控制

同ISO/IEC 27002:2022中8.24

10.1.3 密钥管理控制

同ISO/IEC 27002:2022中8.24

保护PII的实施要求

无。

11.1.1简介

同ISO/IEC 27002:2022 中 7.1、7.2、7.3、7.5、7.6

防止对组织信息和信息处理设施的未授权物理访问、损坏和干扰。

11.1.2物理安全边界

控制

同ISO/IEC 27002:2022中7.1

11.1.3 物理人口控制

控制

同ISO/IEC 27002:2022中7.2

11.1.4 办公室、房间和设施的安全保护控制

同ISO/IEC 27002:2022中7.3

11.1.5外部和环境威胁的安全防护

控制

同ISO/IEC 27002:2022中7.5

11.1.6 安全区城工作

控制

同ISO/IEC 27002:2022中7.6

11.1.7 交接区

控制

同ISO/IEC 27002:2022中7.2

11.2 设备

11.2.1 简介

同ISO/IEC 27002:2022中7.7、7.8、7.9、7.10、7.11、7.12、7.13、7.14、8.1

防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。

11.2.2 设备安置和保护

控制

同ISO/IEC 27002:2022中7.8

11.2.3 支持性设施

控制

同ISO/IEC 27002:2022中7.11

11.2.4 布缆安全

控制

同ISO/IEC 27002:2022中7.12

11.2.5设备维护

控制

同ISO/IEC 27002:2022中7.13

11.2.6资产移动

控制

同ISO/IEC 27002:2022中7.10

11.2.7 组织场所外的设备与资产安全

控制

同ISO/IEC 27002:2022中7.9

11.2.8设备的安全处置和再利用

控制

同ISO/IEC 27002:2022中7.14

保护PII的实施要求

出于安全处置或重复使用的目的，含有II存储介质的设备应予以物理销毁，或根据定义明确的文件化程序，使用经批准的技术销毁，删除或覆盖PII使原始PII 无法恢复，而不是简单地使用标准删除或格式化功能，对于加密的存储介质，解密密钥、密钥设备(如智能卡)，受控销毁可能就足够了。

11.2.9无人值守的用户设备

控制

同ISO/IEC 27002:2022中8.1

11.2.10 清理桌面和屏幕策略控制

同ISO/IEC 27002:2022中7.7

12 运行安全

12.1 运行规程和责任

12.1.1 简介

同ISO/IEC 27002:2022中5.37、8.6、8.31、8.32确保正确、安全的运行信息处理设施。

12.1.2文件化的操作规程

控制

同ISO/IEC 27002:2022中5.37

12.1.3 变更管理

控制

同ISO/IEC 27002:2022中8.32

12.1.4 容量管理

控制

同ISO/IEC 27002:2022中8.6

12.1.5 开发、测试和运行环的分离

控制

同ISO/IEC 27002:2022中8.31

保护PII的实施要求

开发，测试和运行环境应该是逻辑上的、尽可能的情况下应该是物理上的，独立的环境，应实施适当的访问控制措施，以确保访问仅限于获得适当授权的个人。

如果测试、开发网络或设备，需要访问运行网络，则应实施强有力的访问控制。

无论使用何种环境，组织都应评估包含PII的可移动介质，具有无线功能的风险。如果未经法律允许或未经PII主体明确同意，PII不得用于未事先声明的，匿名开发和测试。

12.2 恶意软件防范

12.2.1 简介

同ISO/IEC 27002:2022中8.7确保信息和信息处理设施防范恶意软

12.2.2恶意软件的控制

控制

同ISO/IEC 27002:2022中8.7

12.3 备份

12.3.1简介

同ISO/IEC 27002中8.13防止数据丢失。

12.3.2 信息备份

控制

同ISO/IEC 27002:2022中8.13

保护PII的实施要求

信息系统通过引人其他替代机制处理PII，例如异地备份，用于防止的PII丢失，确保PII处理操作的连续性，并提供在中断事件后恢复PII处理操作的能力(如果严格必要的话)。

注：备份和恢复操作之间需要一段时间。存储在备份中的PI在访问时可能不再是最新的，任何基于过时PII的操作都可能导致结果不正确，并构成隐私风险。

12.4 日志和监视

12.4.1 简介

同ISO/IEC 27002:2022中8.15、8.17记录事态并生成证据。

12.4.2事态日志

控制

同ISO/IEC 27002:2022中8.15

保护PII的实施要求

在可能的情况下，事态日志应记录哪些PII被访问，PII做了什么(例如，读取，打印，添加，修改，删除)，何时何人访问，特别是某些敏感度高的PII(例如健康数据)。在多个服务提供商参与提供服务的情况下，在实施本规范时可能会有不同或共享的角色。

应该建立一个流程，以指定的，记录在案的周期来审查事态日志，以确定违规行为并提出补救措施。

PII控制者应定义有关是否何时、如何将日志信息提供给管理员使用，以及如何安全监控、操作、诊断。

12.4.3 保护日志信息

控制

同ISO/IEC 27002:2022中8.15

保护PII的实施要求

保护PII日志信息的安全监控、操作、诊断等实施。

应采取措施，如访问控制(见 9.2.3)，以确保记录的信息仅用于预期目的，应采取措施确保日志文件的完整性。

12.4.4 管理员和操作员日志

控制

同ISO/IEC 27002:2022中8.15

保护PI1的实施要求

组织应监视PII的特权访问(例如系统管理员和操作员)以及访问后的处理过程,这利监测应构成对信息系统全面监测PII的一部分。

组织应该定义他们认为是异常活动的内容，并应实施自动化程序，将此类活动报告给组织内的相关责任人。

12.4.5 时钟同步

控制

同ISO/IEC 27002:2022中8.17

12.5 运行软件控制

12.5.1简介

同ISO/IEC 27002中8.19确保运行系统的完整性。

12.5.2 运行系统软件的安装控制

同ISO/IEC 27002:2022中8.19

12.6 技术脆弱性管理

12.6.1 简介

同ISO/IEC 27002中8.8、8.19防止对技术脆弱性的利用。

12.6.2 技术脆弱性的管理

控制

同ISO/IEC 27002:2022中8.8

12.6.3软件安装限制

控制

同ISO/IEC 27002:2022中8.19

12.7 技术脆弱性管理

12.7.1 介绍

同ISO/IEC 27002中8.34使审计活动对运行系统的影响最小化。

12.7.2 信息系统审计控制

控制

同ISO/IEC 27002:2022中8.34

13 通信安全

13.1 网络安全管理

13.1.1 简介

同ISO/IEC 27002中8.20、8.21、8.22确保网络中的信息及其支持性的信息处理设施得到保护。

13.1.2 网络控制

控制

同ISO/IEC 27002:2022中8.20

13.1.3 网络服务安全

控制

同ISO/IEC 27002:2022中8.21

13.1.4 网络隔离

控制

同ISO/IEC 27002:2022中8.22

13.2 信息传输

13.2.1简介

同ISO/IEC 27002中5.14、6.6保持在组织内及与外部实体间传输信息的安全。

13.2.2信息传输策略和规程

控制

同ISO/IEC 27002:2022中5.14

保护PII的实施要求

应该采取适当的措施来降低信息传递过程中PII泄漏的风险。这通常通过加密手段来实施，其他措施包括：识别化，掩蔽化，混淆化。

13.2.3 信息传输协议

控制

同ISO/IEC 27002:2022中5.14

13.2.4电子信息发送

控制

同ISO/IEC 27002:2022中5.14

13.2.5 保密或不泄露协议

控制

同ISO/IEC 27002:2022中6.6

保护PII的实施要求

组织应制定外部处理PII的条件。这些条件包括：合同、保密、保密协议的一部分。

14 系统获取、开发和维护

14.1 信息系统的安全要求

14.1.1 简介

同ISO/IEC 27002:2022中5.8、8.26确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求。

14.1.2 信息安全要求分析和说明

控制

同ISO/IEC 27002:2022中5.8

保护PII的实施要求

开发或处理PII的信息系统进行重大改变时，应该进行PIA。PIA的实施可以在ISO29134中找到。

PIA的结果应该用来确定治理风险所采用的控制措施。

14.1.3 公共网络上应用服务的安全保护控制

同ISO/IEC 27002:2022中8.26

14.1.4应用服务事务的保护

控制

同ISO/IEC 27002:2022中8.26

14.2 开发和支持过程的安全性

14.2.1 简介

同ISO/IEC 27002:2022中8.25、8.27、8.29、8.30、8.31、8.32确保信息安全在信息系统开发生命周期中得到设计和实现。

14.2.2 安全的开发策略

控制

同ISO/IEC 27002:2022中8.25

14.2.3 系统变更控制规程

控制

同ISO/IEC 27002:2022中8.32

14.2.4 运行平台变更后对应用的技术评审

控制

同ISO/IEC 27002:2022中8.32

14.2.5 软件包变更的限制

控制

同ISO/IEC 27002:2022中8.32

14.2.6系统安全工程原则

控制

同ISO/IEC 27002:2022中8.27

14.2.7 安全的开发环境

控制

同ISO/IEC 27002:2022中8.31

14.2.8 外包开发

控制

同ISO/IEC 27002:2022中8.30

14.2.9系统安全测试

控制

同ISO/IEC 27002:2022中8.29

14.2.10 系统验收测试

控制

同ISO/IEC 27002:2022中8.29

保护PII的实施要求

系统验收测试还应包括对隐私保护要求的测试。

14.3 测试数据

14.3.1简介

同ISO/IEC 27002:2022中8.33确保用于测试的数据得到保护。

14.3.2 测试数据的保护

控制

同ISO/IEC 27002:2022中8.33

保护PII的实施要求

包含PII的操作数据通常不应用于开发和测试，在测试环境中使用真实的PII会增加信息危害的风险。相反，组织应该使用合成数据，或者应采取措施“隐藏”(例如，掩盖，混淆，识别化)任何正在使用的真实PII。

15供应商关系

15.1供应商关系中的信息安全

15.1.1 简介

同ISO/IEC 27002:2022中5.19、5.20、5.21确保供应商可访问的组织资产得到保护。

15.1.2 供应商关系的信息安全策略

控制

同ISO/IEC 27002:2022中5.19

保护PII的实施要求

如果组织需要利用PII处理服务，对PII处理者，应根据经验、可信度、符合适用法律法规、合同、其他法律协议规定的PII保护要求的能力进行评估。

作为PII控制者的组织应与任何作为PI1处理者的供应商签订书面合同。

合同应明确分配PII控制者和PII处理者之间的角色和责任，并应包含与PII保护相关的适当条款，以便PII处理者对所执行的处理负责。

PII 控制者合同至少应提供：

-根据合同进行处理的规模，性质和目的的适当声明；

-赋予PII主体访问和审查其PII，处理PII主体提出的任何投诉的能力(见条款A.10)；

-为履行法律或监管要求而采取的其他组织措施；

-授权PII控制人员在PII处理者的场所进行审计；

-在数据泄露，未经授权的处理，其他不履行合同条款和条件的情况下，有报告的义务，包括双方的联系点的身份验证；

-PII控制者对PII处理者的指令方法；

-适用于终止合同的措施，特别是关于安全地删除PII或退还PII和实体介质，PII控制者应确保其PII处理者在 未事先获得PII控制者批准的情况下不进行任何进-步的分包处理(即使用子处理者)。PII控制者在这方面应遵守所有相关法律和法规，PII控制人员应确保其PII处理人员不会将PII用于合同协议中或其他法律以外的用途，PII控制者应确保PII处理者安全地处理PI1。

15.1.3 在供应商协议中强调安全

控制

同ISO/IEC 27002:2022中5.20

15.1.4信息与通讯技术供应链

控制

同ISO/IEC 27002:2022中5.21

15.2 供应商服务交付管理

15.2.1 简介

同ISO/IEC 27002:2022 中5.22维护与供应商协议一致的信息安全和服务交付的商定级别。

15.2.2供应商关系的信息安全策略

控制

同ISO/IEC 27002:2022中5.22

15.2.3供应商服务的变更管理

控制

同ISO/IEC 27002:2022中5.22

16 信息安全事件管理

16.1 信息安全事件的管理和改进

16.1.1 简介

同ISO/IEC 27002中5.24、5.25、5.26、5.27、5.28、6.8确保采用一致和有效的方法对信息安全事件进行管理，包括对安全事态和弱点的沟通。

16.1.2责任和规程

控制

同ISO/IEC 27002:2022中5.24

保护PII的实施要求

组织应对隐私事件的有组织、有效的回应，因此，组织应该制定和实施隐私事件响应计划，组织隐私事件响应计划应包括：

a)隐私事件的定义和隐私事件响应的范围；

b)建立一个跨部门的隐私事件响应团队，开发，实施，测试，执行和审查隐私事件应对计划(该计划的批准应由组织内的高级管理人员决定)；

c)为隐私事件响应团队的所有成员明确规定角色，职责和权限；

d)在发生跨境事件时，依据国内、国际法规，澄清与外部各自组织承担的流程；

组织隐私事件响应计划应包括：

e)根据组织事件，确保所有受内部隐私政策影响的人(例如，员工，承包商及时向信息安全官员和负责PII保护的人有时称为CPO)进行快速报告的流程；

f)评估事故影响，以确定受影响的人、组织的，任何潜在或实际危害的性质、程度；

g)确定需要采取的措施来减轻上述危害并减少危害的过程以防止复发；

h)确定通知受影响的人，其他指定实体的流程，该通知的时间、形式，以及在什么样情况下发出通知。

组织可以选择将他们的隐私事件响应计划与他们的安全事件响应计划进行整合，也可将它们分开，作为其信息安全事件管理流程的一部分，信息安全事件应引发PII控制者进行审查，以确定是否发生了涉及PII的数据泄露事件。

信息安全事件可能包括但不限于：对防火或边缘服务器的ping，其他广播攻击，端口扫描，登录尝试，拒绝服务攻击，数据包嗅探，信息安全事件不一定会导致PII的处置设备设施产生可能的或实际的损害，

16.1.3 报告信息安全事态

控制

同ISO/IEC 27002:2022中6.8

保护PII的实施要求

当PII受到损害时，PII所有者的权益可能不能立即得到保护，同法管辖区可能会对报告或通知提出县体要求(例如，在立法或条例中)，当发生涉及PII的安全事件(例如，未经授权的处理、违反合同)，事件的细节，包括组织的建议响应(可能遭受披露)，应尽快通知有关当局。当局包括数据保护责任人、执法机构、受事件影响的人。

如果发生隐私违规，组织应向受影响的PII所有者提供适当和有效的补救措施，例如更正或删除不正确的信息。

16.1.4 报告信息安全弱点

控制

同ISO/IEC 27002:2022中6.8

16.1.5 信息安全事态的评估和决策

控制

同ISO/IEC 27002:2022中5.25

16.1.6 信息安全事件的响应

控制

同ISO/IEC 27002:2022中5.26

16.1.7 从信息安全事件中学习

控制

同ISO/IEC 27002:2022中5.27

16.1.8 证据的收集

控制

同ISO/IEC 27002:2022中5.28

17 业务连续性管理的信息安全方面

17.1 信息安全的连续性

17.1.1 简介

同ISO/IEC 27002:2022中5.29宜将信息安全连续性纳人组织业务连续性管理之中。

17.1.2 规划信息安全连续性

控制

同ISO/IEC 27002:2022中5.29

17.1.3 实现信息安全连续性

控制

同ISO/IEC 27002:2022中5.29

17.1.4验证、评审和评价信息安全连续性

控制

同ISO/IEC 27002:2022中5.29

17.2 几余

17.2.1 简介

同ISO/IEC 27002:2022中8.14确保信息处理设施的可用性。

17.2.2 信息处理设施的可用性

控制

同ISO/IEC 27002:2022中8.14

18 符合性

18.1 符合法律和合同要求

18.1.1引言

同ISO/IEC 27002:2022中5.31、5.32、5.33、5.34避免违反与信息安全有关的法律、法规、规章或合同义务以及任何安全要求。

18.1.2适用的法律和合同要求的识别

控制

同ISO/IEC 27002:2022中5.31

保护PII的实施要求

组织应确定与他们的PII保护相关的法律和法规，如果确定了这些要求，那么组织该为这些要求采取必要的措施，以下情况是这些要求的例子：

a) 如果需要为某些类别的个人识别信息(例如身份证，护照号码或信用卡号码)提供额外保护，则应使用加密技术(加密算法的类型，强度，质量)。加密算法只能从批准的算法列表中选择，与此要求有关的安全控制在10.1.2中规定。

b) 司法管辖区可能要求对信息进行最低限度的数据备份周期，并对数据、数据恢复进行评审。

与此要求有关的安全控制在12.3.2中规定。

组织应执行PIA并实施所产生的隐私处理计划,以确保与PII处理相关的计划和服务符合隐私保护要求。

从ISO29134中可以找到进一步的指导。

组织应建立一个审计计划,以帮助验证PII处理是否符合相关隐私保护要求。该计划应规定审计的频率，审核可以由组织进行(例如通过内部审核部分)，也可以由合格的独立第三方进行。

其他信息用于保护PII

虽然在许多同法管辖区中，PII控制者最终将负 责确保合规性，但涉及PII处理过程的所有参与者都应采取积极主动的方式来确 定相关隐私保护要求。PII控制者和PII处理者之间的合同提供了确保PII处理者支持和管理合规性的机制。

合同应要求PII处理者可接受独立的合规性审计，例如ISO27002和ISO27018中的相关控制要求。

18.1.3 知识产权

控制

同ISO/IEC 27002:2022中5.32

18.1.4 记录保护

控制

同ISO/IEC 27002:2022中5.33

18.1.5 隐私和个人可识别信息保护控制

同ISO/IEC 27002:2022中5.34

18.1.6密码控制规则

控制

同ISO/IEC 27002:2022中5.31

18.2 信息安全评审

18.2.1 介绍

同ISO/IEC 27002:2022中5.35、5.36、8.8确保依据组织策略和规程来实现和运行信息安全。

18.2.2 信息安全的独立评审

控制

同ISO/IEC 27002:2022中5.35

保护PII的实施要求

如果个人利益相关方的审计不切实际或可能增加安全风险，组织应在签订合同前向潜在利益相关方提供独立证据，证明信息安全是根据PII控制者的策略和程序实施和运作的，只要提供了足够的透明度，PII控制者所选择的相关独立审计通常应是一种可接受的方法，用于满足相关方对PII控制者的处理操作过程的兴趣。

18.2.3 符合安全策略和标准

控制

同ISO/IEC 27002:2022中5.36

18.2.4 技术符合性评审

控制

同ISO/IEC 27002:2022中5.36、8.8

附件A

用于PII保护的扩展控制集

A.1 总则

本附件提供了新目标、新控制和新实施要求，构成了扩展控制集以满足保护PII的具体要求。

条款A.2描述了保护PII的一般性策略，而后续条款反映了ISO/IEC 29100中描述的隐私原则。

A.2 使用和保护PII的一般策略

目标：根据业务要求和相关法律法规，为PII保护提供管理指导和支持。

控制

参与处理PII的组织应制定使用和保护PII的策略。

保护PII实施要求

隐私策略应包含适当的声明（可单独制定隐私策略，也可作为现有政策的补充），以表明支持并致力于遵守适用的PII保护法律、合同要求和其他内部政策。

隐私和安全政策可能涵盖不同的主题，尽管它们密切相关。信息安全政策和隐私策略都应涉及信息的保密性、完整性和可用性，此外，隐私策略还应涉及同意和个人访问等主题。

ISO/IEC 29100提供了有关实施隐私框架的指南。PII保护策略应：

-适合组织的宗旨；

-对组织收集和处理PII透明；

-为制定保护PII目标提供框架；

-为保护PII的问题制定决策规则；

- 定义隐私风险接受准则（另见ISO/IEC 29134的6.3.1）；

-包括承诺满足适用的隐私保护要求；

-包括对持续改进的承诺；

-在组织内传达和酌情提供给感兴趣的各方。

A.3 同意和选择

A.3.1 同意

目标：通过行使有意义、知情、自由的同意权，使PII主体积极参与有关处理其PII的决策过程，除非法律和法规另有限制。

控制

组织应为PII主体提供必要的手段,以行使有意义的、知情的、明确的和自由的同意权,除非：PII主体不能自由拒绝同意，适用法律允许在没有主体同意的情况下处理PII。

保护PII的实施要求

组织应该：

a)确定获得PII主体同意的流程，并分析所选择的流程不可用的情况下，确定替代解决方案，以确保在任何处理开始前获得同意；

b)在可行、适当、法律上要求的情况下，为PII主体提供同意的手段，以确保在任何处理开始前获得同

意。

处理内容包括收集，存储，更改，检索，咨询，披，识别，名，传播或以其他方式提供，删除或销毁PII；

c)在法律代理人(例如代表儿童或法定无行为能力的人)提供同意的情况下，存储同意记录；

d)如有必要，向PII主体通报PII转让给第三方的所有情况，并为PII主体提供他们同意此类转让的适当方式；

e)在任何新的使用或披露先前收集的PII之前，从PII主体获得同意，并确保在进一步处理开始前获得该同意；

f)确保在处理目的方面以知情和透明的方式获得同意，并确保为某一种特定目的而获得同意；

g)例如通过更新的公告通知；

h)为PII主体修改其同意范围提供了一种机制：

任何修改同意都应该及时采取行动，并且应该根据修改后的同意，修改或停止处理。

i)确保同意遵守所有适用的法律要求，包括在适当情况下明确同意敏感PII的要求；

j)在适当的情况下，允许隐含的同意，其中PII主体已经清楚地知道处理并且没有反对；

k)在所有加工操作实施之前事先通知所有加工操作；

1)在需要时确认PII主体或PII主体授权代理人的身份，提交处理同意书；

要求评审的信息应保持在最低限度，只有在必要时才能保留，并且在不再需要时应妥善处理，

其他信息用于保护PII

根据适用法律，组织应通过选择或默示同意方式获得同意，选择同意是首选的方法，但并不总是可行的，选择加入，则要求PII主体应采取肯定行动，允许组织收集或使用PII，如果使用电子介质收集同意，则组织应确定是否需要简单的选择，或是否需要双重选择。

如果选择退出，组织可以假定PII主体已经隐含同意处理其PII，除非PII主体采取肯定行动以其他方式发出信号。

默示同意通常是由个人的行为、缺省行为、特殊情况推断出来的。

默示同意示例：客户向在线零售商提供送货地址，零售商严格使用该信息以交付客户购买的商品。

在收集识别号码(例如，社会安全号码，居民身份证号码，护照号码)时，组织应提供切实可行的手段以获得PII主体的单独同意。

例如，组织可以提供PII主体的分项选择，以便他们为了不同目的而联系他们。在这种情况下，组织会建立同意机制，以确保组织的运营尽可能符合PII主体的选择。

根据适用的监管要求和实际考虑，同意可以是电子版或硬拷贝。

如果PII转移到另一个组织或从另一个组织转移而来，那么组织应建立一个更新其记录的流程，以反映PII主体做出的内容更新和同意变更(例如，修改，撤销)，并确保这些更新/更改将传递给与其共享PII的组织。

只有确保所需记录、更新的信息最小量，才能从PII主体收集并与其他组织共享。组织应定期审查他们的过程，以确保不会处理不必要PII。

A.3.2 选择

目标：在适当和可行的情况下，向PII主体提供：不允许控制者处理PI、拒绝、撤回同意、反对特定类型处理的选择；并向PII主体解释，投予或拒绝同意的含义。

控制组织应向PII主体提供清晰，突出，易于理解，可访问和负担得起的机制，以便主体行使选择权，但PII主体不能自由同意，或适用法律明确允许在未经PI委托人同意的情况下处理PII除外。

保护PII的实施要求

组织应该：

a)确保PII主体在处理其 PI时能够做出选择，然后再进行处理；

b)拒给PII主体提供与该服务无关的服务；

c)在相关立法或条例规定的情况下，确保PII主体拥有能够行使其反对处理PII权利的手段；

PII主体应获得多种行使该权利的手段(例如，通过邮件，电子邮件，电话)。

d)在适用法律规定的时间范围内或组织政策中规定的时限内确认异议声明；

e)分析所选择措施失效的情况，并在必要时确定备用解决方案，以便PII主体能持续、及时的行使其反对权利；

f)确保PII的分类，标签和存储方式有利于行使反对权，并确保PII主体能够及时无偿地行使其反对权；

8)确认PII主体或PII主体授权代理人的身份，对处理提交异议要求验证的信息应保持在最低限度，只有在必要时才能保留，并且在不再需要时应妥善处理；

h)如果PII主体依法行使诉讼,客体应为异议提供了合理的解释任何拒绝遵守异议应详细说明为什么不认为PII主体的这些理由是合法的；

i)确保与PII共享的所有组织都知道PII主体提交的所有的异议,并且他们遵守了这些有效的反对意见;

j)在可能的情况下，为PII主体提供反对处理部分PII的能力，而不必接受或反对整个处理。

其他信息用于保护PII

在许多情况下，根据适用法律，在收集公开可用信息时提供一种机制来行使选择的机制可能并非必要或可行。例如当从公共记录或报纸上收集他们的姓名和地址时，无需提供一种机制来为PII主体提供选择。

A.4 目的合法性

A.4.1 目的合法性

目标:确保处理PII的目的符合适用法律，并依赖于可允许的法律依据。

控制

组织应采取适当措施确保PII处理符合适用法律并依赖于可允许的法律依据保护PII的实施要求。

组织应该:

a)提出的处理是基于法律基础(例如，执法、公共安全、法律义务或PII主体的合法利益)的同意进行的；

b)确定拟处理过程是否受法律(例如执法，公共安全或法律义务)的约束，该法律禁止PII主体在处理其PII时行使其选择权；

注:如果PII的收集或处理是在国际上执行的，则在适用的不同法律框架下，需要同意以及处理它的正确方法可能会有所不同。

c)使用特定的流程或信息系统，确定允许处理PII的合法权限；

d)确保处理流程符合所有适用的法规、主管当局的解释。在确定其目的的合法性时，应考虑处理的情况包括：PII控制者与PII主体之间潜在关系的性质，科学技术发展、社会和文化态度的变化。

组织应制定程序确保PII的处理不以违反或可能违反法律义务的方式进行,包括法定条款普通法或合同条款。

如果组织有工作委员会或工会，按照适用的法律，处理雇员的PI时，要求与这些机构协商。

收集记录PII应咨询负责PII保护的人(有时称为CPO)，或者就收集PII的计划或活动的授权时，同法律顾问进行咨询。

A.4.2 目的要求

目标：在不迟于收集个人身份信息时指出收集个人身份信息的目的，并限制后续使用以达到原始目的。

控制

组织应该与他们将要收集的PII主体沟通，明确收集、处理PII的目的。这样的通信应该在PII被收集之前。

保护PII的实施要求

组织应在收集或首次使用信息之前向PII主体传达目的,使用本规范的语言要既清楚又适合于具体情况，并在处理敏感的PII时给出充分的解释，通常，应用法定语言明确的授权PII具体收集和使用。当法定书面语言被广泛书写并因此需要解释时，组织应与CPO和法律顾问协商，确保授权与具体的PI收集之间存在明确的联系。一旦确定了具体目的，当组织用于收集PI时，应在相关的隐私合规文件或表格中明确说明目的。此外，为避免未经授权收集或使用个人识别信息，处理个人识别信息的人员应接受组织机构的培训。

组织应该：

a)确定PII 仅在业务流程中使用；

b)以逻辑方式分离对每个过程有用的PII；

c)业务流程(包括工资管理，休假请求管理，职业发展)管理不同的访问权限，并建立专门的IT环境处理最敏感的PII的系统；

d)定期确认PII有效分离，未被授权的人不能接入网络。

A.5 收集限制

目标：将PII的收集范围限制在适用法律界限范围内，并且严格限于满足特定需求的范围内。

控制

组织应实施适当的措施，将PII的类型、数量的收集限制在通知(见A.9.1)和适用法律法规范围内的最小元素。

保护PII的实施要求

组织应该：

a)将PII的收集范围限制为通知所述目所确定的最小元素(见A.9.1)，并且PII主体已经同意；

b)不收集敏感的PII，除非收集敏感的PII得到合法授权或获得同意；

c)限制间接的从PII主体收集的信息量(例如，通过网络日志，系统日志)。

组织应确定处理PII的目的，确定实现该目的所需的PII，确定不需要收集的信息，并确认仅收集基本信息。

在继续收集之前，组织应仔细考虑需要收集哪些PII以实现特定目的。组织不应该不分青红皂白地收集PII。

定期审查其收集PII的目的，以确保其仍然有效。他们还应该定期审查他们正在收集的个人身份信息，以确保它仍然只是达成该目的所需的最基本元素。

除非获得收集此类信息的合法授权，否则组织不应收集敏感的PII，例如国家识别号码(身份证、护照、社会保险号)。

其他信息用于保护PII

一些同法管辖区可能将某些类别的PII(例如科族出身，政治观点、宗教或其他信仰、关于健康的个人数据、性生活、刑事定罪等)定义为敏感。这些同法管辖区可能会对收集这类PII施加限制或条件，组织在决定收集PII时应考虑这些限制和条件。

A.6 数据最小化

目标：控制者处理 PI应限制在为达到合法利益所必需的最低限度，并将PII隐私的披露，限制到最低数量的利益相关者。

控制

组织应采取适当措施，将正在处理的个人身份信息的数量减至符合个人信息管理控制人合法利益的程度(例如，组织可寻求增加或延长其业务运营的方式，合法增加PII处理和存储)。

保护PII的实施要求

组织应该：

a)确保采用“需要知道”的原则，只有在PII处理的合法目的框架内，才可获得职责所必需的PII的访问权；

b)使用和提供默认选项时，尽可能不包含PII主体的身份；

c)限制PII 收集的可联系性；

d)对组织保留的个人身份信息进行初步评估，并制定、遵循定期对其进行审查的时间表以确保仅收集通知中确定的个人身份信息，并且仅限于为了达成业务目的，有必要继续使用；

e)将包含PII的电子文档传输给与其工作相关的利益相关者，利益相关者应最小量化；

f)依据PII的存储形式(例如数据库字段或文本摘录)和风险识别，确定应对哪些PII进行匿名或去标识化；

g)基于待识别数据的形式(例如，数据库和文本记录)和所识别的风险，去标识这些数据；

h)当PII处理的目的已经过期时，又没有法定义务需要保留PII，应删除和处置PII；

i)考虑采用隐私增强技术 (PET)

支持特定组织业务流程所需的最小量的PII元素，可能是该组织被授权收集的PII的子集。应将PII分类为：强制性PII、可选PII，以供收集。

在收集可选的PII时，组织应仅收集提供服务所需的强制性PII，并从PII主体获得适当的同意。当PII

主体拒绝提供可选的PII时，组织不应拒绝提供服务。

CPO和法律顾问应该提出PII处理合理性的质疑和建议，以确保信息系统或活动达到法定授权目的的最低限度。

注1：ISO29100中定义的匿名化是一种过程，通过该过程，PII不可逆转地改变，使得PII主体不能直接、间接的被识别。这样的过程必然涉及(不可逆转的)信息丢失，在某些情况下，只要删除部分数据可以达到所需的目标。

注2：根据ISO29100中的隐私原则，隐私增强和去标识技术，被用来描述和设计去身份识别措施，作为符合本国际标准的计划。为了鉴别过程符合法律的结论，可以通过删除或概括属性、强有力的组织和技术措施，来进行识别过程。

注3：当为某种目的处理个人身份信息时，处理的个人身份信息的范围应被最小化，以便仅用于预期目的，而不会泄露主体的过多信息，例如，交通相关调查的答复者的地理区域，需要考虑只收集附近的地标而不是确切的地址。

注4：当输出是一个小数据集时，通常在分析匿名数据时，可以揭示PII主体的身份。因此，当记录数量小于阈值数量时(例如10条记录，防止输出是一种好的做法。根据数据分布模式，需要仔细设计输出阈值。在适当的情况下，组织应该通过减少他们的PI库存来降低他们的隐私和安全风险。组织应对其持有的PI进行初步审查和随后的审查，在最大可能的范围内确保这些数据堆栈的准确性，相关性，及时性和完整性。

组织也应该被指示将其PII持有量减少到履行业务目的所需的最低限度。组织应制定并公布定期审查其数据堆栈的计划，作为初始审查的补充。

通过定期评估，组织可以降低风险，确保他们仅收集通知中指定的数据，并确保收集的数据仍然是相关且必要的。

A.7 使用、保留和披露限制

A.7.1 使用、保留和披露限制

目标：为了具体的，明确的和合法的目的限制PII的使用和披露，保留的PII不能超过实现所述目的或遵守适用的法律。

控制

各组织应采取适当措施限制PII的处理，以用于合法目的和预期目的，并且仅在必要时保留PII，实现所述目的或遵守适用法律。

保护PII的实施要求

组织应该：

a)将PII的使用，保留和披露(包括转让)限制在为实现特定，明确和合法目的必要的范围内；

b)配置其信息系统，以记录：收集，创建、更新PII的日期、何时将PII 删除、归档的时间。

保护PII的实施要求

组织应该：

a)当所述目的已经过期时，锁定(即归档，保护和免除进一步处理)任何PII，并满足适用法律的保留要

求；

b)使用适当的技术或方法确保安全删除或销毁PI(包括原件，副本和存档记录)；

c)仅将PII用于在收集之前或收集时向PII主体商定披露的目的，并且在为任何新用途进行之前获得必要的同意；

d)将外部组织对PII的访问权，限制在必要且已获得正式授权的范围内。

如果业务确实需要访问，则应遵循适当的审批程序。

e)确认被允许连接到本组织系统的外部系统在被允许连接之前已经实施了适当的保护措施；

f)定期审查第三方实施的保障措施，以确保它们继续满足本组织的安全要求：如果由于此类审查而发现保障措施不足，应立即断开第三方的连接，直到已经恢复了适当的保障措施；

g)当通过远程接口访问PII时，实施适当的访问认证机制：记录PII访问的日志；

h)利用安全监控持续收集PII的变更，应向公众提供警示。

保护PII的实施要求

组织应该：

a)仅保留授权时间段的PII，以履行通知中确定的目的或法律和组织的要求，并在保留期届满时立即删除PII；

b)如果需要保留PII的时间超过特定商业目的所需时间，则应实施诸如去识别化等措施以保护PII；

c)定义有时间限制的、适合于处理目的的PII保留期；

d)确认信息系统可以检测到保留期限到期；

e)确保实施商定的保留期限并根据保留期限处置PII；

f)开发一种自动化功能，在其保留期限到期时删除PII，这种删除应立即发生或尽快实施；

g)PII的存储形式(包括数据库字段或文本摘录)以及确定的风险，应该是“去标识”的内容；

h)根据待识别数据的形式(包括数据库和文本记录)和已确定的风险，去识别化数据；

i)如果数据不能被“去识别”，则选择用于保护PII的工具(包括部分删除，哈希，密钥散列和索引)。

保护PII的实施要求

组织应该：

a)未经PII主体事先知情同意,不得将PII披露给外部各方，除非相关法律允许此类披露:如果向需要了解的内部各方(例如员工)披露,则可能不需要PII主体的知情和同意；

b)在转让个人身份信息时提供强有力的保护机制，包括数据加密和完整性保护。员工个人身份信息应按照适用的法律和法规、组织处置策略，适当情况下需征得员工同意才能进行处置(即安全删除或存档)。

A.7.2 安全删除临时文件

目标：提供在特定时期内删除临时文件的技术措施。

控制

临时文件和可能包含个人身份信息的文件应在指定的记录期内处置保护PII的实施要求。

信息系统可能会在正常的操作过程中创建包含PII的临时文件。

临时文件是特定于系统和应用程序的文件，可能包括具有回滚功能的文件系统、与更新数据库和其他

应用程序软件操作相关的临时文件。相关信息处理任务完成后通常不需要临时文件，但有些情况下可能不会自动删除它们。这些文件保持使用的时间长度并不总是确定性的，但“无用数据收集”过程应该识别相关的临时文件，并确定它们上次使用的时间。

PII处理信息系统应执行定期检查，以确保删除指定超出日期未使用的临时文件。

A.7.3PII披露通知

目标：确保PII处理者向PII控制者通报任何披露PII的具有法律约束力的请求。

控制

PII控制者与PII处理者之间的合同应要求：依据法规，PII处理者根据合同中约定的流程和时间段，向PII控制者通报披露PII的请求，除非法律另有禁止。

保护PII的实施要求

组织应实施措施(例如合同义务)以确保：

a)除法律另有禁止外，PII处理者在披露PII请求之前，应先咨询相关的PII控制者；

b)除非法律另有规定，PII处理者应接受经相关PII控制方授权的披露请求。

A.7.4 记录PII披露

目标：确保将 PI披露给第三方。

控制

应记录PII向第三方的披露情况，包括披露哪些PII，何时向何人及为何目的。

保护PII的实施要求

PII可能在正常运营过程中披露。这些披露应该被记录下来。任何对第一方的额外披露，例如合法调查或外部审计引起的披露，都应该记录在案。记录应包括披露的权力来源。

A.7.5 披露分包的PII处置

目标：确保PII处理者向PII控制者披露任何分包商的使用情况。

控制

PII处理者使用分包商处理PII，应事先向PII控制者披露。

保护PII的实施要求

应在PII处理者与PII控制者之间的合同中约定使用分包商处理PII的规则。合同中应规定分包商只能在获得PII控制人的事先授权的情况下进行外包。

PII处理者应及时通知PII控制者有关此方面的任何预期变更,以便PII控制者有能力反对此类变更或终止同意。

披露的信息应包括:使用分包的情况和相关分包商的名称,但不包括任何特定的业务细节披露的信息还应包括分包商可能处理数据的国家和分包商有义务达到或超过PII处理者义务的方式。

在评估分包商信息的公开披露所增加安全风险没有超出可接受的范围内,应根据保密协议或应PII控制者的要求进行披露。应使PII控制者知道分包商信息是可用的。

A.8 准确性和质量

目标：确保PII处理的准确性，完整性，最新性，充分性和相关性以达到使用目的。

控制

组织应采取适当措施确保从PII主体直接或间接收集的PII具有适当的质量。

保护PII的实施要求

实现数据质量意味着正在处理的PII是准确的，具有足够的精确度，完整性，最新性，充分性和适用性。

组织应该：

a)建立PI收集程序，以确保准确性和质量；

b)收集PII的方式是，任何修改在离开权威来源后都可以被检测到；

c)在收集或创建PII时，尽可能确认PII的准确性，相关性，及时性和完整性；

d) 确保在处理PII之前从PII主体以外的渠道收集的PII的可靠性；

e)在对PI做出任何修改之前，通过适当手段核实PII主体提出的纠正请求的正确性和有效性；

f)定期检查并根据需要纠正:其程序或系统使用的任何不准确或过时的PII；

g)制定准则，确保传播信息的准确性，完整性，充分性和相关性最大化。组织应采取合理措施确认PII的准确性。这些步骤可以包括：使用自动地址验证查找APII，将地址收集或输人到信息系统中进行编辑和验证。

当PII具有足够的敏感性时(例如，当它用于每年确认纳税人的收人以获得经常性收益时)。

组织应将机制纳人信息系统，并制定相应的程序：多久、通过什么方法，信息将被更新。为尽量减少数据不准确的范围，应尽可能将PII直接由PII主体录入信息系统，而无需另一人录人数据。但是，如果PII的转录是不可避免的，组织应考虑启用PII主体来验证转录的PII，这有助于在处理不准确的PII导致的间接损害之前纠正错误。

其他信息用于保护PII

为保护数据质量采取的措施类型可能基于：PII的性质和背景、如何使用、如何获得。为验证任何敏感PII的准确性而采取的措施应该比用于验证较不敏感PII的措施更全面。可能需要执行其他步骤来验证从PII主体或PII主体的授权代表以外的渠道获得的PII。

A.9 公开性，透明度和通知

A.9.1 隐私声明

目标：确保隐私声明包含适当的细节，用简单的语言编写，并且易于访问。

控制

组织应采取适当措施，向PII主体提供适当的PII处理目的通知。

保护PII的实施要求

组织应该：

a)向PII主体提供有关下列事项的有效通知：

1)影响隐私的活动，包括但不限于：收集，使用，共享，保护和安全处置PII；

2)收集PII的权利；

3)PII主体的选择：同意组织如何使用PII的后果；

4)反对处理的能力。

b)提供适合运营需求的通知和许可机制；

c)在变更之前或之后尽快修改其通知，以反映影响PII的实施或策略的变更；

d)根据个人身份信息的性质，提供通知所选择的方法，考虑个人身份信息管理员与个人信息负责人之间的关系，确保通知对目标受众是完整和适当的；

e)以不熟悉信息技术、互联网、法律术语的人，可以理解的清晰方式提供信息,f确保通知在PII收集之前或之时提供；

f)确保在未提供通知的情况下无法收集个人身份信息；

h)如果现行方法失效，则确定替代解决方案；

i)如果可能的话，提供一种方式来表明提供了通知；

j)如果通过实际手段提供隐私声明，请将此信息在PII主体应该看到、要求签署的文件的上标志；

k)提供一项策略，告知PII主体相关标签、标记技术正在被使用[如:闭路电视(CCTV)系统,WiFi和射频识别 (RFID)]。

应尽可能在收集点(例如，在组织的网站或实际位置)突出显示通知，而不需要PII主体主动发出请求。

A.9.2 公开性和透明度

目标：向PII主体提供关于PII控制人清晰且易于获取的策略信息，有关处理PII的程序和做法。

控制

组织应实施适当的措施，向PII主体提供有关PII处理的策略，程序和实践的适当信息。

保护PII的实施要求

组织应该：

a)向PII主体提供关于PII控制方有关策略,，程序和实践的清晰且易于获取的信息；

b)披露PII控制方为了限制，访问，纠正，删除其信息，而向PII主体提供的选择和方式。

另外，组织应该描述：

a)组织收集的PII和收集该信息的目的；

b)组织如何在内部使用PII；

c)该组织是否与外部实体共享PII，这些实体的类别以及此类共享的目的；

d)PII主体是否有能力同意PII的具体使用或分享以及如何行使此类同意权；

另外，组织应该描述：

e)PII将被保留多久；

f)组织是否销售或转发数据以供数据分析组织处理，以及适用于PI风险的控制细节；

g)在适当的情况下，PII主体如何获得PII的访问权限，以便修改、更正；

h)关于个人身份信息如何得到保护的适当信息；

i)确保PII主体获得其隐私活动信息的访问权，并能够与其CPO进行沟通；

j)根据要求提供有关隐私违规的信息，这些信息已经或可能导致了请求人PII的隐私泄露，以及请求人可以采取的相关行动，以减轻由于违规所引起的额外风险。组织还应该采用不同的机制向公众宣传他们的隐私惯例，包括但不限于PIA报告，隐私报告，公开可用网页，电子邮件发布，博客和定期出版物(例如季

度通讯)。组织还应该使用面向公众的电子邮件地址或电话热线，以便公众提供反馈，或向隐私办公室提出有关隐私惯例的问题.

A.10PII主体参与和访问

A.10.1 主体访问

目标：为PII主体提供访问和审核其PII的能力，并对其准确性和完整性提出质疑。

控制

各组织应采取适当措施，为PII主体提供访问其PII的能力，并获得PII的更正或删除PII。

保护PII的实施要求

组织应该：

a)在适用法律允许的情况下，类似于最初收集PII的方法(例如通过邮件或电子邮件)，采用PII主体可以理解和接受的形式，使得个人应该能够及时行使这一访问权；

b)分析所选择的方法不可用的情况，在必要时确定备用解决方案；

c)向PII主体提供访问组织所持有的PII的权利，以评估其准确性并在必要时更正；

d)在可能的范围内，答复应以与提出请求相同的形式提供(例如，如果请求是通过普通邮件提出的，应以普通邮件提供答复)；

e)发布关于PII主体如何请求访问其系统中记录的规则和条件；

f)允许PII主体直接或间接对PII的准确性和完整性提出质疑，并在可能的情况下对其进行修改，更正或删除；

g)制定程序，使PII主体能够以简单，快速和有效的方式行使这些权利，而不会造成不适当的延误(例如，应根据适用的立法或法规或按照组织策略的规定提供回应)或成本；

h)建立一个程序，通知PII主体提交：其请求和成功处置的状态(例如，通过邮寄或电子邮件，注意的是:已收到请求以及他们可能收到答复的日期)，对于已存档的档案，如果PII控制者通知PII主体提交请求处理的时间表，并提供了合理的响应时间，那么在答复日期方面可能需要留有一些余地；

i)在法律允许的范围内，确保始终可以行使获取权;

j)确保PII只能由与该信息相关的人或该人的授权代理人访问:这可能要求请求访问的人以令人满意的方式证明自己(基于适用的法律或法规，可以要求此类身份验证)；

k)如果需要识别和验证请求者，除非法律或法规另有规定，否则应确定适当的身份识别和身份验证形式：组织应仅要求提供确保正确识别所需最低限度信息；应妥善保护这些信息，并应只要有必要才能保留；

l)确保只将PI发送给相关的PII主体，并以安全的方式发送；

m)确保可以提供PII主体可能要求的所有信息，同时仍保护其他PII主体的PII信息；

n)在隐私声明中通知他们是否打算就访问征收任何费用(在某些同法管辖区，这可能是法律允许的)；

o)要求PII处理者支持PII控制者，以促进PII主体对其数据的访问、更正或删除权利的行使。

PII主体应拥有审香组织记录系统中保存的PII的访问权，访问包括及时，简化和廉价的数据访问，允许访问记录的组织，可能因资源，法律要求，其他因素而异。

A.10.2 补救和参与

目标：对披露个人数据的PII处理者和第三方提供修改，更正或删除。

控制

除非相关立法或法规禁止，组织应采取适当措施，为PII主体提供纠正，修改或删除组织维护的PII，组织还应建立一种机制，通过该机制将任何更正，修改或删除通知PII处理者,并尽可能通知披露个人身份信息的第三方。

保护PII的实施要求

组织应该：

a)确保委托人总是可以行使纠正的权利；

b)分析所选择的实际手段失效时，有必要的备用解决方案；

c)在相关立法或法规允许的范围内，确保PII主体能够行使更正权；

d)确保所要求的更正的准确性；

e)确保PII主体提交的请求得到确认；

f)确保可能被发送第三方的PII被告知改正；

g)为PII主体提供仅访问他们需要纠正，修改和删除的PI的权限。

A.10.3 投诉管理

目标：建立有效的内部投诉处理和纠正程序，以供PII主体使用。

控制

组织应采取适当措施，有效处理来自PII主体的投诉。

保护PII的实施要求

组织应该：

组织应实施投诉管理流程，并保持一个联系点，以接收和回应PII主体关于组织隐私惯例的抱怨，疑点或问题。

各组织应提供以下投诉机制:PII主体随时可以访问这些投诉机制，包括成功提交投诉所需的所有信息(包括 CPO 或指定接受投诉的其他官员的联系信息)且易于使用。

组织投诉管理流程应包括跟踪机制，以确保所有投诉都得到及时审查和适当处理。投诉管理还应包括由投诉引发的纠正措施。

其他信息用于保护PII

来自PII主体的投诉，担忧和问题可以作为外部输人的宝贵来源，最终改进运营模式，技术使用，数据处理实践以及隐私和安全保护措施。

A.11 问责制

A.11.1 治理

目标：建立有效的PII治理。

控制

组织应采取适当措施，建立与PII处理相关的有效治理保护PII的实施要求。

组织应该：

a)任命一名负责制定、实施、维护整个组织范围内治理隐私的人员，确保遵守所有和信息系统处理P相关的适用法律、法规；被指定的人员可以是CPO；董事会成员可以在专职工作人员的支持下承担该责任；

b)确保被任命的人员具有监督PII处理的必要专业知识；

c)确保指定人员参与与保护个人识别信息有关的所有问题，并能及时向高级管理层报告；

d)向指定人员提供履行其任务所需的人力资源，场所，设备和其他资源；

e)为影响PII保护计划的变更提供隐私法律和策略符合性的监测过程；

f)开发、发布和执行PII的保护策略和程序，管理PII的保护和安全控制，包括：PII的程序信息系统、技术；

g)定期更新PII保护计划，策略和程序；

h)定期监督组织对PII保护的表现；高级管理层代表或董事会成员应该对其进行管理，以便定期对量化指标，风险和违规等方面的可见性进行管理。

A.11.2 隐私影响评估

目标：建立隐私影响评估流程，并在必要时执行隐私影响评估。

控制

如果一个组织正在处理PII，那么组织应该建立进行PIA所需的程序。

保护PII的实施要求

隐私影响评估通常由认真负责并充分对待PII原则的组织进行，在某些国家地区，PIA可能需要满足法律和监管要求。ISO/IEC29134可以用作PIA的指导。

在执行隐私风险评估时，组织应考虑资产，威胁，漏洞和安全措施(现有和建议)，组织应该：

a)PIA 的结果，包括但不限于正在处理的PII；

b)确定的隐私风险；

c)拟定的控制措施。

A.11.3 承包商和PII处理者的隐私保护要求

目标：通过合同或其他方式(如内部的强制性策略)确保第三方接受者至少提供同等水平的PII保护。

控制

各组织应采取适当措施，确保承包商和PII处理商实施适当水平的PII保护。

保护PII的实施要求

组织应该：

a)服务级别协议中规定了PII处理者必须满足PII保护要求；

b)监督和审核承包商对这些要求的执行情况；

c)为承包商和PII处理者建立PII保护的角色和责任；

d)通过合同确定提供服务的时间框架，PII处理程序，处理PII的程度，方式和目的，以及处理的PII的类型；

e)在服务结束后，终止任何管理协议，或根据PII控制人的请求，PII处理者应返还或安全处置PII的条件；

f)包含一个保密条款，对承包商及其任何可能能够访问 PI的员工均具有约束力；

g)除非合同中明确允许，确保服务承包商不会将PII传达给第三方(即使仅仅是为了保存);h)阐明服务承包商在发生影响PII的数据泄露事件时，具有通知PII控制人的义务；

i)通过合同确定，服务承包商应通知PII控制者有关服务的相关变更，例如执行了其他功能；

j)文件化并酌情沟通所有与PII保护相关的策略，程序和做法。

组织应向法律顾问，CPO和合同人员咨询可能影响本控制措施实施的适用法律，指令，策略或法规。

注：还应实施15.1.2的其他要求。

其他信息用于保护PII

承包商和PII处理者可能包括但不限于服务部门，信息提供者，信息处理者、提供信息系统开发，信息技术服务和其他外包应用的组织。

A.11.4 隐私监督和审核

目标：监测和审核个人身份信息保护控制措施和内部个人身份信息保护政策的有效性。

控制

监测和审核个人身份信息保护控制措施和内部个人身份信息保护策略的有效保护PII的实施要求。

组织应该：

a)定期监督和审计PII处理操作，尤其是涉及敏感PII的处理操作，确保其符合适用的法律,法规和合同条款；

b)定期监督和审核PII保护控制和策略，确保其符合适用的法律，法规和合同条款；

c)确保审核工作由合格的独立方(组织内部或外部)进行；

d)如果使用内部资源进行审核，则宜定期让外部方进行审核，以进行独立的评估。

A.11.5PII保护意识和培训

目标：为将有权访问PII的PII控制人员提供适当的PII保护培训和意识。

控制

组织应采取适当措施为PII控制人员提供适当的培训。

保护PII的实施要求

组织应该：

a)实施和维护全面的培训和意识战略，旨在确保人员了解他们的 PI保护责任和程序；

b)建立机制，以使员工及时更新在管理、合同和技术环境的发展中对PII的保护责任，从而影响组织的隐私遵守；

c)定期(例如，每年)或根据需要(例如，事件发生后)，对基于角色的PII保护培训进行管理，这对于偶尔处理PII的活动尤为重要；

d)确保人员定期(手动或电子方式)接受PII保护要求的责任。

A.11.6PII保护报告

目标：制定，传播和更新PII保护报告。

控制

各组织应酌情制定，散发和更新报告(例如报告违规行为，调查，审计)给负责监督PII保护的高级管理层和其他人员，以证明满足具体的，法定和监管PII保护计划的责任要求。

保护PII的实施要求

通过外部和内部PII保护报告，组织应促进保护操作的度量和透明度。报告还可帮助组织确定满足PII保护合规性要求和PII保护控制的进展情况，比较整个组织的绩效，找出策略和实施中的漏洞和差距，并确定成功模式。

A.12 信息安全

目标：确保PII根据风险评估的结果得到适当的保护。

控制

根据风险评估或PIA 的结果，通过适当的控制来保护组织的PII。

保护PII的实施要求

组织应该：

a)在运营功能和战略层面采用适当的控制措施保护PII，以确保PII的完整性，机密性和可用性，在其生命周期内保护其免受未经授权的访问，销毁，使用，修改，披露;

b)选择个人识别信息处理的适当合同，为PII的处理在组织，物理和技术控制层面提供充分控制要求并确保遵守这些控制措施;

c)根据适用的法律要求、安全标准、ISO31000中描述的系统安全风险评估结果、成本效益分析结果，进行基本安全控制;

d)PII的访问权限制在那些需要这样的访问权来履行其职责的个人,并限制他们只能访问为履行其职责而访问必要的PII;

e)解决通过隐私影响评估和审核流程发现的风险和漏洞;

f)在持续的安全风险管理过程中对控制进行定期审查和重新评估;

安全要求有时是由某些数据隐私法律规定的，在这种情况下，应将这些安全要求传达给数据安全功能责任者，以供实施。

在设计和实施安全控制时应该尽职尽责。

A.13 隐私合规

A.13.11合规性

目标：避免违反与隐私、任何隐私要求相关的法律，法规，监管，隐私策略或合同义务。

控制

组织应采取适当措施确保PII处理符合合规要求。

保护PII的实施要求

组织应该：

a)制作年度报告，详述现有风险，陈述合规立场，包括未完成行动的总结;

b)遵循明确的违规响应流程，在某些同法管辖区可能包括通知PII主体和其他机构(如数据保护机构)的要求。

A.13.2 某些国家地区的跨境数据转移的限制

目标：保护跨境转移的PII。

控制

组织应采取适当措施确保跨境个人身份信息的转移符合相关合规要求。

保护PII的实施要求

当PII需要转移到PII目前所在国家地区以外时，某些国家地区的数据隐私条例可能会施加限制，通常可能包括以下一项或多项：

a)通知数据保护机构；

b)获得数据保护机构的批准，特别是在数据敏感的情况下；

c)进行适当的尽职调查，确保通过跨境转移的PII获得与原产国相同的保护；

d)使用特定的数据传输工具，遵照：标准的合同条款、有约束力的公同规则(BCR)。组织应实施措施，检查是否有针对计划转移的特定限制，在执行之前被遵守。