INTERNATIONAL **ISO/IEC 27701**

STANDARD Frist Edition

2019.08

安全技术----

ISO/IEC 27001 和 ISO/IEC 27002 的隐私信

息管理扩展----

要求和指南

Reference number
ISO/IEC 27701:2019(E)

Contents

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业系统。作为 ISO 或 IEC 成员的国家机构通过各自组织设立的技术委员会参与国际标准的制定，以处理特定的技术领域活动。ISO 和 IEC 技术委员会在共同感兴趣的领域开展合作。与 ISO 和 IEC 联络的其他国际组织、政府和非政府组织也参与了这项工作。

用于开发本文档的程序和用于进一步维护的程序在 ISO / IEC 指令第 1 部分中有所描述。特别是，应注意不同类型文档所需的不同批准标准。本文件是根据 ISO / IEC 指令第 2 部分的编辑规则起草的（参见 www.iso.org/directives）。

需要注意的是，本文件的某些要素可能是专利权的主体。ISO 和 IEC 不负责识别任何或所有此类专利权。在文件制定过程中确定的任何专利权的详细信息将在收到的专利声明的引言和/或 ISO 列表中（参见 www.iso.org/patents）或 IEC 收到的专利声明清单中（见 http：//patents.iec.ch）。

本文档中使用的任何商标名称是为方便用户而提供的信息，并不构成认可。

有关标准的自愿性质的解释，与符合性评定相关的 ISO 特定术语和表达的含义，以及 ISO 在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请参阅 www.iso.org/iso/foreword.html。

本文件由联合技术委员会 ISO/IEC JTC 1 信息技术分技术委员会 SC27 安全技术编写。

有关本文档的任何反馈或问题，请直接与用户的国家标准组织联系。有关这些机构的完整列表，请访问 www.iso.org/members.html。

引言

0.1 概述

几乎每个组织都处理个人身份信息（PII）。此外，处理的 PII 的数量和类型正在增加，组织需要与其他组织合作处理 PII 的情况也在增加。在处理 PII 的背景下保护隐私是一项社会需求，也是全世界专门立法和/或监管的主题。

ISO/IEC 27001 中定义的信息安全管理体系（ISMS）旨在允许增加部门特定要求，而无需开发新的管理系统。ISO 管理体系标准，包括行业特定标准，旨在单独实施或作为综合管理体系实施。

PII 保护的要求和指导取决于组织的背景，特别是在存在国家立法和/或法规的情况下。ISO/IEC 27001 要求理解并考虑该背景。本文档包括映射到：

— ISO/IEC 29100 中定义的隐私框架和原则;

— ISO/IEC 27018;

— ISO/ IEC 29151;和

— 欧盟通用数据保护条例（DGPR）。

但是，这些可能需要解释为考虑到当地立法和/或法规。

本文档可供 PII 控制者（包括联合 PII 控制者）和 PII 处理者（包括使用分包 PII 处理者的那些处理者和处理 PII 作为 PII 处理者的分包商的处理者）使用。

符合本文件要求的组织将生成有关如何处理 PII 处理的文件证据。这些证据可用于促进与商业伙伴的协议，其中 PII 的处理是相互关联的。这也可以帮助与其他利益相关者建立关系。如果需要，可以将本文档与 ISO/IEC 27001 结合使用，对该证据进行独立验证。

该文件最初是作为 ISO/IEC 27552 开发的。

0.2 与其他管理体系标准的兼容性

本文件应用 ISO 开发的框架，以改善其管理体系标准之间的一致性。

该文档使组织能够将其 PIMS 与其他管理系统标准的要求匹配或集成。

安全技术–用于隐私信息管理 ISO/IEC 27001 和 ISO/IEC 27002 的扩展–要求和指南

1 范围

本文件规定了要求，对以 ISO / IEC 27001 和 ISO / IEC 27002 扩展形式建立、实施、维护和持续改进隐私信息管理体系（PIMS）提供指导，以便在组织范围内进行隐私管理。

本文件规定了与 PIMS 相关的要求，并为 PII 控制者和 PII 处理者处理 PII 承担的责任和义务提供指导。

本文档适用于所有类型和规模的组织，包括公有和私有公司，政府实体和非营利组织，这些组织是在其 ISMS 中 PII 控制者和/或 PII 处理者处理 PII。

2 引用标准

文中提到了以下文件，其中部分或全部内容构成了本文件的要求。凡是注日期的引用文件，仅引用的版本适用。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

ISO/IEC 27000, *Information technology — Security techniques — Information security management* systems *— Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 术语和定义

ISO/IEC 27000 和 ISO/IEC 29100 中给出的术语和定义适用于本文档 。

ISO 和 IEC 标准化的术语数据库可从如下地址获得：

— ISO 在线浏览平台：https://www.iso.org/obp

— IEC 电子百科全书：http://www.electropedia.org

— IEC Electropedia：availableathttp：//www.electropedia.org/

— ISO Online browsing platform：availableathttp：//www.iso.org/obp

3.1 **Joint PII controller 联合 PII 控制者**

与一个或多个其他 PII 控制者共同确定处理 PII 的目的和方法的 PII 控制者

3.2 **privacy information management system （PIMS）隐私信息管理体系**

处理受 PII 处理影响的隐私保护的信息安全管理系统

4 概述

4.1 文档结构

这是一个与 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013 相关的特殊成分的文档。

本文档重点介绍 PIMS 特定的要求。遵守本文档的基础是遵守这些特定要求和 ISO/IEC 27001:2013 中的要求。除了信息安全之外，本文件还扩展了 ISO/IEC 27001:2013 的要求，以考虑到可能受 PII 处理影响的 PII 主体的隐私保护。以便于更好地理解，被包含的有关实施指南和其他信息。

第 5 节给出了适用于作为 PII 控制者或 PII 处理者组织的 ISO/IEC 27001 中信息安全要求的 PIMS 特定要求和其他信息。

注 1：为完整起见，第 5 章包含了由 ISO/IEC 27001:2013 要求的每个条款组成的子条款，即使在没有 PIMS 特定要求或其他信息的情况下也是如此。

第 6 节给出了适用于作为 PII 控制者或 PII 处理者组织的 ISO/IEC 27002 中信息安全要求的 PIMS 特定要求和其他信息。

注 2：为完整起见，第 6 章包含了由 ISO/IEC 27002:2013 目标或控制措施的每个条款的子条款，即使在没有 PIMS 特定指南或其他信息的情况下也是如此。

第 7 节为 PII 控制者提供了额外的 ISO / IEC 27002 指南，且第 8 节为 PII 处理者提供了额外的 ISO / IEC 27002 指南。

附件 A 列出了作为 PII 控制者的组织的 PIMS 特定控制目标和控制措施（无论是否使用 PII 处理者，以及是否与另一个 PII 控制者共同作用）。

附件 B 列出了作为 PII 处理者的组织的 PIMS 特定控制目标和控制措施（是否将 PII 的处理分包给独立的 PII 处理者，包括那些作为分包商处理 PII 的 PII 处理者）。

附件 C 包含 ISO/IEC 29100 的映射。

附件 D 包含本文件中的控制措施与欧盟通用数据保护条例（GDPR）的映射。

附件 E 包含 ISO/IEC 27018 和 ISO/IEC 29151 的映射。

附件 F 解释了在处理 PII 时 ISO/IEC 27001 和 ISO/IEC 27002 如何延伸到隐私保护。

4.2 ISO/IEC 27001:2013 要求的应用

表 1 给出了本文档中与 ISO / IEC 27001 相关的 PIMS 特定要求的位置。

表 1 ---- 在 ISO/IEC 27001:2013 中实施控制措施的 PIMS 特定要求和其他信息的位置

ISO/IEC 27001:2013 条款	标题	本文档的子条款	备注
4	组织情景	5.2	附加要求
5	领导力	5.3	没有 PIMS 特定要求
6	计划	5.4	附加要求
7	支持	5.5	没有 PIMS 特定要求

8	**运行**	**5.6**	**没有 PIMS 特定要求**
9	**绩效评估**	**5.7**	**没有 PIMS 特定要求**
10	**改进**	**5.8**	**没有 PIMS 特定要求**

注：即使没有 PIMS 的特定要求，依据 5.1 的“信息安全”的扩展解释也始终适用。

4.3 ISO/IEC 27002:2013 指南的应用

表 2 给出了本文档中与 ISO / IEC 27002 相关的 PIMS 特定要求的位置。

表 2 ---- 在 ISO/IEC 27002:2013 中实施控制措施的 PIMS 特定要求和其他信息的位置

ISO/IEC 27002:2013 条款	标题	本文档的子条款	备注
5	**信息安全策略**	**6.2**	**附加指南**
6	**信息安全组织**	**6.3**	**附加指南**
7	**人力资源安全**	**6.4**	**附加指南**
8	**资产管理**	**6.5**	**附加指南**
9	**访问控制**	**6.6**	**附加指南**
10	**密码学**	**6.7**	**附加指南**
11	**物理环境安全**	**6.8**	**附加指南**
12	**操作安全**	**6.9**	**附加指南**
13	**通信安全**	**6.10**	**附加指南**
14	**系统获取、开发和维护**	**6.11**	**附加指南**
15	**供应商关系**	**6.12**	**附加指南**
16	**信息安全事件管理**	**6.13**	**附加指南**
17	**信息安全方面的业务连续性管理**	**6.14**	**没有 PIMS 附加指南**
18	**合规**	**6.15**	**附加指南**

注：即使没有 PIMS 的特定指南，依据 6.1 的“信息安全”的扩展解释也始终适用。

4.4 客户

根据组织的角色（见 5.2.1），“客户”可以理解为：

a) 与 PII 控制者签订合同的组织（例如 PII 控制者的客户）；

注 1：这可以是联合控制者组织的情况。

注 2：与组织建立企业对消费者关系的在本文中称为“PII 当事人”的个人。

b) 与 PII 处理者签订合同的 PII 控制者（例如 PII 处理者的客户）;或

c) 与 PII 处理分包商签订合同的 PII 处理者（例如，分包 PII 子处理者的客户）。

注 3：第 6 节中提到“客户”的地方，则相关条款可适用于上文的 a），b）或 c）。

注 4：第 7 节和附录 A 中提到“客户”的地方，则关联条款适用于上文的 a）。

注 5：第 8 节和附录 B 中提到“客户”的地方，则关联条款适用于上文的 b）和/或 c）。

5 PIMS 关于 ISO/IEC 27001 的具体要求

5.1 概述

ISO/IEC 27001:2013 中提及“信息安全”的要求应延伸到可能受 PII 处理影响的隐私保护。

注：实际上，在 ISO/IEC 27001:2013 中使用“信息安全”的地方，由“信息安全和隐私”替代（见附件 F）。

5.2 组织情景

5.2.1 理解组织及其背景

ISO/IEC 27001:2013 中 4.1 的附加要求是：

组织应确定其作为 PII 控制者（包括联合 PII 控制者）和/或 PII 处理者的角色。

组织应确定与其背景相关的并影响其实现 PIMS 预期结果的能力的外部和内部因素。例如，这些因素可能包括：

— 适用的隐私法规;

— 适用的法规;

— 适用的司法判决;

— 适用的组织背景、治理、政策和程序;

— 适用的行政决定;

— 适用的合同要求。

如果组织同时扮演两个角色（例如 PII 控制者和 PII 处理者），则应确定单独角色时每个角色独立的控制措施的主题。

注：对于 PII 处理的每个实体，组织的角色可能不同，因为它取决于谁确定处理的目的和方式。

5.2.2 理解利益相关方的需求和期望

ISO/IEC 27001:2013 中 4.2 的附加要求是：

组织应将与 PII 处理相关的利益或责任的各方，包括 PII 主体包含在其利益相关方（参见 ISO/IEC 27001:2013 中 4.2）之内。

注 1：其他利益相关方可以包括客户（见 4.4）、监管机构、其他 PII 控制者、PII 处理者及其分包商。

注 2：与 PII 处理相关的要求可以通过法律法规要求、合同义务和自我规定的组织目标来确定。ISO/IEC 29100 中规定的隐私原则提供了有关 PII 处理的指导。

注 3：作为证明符合组织义务的要素，一些利益相关方可以期望组织符合特定的标准，例如本文件中规定的管理体系和/或任何相关的规范。利益各方可以要求进行独立审计，判定是否符合这些标准。

5.2.3 确定信息安全管理体系范围

ISO/IEC 27001:2013 中 4.3 的附加要求是：

在确定 PIMS 的范围时，组织应包括 PII 的处理。

注：由于根据 5.1 对“信息安全”的扩展解释，确定 PIMS 范围时，可能需要修改信息安全管理体系的范围。

5.2.4 信息安全管理体系

ISO/IEC 27001:2013 中 4.4 的附加要求是：

组织应根据 ISO/IEC 27001:2013 第 4 至 10 条的要求，建立、实施、维护和持续改进 PIMS，并按照第 5 条的要求进行扩展。

5.3 领导力

5.3.1 领导力和承诺

适用于 ISO/IEC 27001:2013 中 5.1 规定的要求和本文 5.1 特定的解释。

5.3.2 方针

适用于 ISO/IEC 27001:2013 中 5.2 规定的要求和本文 5.1 特定的解释。

5.3.3 组织的角色、职责和权限

适用于 ISO/IEC 27001:2013 中 5.3 规定的要求和本文 5.1 特定的解释。

5.4 计划

The data

5.4.1 处理风险和机遇的活动

5.4.1.1 概述

适用于 ISO/IEC 27001:2013 中 6.1.1 规定的要求和本文 5.1 特定的解释。

5.4.1.2 信息安全风险评估

适用于 ISO/IEC 27001:2013 中 6.1.2 规定的要求和下列的改进：

ISO/IEC 27001:2013 中 6.1.2 c）1）改进如下：

组织应在 PIMS 范围内应用信息安全风险评估过程，识别保密性、完整性和可用性丧失相关的风险。

组织应在 PIMS 范围内应用隐私风险评估过程，识别与 PII 处理相关的风险。

组织应在整个风险评估过程中确保信息安全与 PII 保护之间的关系得到适当管理。

注：组织可以应用集成的信息安全和隐私风险评估过程，也可以应用各自独立的风险评估过程。

ISO/IEC 27001:2013 中 6.1.2 d）1）改进如下：

组织应评价假如上述 ISO/IEC 27001:2013 中 6.1.2 c）中识别的风险出现时，对组织和 PII 主体双方产生的潜在后果。

5.4.1.3 信息安全风险处置

适用于 ISO/IEC 27001:2013 中 6.1.3 规定的要求和下列的增补：

ISO/IEC 27001:2013 中 6.1.3 c）改进如下：

ISO/IEC 27001:2013 中 6.1.3 b）中确定的控制措施应与附录 A 和/或附录 B 和 ISO/IEC 27001:2013 附录 A 中的控制措施进行比较，以验证没有遗漏任何必要的控制措施。

在评估 ISO/IEC 27001:2013 附录 A 中控制目标和控制措施对风险处置的适用性时，应在信息安全风险和 PII 处理风险背景下考虑控制目标和控制措施，包括对 PII 主体的风险。

ISO/IEC 27001:2013 中 6.1.3 d）改进如下：

制作适用性声明 SOA，其中包含：

— 必要的控制措施 [见 ISO/IEC 27001:2013 中 6.1.3 b）和 c）];

— 将其纳入的理由;

— 是否实施了必要的控制措施;和

— 根据组织对其作用的确定，在附录 A 和/或附录 B 和 ISO/IEC 27001:2013 附录 A 中删除任何控制措施的理由（见 5.2.1）。

并非附录中列出的所有控制目标和控制措施都需要包含在 PIMS 实施中。删除的理由可以包括，风险评估认为不需要控制的地方，以及法律和/或法规（包括适用于 PII 主体的法律和/或法规）不要求（或受其限制）的情况。

5.4.2 信息安全目标和实现

适用于 ISO/IEC 27001:2013 中 6.2 规定的要求和本文 5.1 特定的解释。

5.5 支持

5.5.1 资源

适用于 ISO/IEC 27001:2013 中 7.1 规定的要求和本文 5.1 特定的解释。

5.5.2 能力

适用于 ISO/IEC 27001:2013 中 7.2 规定的要求和本文 5.1 特定的解释。

5.5.3 沟通

适用于 ISO/IEC 27001:2013 中 7.3 规定的要求和本文 5.1 特定的解释。

5.5.4 沟通

适用于 ISO/IEC 27001:2013 中 7.4 规定的要求和本文 5.1 特定的解释。

5.5.5 文件化信息

5.5.5.1 概述

适用于 ISO/IEC 27001:2013 中 7.5.1 规定的要求和本文 5.1 特定的解释。

5.5.5.2 建立和更新

适用于 ISO/IEC 27001:2013 中 7.5.2 规定的要求和本文 5.1 特定的解释。

5.5.5.3 文档化信息的控制

适用于 ISO/IEC 27001:2013 中 7.5.3 规定的要求和本文 5.1 特定的解释。

5.6 运行

5.6.1 运行计划和控制

适用于 ISO/IEC 27001:2013 中 8.1 规定的要求和本文 5.1 特定的解释。

5.6.2 信息安全风险评估

适用于 ISO/IEC 27001:2013 中 8.2 规定的要求和本文 5.1 特定的解释。

5.6.3 信息安全风险处置

适用于 ISO/IEC 27001:2013 中 8.3 规定的要求和本文 5.1 特定的解释。

5.7 绩效评估

5.7.1 监视、测量、分析和评价

适用于 ISO/IEC 27001:2013 中 9.1 规定的要求和本文 5.1 特定的解释。

5.7.2 内部审核

适用于 ISO/IEC 27001:2013 中 9.2 规定的要求和本文 5.1 特定的解释。

5.7.3 管理评审

适用于 ISO/IEC 27001:2013 中 9.3 规定的要求和本文 5.1 特定的解释。

5.8 改进

5.8.1 不符合和纠正措施

适用于 ISO/IEC 27001:2013 中 10.1 规定的要求和本文 5.1 特定的解释。

5.8.2 持续改进

适用于 ISO/IEC 27001:2013 中 10.2 规定的要求和本文 5.1 特定的解释。

6 PIMS 关于 ISO/IEC 27002 的具体要求

6.1 概述

ISO/IEC 27002:2013 中提及“信息安全”的指南应延伸到可能受 PII 处理影响的隐私保护。

注 1：实际上，在 ISO/IEC 27002:2013 中使用“信息安全”的地方，由“信息安全和隐私”替代（见附件 F）。

所有控制目标和控制措施都应考虑信息安全风险和 PII 处理时的隐私风险。

注 2：同样的指南适用于 PII 控制者和 PII 处理者，除非第 6 条中的具体规定另有说明，或由组织根据适用的司法管辖区确定，。

6.2 信息安全策略

6.2.1 信息安全管理方向

6.2.1.1 信息安全管理策略

适用于 ISO/IEC 27002:2013 中 5.1.1 中规定的控制措施、实施指南和其他信息和下列附加的指南：

ISO/IEC 27002:2013 中 5.1.1 信息安全策略附加的实施指南：

无论是制定单独的隐私策略，还是在信息安全策略中扩展，组织都应该制定一份声明，说明是否支持并致力于遵守适用的 PII 保护法规和/或法规，且与合作伙伴、分包商及其适用的第三方（客户、供应商等）签订的合同保持一致，应明确分配它们之间的职责。

ISO/IEC 27002:2013 中 5.1.1 信息安全策略附加的其他信息：

处理 PII 的任何组织，无论是 PII 控制者还是 PII 处理者，在制定和维护信息安全策略期间，都应考虑适用的 PII 保护法律和/或法规。

6.2.1.2 信息安全策略评审

适用于 ISO/IEC 27002:2013 中 5.1.2 规定的控制措施、实施指南和其它信息。

6.3 信息安全组织

6.3.1 内部组织

6.3.1.1 信息安全角色和职责

适用于 ISO/IEC 27002:2013 中 6.1.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 6.1.1 信息安全角色和职责附加的实施指南：

组织应选定一个联络点，供客户 PII 处理时联系。当组织是 PII 控制者时，选定的联络点，是为 PII 主体处理他们的 PII 时联系（见 7.3.2）。

组织应指派一名或多名人员，负责开发、实施、维护和监视组织治理和隐私程序，以确保遵守关于 PII 处理的所有适用的法律法规。

负责的人员应酌情：

— 独立并直接向组织的适当管理层报告，以确保有效管理隐私风险;

— 参与管理与 PII 处理有关的所有问题;

— 是数据保护法律、法规和实践方面的专家;

— 担当监管机构的联络点;

— 告知最高管理层和组织员工在 PII 处理方面的义务;

— 就组织进行的隐私影响评估提供建议。

注：在某些司法管辖区，这样的人被称为数据保护官员（DPO），当这样的职位需要的时候连同职位和任务一起进行定义。该职位可由工作人员或外包人员履行。

6.3.1.2 职责分离

适用于 ISO/IEC 27002:2013 中 6.1.2 规定的控制措施、实施指南和其它信息。

6.3.1.3 与监管当局的联系

适用于 ISO/IEC 27002:2013 中 6.1.3 规定的控制措施、实施指南和其它信息。

6.3.1.4 与特定利益团体的联系

适用于 ISO/IEC 27002:2013 中 6.1.4 规定的控制措施、实施指南和其它信息。

6.3.1.5 项目管理中的信息安全

适用于 ISO/IEC 27002:2013 中 6.1.5 规定的控制措施、实施指南和其它信息。

6.3.2 移动设备和远程工作

6.3.2.1 移动设备策略

适用于 ISO/IEC 27002:2013 中 6.2.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 6.2.1 移动设备策略附加的实施指南：

组织应确保移动设备的使用不会导致违背 PII 的原则。

6.3.2.2 远程工作

适用于 ISO/IEC 27002:2013 中 6.2.2 规定的控制措施、实施指南和其它信息。

6.4 人力资源安全

6.4.1 雇用前

6.4.1.1 筛选

适用于 ISO/IEC 27002:2013 中 7.1.1 规定的控制措施、实施指南和其它信息。

6.4.1.2 雇佣的条件和协议

适用于 ISO/IEC 27002:2013 中 7.1.2 规定的控制措施、实施指南和其它信息。

6.4.2 雇用中

6.4.2.1 管理职责

适用于 ISO/IEC 27002:2013 中 7.2.1 规定的控制措施、实施指南和其它信息。

6.4.2.2 信息安全意识、教育和培训

适用于 ISO/IEC 27002:2013 中 7.2.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 7.2.2 信息安全意识、教育和培训附加的实施指南：

应采取措施，包括对事件报告的认识，以确保相关工作人员了解违反隐私或安全规则和程序，尤其是那些涉及 PII 处理的规则和程序，可能对组织（例如法律的、业务损失和品牌或声誉受损）、对职员（例如纪律的）、对 PII 主体（例如身体的、物质的和情感的）造成的后果。

注：这些措施包括对有权访问 PII 的人员进行适当的定期培训。

6.4.2.3 惩戒程序

适用于 ISO/IEC 27002:2013 中 7.2.3 规定的控制措施、实施指南和其它信息。

6.4.3 雇用终止或变更

6.4.3.1 雇用职责的终止或变更

适用于 ISO/IEC 27002:2013 中 7.3.1 规定的控制措施、实施指南和其它信息。

6.5 资产管理

6.5.1 对资产负责

6.5.1.1 资产清单

适用于 ISO/IEC 27002:2013 中 8.1.1 规定的控制措施、实施指南和其它信息。

6.5.1.2 资产所有权

适用于 ISO/IEC 27002:2013 中 8.1.2 规定的控制措施、实施指南和其它信息。

6.5.1.3 资产的可接受使用

适用于 ISO/IEC 27002:2013 中 8.1.3 规定的控制措施、实施指南和其它信息。

6.5.1.4 资产的归还

适用于 ISO/IEC 27002:2013 中 8.1.4 规定的控制措施、实施指南和其它信息。

6.5.2 信息分类

6.5.2.1 信息的类别

适用于 ISO/IEC 27002:2013 中 8.2.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 8.2.1 信息的类别附加的实施指南：

组织信息分类系统应明确将 PII 视为其实施方案的一部分。在整个分类系统中，了组织处理的 PII（例如类型，特殊类别）、PII 存储位置和流经的系统是不可或缺的。

6.5.2.2 信息的标记

适用于 ISO/IEC 27002:2013 中 8.2.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 8.2.2 信息的标记附加的实施指南：

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 信息。

6.5.2.3 资产的处理

适用于 ISO/IEC 27002:2013 中 8.2.3 规定的控制措施、实施指南和其它信息。

6.5.3 介质处理

6.5.3.1 可移动介质的管理

适用于 ISO/IEC 27002:2013 中 8.3.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 8.3.1 可移动介质的管理附加的实施指南：

组织应记载存储 PII 可移动介质和/或设备所有的使用情况。如果可行，组织应使用可加密的可移动物理介质和/或设备存储 PI。未加密的介质仅用在不可避免的情况下，并且对未加密的介质和/或设备提供补偿控制措施（例如抗破坏证据的包装），以降低 PII 的风险。

ISO/IEC 27002:2013 中 8.3.1 可移动介质的管理附加的其它信息：

拿到组织场所外的可移动介质容易丢失、损坏和不当访问。加密可移动介质可为 PII 增加一定程度的保护，从而降低可移动介质安全风险和隐私风险的可能性。

6.5.3.2 介质的废弃处置

适用于 ISO/IEC 27002:2013 中 8.3.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 8.3.2 介质的废弃处置附加的实施指南：

在处理存储 PII 可移动介质的时候，安全处理规程应包括信息记录和执行记录，以确保不能访问先前存储的 PII。

6.5.3.3 物理介质的传递

适用于 ISO/IEC 27002:2013 中 8.3.3 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 8.3.3 物理介质的传递附加的实施指南：

如果使用物理介质进行信息传递，则应采用系统来记录 PII 传入和传出物理介质的信息，包括物理介质的类型、授权的发件人/收件人、日期和时间以及物理介质的数量。如果可能，应实施其他措施（如加密），以确保数据只能在目的地而非传输途中被访问。

组织应对包含 PII 的物理介质离开其场所前实施授权，确保除授权人员之外的任何人都无法访问 PII。

注：对离开组织场所包含 PII 的物理介质实施可能的措施，加密 PII 不能被授权人员采用一般的方法访问，并限制授权人员的解密能力。

6.6 访问控制

6.6.1 访问控制的业务要求

6.6.1.1 访问控制策略

适用于 ISO/IEC 27002:2013 中 9.1.1 规定的控制措施、实施指南和其它信息。

6.6.1.2 访问网络和风险服务

适用于 ISO/IEC 27002:2013 中 9.1.2 规定的控制措施、实施指南和其它信息。

6.6.2 用户访问管理

6.6.2.1 用户注册和注销

适用于 ISO/IEC 27002:2013 中 9.2.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 9.2.1 用户注册和注销附加的实施指南：

用于处理 PII 的系统和服务的管理或操作用户的注册和注销程序，应解决那些访问控制违背的用户的情况，例如密码或其他用户注册数据的损坏或违背（例如，无意泄密的结果）。

组织不应补发用于处理 PII 的系统和服务的已暂停或已过期的用户 ID。

组织提供 PII 处理服务的情况下，客户负责用户 ID 管理的某些或所有方面。这种情况应包括在文档化的信息中。

某些司法管辖区对处理 PII 的系统从未用过的身份认证凭证的检查频率强加了一些特定的要求。在这些司法管辖区运营的组织应考虑遵守这些要求。

6.6.2.2 用户服务开通

适用于 ISO/IEC 27002:2013 中 9.2.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 9.2.2 用户服务开通附加的实施指南：

组织应维护一个准确、最新的用户配置文件，此文件是被授权访问包含 PII 的信息系统的用户创建的。此用户配置文件包含了该用户的数据组，包括用户 ID、必须执行的提供授权访问的可识别的技术控制措施。

通过实施独立的用户访问 ID，适当的配置的系统，就能识别访问 PII 的用户以及他们所做的添加、删除或更改操作。除了保护组织外，用户还可以获得保护，因为他们可以

识别他们处理的内容以及未处理的内容。

组织提供 PII 处理服务的情况下，客户可以负责访问管理的某些或所有方面。在适当的情况下，组织应向客户提供执行访问管理的方法，如，提供管理权限来管理或终止访问。这种情况应包括在文档化的信息中。

6.6.2.3 特殊访问权的管理

适用于 ISO/IEC 27002:2013 中 9.2.3 规定的控制措施、实施指南和其它信息。

6.6.2.4 用户秘密认证信息的管理

适用于 ISO/IEC 27002:2013 中 9.2.4 规定的控制措施、实施指南和其它信息。

6.6.2.5 用户访问权的复查

适用于 ISO/IEC 27002:2013 中 9.2.5 规定的控制措施、实施指南和其它信息。

6.6.2.6 访问权的撤销和调整

适用于 ISO/IEC 27002:2013 中 9.2.6 规定的控制措施、实施指南和其它信息。

6.6.3 用户职责

6.6.3.1 秘密认证信息的使用

适用于 ISO/IEC 27002:2013 中 9.3.1 规定的控制措施、实施指南和其它信息。

6.6.4 系统和应用访问控制

6.6.4.1 信息访问控制

适用于 ISO/IEC 27002:2013 中 9.4.1 规定的控制措施、实施指南和其它信息。

6.6.4.2 安全登录程序

适用于 ISO/IEC 27002:2013 中 9.4.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 9.4.2 安全登录程序附加的实施指南：

如果客户要求，组织应为客户控制下的任何用户帐户提供安全登录程序的能力。

6.6.4.3 密码管理系统

适用于 ISO/IEC 27002:2013 中 9.4.3 规定的控制措施、实施指南和其它信息。

6.6.4.4 有特权的实用程序的使用

适用于 ISO/IEC 27002:2013 中 9.4.4 规定的控制措施、实施指南和其它信息。

6.6.4.5 对程序源代码的访问控制

适用于 ISO/IEC 27002:2013 中 9.4.5 规定的控制措施、实施指南和其它信息。

6.7 密码学

6.7.1 密码控制

6.7.1.1 加密控制的使用策略

适用于 ISO/IEC 27002:2013 中 10.1.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 10.1.1 加密控制的使用策略附加的实施指南：

某些司法管辖区可能要求使用加密技术来保护特定类型的 PII，例如健康数据、居民登记号码、护照号码和驾驶执照号码。

组织应向客户提供其使用加密技术保护其 PII 处理情况的信息。组织还应向客户提供帮助客户应用自己的加密保护功能的信息。

6.7.1.2 密钥管理

适用于 ISO/IEC 27002:2013 中 10.1.2 规定的控制措施、实施指南和其它信息。

6.8 物理和环境安全

6.8.1 安全区域

6.8.1.1 物理安全边界

适用于 ISO/IEC 27002:2013 中 11.1.1 规定的控制措施、实施指南和其它信息。

6.8.1.2 物理入口控制

适用于 ISO/IEC 27002:2013 中 11.1.2 规定的控制措施、实施指南和其它信息。

6.8.1.3 确保办公室、房间和设施的安全

适用于 ISO/IEC 27002:2013 中 11.1.3 规定的控制措施、实施指南和其它信息。

6.8.1.4 保护免受外部和环境威胁

适用于 ISO/IEC 27002:2013 中 11.1.4 规定的控制措施、实施指南和其它信息。

6.8.1.5 在安全区域工作

适用于 ISO/IEC 27002:2013 中 11.1.5 规定的控制措施、实施指南和其它信息。

6.8.1.6 交货和装货区域

适用于 ISO/IEC 27002:2013 中 11.1.6 规定的控制措施、实施指南和其它信息。

6.8.2 设备

6.8.2.1 设备选址和保护

适用于 ISO/IEC 27002:2013 中 11.2.1 规定的控制措施、实施指南和其它信息。

6.8.2.2 支持性公共事业设备

适用于 ISO/IEC 27002:2013 中 11.2.2 规定的控制措施、实施指南和其它信息。

6.8.2.3 布缆安全

适用于 ISO/IEC 27002:2013 中 11.2.3 规定的控制措施、实施指南和其它信息。

6.8.2.4 设备维修

适用于 ISO/IEC 27002:2013 中 11.2.4 规定的控制措施、实施指南和其它信息。

6.8.2.5 搬迁资产

适用于 ISO/IEC 27002:2013 中 11.2.5 规定的控制措施、实施指南和其它信息。

6.8.2.6 外部设备和资产的安全

适用于 ISO/IEC 27002:2013 中 11.2.6 规定的控制措施、实施指南和其它信息。

6.8.2.7 设备的安全处置和再利用

适用于 ISO/IEC 27002:2013 中 11.2.7 中规定的控制措施、实施指南和其他信息和下列

的附加指南：

ISO/IEC 27002:2013 中 11.2.7 设备的安全处置和再利用附加的实施指南：

组织应确保不论什么时候重新分配存储空间，以前驻留在该存储空间中的任何 PII 都不可访问。

由于信息系统的性能问题，删除其中保留的 PII 是不切实际的。这会导致其他用户可以访问 PII 的风险。应通过具体的技术措施避免这种风险。

安全处置或再利用含有 PII 的存储介质的设备，应该被视为包含 PII。

6.8.2.8 无人值守的用户设备

适用于 ISO/IEC 27002:2013 中 11.2.8 规定的控制措施、实施指南和其它信息。

6.8.2.9 安全桌面和安全屏幕策略

适用于 ISO/IEC 27002:2013 中 11.2.9 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 11.2.9 安全桌面和安全屏幕策略附加的实施指南：

组织应将创建包含 PII 的硬拷贝材料限制在最低需求，满足已确定的目的即可。

6.9 操作安全

6.9.1 操作程序和职责

6.9.1.1 操作程序文件化

适用于 ISO/IEC 27002:2013 中 12.1.1 规定的控制措施、实施指南和其它信息。

6.9.1.2 变更管理

适用于 ISO/IEC 27002:2013 中 12.1.2 规定的控制措施、实施指南和其它信息。

6.9.1.3 容量管理

适用于 ISO/IEC 27002:2013 中 12.1.3 规定的控制措施、实施指南和其它信息。

6.9.1.4 开发、测试和运行环境分离

适用于 ISO/IEC 27002:2013 中 12.1.4 规定的控制措施、实施指南和其它信息。

6.9.2 防范恶意软件

6.9.2.1 控制恶意软件

适用于 ISO/IEC 27002:2013 中 12.2.1 规定的控制措施、实施指南和其它信息。

6.9.3 备份

6.9.3.1 信息备份

适用于 ISO/IEC 27002:2013 中 12.3.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 12.3.1 信息备份附加的实施指南：

组织应制定策略，以满足 PII 的备份、修复和恢复要求（可以是信息备份策略的一部分），以及删除因备份要求保留信息中的 PII 的更进一步要求（例如合同和/或法律要求）。

PII 的具体职责方面可能取决于客户。组织应确保已向客户通告有关备份服务的限制。

如果组织明确向客户提供备份和恢复服务，组织应向他们提供有关其备份和恢复 PII 能力的明确信息。

某些司法管辖区对 PII 的备份频率、备份审查和测试频率或 PII 的恢复程序提出了具体要求。在这些司法管辖区运营的组织应证明符合这些要求。

可能由于系统故障、攻击或灾难，导致需要恢复 PII 的情况。当 PII 恢复时（通常来自备份介质），需要建立流程以确保 PII 恢复到可以确保 PII 完整性的状态，和/或识别 PII 不准确和/或不完整的状态，并且流程落实到位解决它们（可能涉及 PII 主体）。

组织应该有 PII 恢复工作的程序和日志。 PII 恢复工作的日志至少应包含：

— 负责恢复人的姓名;

— 恢复的 PII 的描述。

一些司法管辖区规定了 PII 恢复工作日志的内容。组织应该能够记录适用于管辖区对恢复日志内容特定要求的遵从情况。审议的结论应包括在书面信息中。

使用分包商来存储 PII 处理的复制或备份副本，本文件适用于分包的 PII 处理中的控制（见 6.5.3.3,6.12.1.2）。用于备份和恢复的物理介质发生传递的情况下，本文档（6.10.2.1）的控制措施也能涵盖。

6.9.4 日志和监控

6.9.4.1 事态日志

适用于 ISO/IEC 27002:2013 中 12.4.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 12.4.1 事态日志附加的实施指南：

应建立一个流程能连续、自动的对监控和告警的事件日志进行审查，或者，执行指定的、周期性文件化的审查，以识别违规行为并提出补救措施。

在可能的情况下，事件日志应记录对 PII 的访问情况，包括谁访问、何时访问、访问哪个 PII 主体的 PII、什么（如果有）变更产生（添加、修改或删除），作为事态的结果。

如果多个服务提供商参与提供服务，则在实施本指南时可能会有不同或共同的角色。应明确定义这些角色，并形成文件化记录，提供者之间任何日志访问形成一致意见。

PII 处理者实施指南：

组织应定义一个关于客户是否、何时、如何可获得日志信息和可使用日志信息的标准。这些标准应该提供给客户。

如果组织允许其客户访问组织控制的日志记录，组织应实施适当的控制措施以确保客户只能访问与该客户活动相关的记录，不能访问与其他客户活动相关的任何日志记录，并且不能以任何方式修改日志。

6.9.4.2 日志信息保护

适用于 ISO/IEC 27002:2013 中 12.4.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 12.4.2 日志信息保护附加的实施指南：

被记录的日志信息可能包含 PII（例如，安全监视和操作诊断）。应采取措施控制访问（参见 ISO/IEC 27002:2013 中 9.2.3）以确保日志信息仅被预期的使用。

应建立一个尽可能自动化的程序，以确保按照保留计划中的规定删除或取消识别日志信息（见 7.4.7）。

6.9.4.3 管理员和操作员日志

适用于 ISO/IEC 27002:2013 中 12.4.3 规定的控制措施、实施指南和其它信息。

6.9.4.4 时钟同步

适用于 ISO/IEC 27002:2013 中 12.4.4 规定的控制措施、实施指南和其它信息。

6.9.5 控制操作系统软件

6.9.5.1 在操作系统上安装软件

适用于 ISO/IEC 27002:2013 中 12.5.1 规定的控制措施、实施指南和其它信息。

6.9.6 技术漏洞管理

6.9.6.1 技术漏洞的管理

适用于 ISO/IEC 27002:2013 中 12.6.1 规定的控制措施、实施指南和其它信息。

6.9.6.2 软件安装限制

适用于 ISO/IEC 27002:2013 中 12.6.2 规定的控制措施、实施指南和其它信息。

6.9.7 信息系统审计考量

6.9.7.1 信息系统审计控制

适用于 ISO/IEC 27002:2013 中 12.7.1 规定的控制措施、实施指南和其它信息。

6.10 通信安全

6.10.1 网络安全管理

6.10.1.1 网络控制

适用于 ISO/IEC 27002:2013 中 13.1.1 规定的控制措施、实施指南和其它信息。

6.10.1.2 网络服务安全

适用于 ISO/IEC 27002:2013 中 13.1.2 规定的控制措施、实施指南和其它信息。

6.10.1.3 网络隔离

适用于 ISO/IEC 27002:2013 中 13.1.3 规定的控制措施、实施指南和其它信息。

6.10.2 信息传输

6.10.2.1 信息传输策略和程序

适用于 ISO/IEC 27002:2013 中 13.2.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 13.2.1 信息传输策略和程序附加的实施指南：

组织应考虑制定程序，在适用的情况下，PII 处理规则强制贯穿整个系统或超出系统范围。

6.10.2.2 信息传输协议

适用于 ISO/IEC 27002:2013 中 13.2.2 规定的控制措施、实施指南和其它信息。

6.10.2.3 电子消息

适用于 ISO/IEC 27002:2013 中 13.2.3 规定的控制措施、实施指南和其它信息。

6.10.2.4 保密或不泄露协议

适用于 ISO/IEC 27002:2013 中 12.4.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 12.4.1 事态日志附加的实施指南：

组织应确保在其控制下访问 PII 的个人操作要承担保密义务。 保密协议无论是合同的一部分还是单独的，都应规定履行义务的时间长度。

当组织是 PII 处理者时，组织、其员工及其代理之间的任何形式的保密协议，应确保员工和代理遵守数据处理和保护的策略和程序。

6.11 系统获取、开发和维护

6.11.1 信息系统的安全要求

6.11.1.1 信息安全需求分析和规格说明

适用于 ISO/IEC 27002:2013 中 14.1.1 规定的控制措施、实施指南和其它信息。

6.11.1.2 保护公共网络上的应用服务

适用于 ISO/IEC 27002:2013 中 14.1.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 14.1.2 保护公共网络上的应用服务附加的实施指南：

组织应确保通过不受信任的数据传输网络传输 PII 应被加密传输。

不受信任的网络可以包括公共互联网和组织运营控制之外的其他设施。

注：在某些情况下（例如电子邮件的交换），不受信任的数据传输网络系统的固有特性，可能要求暴露某些报头或业务数据以进行有效传输。

6.11.1.3 保护应用服务事务

适用于 ISO/IEC 27002:2013 中 14.1.3 规定的控制措施、实施指南和其它信息。

6.11.2 开发和支持过程中的安全

6.11.2.1 安全的开发策略

适用于 ISO/IEC 27002:2013 中 14.2.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 14.2.1 安全的开发策略附加的实施指南：

系统开发和设计策略应包括组织处理 PII 需求的指南，基于对 PII 主体和/或任何适用法律和/或法规的义务，以及组织执行的处理类型。 第 7 条和第 8 条提供了处理 PII 控制措施的考虑因素，这可用于制定系统设计中的隐私政策。

默认情况下，有助于设计隐私和隐私的政策应考虑以下几个方面：

a) PII 保护指南和软件开发生命周期中隐私原则的实现（参见 ISO/IEC 29100）;

b) 设计阶段的隐私和 PII 保护要求，可以基于隐私风险评估和/或隐私影响评估的输出来获得（见 7.2.5）;

c) 项目里程碑的 PII 保护检查点;

d) 必须的隐私和 PII 保护知识;

e) 默认情况下最小化 PII 的处理。

6.11.2.2 系统变更控制程序

适用于 ISO/IEC 27002:2013 中 14.2.2 规定的控制措施、实施指南和其它信息。

6.11.2.3 操作平台更改后的应用技术评审

适用于 ISO/IEC 27002:2013 中 14.2.3 规定的控制措施、实施指南和其它信息。

6.11.2.4 对软件包更改的限制

适用于 ISO/IEC 27002:2013 中 14.2.4 规定的控制措施、实施指南和其它信息。

6.11.2.5 安全系统工程原理

适用于 ISO/IEC 27002:2013 中 14.2.5 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 14.2.5 安全系统工程原理附加的实施指南：

与 PII 处理相关的系统和/或组件应按照默认设计和隐私原则设计，并预测和促进相关控制措施的实施（如第 7 条和第 8 条章所述，分别为 PII 控制者和 PII 处理者）。因此，在那些系统中 PII 的收集和处理仅限于确定的 PII 处理目的所必需的详细说明（见 7.2）。

例如，处理 PII 的组织应确保根据相关管辖区在指定期限后处置 PII。处理该 PII 的系统应该以便于删除要求的方式设计。

6.11.2.6 安全的开发环境

适用于 ISO/IEC 27002:2013 中 14.2.6 规定的控制措施、实施指南和其它信息。

6.11.2.7 外包开发

适用于 ISO/IEC 27002:2013 中 14.2.7 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 14.2.7 外包开发附加的实施指南：

默认情况下，如果适用，对外包信息系统采用同设计隐私和隐私相同的原则（见 6.11.2.5）。

6.11.2.8 系统安全测试

适用于 ISO/IEC 27002:2013 中 14.2.8 规定的控制措施、实施指南和其它信息。

6.11.2.9 系统验收测试

适用于 ISO/IEC 27002:2013 中 14.2.9 规定的控制措施、实施指南和其它信息。

6.11.3 测试数据

6.11.3.1 测试数据的保护

适用于 ISO/IEC 27002:2013 中 14.3.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 14.3.1 测试数据的保护附加的实施指南：

PII 不应该用于测试目的；应使用假的或合成的 PII。如果无法避免将 PII 用于测试目的，则应实施与生产环境中相当的技术和组织措施，以最大限度地降低风险。如果这种等效措施不可行，则应进行风险评估，要通告选择适当的减缓控制措施。

6.12 供应商关系

6.12.1 供应商关系中的信息安全

6.12.1.1 供应商关系的信息安全策略

适用于 ISO/IEC 27002:2013 中 15.1.1 规定的控制措施、实施指南和其它信息。

6.12.1.2 解决供应商协议中的安全问题

适用于 ISO/IEC 27002:2013 中 15.1.2 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 15.1.2 解决供应商协议中的安全问题附加的实施指南：

组织应在与供应商的协议中规定，是否处理 PII，以及供应商为满足其信息安全和 PII 保护义务而需要满足的最低技术和组织措施（见 7.2.6 和 8.2.1）。

供应商协议应在考虑到处理的 PII 类型的情况下，明确分配组织、其合作伙伴、供应商和适用的第三方（客户、供应商等）之间的职责。

组织与其供应商之间的协议中应提供一种机制，确保组织的支持和管理遵守适用的法律和/或法规。协议应要求客户接受独立的审计合规性。

注：出于此类审计目的，可以考虑遵守相关的和适用的安全和隐私标准，如 ISO/IEC 27001 或本文档。

PII 处理者实施指南

在与任何供应商的合同中，组织应指明 PII 仅按其指示处理。

6.12.1.3 信息和通信技术供应链

适用于 ISO/IEC 27002:2013 中 15.1.3 规定的控制措施、实施指南和其它信息。

6.12.2 供应商服务交付管理

6.12.2.1 监视和评审供应商服务

适用于 ISO/IEC 27002:2013 中 15.2.1 规定的控制措施、实施指南和其它信息。

6.12.2.2 管理供应商服务的变更

适用于 ISO/IEC 27002:2013 中 15.2.2 规定的控制措施、实施指南和其它信息。

6.13 信息安全事件管理

6.13.1 信息安全事件的管理和改进

6.13.1.1 职责和程序

适用于 ISO/IEC 27002:2013 中 16.1.1 中规定的控制措施、实施指南和其他信息和下

列的附加指南：

ISO/IEC 27002:2013 中 16.1.1 职责和程序附加的实施指南：

作为整个信息安全事件管理过程的一部分，组织应建立识别和记录违反 PII 的责任和程序。 此外，组织应考虑适用的法律和/或法规，确定相关的责任和程序，向 PII 违规当事方发出通知（包括通知的时机），并向当局披露。

一些司法管辖区对违规响应实施了具体规定，包括通知。在这些司法管辖区运营的组织，应确保他们能够证明遵守这些法规。

6.13.1.2 报告信息安全事态

适用于 ISO/IEC 27002:2013 中 16.1.2 规定的控制措施、实施指南和其它信息。

6.13.1.3 报告信息安全漏洞

适用于 ISO/IEC 27002:2013 中 16.1.3 规定的控制措施、实施指南和其它信息。

6.13.1.4 评估和决策信息安全事态

适用于 ISO/IEC 27002:2013 中 16.1.4 规定的控制措施、实施指南和其它信息。

6.13.1.5 对信息安全事件的响应

适用于 ISO/IEC 27002:2013 中 16.1.5 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 16.1.5 对信息安全事件的响应附加的实施指南：

PII 控制者实施指南

涉及 PII 的事件组织应触发一个审查，作为其信息安全事件管理流程的一部分，以确定是否发生了需要响应的 PII 违规行为。

事件不一定会触发此类审查。

注 1：信息安全事态不一定导致一个实际的或大概率的未经授权的 PII 或组织的存储 PII 的设备或设施的访问。这些可能包括但不限于，对防火墙或边缘服务器的 ping 和其他广播攻击、端口扫描、不成功的登录尝试、拒绝服务攻击和数据包嗅探。

当违反 PII 时，响应程序应包括相关的通知和记录。

某些司法管辖区定义了应将违反行为通知监管机构的情况，以及何时应通知 PII 主体。

通知应该是明确的，也可能是必需的。

注 2：通知可包含以下详细信息：

— 可以获得更多信息的联络点;

— 违反行为的描述和可能的后果;

— 对违规行为的描述，包括有关的人员数量以及有关的记录数量;

— 已采取或计划采取的措施。

注 3：有关安全事件管理的信息可在 ISO/IEC 27035 系列中找到。

如果发生涉及 PII 的违规行为，应保留一份提供足够信息的记录，以便为监管和/或法庭目的提供报告，例如：

— 对事件的描述;
— 时间段;
— 事件的后果;
— 报告人的名字;
— 事件被报告的人;
— 为解决事件所采取的步骤（包括责任人和恢复的数据）;
— 事件导致 PII 无法获得、丢失、披露或改变的事实。

如果发生涉及 PII 的违规行为，该记录还应包括 PII 被违背的描述（如果已知）；如果进行了通知，则采取措施通知 PII 主体、监管机构或客户。

PII 处理者实施指南

涉及 PII 违约通知的规定应构成组织与客户之间合同的一部分。合同应规定组织如何提供必需的信息，让客户履行其通知相关机构的义务。此通知义务不会延伸到由客户、PII 主体或其负责的系统组件引起的违规。合同还应定义通知响应时间的预期和外部强制限制。

在某些司法管辖区，PII 处理者应该在没有不当延迟的情况下（即尽快）通知 PII 控制者存在违规行为，最好是，一发现立即通知，以便 PII 控制者立即采取适当的行动。

如果发生涉及 PII 的违规行为，应保留一份提供足够信息的记录，以便为监管和/或法庭目的提供报告，例如：

— 对事件的描述;
— 时间段;
— 事件的后果;
— 报告人的名字;
— 事件被报告的人;
— 为解决事件所采取的步骤（包括责任人和恢复的数据）;
— 事件导致 PII 无法获得、丢失、披露或改变的事实。

如果发生涉及 PII 的违规行为，该记录还应包括 PII 被违背的描述（如果已知）；如果进行了通知，则采取措施通知客户和/或监管机构。

在某些司法管辖区，适用的法律和/或法规可要求组织直接通知适当的监管机构（例如 PII 保护机构）涉及 PII 的违规行为。

6.13.1.6 从信息安全事件中学习

适用于 ISO/IEC 27002:2013 中 16.1.6 规定的控制措施、实施指南和其它信息。

6.13.1.7 收集证据

适用于 ISO/IEC 27002:2013 中 16.1.7 规定的控制措施、实施指南和其它信息。

6.14 信息安全方面的业务连续性管理

6.14.1 信息安全连续性

6.14.1.1 规划信息安全连续性

适用于 ISO/IEC 27002:2013 中 17.1.1 规定的控制措施、实施指南和其它信息。

6.14.1.2 实施信息安全连续性

适用于 ISO/IEC 27002:2013 中 17.1.2 规定的控制措施、实施指南和其它信息。

6.14.1.3 验证、更新和评估信息安全连续性

适用于 ISO/IEC 27002:2013 中 17.1.3 规定的控制措施、实施指南和其它信息。

6.14.2 冗余

6.14.2.1 信息处理设施的可用性

适用于 ISO/IEC 27002:2013 中 17.2.1 规定的控制措施、实施指南和其它信息。

6.15 合规性

6.15.1 遵守法律和合同要求

6.15.1.1 确定适用的法律和合同要求

适用于 ISO/IEC 27002:2013 中 18.1.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 18.1.1 确定适用的法律和合同要求附加的实施指南：

组织应识别处理 PII 相关的任何潜在的法律制裁（可能由于某些义务被遗漏而导致），包括直接来自当地监管机构的巨额罚款。在某些司法管辖区，本文档等国际标准可用于构成组织与客户之间合同的基础，概述其各自的安全性、隐私和 PII 保护责任。如果违反这些责任，合同条款可以为合同处罚提供依据。

6.15.1.2 知识产权

适用于 ISO/IEC 27002:2013 中 18.1.2 规定的控制措施、实施指南和其它信息。

6.15.1.3 保护记录

适用于 ISO/IEC 27002:2013 中 18.1.3 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 18.1.3 保护记录附加的实施指南：

可能需要审查当前和历史的策略和程序（例如，由监管机构调解纠风和调查的情况下）。

组织应依据保留计划的规定，保留其隐私政策和相关程序的副本一段时期（见 7.4.7）。包括更新文档时的先前版本。

6.15.1.4 个人身份信息的隐私和保护

适用于 ISO/IEC 27002:2013 中 18.1.4 规定的控制措施、实施指南和其它信息。

6.15.1.5 加密控制的监管

适用于 ISO/IEC 27002:2013 中 18.1.5 规定的控制措施、实施指南和其它信息。

6.15.2 信息安全评审

6.15.2.1 信息安全独立评审

适用于 ISO/IEC 27002:2013 中 18.2.1 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 18.2.1 信息安全独立评审附加的实施指南：

如果组织担当 PII 处理者，并且个别客户的审核是不切实际的，或可能增加安全风险，组织应在订立合同之前和合同期间，向客户提供的信息安全独立证据是根据客户的策略和程序实施和运作的。组织选择的独立审计，通常应该是一种可接受的方法，以满足客户审查组织处理业务操作的兴趣，如果它涵盖了预期用户的需求，是否以足够透明的方式提供结果。

6.15.2.2 遵守安全政策和标准

适用于 ISO/IEC 27002:2013 中 18.2.2 规定的控制措施、实施指南和其它信息。

6.15.2.3 技术符合性评审

适用于 ISO/IEC 27002:2013 中 18.2.3 中规定的控制措施、实施指南和其他信息和下列的附加指南：

ISO/IEC 27002:2013 中 18.2.3 技术符合性评审附加的实施指南：

作为遵守安全策略和标准的技术审查的一部分，组织应包括审查与处理 PII 相关的工具和组件的方法。可以包括：

— 持续监控以确认只进行了允许的处理;和/或

— 特定的渗透或漏洞测试（例如，去除识别的数据集可以进行有动机的入侵测试，以验证去除识别方法是否符合组织要求）。

7 针对 PII 控制者 ISO/IEC 27002 的附加指南

7.1 概述

第 6 章中的指导和本节中的补充为 PII 控制者创建了针对 PIMS 的指南。本节中记录的实施指南与附录 A 中列出的控制措施有关联。

7.2 收集和处理的条件

目标：根据适用的司法管辖区的法律依据，以明确界定和合法目的，确定并记录处理是合法的。

7.2.1 识别并记录目的

控制措施

组织应识别并记录 PII 将被处理的具体目的。

实施指南

组织应确保 PII 主体了解其 PII 处理的目的。组织有责任向 PII 主体清楚地记录并传

达此信息。如果没有明确说明处理目的，就不能充分给予同意和选择。

处理 PII 目的的文件应足够清晰和详细，以便可用于向 PII 主体提供所需的信息（见 7.3.2）。这包括获得同意所需的信息（见 7.2.3），以及政策和程序的记录（见 7.2.8）。

其它信息

在云计算服务的部署中，ISO/IEC 19944 中的分类和定义有助于提供用于描述 PII 处理目的的术语。

7.2.2 确定合法的基础

控制措施

组织应为已确定的目的，确定、记录并遵守处理 PII 的相关合法依据。

实施指南

某些司法管辖区要求该组织能够证明在处理之前已正确建立了处理的合法性。

处理 PII 的法律依据包括：

— PII 主体的同意;

— 履行合同;

— 遵守法律义务;

— 保护 PII 主体的切身利益;

— 履行为公共利益而执行的任务;

— PII 控制者的合法利益。

组织应以记录每个 PII 处理活动为基础（见 7.2.8）。

例如，组织的合法利益可以包括信息安全目标，这些目标应与 PII 主体在隐私保护方面的义务相平衡。

当定义 PII 特殊类别的时候，组织应考虑 PII 的自然特性（例如健康信息）或 PII 主体关心的（例如与儿童有关的 PII），并将其包括在 PII 分类方案中。

属于这些类别的 PII 分类可能因司法管辖区而异，并且可能因适用于不同类型的业务的不同监管制度而有所不同，因此组织需要了解适用于正在执行的 PII 处理的分类。

使用特殊类别的 PII 也可能受到更严格的控制。

变更或扩展处理 PII 的目的可能需要更新和/或修订法律依据。它还可能需要从 PII 主体那里获得额外的同意。

7.2.3 确定何时以及如何获得同意

控制措施

组织应确定并记录一个过程，通过该过程，它可以证明是否、何时以及如何从 PII 主体获得 PII 处理的同意。

实施指南

除非有其他合法理由，否则处理 PII 可能需要同意。组织应明确记录何时需要获得同意以及获得同意的要求。将处理目的与关于是否以及如何获得同意的信息相关联可能是有

用的。

某些司法管辖区对如何收集和记录同意（例如未与其他协议捆绑在一起）有特定要求。此外，某些数据收集的类型（例如用于科学研究）和 PII 主体的某些类型（例如儿童）可能需要额外的要求。组织应考虑此类要求并记录如何同意的机制，来满足这些要求。

7.2.4 获得并记录同意

控制措施

组织应根据文件化流程获取并记录 PII 主体的同意。

实施指南

组织应获得并记录 PII 主体的同意，以便能够提供所需要同意的详细信息（例如，提供同意的时间、PII 主体的身份和同意声明）。

在同意过程之前提交给 PII 主体的信息应遵循 7.3.3 中的指南。

同意应该是：

— 自由地给予;

— 规定处理目的; 和

— 清晰的和明确的。

7.2.5 隐私影响评估

控制措施

每当计划对 PII 进行新的处理或改变现有的 PII 处理时，组织应评估隐私影响评估的必要性并在适当时实施。

实施指南

PII 处理为 PII 主体带来风险。应通过隐私影响评估来评估这些风险。某些司法管辖区定义了要求进行隐私影响评估的案例。标准可包括对 PII 主体产生法律效力的自动化决策，特殊类别 PII 的大规模处理（例如健康相关信息、种族或民族血统、政治观点、宗教或哲学信仰、工会会员资格、遗传数据或生物识别数据），或大规模公共可访问区域的系统化监测。

组织应确定完成隐私影响评估所必需的元素。这些可以包括已处理的 PII 类型的列表、存储 PII 的位置以及可以传输的位置。在这种情况下，数据流图和数据图也很有用（有关可以通知隐私影响或其他风险评估的 PII 处理记录的详细信息，请参见 7.2.8）。

其它信息

有关 PII 处理的隐私影响评估指南可在 ISO/IEC 29134 中找到。

7.2.6 与 PII 处理者签订合同

控制措施

组织应与任何使用 PII 的处理者签订书面合同，并应确保这些 PII 处理者的合同中提出附录 B 中相应控制措施的实施。

实施指南

组织与代表其处理 PII 的任何 PII 处理者之间的合同，应要求 PII 处理者实施附件 B 中规定的适当的控制措施，同时考虑到信息安全风险评估过程（见 5.4.1.2）和由 PII 处理者执行的 PII 处理范围（见 6.12）。 默认情况下，附件 B 中规定的所有控制措施均应视为相关。如果组织决定不要求 PII 处理者实施附件 B 中的控制措施，则应证明不要求的合理性（见 5.4.1.3）。

合同可以定义每个不同方的责任，但为了与本文档保持一致，应考虑所有控制措施，并将其包含在记录的信息中。

7.2.7 联合 PII 控制者

控制措施

组织应与所有联合 PII 控制者确定，处理 PII（包括 PII 保护和安全要求）的各自角色和职责。

实施指南

处理 PII 的角色和职责应以透明的方式确定。

这些角色和职责应记录在合同或任何类似的有约束力的文件中，其中包含联合处理 PII 的条款和条件。在某些司法管辖区，此类协议称为数据共享协议。

这些角色和职责应记录在合同或任何类似的有约束力的文件中，其中包含联合处理 PII 的条款和条件。在某些司法管辖区，此类协议称为数据共享协议。

联合 PII 控制器协议可以包括（此列表既不是明确的也不是详尽的）：

— PII 共享的目的/联合 PII 控制者关系;

— 作为联合 PII 控制者关系一部分的组织（PII 控制者）的身份;

— 协商一致的共享和/或转移和处理的 PII 类别;

— 处理操作的概述（例如转移、使用）;

— 各自角色和职责的描述;

— 实施 PII 保护的技术和组织安全措施的职责;

— 在 PII 违约的情况下职责的定义（例如，谁将通知、何时、彼此的信息）;

— PII 保留和/或处置的条款;

— 未遵守协议的责任;

— 如何履行对 PII 主体的义务;

— 如何向 PII 主体提供有关联合 PII 控制者之间安排重要的信息;

— PII 主体如何获得他们有权享有的其他信息;和

— PII 主体的联络点。

7.2.8 与 PII 处理相关的记录

控制措施

组织应确定并安全地保存必要的记录，以支持其处理 PII 的义务。

实施指南

维护 PII 处理记录的一种方法是，拥有组织执行的 PII 处理活动的清单或列表。 这样的清单可以包括：

— 处理的类型;

— 处理的目的;

— 对 PII 和 PII 主体（例如儿童）类别的描述;

— 已经或将要披露 PII 的接收者类别，包括第三国或国际组织的接收者;

— 技术和组织安全措施的一般描述; 和

— 隐私影响评估报告。

这样的库存应该有一个所有者，负责其准确性和完整性。

7.3 对 PII 主体的义务

目标：确保为 PII 主体提供其 PII 处理的适当信息，并履行与 PII 处理相关的任何其他适用义务。

7.3.1 确定并履行对 PII 主体的义务

控制措施

组织应确定并记录与 PII 处理相关的对 PII 主体的法律、法规和业务义务，并提供履行这些义务的方法。

实施指南

对 PII 主体的义务及其支持他们的方法因司法管辖区而异。

组织应确保他们提供适当的方法，以可理解并及时地履行对 PII 主体的义务。应向 PII 主体提供明确的文件，说明他们履行义务的程度、如何履行、以及处理他们请求的最新联系点。

联系点提供的方式应与收集 PII 和同意的方式相同（例如，如果通过电子邮件或网站收集 PII，联系点应通过电子邮件或网站，而不是电话或传真等替代方案）。

7.3.2 确定 PII 主体的信息

控制措施

组织应确定并记录向 PII 主体提供有关其 PII 处理和此类规定的时间信息。

实施指南

组织应确定何时（例如，在处理之前，在请求之后的某个时间内等）向 PII 主体提供信息和信息类型的法律，法规和/或业务要求。

根据要求，信息可以采用公告的形式。可以提供给 PII 主体的信息类型的示例如下：

— 关于处理目的的信息;

— PII 控制者或其代表的联系方式;

— 关于处理的合法依据信息;

— 获取 PII 的地点信息，如果不是直接从 PII 主体那里获得;

— 关于 PII 是否是法律或合同要求规定的信息，以及在适当情况下，未能提供 PII 可能的后果;

— 关于对 PII 主体义务的信息，如 7.3.1 中所确定的，以及 PII 主体如何从中受益，特别是在访问、修改、纠正、请求删除、接收其 PII 副本和反对处理方面;

— 关于 PII 主体如何撤回同意的信息;

— 关于 PII 转移的信息;

— 关于 PII 接收者或接收者类别的信息;

— 关于 PII 保留期的信息;

— 关于 PII 基于自动化处理的自动决策使用的信息;

— 关于提起诉讼权利和如何提起诉讼的信息;

— 关于提供信息频率的信息（例如，“及时”通知、组织定义的频率等）。

如果更改或扩展 PII 处理的目的，组织应提供最新信息。

7.3.3 向 PII 主体提供信息

控制措施

组织应向 PII 主体提供清晰且易于理解的信息，以说明 PII 控制者身份和 PII 处理的描述。

实施指南

组织应向 PII 主体提供 7.3.2 中详述的信息，使用清晰明了的语言，以及时、简洁、完整、透明、易懂和易于访问的形式，给适当的目标受众。

在适当的情况下，应在收集 PII 时提供信息。它也应该是永久可访问的。

注意，图标和图像有助于为 PII 主体提供预期处理的可视化概览。

7.3.4 提供修改或撤销同意的机制

控制措施

组织应为 PII 主体提供修改或撤销其同意的机制。

实施指南

组织应随时告知 PII 主体其撤销同意（可能因司法管辖区而异）的权利，并提供相应的机制。用于撤销的机制取决于系统; 如果可能，它应该与获得同意的机制一致。 例如，如果通过电子邮件或网站收集同意，则撤销它的机制应该相同，而不是电话或传真等替代解决方案。

修改的同意可能包括对 PII 的处理施加限制，这可能包括在某些情况下限制 PII 控制者删除 PII。

某些司法管辖区，对 PII 主体何时及如何修改或撤销其同意施加限制。

组织应以与记录同意本身类似的方式，记录撤回或更改同意的任何请求。

应通过适当的系统将任何更改的同意，传播给授权用户和相关第三方。

组织应该定义响应时间，据此来处理请求。

其它信息

当撤销对特定 PII 处理的同意时，撤销之前执行的所有 PII 处理正常进行才是合适的，在适当的时候考虑，但这种处理的结果不应用于新处理。例如，如果 PII 主体撤销其个人配置信息的同意，则其个人配置信息不应进一步被使用或被咨询。

7.3.5 提供反对 PII 处理的机制

控制措施

组织应为 PII 主体提供一种机制，以反对处理其 PII。

实施指南

某些司法管辖区为 PII 主体提供反对处理其 PII 的权利。受这些管辖区法律和/或法规约束的组织，应确保他们采取适当措施，使 PII 主体能够行使这一权利。

组织应记录 PII 主体对处理异议的相关法律和法规要求（例如，出于直接营销目的而处理 PII 的异议）。组织应向主体提供在这些情况下有反对能力的相关信息。反对机制可能有所不同，但应与所提供的服务类型一致（例如，在线服务应提供在线功能）。

7.3.6 访问、更正和/或删除

控制措施

组织应实施策略、程序和/或机制，以履行其对 PII 主体访问、更正和/或删除其 PII 的义务。

实施指南

组织应实施策略、程序和/或机制，以使 PII 主体能够在没有不当延迟的情况下获取访问、更正和删除其 PII。

组织应定义响应时间，并且应该据此来处理请求。

任何更正或删除都应通过系统和/或授权用户传播，并应传递给已转移 PII 的第三方（见 7.3.7）。

注意 7.5.3 中规定的控制措施产生的记录可以在这方面提供帮助。

组织应实施策略、程序和/或机制，当 PII 主体对数据的准确性或更正存在争议时使用。这些策略、程序和/或机制应包括告知 PII 主体所做的更改，以及无法进行更正的原因（在这种情况下）。

某些司法管辖区对 PII 主体何时和如何要求更正或删除其 PII 施加限制。组织应确定这些限制是适用的，并使其保持最新状态。

7.3.7 PII 控制者告知第三方的义务

控制措施

组织应实施适当的政策、程序和/或机制，有关共享 PII 的任何修改、撤回或异议，通知共享 PII 的第三方。

实施指南

组织应考虑到现有技术，采取适当措施，任何修改或撤销的同意或与共享 PII 有关的异议，通知第三方。某些司法管辖区强制要求向这些第三方通报这些行为。

组织应确定并维持与第三方的积极沟通渠道。相关责任可以分配给负责其运营和维护的个人。在通知第三方时，组织应监控其收到信息的回执。

注：对 PII 主体义务所产生的变更，可包括根据 PII 主体的要求，修改或撤销同意、更正请求、删除、或处理限制，或 PII 处理反对。

7.3.8 提供已处理 PII 的副本

控制措施

组织应能够在 PII 主体要求时，提供被处理 PII 的副本。

实施指南

组织应提供被处理 PII 的副本，该副本应是 PII 主体可理解的、结构化的、通用的格式。

某些司法管辖区定义了组织应提供 PII 副本的情况，PII 副本对于 PII 主体或接收方 PII 控制者处理是可移植的格式（通常是结构化的、常用的和机器可读的）。

组织应确保提供给 PII 主体的任何 PII 副本，对该 PII 主体是明确的。

如果请求的 PII 已根据保留和处置策略（如 7.4.7 所述）被删除，则 PII 控制者应通知 PII 主体请求的 PII 已被删除。

在组织不再能识别 PII 主体（例如，由于去除识别过程的结果）的情况下，组织不应寻求（重新）识别 PII 主体，这是实施此控制措施的唯一原因。但是，在某些司法管辖区，合法请求可能要求从 PII 主体请求其他信息，以便重新识别和随后披露。

在技术上可行的情况下，应 PII 主体的要求，可以将 PII 副本从一个组织直接转移到另一个组织。

7.3.9 处理请求

控制措施

组织应定义并记录策略和程序，处理和响应来自 PII 主体的合法请求。

实施指南

合法请求可包括 PII 处理副本的请求或提起诉讼的请求。某些司法管辖区允许组织在某些情况下收取费用（例如过多或重复的请求）。

请求应在适当的定义响应时间内处理。

某些司法管辖区定义了响应时间，具体取决于请求的复杂程度和数量，以及任何延迟通知 PII 主体的要求。应在隐私政策中定义适当的响应时间。

7.3.10 自动决策

控制措施

组织应确定并解决 PII 主体的义务，包括法律义务，这些义务是由组织做出的决定产

生的，这些决定仅与 PII 主体有关，而且完全基于 PII 的自动处理。

实施指南

当完全基于 PII 自动处理的决策对他们产生重大影响时，某些司法管辖区定义了对 PII 主体的具体义务。例如通知自动决策的存在，允许 PII 主体反对此类决策，和/或获得人为干预。

注：在某些司法管辖区，某些 PII 处理无法完全自动化。

在这些司法管辖区运营的组织应遵守这些义务的规定。

7.4 设计的隐私和默认的隐私

目标：确保设计流程和系统，使收集和处理（包括使用、披露、保留、传输和处置）限于所确定的必需的目的。

7.4.1 限制收集

控制措施

组织应将 PII 的收集限制在与确定目的相关的、相称的和必要的最小值。

实施指南

组织应将 PII 的收集限制在与确定目的适当的、相关的和必要的范围内。这包括限制组织间接收集的 PII 数量（例如，通过 Web 日志、系统日志等）。

缺省隐含的隐私，存在 PII 收集和处理中的任何选项，默认情况下应被禁用，且仅通过 PII 主体的明确选项来启用。

7.4.2 限制处理

控制措施

组织应将 PII 处理限制在对已确定的目的而言，是适当的、相关的和必须的。

实施指南

应通过信息安全和隐私政策（见 6.2），连同采纳和遵守的文件化程序，来管理限制 PII 处理。

PII 处理，包括：

— 披露;

— PII 存储期; 和

— 谁能够访问他们的 PII;

应默认限制为对已确定目的而言，是最小的和必须的。

7.4.3 准确性和质量

控制措施

在 PII 的整个生命周期中，组织应确保 PII 尽可能是准确的、完整的和最新的，且是

被记录的，这对于处理目的而言是必需的。

实施指南

组织应实施策略、程序和/或机制，以尽量减少其 PII 处理的不准确性。还应该有策略、程序和/或机制，来应对不准确 PII 的情况。这些策略、程序和/或机制应包含在文件化信息中（例如，通过技术的系统配置等），并应适用于整个 PII 生命周期。

其它信息

有关 PII 处理生命周期的更多信息，请参见 ISO/IEC 29101:2018 中 6.2。

7.4.4 PII 最小化目标

控制措施

组织应定义和记录数据最小化目标，以及为满足这些目标采用的机制（例如，去标识）。

实施指南

组织应确定相对于确定的目的，收集和处理特定 PII 和 PII 的数量是如何受限的。 这可以包括使用去标识或其他数据最小化技术。

确定的目的（见 7.2.1）可能要求，未被标识的 PII 的处理，在这种情况下，组织应该能够描述这种处理。

在其他情况下，确定的目的不需要处理原始 PII，并且去标识的 PII 处理足以满足所确定的目的。在这些情况下，组织应定义并记录 PII 需要与 PII 主体的关联程度，以及为处理 PII 而设计的机制和技术，以便实现去标识和/或 PII 最小化目标。

用于最小化 PII 机制的变化，取决于处理类型和用于处理的系统。组织应记录用于实现数据最小化的任何机制（技术系统配置等）。

如果处理去标识数据足以达到目的，组织应记录旨在及时实施组织设定的去标识目标的任何机制（技术系统配置等）。例如，删除与 PII 主体相关联的属性可足以使组织实现其已确定的目的。在其他情况下，可以使用其他去标识技术，例如泛化（例如舍入）或随机技术（例如，噪声添加）来实现适当水平的去标识。

注 1：有关去标识技术的更多信息，请参阅 ISO/IEC 20889。

注 2：对于云计算，ISO/IEC 19944 提供了数据限定符的定义，可用于对数据能识别 PII 主体的程度，或将 PII 主体与 PII 中的一组特征相关联的程度，进行分类。

7.4.5 PII 处理结束时去除标识和删除

控制措施

一旦原始 PII 不再需要用于确定的目的，组织应删除 PII 或以不允许识别或重新识别 PII 主体的形式呈现它。

实施指南

当预料不再有进一步处理时，组织应有机制清除此 PII。或者，可以使用一些去除识别技术，那些去除识别的数据不能再识别出 PII 主体。

7.4.6 临时文件

控制措施

组织应确保由于处理PII而创建的临时文件在规定记录期内按照文档化程序进行处理（例如删除或销毁）。

实施指南

组织应定期检查在指定的时间段内删除未使用的临时文件。

其它信息

信息系统在正常运行过程中可以创建临时文件。此类文件针对系统或应用程序，但可包括与数据库更新和其他应用程序软件运行相关的文件系统回滚日志和临时文件。相关信息处理任务完成后不需要临时文件，但有些情况下它们不能被删除。这些临时文件保存的时间长度并不总是确定的，但“垃圾收集”程序应识别相关文件并确定自上次使用以来已存在的时间。

7.4.7 保留

控制措施

组织保留 PII 的时间不应超过处理 PII 所需的时间。

实施指南

组织应开发和维护其保留信息的保留时间表，同时考虑到保留 PII 的要求不超过必要的时间。此类时间表应考虑法律、法规和业务要求。如果此类要求发生冲突，则需要做出业务决策（基于风险评估）并在适当的时间表中记录。

7.4.8 处置

控制措施

组织应具有处置 PII 的文件化政略、程序和/或机制。

实施指南

PII 处理技术的选择取决于许多因素，因为处置技术的性质和结果不同（例如，由此导致的得物理介质的颗粒度，或在电子介质上恢复已删除信息的能力）。在选择合适处置技术时要考虑的因素包括但不限于，待处置 PII 的性质和程度、是否存在与 PII 相关的元数据、以及存储 PII 介质的物理特征。

7.4.9 PII 传输控制

控制措施

组织应对通过数据传输网络传输（例如发送到另一个组织）的 PII 进行适当的控制，以确保数据到达其预定目的地。

实施指南

需要控制 PII 的传输，通常是通过确保只有经过授权的个人可以访问传输系统，并遵循适当的流程（包括保留审计日志）来确保 PII 不会违背的传输给正确的接收者。

7.5 PII 共享、转移和披露

目标：确定 PII 有无被共享、转移到其他司法管辖区或第三方和/或根据适用的义务被披露，当以上的情况发生时是否被记录。

7.5.1 确定司法管辖区之间 PII 转移的基础

控制措施

组织应确定并记录管辖区之间 PII 转移的相关基础。

实施指南

PII 转移可能受到法律和/或法规的约束，具体取决于数据将被转移到的管辖区域或国际组织（以及从何处转移）。组织应记录对作为转移依据要求的遵守情况。

某些司法管辖区可以要求指定的监管机构审查信息转移协议。在这些司法管辖区内运营的组织应该了解任何此类要求。

注：如果转移发生在特定的司法管辖区内，则适用的法律和/或法规对于发件人和收件人是相同的。。

7.5.2 可以转移 PII 的国家和国际组织

控制措施

组织应指定并记录可能转移 PII 的国家和国际组织。

实施指南

可以向客户提供在正常运营中，可能转移 PII 的国家和国际组织的身份。应包括使用分包 PII 处理产生的国家身份。所包含的国家应与 7.5.1 相关。

在正常运营之外，可能会出现执法机关要求进行转移的情况，这些国家的身份不能提前确定，或者被适用的司法管辖区禁止，以保护执法调查的机密性（见 7.5.1,8.5.4 和 8.5.5）。

7.5.3 PII 转移记录

控制措施

组织应记录到第三方的 PII 转移或来自第三方的 PII 转移，并确保与这些方的合作，以支持与 PII 主体义务相关的未来请求。

实施指南

记录可以包括来自 PII 第三方的转移，该转移由于 PII 控制者管理其义务而被修改，或转移给第三方以实施来自 PII 主体的合法请求，包括删除 PII 的请求（例如，在同意撤销后）。

组织应该有一个策略来定义这些记录的保留期。

组织应通过仅保留严格需要的信息，将数据最小化原则应用于转移记录。

7.5.4 向第三方披露 PII 的记录

控制措施

组织应记录向第三方的 PII 披露，包括已披露的 PII、向谁和何时披露。

实施指南

PII 可以在正常运行过程中披露，应记录这些披露。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。记录应包括披露的来源和进行披露的授权来源。

8 针对 PII 处理者 ISO/IEC 27002 的附加指南

8.1 概述

第 6 章中的指导和本节中的补充为 PII 处理者创建了针对 PIMS 的指南。本节中记录的实施指南与附录 B 中列出的控制措施有关联。

8.2 收集和处理的条件

目标：根据适用的司法管辖区的法律依据，以明确界定和合法目的，确定并记录处理是合法的。

8.2.1 客户协议

控制措施

组织应在必要处确保处理 PII 的合同，解决组织在提供客户义务帮助方面的作用（考虑到处理的性质和组织可用的信息）。

实施指南

组织与客户之间的合同应包括以下相关内容，并取决于客户的角色（PII 控制者或 PII 处理者）（此列表既不是明确的也不是详尽的）：

— 设计隐私和默认隐私（见 7.4,8.4）；

— 实现处理安全;

— 向监管机构通报涉及 PII 的违规行为;

— 向客户和 PII 主体通报涉及 PII 的违规行为;

— 进行隐私影响评估（PIA）；和

— 如果需要事先与相关 PII 保护机构进行磋商，PII 处理者将提供协助。

某些司法管辖区要求合同包括处理的主题和持续时间、处理的性质和目的、PII 的类型和 PII 主体的类别。

8.2.2 组织的目的

控制措施

组织应确保代表客户处理的 PII 仅按照客户的书面说明中所述的目的进行处理。

实施指南

组织与客户之间的合同应包括但不限于，服务要达到的目标和时间范围。

为了实现客户的目的，可能存在技术原因，为什么组织确定处理 PII 的方法是合适的，

与客户的一般指令一致，但没有客户的明确指示。例如，为了有效地利用网络或处理能力，可能需要根据 PII 主体的某些特性来分配特定的处理资源。

组织应允许客户验证其是否符合目的规范和限制原则。这也确保组织或其任何分包商不会出于其他目的而处理 PII，除了客户的书面说明中所表达的其他目的。

8.2.3 营销和广告使用

控制措施

组织不应使用合同下 PII 处理进行营销和广告，而不必确定事先获得相应 PII 主体的同意。

实施指南

应记录 PII 处理者与客户合同要求的合规性，尤其是在计划营销和/或广告的情况下。

如果未经 PII 主体明确同意，组织不应坚持包含营销和/或广告用途。

注：此控制措施是 8.2.2 中更一般控制措施的补充，不替换或以其他方式取代它。

8.2.4 侵权指令

控制措施

如果处理指令违反适用了法律和/或法规，组织应通知客户。

实施指南

组织验证指令是否违反法律和/或法规的能力，取决于技术背景、指令本身和组织与客户之间的合同。

8.2.5 客户义务

控制措施

组织应向客户提供适当的信息，以便客户证明其履行义务。

实施指南

客户所需的信息可包括组织是否允许产菜助于，客户或由客户授权或以其他方式同意的其他审核员进行的审核。

8.2.6 与处理 PII 相关的记录

控制措施

组织应确定并保持必要的记录，以支持证明其代表客户实施 PII 处理的义务（如适用的合同中所规定）。

实施指南

某些司法管辖区可能要求组织记录以下信息：

— 代表每个客户实施的处理类别;

— 转移到第三国或国际组织; 和

— 技术和组织安全措施的一般描述。

8.3 对 PII 主体的义务

目标：确保为 PII 主体提供其 PII 处理的适当信息，并履行与 PII 处理相关的任何其他适用义务。

8.3.1 对 PII 主体的义务

控制措施

组织应为客户提供遵守与 PII 主体相关义务的方法。

实施指南

PII 控制者的义务可以通过法律、法规和/或合同来定义。这些义务可以包括客户使用组织服务来履行这些义务的事项。例如，这可以包括及时更正或删除 PII。

如果客户依赖于组织的信息或技术措施来促进履行对 PII 主体的义务，则应在合同中规定相关信息或技术措施。

8.4 设计的隐私和默认的隐私

目标：确保设计流程和系统，使收集和处理（包括使用、披露、保留、传输和处置）限于所确定的必需的目的。

8.4.1 临时文件

控制措施

组织应确保在指定的记录期内按照文件化程序处理（例如删除或销毁）由于处理 PII 而创建的临时文件。

实施指南

组织应定期验证在指定的时间段内删除未使用的临时文件。

其它信息

信息系统可以在正常的运行过程中创建临时文件。 此类文件是针对系统或应用程序的，但可包括与数据库更新和其他应用程序软件运行相关的文件系统回滚日志和临时文件。 相关信息处理任务完成后不需要临时文件，但有些情况下无法删除它们。 这些文件在使用中保持时间长度并不总是确定的，但“垃圾收集”程序应识别相关文件并确定自上次使用以来已经存在多长时间。

8.4.2 归还、转移和处置 PII

控制措施

组织应提供以安全的方式收回、转移和/或处置 PII 的能力。还应该创建一个对客户有效的策略。

实施指南

在某个时间点，PII 可能需要以某种方式处理。这可能涉及将 PII 返回给客户，将其转移到另一个组织或 PII 控制者（例如，作为合并的结果），删除或以其他方式销毁它，去除标识或将其存档。 应以安全的方式管理返回、转移和/或处置 PII 的能力。

组织应提供必要的保证，以使客户能够确保根据合同处理的 PII（由组织及其任何分包商）从存储的任何位置删除，包括为了备份和业务连续性，一旦它们不再是客户确定目的所必需的。

组织应制定并实施有关 PII 处置的策略，并应在当要求时对客户有效。

该策略应涵盖合同终止前 PII 处置之前的保留期，以保护客户不会因合同意外失效而失去 PII。

注：该控制措施和指南也与保留原则相关（见 7.4.7）。

8.4.3 PII 传输控制

控制措施

组织应对通过数据传输网络传输的PII进行适当的控制，以确保数据到达预定目的地。

实施指南

需要控制 PII 的传输，通常是通过确保只有经过授权的个人才能访问传输系统，并遵循适当的流程（包括保留审计数据），以确保在不违规的情况下传输 PII 给正确的接收者。传输控制的要求可以包含 PII 处理者 - 客户合同中。

如果没有与传输相关的合同要求，则在传输之前接受客户的建议是适当的。

8.5 PII 共享、转移和披露

目标：确定 PII 有无被共享、转移到其他司法管辖区或第三方和/或根据适用的义务被披露，当以上的情况发生时是否被记录。

8.5.1 司法管辖区之间 PII 转移的基础

控制措施

组织应及时告知客户在周司法管辖区之间进行PII转移的基础以及此方面的任何预期更改，以便客户能够反对此类更改或终止合同。

实施指南

司法管辖区之间的 PII 转移可能受到法律和/或法规的约束，具体取决于 PII 要转移到的管辖区域或组织（以及它来自何处）。组织应记录对作为转移基础的要求的遵守情况。

组织应告知客户任何 PII 转移，包括转移到：

— 供应商;

— 其他团体;

— 其他国家或国际组织。

如果发生变更，组织应根据约定的时间表提前通知客户，以便客户能够反对此类变更或终止合同。

组织与客户之间的协议可以包含组织可以在不通知客户的情况下实施更改的条款。在这些情况下，应设置允许的限制（例如，组织可以在不通知客户的情况下更改供应商，但不能将 PII 转移到其他国家/地区）。

在国际转移 PII 的情况下，应确定诸如示范合同条款，具有约束力的公司规则或跨境隐私规则，相关国家以及此类协议适用的环境等协议。

8.5.2 可以转移 PII 的国家和国际组织

控制措施

组织应指定并记录可能转移 PII 的国家和国际组织。

实施指南

可以向客户提供在正常运营中可能转让 PII 的国家和国际组织的身份。应包括使用分包 PII 处理产生的国家身份。所包含的国家应与 8.5.1 相关。

在正常运营之外，可能会出现执法机关要求进行转移的情况，这些国家的身份不能提前确定，或者被适用的司法管辖区禁止，以保护执法调查的机密性（ 见 7.5.1,8.5.4 和 8.5.5）。

8.5.3 向第三方披露 PII 的记录

控制措施

组织应记录向第三方的 PII 披露，包括已披露的 PII，向谁和何时披露。

实施指南

PII 可以在正常运行过程中披露。 应记录这些披露。还应记录向第三方的任何其他披露，例如合法调查或外部审计产生的披露。记录应包括披露的来源和进行披露的授力来源。

8.5.4 PII 披露请求的通知

控制措施

组织应通知客户任何具有法律约束力的 PII 披露的请求。

实施指南

该组织可以收到具有法律约束力的 PII 披露的请求（例如来自执法机构）。 在这些情况下，组织应在约定的时间范围内并根据商定的程序（可包括在客户合同中）通知客户任何此类请求。

在某些情况下，具有法律约束力的请求包括要求组织不要将此事件通知任何人（可能禁止披露的一个例子是，根据刑法禁止执法调查的机密性保护）。

8.5.5 具有法律约束力的 PII 披露

控制措施

组织应拒绝任何不具有法律约束力的 PII 披露请求，在进行任何 PII 披露并接受相应客户授权的任何合同约定的 PII 披露请求之前，请咨询相应的客户。

实施指南

与控制实施相关的细节可以包含在客户合同中

此类请求可能来自多个来源，包括法院、法庭和行政当局。 它们可以来自任何司法管辖区。

8.5.6 披露用于处理 PII 的分包商

控制措施

组织应在使用前，披露任何 PII 处理分包商。

实施指南

使用分包商处理 PII 的规定应包括在客户合同中。

披露的信息应涵盖使用分包合同和相关分包商名称的事实。披露的信息还应包括分包商可以转让数据的国家和国际组织（见 8.5.2）以及分包商有义务达到或超过组织义务的方式（见 8.5.7）。

如果评估分包商信息的公开披露以增加超出可接受限度的安全风险，则应根据保密协议和/或应客户要求进行披露。应让客户知道该信息是可用的。

这与可以转移 PII 的国家名单无关。该清单应在所有情况下以允许他们通知相应 PII 主体的方式向客户披露。

8.5.7 分包商处理 PII 的约束

控制措施

组织应仅依据客户合同雇用分包商处理 PII。

实施指南

如果组织将该 PII 的部分或全部处理分包给另一个组织，则在分包商处理 PII 之前，需要客户的书面授权。

这可以是客户适当条款形式的合同，也可以是特定的“一次性”协议。

组织应与代表其用于 PII 处理的任何分包商签订书面合同，并应确保其与分包商的合同提出实施附件 B 中适当控制措施。

组织与代表其处理 PII 的任何分包商之间的合同应要求分包商实施附录 B 中规定的适当控制措施，同时考虑到信息安全风险评估过程（见 5.4.1.2）和 PII 处理的范围。由 PII 处理者执行（见 6.12）。默认情况下，附录 B 中规定的所有控制措施均应视为相关的。如果组织决定不要求分包商实施附件 B 中的控制措施 ，则应将其排除在外。

合同可以定义每一方不同地责任，但为了与本文档保持一致，应考虑所有控制措施并将其包含在记录的信息中

8.5.8 分包商处理 PII 的变更

控制措施

在拥有常规书面授权的情况下，组织应将有关添加或更换分包商处理 PII 的任何预期变更通知客户，从而使客户有机会反对此类变更。

实施指南

如果组织更改与其分包该 PII 处理的部分或全部组织，则在新分包商处理 PII 之前，这样的变更需要客户的书面授权。这可以是客户适当条款形式的合同，也可以是特定的“一次性”协议。

Annex A

（规范性）

PIMS--规定的参考控制目标和控制措施（PII 控制者）

本附录供作为 PII 控制者的组织使用，无论 PII 处理者是否使用。 它扩展了 ISO/IEC 27001:2013，附录 A。

表 A.1 中列出的附加或修改的控制目标和控制措施直接源自本文档中定义的控制目标和控制措施，并与 ISO/IEC 27001:2013，6.1.3 一起使用，并由 5.4.1.3 进行了细化。

并非本附录中列出的所有控制目标和控制措施都必须包含在 PIMS 实施中。删除任何控制目标的理由应包括在适用性声明中（见 5.4.1.3）。 删除的理由可包括风险评估认为不需要控制的地方，以及适用法律和/或法规不要求（或受其限制）的情况。

注：本附件中的条款编号与第 7 章中的子条款编号有关。

Table A.1 – 控制目标和控制措施

A7.2 收集和处理的条件 目标：根据适用的司法管辖区的法律依据，以明确界定和合法目的，确定并记录处理是合法的。		
条款号	条款名称	控制措施
A7.2.1	识别并记录目的	组织应识别并记录 PII 将被处理的具体目的。
A7.2.2	确定合法的基础	组织应为已确定的目的，确定、记录并遵守处理 PII 的相关合法依据。
A7.2.3	确定何时以及如何获得同意	组织应确定并记录一个过程，通过该过程，它可以证明是否、何时以及如何从 PII 主体获得 PII 处理的同意。
A7.2.4	获得并记录同意	组织应根据文件化流程获取并记录 PII 主体的同意。
A7.2.5	隐私影响评估	每当计划对 PII 进行新的处理或改变现有的 PII 处理时，组织应评估隐私影响评估的必要性并在适当时实施。
A7.2.6	与 PII 处理者签订合同	组织应与任何使用 PII 的处理者签订书面合同，并应确保这些 PII 处理者的合同中提出附录 B 中相应控制措施的实施。
A7.2.7	联合 PII 控制者	组织应与所有联合 PII 控制者确定，处理 PII（包括 PII 保护和安全要求）的各自角色和职责。
A7.2.8	与 PII 处理相关的记录	组织应确定并安全地保存必要的记录，以支持其处理 PII 的义务。
A7.3 对 PII 主体的义务 目标：确保为 PII 主体提供其 PII 处理的适当信息，并履行与 PII 处理相关的任何其他适用义务。		
A7.3.1	确定并履行对 PII 主体的义务	组织应确定并记录与 PII 处理相关的对 PII 主体的法律、法规和业务义务，并提供履行这些义务的方法。
A7.3.2	确定 PII 主体的信息	组织应确定并记录向 PII 主体提供有关其 PII 处理和此类规定的时间信息。

A7.3.3	向 PII 主体提供信息	组织应向 PII 主体提供清晰且易于理解的信息，以说明 PII 控制者身份和 PII 处理的描述。
A7.3.4	提供修改或撤销同意的机制	组织应为 PII 主体提供修改或撤销其同意的机制。
A7.3.5	提供反对 PII 处理的机制	组织应为 PII 主体提供一种机制，以反对处理其 PII。
A7.3.6	访问、更正和/或删除	组织应实施策略、程序和/或机制，以履行其对 PII 主体访问、更正和/或删除其 PII 的义务。
A7.3.7	PII 控制者告知第三方的义务	组织应实施适当的政策、程序和/或机制，有关共享 PII 的任何修改、撤回或异议，通知共享 PII 的第三方。
A7.3.8	提供已处理 PII 的副本	组织应能够在 PII 主体要求时，提供被处理 PII 的副本。
A7.3.9	处理请求	组织应定义并记录策略和程序，处理和响应来自 PII 主体的合法请求。
A7.3.10	自动决策	组织应确定并解决 PII 主体的义务，包括法律义务，这些义务是由组织做出的决定产生的，这些决定仅与 PII 主体有关，而且完全基于 PII 的自动处理。
A7.4 设计的隐私和默认的隐私 目标：确保设计流程和系统，使收集和处理（包括使用、披露、保留、传输和处置）限于所确定的必需的目的。		
A7.4.1	限制收集	组织应将 PII 的收集限制在与确定目的相关的、相称的和必要的最小值。
A7.4.2	限制处理	组织应将 PII 处理限制在对已确定的目的而言，是适当的、相关的和必须的。
A7.4.3	准确性和质量	在 PII 的整个生命周期中，组织应确保 PII 尽可能是准确的、完整的和最新的，且是被记录的，这对于处理目的而言是必需的。
A7.4.4	PII 最小化目标	组织应定义和记录数据最小化目标，以及为满足这些目标采用的机制（例如，去标识）。
A7.4.5	PII 处理结束时去除标识和删除	一旦原始 PII 不再需要用于确定的目的，组织应删除 PII 或以不允许识别或重新识别 PII 主体的形式呈现它。
A7.4.6	临时文件	组织应确保由于处理 PII 而创建的临时文件在规定记录期内按照文档化程序进行处理（例如删除或销毁）。
A7.4.7	保留	组织保留 PII 的时间不应超过处理 PII 所需的时间。
A7.4.8	处置	组织应具有处置 PII 的文件化政略、程序和/或机制。
A7.4.9	PII 传输控制	组织应对通过数据传输网络传输（例如发送到另一个组织）的 PII 进行适当的控制，以确保数据到达其预定目的地。
A7.5 PII 共享、转移和披露 目标：确定 PII 有无被共享、转移到其他司法管辖区或第三方和/或根据适用的义务被披露，当以上的情况发生时是否被记录。		
A7.5.1	确定司法管辖区之间 PII 转移的基础	组织应确定并记录管辖区之间 PII 转移的相关基础。
A7.5.2	可以转移 PII 的国家和国际组织	组织应指定并记录可能转移 PII 的国家和国际组织。
A7.5.3	PII 转移记录	组织应记录到第三方的 PII 转移或来自第三方的 PII 转移，并确保与这些方的合作，以支持与 PII 主体义务相关的未来请求。
A7.5.4	向第三方披露 PII 的记录	组织应记录向第三方的 PII 披露，包括已披露的 PII、向谁和何时披露。

Annex B

（规范性）

PIMS--规定的参考控制目标和控制措施（PII 处理者）

本附件供作为 PII 处理者的组织使用，无论 PII 分包商是否使用。 它扩展了 ISO/IEC 27001:2013，附录 A.

表 B.1 中列出的附加或修改的控制目标和控制措施直接源自本文档中定义的控制目标和控制措施，并与 ISO/IEC 27001:2013,6.1.3 的上下文一起使用，如 5.4.1.3 所述。。

并非本附录中列出的所有控制目标和控制措施都必须包含在 PIMS 实施中。删除任何控制目标的理由应包括在适用性声明中（见 5.4.1.3）。 删除的理由可包括风险评估认为不需要控制的地方，以及适用法律和/或法规不要求（或受其限制）的情况。

注：本附件中的条款编号与第 8 章中的子条款编号有关。

Table B.1 – 控制目标和控制措施

B8.2 收集和处理的条件 目标：根据适用的司法管辖区的法律依据，以明确界定和合法目的，确定并记录处理是合法的。		
B8.2.1	客户协议	组织应在必要处确保处理 PII 的合同，解决组织在提供客户义务帮助方面的作用（考虑到处理的性质和组织可用的信息）。
B 8.2.2	组织的目的	组织应确保代表客户处理的 PII 仅按照客户的书面说明中所述的目的进行处理。
B 8.2.3	营销和广告使用	组织不应使用合同下 PII 处理进行营销和广告，而不必确定事先获得相应 PII 主体的同意。
B 8.2.4	侵权指令	如果处理指令违反适用了法律和/或法规，组织应通知客户。
B 8.2.5	客户义务	组织应向客户提供适当的信息，以便客户证明其履行义务。
B 8.2.6	与处理 PII 相关的记录	组织应确定并保持必要的记录，以支持证明其代表客户实施 PII 处理的义务（如适用的合同中所规定）。
B 8.3 对 PII 主体的义务 目标：确保为 PII 主体提供其 PII 处理的适当信息，并履行与 PII 处理相关的任何其他适用义务。		
B 8.3.1	对 PII 主体的义务	组织应为客户提供遵守与 PII 主体相关义务的方法。
B8.4 设计的隐私和默认的隐私 目标：确保设计流程和系统，使收集和处理（包括使用、披露、保留、传输和处置）限于所确定的必需的目的。		
B 8.4.1	临时文件	组织应确保在指定的记录期内按照文件化程序处理（例如删除或销毁）由于处理 PII 而创建的临时文件。
B 8.4.2	归还、转移和处置 PII	组织应提供以安全的方式收回、转移和/或处置 PII 的能力。还应该创建

		一个对客户有效的策略。
B 8.4.3	PII 传输控制	组织应对通过数据传输网络传输的 PII 进行适当的控制，以确保数据到达预定目的地。
B8.5 PII 共享、转移和披露 目标：确定 PII 有无被共享、转移到其他司法管辖区或第三方和/或根据适用的义务被披露，当以上的情况发生时是否被记录。		
B 8.5.1	司法管辖区之间 PII 转移的基础	组织应及时告知客户在周司法管辖区之间进行 PII 转移的基础以及此方面的任何预期更改，以便客户能够反对此类更改或终止合同。
B 8.5.2	可以转移 PII 的国家和国际组织	组织应指定并记录可能转移 PII 的国家和国际组织。
B 8.5.3	向第三方披露 PII 的记录	组织应记录向第三方的 PII 披露，包括已披露的 PII，向谁和何时披露。
B 8.5.4	PII 披露请求的通知	组织应通知客户任何具有法律约束力的 PII 披露的请求。
B 8.5.5	具有法律约束力的 PII 披露	组织应拒绝任何不具有法律约束力的 PII 披露请求，在进行任何 PII 披露并接受相应客户授权的任何合同约定的 PII 披露请求之前，请咨询相应的客户。
B 8.5.6	披露用于处理 PII 的分包商	组织应在使用前，披露任何 PII 处理分包商。
B 8.5.7	分包商处理 PII 的约束	组织应仅依据客户合同雇用分包商处理 PII。
B 8.5.8	分包商处理 PII 的变更	在拥有常规书面授权的情况下，组织应将有关添加或更换分包商处理 PII 的任何预期变更通知客户，从而使客户有机会反对此类变更。

Annex C

（信息的）

映射ISO/IEC 29100

This checklist will provide guidance for governing bodies seeking to develop a governance framework that supports the leveraging of the maximum value from data within their data risk appetite and taking into account external and internal constraints.

Table C.1 – PII控制者与ISO/IEC 29100控制措施的映射

ISO/IEC 29100 隐私原则	PII 控制者的相关控制措施

Annex D

（信息的）

映射通用数据保护条例（GDPR）

The checklist is not exhaustive and governing bodies should evaluate their situation and add additional actions as required.

Table D.1 – ISO/IEC 27701结构映射到GDPR条例

本文档子条款	GDPR 条例

Annex E

（信息的）

映射ISO/IEC 27018和ISO/IEC 29151

Table E.1 – ISO/IEC 27701到ISO/IEC 27018和ISO/IEC 29151的映射

本文档子条款	ISO/IEC 27018 子条款	ISO/IEC 29151 子条款

Annex F

（信息的）

如何应用ISO/IEC 27701到ISO/IEC 27001和ISO/IEC 27002

Table F.1 – 由隐私来映射术语信息安全术语的延伸

ISO/IEC 27001	本文档（延伸）

Bibliography

[1] ISO/IEC 19944, Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use

[2] ISO/IEC 20889, Privacy enhancing data de-identification terminology and classification of techniques

[3] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[4] ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[5] ISO/IEC 27035-1, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

[6] ISO/IEC 29101, Information technology — Security techniques — Privacy architecture framework

[7] ISO/IEC 29134, Information technology — Security techniques — Guidelines for privacy impact assessment

[8] ISO/IEC 29151, Information technology — Security techniques — Code of practice for personally identifiable information protection

[9] ISO/IEC/DIS 29184, Information technology — Security techniques — Guidelines for online privacy notices and consent