目　　录

国际标准 ISO/IEC 27701:2019

第一版
2019-08

安全技术 –
针对 ISO/IEC 27001 和 ISO/IEC 27002
在隐私信息管理的扩展 - 要求和指南

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）是为国际标准化制定专门体制的国际组织。国家机构是 ISO 或 IEC 的成员，他们通过各自的组织建立技术委员会，通过处理特定领域的技术活动来参与国际标准的制定。ISO 和 IEC 技术委员会在共同感兴趣的领域合作。其他国际组织、政府和非政府等机构，通过联络 ISO 和 IEC 参与这项工作。

ISO/IEC 导则第 1 部分中描述了用于开发本标准的过程以及进一步维护的过程。特别是，应注意不同类型的 ISO 文档依据不同的批准标准。本国际标准遵照 ISO/IEC 导则第 2 部分的规则起草（参见 www.iso.org/directives）。

本标准中的某些内容有可能涉及一些专利权问题，这一点应该引起注意。ISO 和 IEC 不负责识别任何这样的专利权问题。在标准制定过程中确定的任何专利权的细节将被列在引言中和 / 或在收到的 ISO 专利声明中（见 www.iso.org/patents）或收到的 IEC 的专利声明清单中（见 http://patents.iec.ch）。

本标准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。

有关标准的自愿性的解释，与符合性评估相关的 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。

本标准由联合技术委员会 ISO/IEC JTC1（信息技术）分委员会 SC27（安全技术）起草。

有关本标准的任何反馈或问题，请直接与本国家的标准组织联系。有关这些机构的完整列表，请访问：www.iso.org/members.html。

引言

0.1 总则

几乎每个组织都会处理个人身份信息（PII）。此外，处理的 PII 的数量和种类以及组织需要与其他组织合作处理 PII 的情况均在增加。在处理 PII 的时候，保护隐私是一项社会需求，也是成为全世界立法和 / 或法规的主题。

信息安全管理体系（ISMS）ISO/IEC 27001 被设计成为容许追加特定领域的要求，而无需开发新的管理体系。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 保护的要求和指南取决于组织的背景，特别是所在国的国家有立法和 / 或法规要求的情况。ISO/IEC 27001 要求理解并考虑该背景。本标准包括映射到：

- ISO/IEC 29100 中定义的隐私框架和原则；
- ISO/IEC 27018；
- ISO/IEC 29151；
- 欧盟通用数据保护条例。

但是，这些可能需要解释为考虑到当地立法和 / 或法规。

本标准可供 PII 控制者（包括 PII 联合控制者）和 PII 处理者（包括使用分包的 PII 处理者和作为分包商处理 PII 的处理者）使用。符合本标准要求的组织将生成有关如何处理 PII 的书面证据。这些证据可用于促进与业务伙伴达成的协议，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，可以将本标准与 ISO/IEC 27001 结合使用，对该证据进行独立验证。

本标准最初是作为 ISO/IEC 27552 开发的。

0.2 与其他管理体系标准的兼容性

本标准应用 ISO 开发的框架，以改善与其管理体系之间的一致性。

本标准使组织能够将其 PIMS 与其他管理体系的要求相协调或整合。

1 范围

本标准规定了要求，并以 ISO/IEC 27001 和 ISO/IEC 27002 扩展的形式为建立、实施、维护和持续改进隐私信息管理体系（PIMS）提供了指南，以便在组织环境内实施隐私管理。

本标准规定了与 PIMS 相关的要求，并为 PII 控制者和 PII 处理者提供了 PII 处理的责任提供了问责的指导。

本标准适用于所有类型和规模的组织，包括公共和私营公司、政府实体和非营利组织，它们是在 ISMS 中处理 PII 的 PII 控制者和 / 或 PII 处理者。

2 规范性引用文件

下列文件全部或部分通过引用而成为本标准的条款。凡是注明日期的引用文件，只有指定版本用于本标准。凡是不注明日期的引用文件，其最新版本（包括对其的任何修订）都适用于本标准。

- ISO/IEC 27000，信息技术 - 安全技术 - 信息安全管理体系 - 总则和词汇
- ISO/IEC 27001:2013，信息技术 - 安全技术 - 信息安全管理体系 - 要求
- ISO/IEC 27002:2013，信息技术 - 安全技术 - 信息安全控制实用规则
- ISO/IEC 29100，信息技术 - 安全技术 - 隐私框架

3 术语、定义和缩写

就本标准而言，ISO/IEC 27000 和 ISO/IEC 29100 中给出的术语和定义同样适用。

ISO/IEC 在以下地址维护用于标准化的术语数据库：

- ISO 在线浏览平台：可从 https://www.iso.org/obp 获得
- IEC Electropedia：可在 http://www.electropedia.org/获得

3.1 PII 联合控制者

与一个或多个 PII 控制者共同决定处理 PII 的目的和方法的 PII 控制者。

3.2 隐私信息管理体系（PIMS）

藉由处置 PII 的过程而可能影响隐私保护的信息安全管理体系。

4 总则

4.1 本标准的结构

这是与 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013 相关特定领域的文档。

本标准专注于 PIMS 领域的要求。遵守本标准的前提是遵守这些要求以及 ISO/IEC 27001:2013 中的要求。在信息安全的基础上，本标准还扩展了 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。为了更好地理解，还包括了实施指南以及其他与要求相关的信息。

第 5 章提供了适用于无论作为 PII 控制者或 PII 处理者的组织，在实施 ISO/IEC 27001 的要求时与 PIMS 相关的特定要求以及其他信息。

注 1：为了完整性，第 5 章包含 ISO/IEC 27001:2013 中包含要求的每个条款的子条款，即使在没有 PIMS 特定要求或其他信息的情况下也一并罗列出。

第 6 章提供了适用于无论作为 PII 控制者或 PII 处理者的组织在实施 ISO/IEC 27002 的控制时相关的 PIMS 特定指南以及其他信息。

注 2：为了完整性，第 6 章包含 ISO/IEC 27002:2013 中包含目标或控制的每个条款的子条款，即使在没有 PIMS 特定要求或其他信息的情况下也一并罗列出。

第 7 章为 PII 控制者提供的 ISO/IEC 27002 补充指南，以及第 8 章为 PII 处理者提供的 ISO/IEC 27002 补充指南。

附录 A 列出了作为 PII 控制者的组织在 PIMS 中特定控制目标和控制（无论是否使用 PII 处理者，以及是否与另一个 PII 控制者联合运作）。

附录 B 列出了作为 PII 处理者的组织在 PIMS 中特定控制目标和控制（无论是否将 PII 处理分包给单独的 PII 处理者，且包括那些对于 PII 处理者将 PII 处理作为 PII 处理分包商的情况）。

附录 C 包含对于 ISO/IEC 29100 的映射。

附录 D 包含本标准中的控制对于 GDPR 的映射。

附录 E 包含对于 ISO/IEC 27018 和 ISO/IEC 29151 的映射。

附录 F 解释了在处理 PII 时如何将 ISO/IEC 27001 和 ISO/IEC 27002 扩展到隐私保护领域。

4.2 ISO/IEC 27001:2013 要求的应用

表 1 给出了本标准中与 ISO/IEC 27001 相关的 PIMS 特定要求的位置。

ISO/IEC 27001:2013 中的条款	标题	本标准子条款	备注
4	组织的背景	5.2	其他要求
5	领导	5.3	没有特定于 PIMS 的要求
6	规划	5.4	其他要求
7	支持	5.5	没有特定于 PIMS 的

			要求
8	运行	5.6	没有特定于 PIMS 的要求
9	绩效评估	5.7	没有特定于 PIMS 的要求
10	改进	5.8	没有特定于 PIMS 的要求

注意：根据 5.1 中的“信息安全”的扩展解释，即使没有特定于 PIMS 的要求，也始终适用。

4.3 ISO/IEC 27002:2013 指南的应用

表 2 给出了本标准中与 ISO/IEC 27002 相关的 PIMS 特定指南的位置。

ISO/IEC 27002:2013 条款	标题	文档子条款	备注
5	信息安全策略	6.2	补充指南
6	信息安全组织	6.3	补充指南
7	人力资源安全	6.4	补充指南
8	资产管理	6.5	补充指南
9	访问控制	6.6	补充指南
10	密码	6.7	补充指南
11	物理安全和环境安全	6.8	补充指南
12	运行安全	6.9	补充指南
13	通信安全	6.10	补充指南
14	信息系统获取、开发	6.11	补充指南

	和维护		
15	供应商关系	6.12	补充指南
16	信息安全事件管理	6.13	补充指南
17	业务连续性管理的信息安全方面	6.14	没有特定于 PIMS 的指南
18	符合性	6.15	补充指南

注意：根据 6.1 的“信息安全”的扩展解释，即使没有特定于 PIMS 的要求，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：组织可以作为联合控制者。

注 2：与组织建立企业对消费者关系的个人在本文档中称为“PII 主体”。

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 处理的分包商签订合同的 PII 处理者（例如，PII 分包处理者的客户）。

注 3：第 6 章中提到的“客户”，相关条款可适用于 a）、b）或 c）的环境中。

注 4：第 7 章和附录 A 中提到的“客户”，相关条款可适用于 a）的环境中。

注 5：第 8 章和附录 B 中提到的“客户”，相关条款可适用于 b）和 / 或 c）的环境中。

5 与 ISO/IEC 27001 相关的 PIMS 特定要求

5.1 总则

ISO/IEC 27001:2013 中提及的“信息安全”的要求应扩展到经由 PII 过程可能影响的隐私保护。

注意：在实践中，ISO/IEC 27001:2013 中所使用的“信息安全”，相当于“信息安全和隐私”（见附录 F）。

5.2 组织环境

5.2.1 了解组织及其环境

ISO/IEC 27001:2013，4.1 的附加要求是：

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

组织应确定与其环境相关，影响其实现 PIMS 预期结果的能力的外部和内部因素。例如，可包括：

- 适用的隐私法律；
- 适用的法规；
- 适用的司法判决；
- 适用的组织环境、治理、政策和规程；
- 适用的行政决定；
- 适用的合同要求。

如果组织在两个角色中都扮演（例如 PII 控制者和 PII 处理者），每个的角色应该被定义，每个角色都应作为一组独立控制的对象。

注：对于 PII 处理的每个实例，组织的角色可能不同，因为角色取决于有谁来决定处理的目的和方式。

5.2.2 理解相关方的需求和期望

ISO/IEC 27001:2013，4.2 的附加要求是：

组织应包括其相关方（参见 ISO/IEC 27001:2013，4.2），包括：与 PII 处理有关的、有利益关系或负有责任的各方，甚至是 PII 主体。

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有法律法规、合同义务和组织自己规定的目标来确定。在 ISO/IEC 29100 中规定的隐私原则提供了有关 PII 处理的指导。

注 3：作为组织符合某一个义务的证明，一些利益相关方可以期望组织符合特定标准，例如本标准中规定的管理体系和 / 或任何相关的规范。利益相关方可以要求对这些标准进行独立审核。

5.2.3 确定信息安全管理体系的范围

ISO/IEC 27001:2013，4.3 的附加要求是：

在确定 PIMS 的范围时，组织应包括 PII 的处理。

注：根据 5.1 中“信息安全”的扩展解释，确定 PIMS 的范围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 27001:2013，4.4 的附加要求是：

组织应根据本标准第 5 章中被扩充的 ISO/IEC 27001:2013 第 4 章至第 10 章的要求建立、实施、维护和持续改进 PIMS。

5.3 领导

5.3.1 领导和承诺

适用 ISO/IEC 27001:2013，5.1 中陈述的要求以及本标准 5.1 中规定的解释。

5.3.2 方针

适用 ISO/IEC 27001:2013，5.2 中陈述的要求以及本标准 5.2 中规定的解释。

5.3.3 组织角色、职责和权限

适用 ISO/IEC 27001:2013，5.3 中陈述的要求以及本标准 5.3 中规定的解释。

5.4 规划

5.4.1 应对风险和机遇的措施

5.4.1.1 总则

适用 ISO/IEC 27001:2013，6.1.1 中陈述的要求以及本标准 5.1 中规定的解释。

5.4.1.2 信息安全风险评估

适用 ISO/IEC 27001:2013，6.1.2 中陈述的要求以及下列改进内容：

ISO/IEC 27001:2013，6.1.2 c）1）改进如下：

组织应在 PIMS 范围内应用信息安全风险评估流程来识别与保密性、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流程来识别与 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：组织可以应用整合的信息安全和隐私风险评估流程，也可以应用两个单独的流程来评估信息安全和 PII 处理相关的风险。

ISO/IEC 27001:2013，6.1.2 d）1）改进如下：

如果上述 ISO/IEC 27001:2013，6.1.2 d）中识别的风险实现的话，组织应评估其对组织和 PII 主体的潜在后果。

5.4.1.3 信息安全风险处理

适用 ISO/IEC 27001:2013，6.1.3 中规定的要求以及以下增补内容：

ISO/IEC 27001:2013，6.1.3 c）改进如下：

ISO/IEC 27001:2013 6.1.3 b）中确定的控制应与附录 A 和 / 或附录 B，以及 ISO/IEC 27001:2013 的附录 A 进行比较，以确认没有遗漏任何必要的控制。

在评估 ISO/IEC 27001:2013 附录 A 中控制目标和控制对风险处理的适用性时，应在信息安全风险以及处理 PII 的风险包括 PII 主体的风险的背景下考虑控制目标和控制。

ISO/IEC 27001:2013，6.1.3 d）改进如下：

制定适用性声明，其中包含：

- 必要的控制 [见 ISO/IEC 27001:2013，6.1.3 b）和 c）]；
- 包含它们的理由；
- 是否实施了必要的控制措施；以及
- 根据组织的角色（见 5.2.1），要明确排除任何附录 A 和 / 或附录 B 以及 ISO/IEC 27001:2013 附录 A 中的控制的理由。

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。排除的理由可能是根据风险评估而确定的不需要控制的地方，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（或不被期待）的地方。

5.4.2 信息安全目标和实现规划

适用 ISO/IEC 27001:2013，6.2 中陈述的要求以及本标准 5.1 中的解释。

5.5 支持

5.5.1 资源

适用 ISO/IEC 27001:2013，7.1 中陈述的要求以及本标准 5.1 中的解释。

5.5.2 能力

适用 ISO/IEC 27001:2013，7.2 中陈述的要求以及本标准 5.1 中的解释。

5.5.3 意识

适用 ISO/IEC 27001:2013，7.3 中陈述的要求以及本标准 5.1 中的解释。

5.5.4 沟通

适用 ISO/IEC 27001:2013，7.4 中陈述的要求以及本标准 5.1 中的解释。

5.5.5 文件记录信息

5.5.5.1 总则

适用 ISO/IEC 27001:2013，7.5 中陈述的要求以及本标准 5.1 中的解释。

5.5.5.2 创建和更新

适用 ISO/IEC 27001:2013，7.5.2 中陈述的要求以及本标准 5.1 中的解释。

5.5.5.3 控制记录的信息

适用 ISO/IEC 27001:2013，7.5.3 中陈述的要求以及本标准 5.1 中的解释。

5.6 运行

5.6.1 运行的规划和控制

适用 ISO/IEC 27001:2013，8.1 中陈述的要求以及本标准 5.1 中的解释。

5.6.2 信息安全风险评估

适用 ISO/IEC 27001:2013，8.2 中陈述的要求以及本标准 5.1 中的解释。

5.6.3 信息安全风险处置

适用 ISO/IEC 27001:2013，8.3 中陈述的要求以及本标准 5.1 中的解释。

5.7 绩效评价

5.7.1 监测、测量、分析和评价

适用 ISO/IEC 27001:2013，9.1 中陈述的要求以及本标准 5.1 中的解释。

5.7.2 内部审核

适用 ISO/IEC 27001:2013，9.2 中陈述的要求以及本标准 5.1 中的解释。

5.7.3 管理评审

适用 ISO/IEC 27001:2013，9.3 中陈述的要求以及本标准 5.1 中的解释。

5.8 改进

5.8.1 不符合和纠正措施

适用 ISO/IEC 27001:2013，10.1 中陈述的要求以及本标准 5.1 中的解释。

5.8.2 持续改进

适用 ISO/IEC 27001:2013，10.2 中陈述的要求以及本标准 5.1 中的解释。

6 与 ISO/IEC 27002 相关的 PIMS 特定指南

6.1 总则

ISO/IEC 27002:2013 中提及 “信息安全” 的指南应扩展到可能受 PII 处理潜在影响的隐私保护。

注 1：在实际使用中，在 ISO/IEC 27002:2013 中使用的 “信息安全” 的地方，等同于 “信息安全和隐私”（见附录 F）。

所有控制目标和控制都应考虑到信息安全风险以及与 PII 处理相关的隐私风险。

注 2：除非在第 6 章中具体规定，或由组织根据适用的司法管辖区决定，相同的指南适用于 PII 控制者和 PII 处理者。

6.2 信息安全策略

6.2.1 信息安全管理指导

6.2.1.1 信息安全策略

适用 ISO/IEC 27002:2013，5.1.1 中规定的控制、实施指南、其他信息以及以下补充指南：

针对 ISO/IEC 27002:2013 5.1.1 信息安全策略的补充指南是：

无论是制定单独的隐私策略，还是通过增加信息安全策略，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 保护法律和 / 或法规以及商定的合同条款（商定范围包括组织之间及其合作伙伴、分包商及其合作伙伴适用的第三方如客户、供应商等，且应明确分配它们之间的责任）。

针对 ISO/IEC 27002:2013 5.1.1 信息安全策略补充的其他信息是：

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

6.2.1.2 信息安全策略的评审

适用 ISO/IEC 27002:2013，5.1.2 中规定的控制、实施指南和其他信息。

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 ISO/IEC 27002:2013，6.1.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，6.1.1 信息安全角色和职责的补充实施指南是：

在处理 PII 方面组织宜指定一个联络点，供客户使用。当组织是 PII 控制者时，组织在处理 PII 方面给 PII 主体指定联络点（参见 7.3.2）。

组织宜指定一名或多名负责制定、实施、维护和监督组织范围的治理和隐私流程（program）的人员，以确保遵守有关处理 PII 的所有适用法律和法规。

在适当时，负责人宜：

- 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；
- 参与管理与处理 PII 有关的所有问题；
- 是数据保护法律、监管和实践方面的专家；
- 作为监管机构的联络点；
- 告知高层管理层和组织内员工在处理 PII 方面的义务；
- 就组织进行的隐私影响评估提供建议。

注：某些司法管辖区会定义何时需要这样的职位，以及他们的职位和角色，这样的人被称为数据保护官。该职位可由内部工作人员或外包人员履行。

6.3.1.2 职责分离

适用 ISO/IEC 27002:2013，6.1.2 中规定的控制、实施指南和其他信息。

6.3.1.3 与职能机构的联系

适用 ISO/IEC 27002:2013，6.1.3 中规定的控制、实施指南和其他信息。

6.3.1.4 与特殊利益集团联系

适用 ISO/IEC 27002:2013，6.1.4 中规定的控制、实施指南和其他信息。

6.3.1.5 项目管理中的信息安全

适用 ISO/IEC 27002:2013，6.1.5 中规定的控制、实施指南和其他信息。

6.3.2 移动设备和远程工作

6.3.2.1 移动设备策略

适用 ISO/IEC 27002:2013，6.2.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，6.2.1 的移动设备策略的补充实施指南是：

组织宜确保移动设备的使用不会导致 PII 的危害。

6.3.2.2 远程办公

适用 ISO/IEC 27002:2013，6.2.2 中规定的控制、实施指南和其他信息。

6.4 人力资源安全

6.4.1 任用前

6.4.1.1 审查

适用 ISO/IEC 27002:2013，7.1.1 中规定的控制、实施指南和其他信息。

6.4.1.2 任用条款和条件

适用 ISO/IEC 27002:2013，7.1.2 中规定的控制、实施指南和其他信息。

6.4.2 任用中

6.4.2.1 管理责任

适用 ISO/IEC 27002:2013，7.2.1 中规定的控制、实施指南和其他信息。

6.4.2.2 信息安全意识、教育和培训

适宜采取措施，包括对事故报告的认识，以确保相关工作人员了解对组织可能造成的后果（例如法律后果、业务损失和品牌或声誉受损）、对工作人员的后果（例如纪律处分的后果）以及对违反隐私或安全规则和流程（尤其是那些涉及 PII 处理的规则和流程）的 PII 主体的后果（例如物理、物质和情感的后果）。

注：这些措施可包括对有权访问 PII 的人员进行适当的定期培训。

6.4.2.3 违规处理过程

适用 ISO/IEC 27002:2013，7.2.3 中规定的控制、实施指南和其他信息。

6.4.3 任用终止和变更

6.4.3.1 任用终止或变更的责任

适用 ISO/IEC 27002:2013，7.3.1 中规定的控制、实施指南和其他信息。

6.5 资产管理

6.5.1 资产责任

6.5.1.1 资产清单

适用 ISO/IEC 27002:2013，8.1.1 中规定的控制、实施指南和其他信息。

6.5.1.2 资产的所属关系

适用 ISO/IEC 27002:2013，8.1.2 中规定的控制、实施指南和其他信息。

6.5.1.3 资产的可接受使用

适用 ISO/IEC 27002:2013，8.1.3 中规定的控制、实施指南和其他信息。

6.5.1.4 资产归还

适用 ISO/IEC 27002:2013，8.1.4 中规定的控制、实施指南和其他信息。

6.5.2 信息分类

6.5.2.1 信息分类

适用 ISO/IEC 27002:2013，8.2.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，8.2.1 信息分类的补充实施指南是：

组织的信息分类系统宜明确将 PII 视为其实施方案的一部分。在整个分类系统中考虑 PII 对于理解组织什么处理 PII（例如种类、特殊类别），以及存储此类 PII 的位置以及它可以在哪些系统内流通是不可或缺的。

6.5.2.2 信息标记

适用 ISO/IEC 27002:2013，8.2.2 中规定的控制、实施指南和其他信息以及以下附加补充指南：

ISO/IEC 27002:2013，8.2.2 信息的标记的补充实施指南是：

组织宜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 ISO/IEC 27002:2013，8.2.3 中规定的控制、实施指南和其他信息。

6.5.3 介质处理

6.5.3.1 可移动介质的管理

适用 ISO/IEC 27002:2013，8.3.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，8.3.1 移动介质的管理的补充实施指南是：

组织应记录用于存储 PII 的移动介质和 / 或设备的任何使用情况。在可行的情况下，组织宜在存储 PII 时，对可移动物理介质和 / 或设备使用加密方法。未加密的介质仅宜在不可避免的情况下使用，并且在使用未加密的介质和 / 或设备的情况，组织宜实施相应规程或补偿控制（例如防篡改包装）以降低 PII 的风险。

ISO/IEC 27002:2013，8.3.1 移动介质管理的其他信息是：

被带出组织的物理范围之外的移动介质容易丢失、损坏、被不当访问。加密移动介质可为 PII 增加一定程度的保护，从而降低移动介质在安全性和隐私方面受到侵害的风险。

6.5.3.2 介质的处置

适用 ISO/IEC 27002:2013，8.3.2 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，8.3.2 介质的处置的补充实施指南是：

在处置存储 PII 的移动介质的情况下，安全处理规程应包括在存档文件中，并实施以确保先前存储的 PII 信息不能被访问。

6.5.3.3 物理介质的转移

适用 ISO/IEC 27002:2013，8.3.3 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，8.3.3 物理介质的转移的补充实施指南是：

如果使用物理介质进行信息传输，则宜建立一个系统来记录包含 PII 的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。在可能的情况下，宜实施其他措施（如加密），以确保数据只能在目的地而非传输途中被访问。

组织宜在物理介质离开所在场所之前对包含 PII 的物理介质实施授权的规程，并确保除授权人员之外的任何人都无法访问 PII。

注：确保离开组织场所的物理介质上的 PII 安全的一种可能的措施是加密 PII 使其不可访问，并且将解密的能力限定在被授权人员身上。

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 ISO/IEC 27002:2013，9.1.1 中规定的控制、实施指南和其他信息。

6.6.1.2 网络和网络服务的访问

适用 ISO/IEC 27002:2013，9.1.2 中规定的控制、实施指南和其他信息。

6.6.2 用户访问管理

6.6.2.1 用户注册和注销

适用 ISO/IEC 27002:2013，9.2.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，9.2.1 用户注册和注销的补充实施指南是：

管理或操作处理 PII 的系统和服务的用户的注册和注销流程宜解决用户对其的访问控制受到危害的情况，例如密码或其他用户注册数据的损坏或危害（例如，无意泄露的情况）。

对于处理 PII 的系统和服务，组织不宜向用户重新发布任何已失效或已过期的用户 ID。

在组织将 PII 处理作为服务提供的情况下，客户可以负责一些或所有方面的用户 ID 管理。此类情况宜包括在文件化信息中。

某些司法管辖区对与处理 PII 的系统相关的未使用的身份验证凭据的检查频率提出了特定要求。在这些司法管辖区运营的组织应考虑到这些要求。

6.6.2.2 用户访问供给

适用 ISO/IEC 27002:2013，9.2.2 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 9.2.2 用户访问配置的补充实施指南是：

组织宜保持为已授权访问信息系统（其中包含 PII）创建的用户信息的记录准确，且保持最新。该记录包括关于该用户的一系列数据，包括用户 ID，以及用于实现提供授权访问的所识别的技术控制。

通过设置用户访问的唯一 ID，实施适当配置以使得系统能够识别访问 PII 的用户、以及用户所做的添加、删除或更改。这样的配置在保护了组织的同时也保护了用户，系统可以识别用户已处理、未处理的内容。

在组织将 PII 处理作为服务提供的情况下，客户可以承担访问管理的部分或全部职责。在适当的情况下，组织宜向客户提供执行访问管理的方法，例如通过提供管理权限来管理或终止访问。此类情况宜包括在文件化信息中。

6.6.2.3 特定访问权管理

适用 ISO/IEC 27002:2013，9.3.3 中规定的控制、实施指南和其他信息。

6.6.2.4 用户的秘密鉴别信息管理

适用 ISO/IEC 27002:2013，9.2.4 中规定的控制、实施指南和其他信息。

6.6.2.5 用户访问权的评审

适用 ISO/IEC 27002:2013，9.2.5 中规定的控制、实施指南和其他信息。

6.6.2.6 访问权的移除或调整

适用 ISO/IEC 27002:2013，9.2.6 中规定的控制、实施指南和其他信息。

6.6.3 用户责任

6.6.3.1 秘密鉴别信息的使用

适用 ISO/IEC 27002:2013，9.3.1 中规定的控制、实施指南和其他信息。

6.6.4 系统和应用程序访问控制

6.6.4.1 信息访问限制

适用 ISO/IEC 27002:2013，9.4.1 中规定的控制、实施指南和其他信息。

6.6.4.2 安全登录规程

适用 ISO/IEC 27002:2013，9.4.2 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，9.4.2 安全登录规程的补充实施指南是：

如果客户要求，组织宜具备为客户控制下的任何帐户提供安全登录规程的能力。

6.6.4.3 口令管理体系

适用 ISO/IEC 27002:2013，9.4.3 中规定的控制、实施指南和其他信息。

6.6.4.4 特权实用程序的使用

适用 ISO/IEC 27002:2013，9.4.4 中规定的控制、实施指南和其他信息。

6.6.4.5 程序源代码的访问控制

适用 ISO/IEC 27002:2013，9.4.5 中规定的控制、实施指南和其他信息。

6.7 密码

6.7.1 密码控制

6.7.1.1 密码控制的使用策略

适用 ISO/IEC 27002:2013，10.1.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，10.1.1 密码控制的使用策略的补充实施指南是：

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。

组织宜向客户提供有关其使用什么样的加密技术来保护其处理的 PII 的信息。组织还宜向客户提供相应的功能信息，以帮助客户应用自己的加密技术保护自身的 PII 信息。

6.7.1.2 密钥管理

适用 ISO/IEC 27002:2013，10.1.2 中规定的控制、实施指南和其他信息。

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 ISO/IEC 27002:2013，11.1.1 中规定的控制、实施指南和其他信息。

6.8.1.2 物理入口控制

适用 ISO/IEC 27002:2013，11.1.2 中规定的控制、实施指南和其他信息。

6.8.1.3 办公室、房间和设施的安全保护

适用 ISO/IEC 27002:2013，11.1.3 中规定的控制、实施指南和其他信息。

6.8.1.4 外部和环境威胁的安全防护

适用 ISO/IEC 27002:2013，11.1.4 中规定的控制、实施指南和其他信息。

6.8.1.5 在安全区域工作

适用 ISO/IEC 27002:2013，11.1.5 中规定的控制、实施指南和其他信息。

6.8.1.6 交接区

适用 ISO/IEC 27002:2013，11.1.6 中规定的控制、实施指南和其他信息。

6.8.2 设备

6.8.2.1 设备安置和保护

适用 ISO/IEC 27002:2013，11.2.1 中规定的控制、实施指南和其他信息。

6.8.2.2 支持性设施

适用 ISO/IEC 27002:2013，11.2.2 中规定的控制、实施指南和其他信息。

6.8.2.3 布缆安全

适用 ISO/IEC 27002:2013，11.2.3 中规定的控制、实施指南和其他信息。

6.8.2.4 设备维护

适用 ISO/IEC 27002:2013，11.2.4 中规定的控制、实施指南和其他信息。

6.8.2.5 资产的移动

适用 ISO/IEC 27002:2013，11.2.5 中规定的控制、实施指南和其他信息。

6.8.2.6 组织场所外的设备与资产安全

适用 ISO/IEC 27002:2013，11.2.6 中规定的控制、实施指南和其他信息。

6.8.2.7 设备的安全处置或再利用

适用 ISO/IEC 27002:2013，11.2.7 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 11.2.7 设备的安全处置或再利用的补充实施指南是：

组织宜确保每次重新分配存储空间时，以前驻留在该存储空间中的任何 PII 都不可访问。

在删除信息系统中保留的 PII 时，受设备性能因素制约，彻底删除该 PII 是可能是不切实际的。这会产生另一个用户可以访问 PII 的风险。宜通过具体的技术措施避免这种风险。

为了安全处置或再利用，可能包含 PII 的存储介质的设备宜被视为包含 PII。

6.8.2.8 无人值守的用户设备

适用 ISO/IEC 27002:2013，11.2.8 中规定的控制、实施指南和其他信息。

6.8.2.9 清理桌面和屏幕策略

适用 ISO/IEC 27002:2013，11.2.9 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 11.2.9 清理桌面和屏幕策略的补充实施指南是：

组织宜将包含 PII 的硬拷贝材料的创建数量，限定在满足已知处理目的最低值。

6.9 运行安全

6.9.1 运行规程和责任

6.9.1.1 文件化的操作规程

适用 ISO/IEC 27002:2013，12.1.1 中规定的控制、实施指南和其他信息。

6.9.1.2 变更管理

适用 ISO/IEC 27002:2013，12.1.2 中规定的控制、实施指南和其他信息。

6.9.1.3 容量管理

适用 ISO/IEC 27002:2013，12.1.3 中规定的控制、实施指南和其他信息。

6.9.1.4 开发、测试和运行环境的分离

适用 ISO/IEC 27002:2013，12.1.4 中规定的控制、实施指南和其他信息。

6.9.2 恶意软件防范

6.9.2.1 恶意软件的控制

适用 ISO/IEC 27002:2013，12.2.1 中规定的控制、实施指南和其他信息。

6.9.3 备份

6.9.3.1 信息备份

适用 ISO/IEC 27002:2013，12.3.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，12.3.1 信息备份的补充实施指南是：

组织宜制定策略，以满足 PII 的备份、恢复和恢复要求（可以是整体信息备份策略的一部分），进而满足删除备份数据中包含的 PII 信息的要求（例如合同和 / 或法律要求）。

在这方面，PII 的具体职责可能取决于客户。组织宜确保已通知客户有关备份的服务限制。

如果组织明确向客户提供备份和还原服务，组织宜向他们提供有关其备份和恢复 PII 功能的明确信息。

某些司法管辖区对 PII 的备份频率、备份的审查频率、测试和恢复频率或者相应的恢复规程提出了具体要求。在这些司法管辖区运营的组织宜证明符合这些要求。

可能存在需要恢复 PII 的情况，可能是由于系统故障、攻击或灾难。当 PII 恢复时（通常来自备份介质），需要建立确保 PII 恢复到可以确保 PII 完整性的状态，和 / 或识别 PII 不准确和 / 或不完整的状态以及解决这些问题的流程（可能涉及 PII 主体）。

组织宜有 PII 恢复工作的流程和日志。至少，PII 恢复的日志宜包含：

- 负责恢复的人的姓名；
- 已恢复的 PII 的说明。

一些司法管辖区规定了 PII 恢复工作日志的内容。组织宜能够记录恢复日志的适当内容以符合辖区特定要求。此类审议的结论宜包括在文档化信息中。

在本标准中记述的关于分包商处理 PII 信息的控制（请参阅 6.5.3.3，6.12.1.2）中，规定了使用分包商来存储 PII 处理的复制或备份的要求。本标准中的控制（6.10.2.1）也包含了与备份和恢复相关的物理介质传输的情况。

6.9.4 日志和监视

6.9.4.1 事态日志

适用 ISO/IEC 27002:2013，12.4.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，12.4.1 事态日志的补充实施指南是：

宜建立一个流程并使用连续的、手动或自动化的监控和警报流程来审查事件日志。手动审查宜以明确的、文档化规定的周期实施，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，包括由谁、何时、访问哪个 PII 主体的 PII，以及由于事件而进行的任何更改（添加、修改或删除）。

如果多个服务提供者参与提供服务，则在实施本指南时可能会有不同或共享角色。宜明确定义这些角色并将其包含在文档化信息中，并宜就供应者实施的任何日志访问达成协议。

PII 处理者的实施指南：

组织宜定义关于客户是否、何时以及如何确保日志信息可用的标准。这些标准宜提供给客户。

如果组织允许其客户访问组织控制的日志记录，组织宜实施适当的控制以确保客户只能访问与该客户的活动相关的记录，不能访问与其他客户的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 日志信息的保护

适用 ISO/IEC 27002:2013，12.4.2 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，12.4.2 日志信息的保护的补充实施指南是：

记录的日志信息例如安全、监视和操作诊断可以包含 PII。宜采取措施如控制访问（参见 ISO/IEC 27002:2013，9.2.3），以确保记录的信息仅按预期使用。

宜建立一个规程，最好是自动规程，以确保按照保留计划删除或去标志记录信息（参见 7.4.7）。

6.9.4.3 管理员和操作员日志

适用 ISO/IEC 27002:2013，12.4.3 中规定的控制、实施指南和其他信息。

6.9.4.4 时钟同步

适用 ISO/IEC 27002:2013，12.4.4 中规定的控制、实施指南和其他信息。

6.9.5 运行软件的控制

6.9.5.1 在运行系统上安装软件

适用 ISO/IEC 27002:2013，12.5.1 中规定的控制、实施指南和其他信息。

6.9.6 技术脆弱性管理

6.9.6.1 技术脆弱性的管理

适用 ISO/IEC 27002:2013，12.6.1 中规定的控制、实施指南和其他信息。

6.9.6.2 软件安装限制

适用 ISO/IEC 27002:2013，12.6.2 中规定的控制、实施指南和其他信息。

6.9.7 信息系统审计的考虑

6.9.7.1 信息系统审计控制

适用 ISO/IEC 27002:2013，12.7.1 中规定的控制、实施指南和其他信息。

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 ISO/IEC 27002:2013，13.1.1 中规定的控制、实施指南和其他信息。

6.10.1.2 网络服务的安全

适用 ISO/IEC 27002:2013，13.1.2 中规定的控制、实施指南和其他信息。

6.10.1.3 网络隔离

适用 ISO/IEC 27002:2013，13.1.3 中规定的控制、实施指南和其他信息。

6.10.2 信息传输

6.10.2.1 信息传输策略和规程

适用 ISO/IEC 27002:2013，13.2.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 13.2.1 信息传输策略和规程的补充实施指南是：

组织宜考虑确保在适用的情况下，在系统内外强制执行与 PII 处理相关的规则程。

6.10.2.2 信息传输协议

适用 ISO/IEC 27002:2013，13.2.2 中规定的控制、实施指南和其他信息。

6.10.2.3 电子消息发送

适用 ISO/IEC 27002:2013，13.2.3 中规定的控制、实施指南和其他信息。

6.10.2.4 保密或不泄漏协议

适用 ISO/IEC 27002:2013，13.2.4 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，13.2.4 保密或不泄漏协议的补充实施指南是：

组织宜确保在其控制下，访问 PII 的操作的个人承担保密义务。无论是合同的一部分还是单独的保密协议，都应规定履行义务的时效。

当组织是 PII 处理者时，组织、员工及其代理之间的任何形式的保密协议宜确保员工遵守有关数据处理和保护的策略、规程。

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 信息安全要求分析和说明

适用 ISO/IEC 27002:2013，14.1.1 中规定的控制、实施指南和其他信息。

6.11.1.2 公共网络上的应用服务的安全保护

适用 ISO/IEC 27002:2013，14.1.2 中规定的控制、实施指南和其他信息及以下补充指南：

ISO/IEC 27002:2013，14.1.2 公共网络上的应用服务的安全保护的补充实施指南是：

组织宜确保在不受信任的数据传输网络上传输的 PII 被加密后方可进行传输。

不受信任的网络包括：公共互联网和组织运营控制之外的其他设施。

注意：在某些情况下（例如，电子邮件的交换），不可信数据传输网络系统的固有特性可能要求暴露一些报头或流量数据，方可进行有效传输。

6.11.1.3 应用服务事务的保护

适用 ISO/IEC 27002:2013，14.1.3 中规定的控制、实施指南和其他信息。

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 ISO/IEC 27002:2013，14.2.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，14.2.1 安全的开发策略的补充指南是：

基于对 PII 原则和 / 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，系统开发以及设计的策略宜包含组织对处理 PII 需求的指南，第 7 章和第 8 章提供处理 PII 的控制考虑因素可用于制定系统设计中的隐私策略。

对隐私有贡献的设计的策略和默认的策略宜考虑以下几个方面：

a) 关于 PII 保护的指南以及软件开发生命周期中隐私原则的实施（参见 ISO/IEC 29100）；

b) 设计阶段的隐私和 PII 的保护要求，可以从隐私风险评估和 / 或隐私影响评估得到输出（参见 7.2.5）；

c) 项目里程碑内的 PII 保护检查点；

d) 必要的隐私和 PII 保护知识；

e) 默认情况下，最小化 PII 的处理。

6.11.2.2 系统变更控制规程

适用 ISO/IEC 27002:2013，14.2.2 中规定的控制、实施指南和其他信息。

6.11.2.3 运行平台变更后对应用的技术评审

适用 ISO/IEC 27002:2013，14.2.3 中规定的控制、实施指南和其他信息。

6.11.2.4 软件包变更的限制

适用 ISO/IEC 27002:2013，14.2.4 中规定的控制、实施指南和其他信息。

6.11.2.5 系统安全工程原则

适用 ISO/IEC 27002:2013，14.2.5 中规定的控制、实施指南和其他信息以及以下附加补充指南：

ISO/IEC 27002:2013，14.2.5 安全系统工程原则的补充实施指南是：

与 PII 处理相关的系统和 / 或组件宜按照设计的隐私原则和默认的隐私原则来设计，并预测和促进相关控制的实施（如第 7 章和第 8 章，分别对于 PII 控制者和 PII 处理者的描述），特别是在这些系统中 PII 的收集和处理仅限于所识别到的必须的 PII 处理目的（见 7.2）。

例如，在相关管辖区内，组织宜确保在指定期限内处置 PII，处理该 PII 的系统宜设计相应功能以便能实施删除操作，来满足该要求。

6.11.2.6 安全的开发环境

适用 ISO/IEC 27002:2013，14.2.6 中规定的控制、实施指南和其他信息。

6.11.2.7 外包开发

适用 ISO/IEC 27002:2013，14.2.7 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，14.2.7 外包开发的补充指南是：

设计的隐私原则和默认的隐私原则（见 6.11.2.5）如果适用，也同样适用于外包信息系统。

6.11.2.8 系统安全测试

适用 ISO/IEC 27002:2013，14.2.8 中规定的控制、实施指南和其他信息。

6.11.2.9 系统验收测试

适用 ISO/IEC 27002:2013，14.2.9 中规定的控制、实施指南和其他信息。

6.11.3 测试数据

6.11.3.1 测试数据的保护

适用 ISO/IEC 27002:2013，14.3.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 14.3.1 测试数据保护的补充实施指南是：

PII 不宜用于测试目的；宜使用假的或合成的 PII。如果无法避免将 PII 用于测试目的，则宜实施与生产环境中使用的等效的技术和组织措施，以最大限度地降低风险。如果这种等效措施不可行，则宜进行风险评估，并用于选择适当的减缓风险的控制措施。

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 ISO/IEC 27002:2013，15.1.1 中规定的控制、实施指南和其他信息。

6.12.1.2 在供应商协议中强调安全

适用 ISO/IEC 27002:2013，15.1.2 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，15.1.2 在供应商协议中强调安全的补充实施指南是：

组织宜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（参见 7.2.6 和 8.2.1）。

供应商协议宜在考虑处理的 PII 种类的情况下，明确地在组织、合作伙伴、供应商和适当的第三方（客户、供应商等）之间分配职责。

组织与其供应商之间的协议宜提供一种机制，以确保组织支持和管理对所有适用法律和 / 或法规的遵守情况。协议宜要求客户接受独立审核以验证其合规性。

注：出于此类审核目的，可以考虑遵守相关和适用的安全和隐私标准，如 ISO/IEC 27001 或本标准。

PII 处理者的实施指南：

组织宜在与任何供应商的合同中指明 PII 仅允许在其指导下进行处理。

6.12.1.3 信息与通信技术供应链

适用 ISO/IEC 27002:2013，15.1.3 中规定的控制、实施指南和其他信息。

6.12.2 供应商服务交付管理

6.12.2.1 供应商服务的监视和审查

适用 ISO/IEC 27002:2013，15.2.1 中规定的控制、实施指南和其他信息。

6.12.2.2 供应商服务的变更管理

适用 ISO/IEC 27002:2013，15.2.2 中规定的控制、实施指南和其他信息。

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 责任和规程

适用 ISO/IEC 27002:2013，16.1.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，16.1.1 责任和规程中的补充指南是：

作为整个信息安全事件管理过程的一部分，组织宜建立识别、记录违反 PII 的责任和处置规程。此外，组织应考虑适用的法律和 / 或法规，规定报告 PII 违规行为的通知方（包括此类通知的时间安排）和向执法当局披露的责任和规程。

一些司法管辖区对违规响应做出了具体规定，包括通知义务。在这些司法管辖区内运营的组织宜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 ISO/IEC 27002:2013，16.1.2 中规定的控制、实施指南和其他信息。

6.13.1.3 报告信息安全弱点

适用 ISO/IEC 27002:2013，16.1.3 中规定的控制、实施指南和其他信息。

6.13.1.4 信息安全事态的评估和决策

适用 ISO/IEC 27002:2013，16.1.4 中规定的控制、实施指南和其他信息。

6.13.1.5 信息安全事件的响应

适用 ISO/IEC 27002:2013，16.1.5 中规定的控制、实施指南和其他信息以及以下补充指南：

PII 控制者的实施指南：

作为其信息安全事件管理流程的一部分，涉及 PII 的事件宜引发组织的评审，以确定是否触发了 PII 违规行为响应流程。

事件不一定会触发此类评审。

注 1：导致未经授权访问 PII、访问存储 PII 的设备或设施，不一定以高频信息安全事件的形式展现。这些事件可以包括但不限于：对防火墙或边缘服务器的 ping 攻击（用来测试数据包能否利用 IP 协议访问特定主机）和其他广播攻击，端口扫描攻击，不成功的登录尝试攻击，拒绝服务攻击和数据包嗅探攻击。

当违反 PII 发生时，响应规程宜包括相关通知和记录。

某些司法管辖区定义了宜将违反行为通知监管机构的情况，以及何时宜通知 PII 主体的情况。

通知宜明确的且是被要求的。

* 注 2：通知可以包含以下详细信息：

- 可以获得更多信息的联络点；
- 违规的可能后果；
- 对违规行为的描述，包括设计有关人员的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，宜保留一份记录，并提供足够的信息，以便为监管和 / 或司法目的提供报告，例如：

- 对事件的描述；
- 时间段；
- 事件的后果；

- 报告者的名字；
- 事件报告给了谁；
- 为解决事件所采取的步骤（包括负责人和恢复的数据）；
- 事件导致 PII 无法获得、丢失、披露或更改的情况。

如果发生涉及 PII 的违规行为，该记录还宜包括已泄露的 PII 描述（如果已知）；如果需要实施通知，宜采取措施通知 PII 主体，监管机构或客户。

PII 处理者的实施指南：

涉及 PII 违约通知的规定宜是组织与客户之间合同的一部分。合同应规定组织如何提供客户必需的信息，以保证顾客履行他们向相关机构通知的义务。此通知义务不会延伸到由客户或 PII 主体触发的由其承担负责的系统组件的违规。合同还宜定义与外部沟通时，双方必须遵守的响应时间。

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，期望事件一旦被发现，PII 控制者就可以采取适当的行动。

如果发生 PII 的违规行为，宜保留一份记录，并提供足够的信息，以便为监管和 / 或司法目的提供报告，例如：

- 对事件的描述；
- 时间段；
- 事件的后果；
- 报告者的名字；
- 事件报告给了谁；
- 为解决事件所采取的步骤（包括负责人和恢复的数据）；
- 事件导致 PII 无法获得、丢失、披露或更改的情况。

如果发生涉及 PII 的违规行为，该记录还宜包括已泄露的 PII 描述（如果已知）；如果执行了通知，则宜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 ISO/IEC 27002:2013，16.1.6 中规定的控制、实施指南和其他信息。

6.13.1.7 证据的收集

适用 ISO/IEC 27002:2013，16.1.7 中规定的控制、实施指南和其他信息。

6.14 业务连续性管理的信息安全方面

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 ISO/IEC 27002:2013，17.1.1 中规定的控制、实施指南和其他信息。

6.14.1.2 实现信息安全连续性

适用 ISO/IEC 27002:2013，17.1.2 中规定的控制、实施指南和其他信息。

6.14.1.3 验证、评审和评价信息安全连续性

适用 ISO/IEC 27002:2013，17.1.3 中规定的控制、实施指南和其他信息。

6.14.2 冗余

6.14.2.1 信息处理设施的可用性

适用 ISO/IEC 27002:2013，17.2.1 中规定的控制、实施指南和其他信息。

6.15 符合性

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 ISO/IEC 27002:2013，18.1.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，18.1.1 适用的法律和合同要求的识别的补充指南是：组织应确定与处理 PII 有关的任何法律制裁（可能由于某些义务被遗漏而导致）风险，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，本标准等国际标准可用于构成组织与客户之间合同的基础，为各自的安全性、隐私和 PII 保护责任提供框架。如果违反这些责任，合同条款可以成为制裁的依据。

6.15.1.2 知识产权

适用 ISO/IEC 27002:2013，18.1.2 中规定的控制、实施指南和其他信息。

6.15.1.3 记录的保护

适用 ISO/IEC 27002:2013，18.1.3 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 18.1.3 记录的保护的补充实施指南是：可能需要审查当前和历史的策略和规程（例如，当客户争议解决和监管机构调查时）。组织宜在其规定的保留期限内保留其隐私策略和相关规程的副本（请参阅 7.4.7），这包括更新这些文档的先前版本。

6.15.1.4 隐私和个人身份信息保护

适用 ISO/IEC 27002:2013，18.1.4 中规定的控制、实施指南和其他信息。

6.15.1.5 密码控制规则

适用 ISO/IEC 27002:2013，18.1.5 中规定的控制、实施指南和其他信息。

6.15.2 信息安全评审

6.15.2.1 信息安全的独立评审

适用 ISO/IEC 27002:2013，18.2.1 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，18.2.1 信息安全的独立评审的补充实施指南是：如果组织为 PII 处理者，当单个客户审核不切实际、可能增加安全风险时，组织宜在订立合同之前，以及在合同期存续期间，向客户提供客观公正的证据以证明安全性是根据组织的策略和规程实施和运作的。如果独立审核能涵盖预期用户的需求，并且结果能以足够透明的方式提供，那么组织实施的独立审核通常被认为满足客户对关注焦点的审核。

6.15.2.2 符合安全政策和标准

适用 ISO/IEC 27002:2013，18.2.2 中规定的控制、实施指南和其他信息。

6.15.2.3 技术符合性评审

适用 ISO/IEC 27002:2013，18.2.3 中规定的控制、实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，18.2.3 技术符合性评审的补充指南是：技术评审作为遵守安全策略和标准的一部分，组织宜定义并实施针对 PII 处理工具和组件的评审。这可以包括：持续监控以确认只允许的技术评审被实施；和 / 或特定的渗透或漏洞测试（例如，去标识化的数据集可以应对有动机的入侵测试，以验证去标识化方法是否符合组织要求）。

7 针对 PII 控制者的附加 ISO/IEC 27002 指南

7.1 总则

指南第 6 章以及本章的补充内容为 PII 控制者创建了 PIMS 的特定指南。本章中记述的关于控制的实施指南在附录 A 中都有列出。

7.2 收集和处理的条件

目标：确定并记录该处理是合法的，具有适用司法管辖区的法律基础以及明确定义的合法目的。

7.2.1 识别并记录目的

- **控制**：组织宜识别并记录 PII 处理的特定目的。
- **实施指南**：组织宜确保 PII 主体了解组织处理 PII 的目的。组织有责任明确形成文件并与 PII 主体沟通。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 目的的文档宜足够清晰和详细，以便用于向 PII 主体提供所需信息（见 7.3.2），这包括获得同意所必需的信息（见 7.2.3），以及策略和规程的记录（见 7.2.8）。
- **其他信息**：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 确定合法的依据

- **控制**：组织宜确定、记录并遵守为确定目的而处理 PII 的相关合法依据。
- **实施指南**：某些司法管辖区要求组织能够在处理之前证明其处理的合法性。处理 PII 的法律依据可以包括：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、实施为公共利益而执行的活动、PII 控制者的合法利益。组织宜以此基础记录每个 PII 处理活动（参见 7.2.8）。组织的合法利益可以包括，例如，信息安全目标，这些目标宜与 PII 主体在隐私保护方面的义务相平衡。无论何时宜根据 PII 的属性（例如健康信息）或有关 PII 主体（例如与儿童有关的 PII）定义特殊类别的 PII，且组织宜在其分类方案中包括这些类别的 PII。PII 的分类准则可能因司法管辖区而异，并且可能因适用于不同类型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 PII 处理类别的内容并予以执行。使用特殊类别的 PII 也可能受到更严格的控制。更改或扩展处理 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**：组织宜确定并记录一个过程，通过该过程，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**：除非有其他适用的合法理由，否则处理 PII 需要主体同意。组织宜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、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具有特定要求（例如，不能与其他协议捆绑在一起）。此外，某些类型的数据收集（例如用于科学研究）和某些类型的 PII 主体（例如儿童）可能需要额外的要求。组织宜考虑此类要求并记录同意机制是如何满足这些要求。

7.2.4 获取并记录同意

- **控制**：组织宜根据文件化的流程获得并记录 PII 主体的同意。
- **实施指南**：组织宜根据请求提供所需同意的详细信息，以便获得 PII 主体的同意（例如，提供同意的时间、PII 主体的身份要求、同意书）。在同意过程之前提交给 PII 主体的信息宜遵循在 7.3.3 的指导。同意宜是：完全出于自愿、根据处理的目的而异、清楚无误。

7.2.5 隐私影响评估

- **控制**：每当计划对 PII 进行新的处理或改变现有的 PII 处理时，组织宜判别实施隐私影响评估的必要性，适当时予以实施。
- **实施指南**：PII 处理为 PII 主体带来风险，宜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情况，触发 PIA 的情形包括：对 PII 主体产生法律效力的自动决策，特殊类别 PII 的大规模处理（例如健康相关信息，种族或民族信息，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性监测数据。组织宜确定完成隐私影响评估所必需的因素，这些因素可以包括：已处理的 PII 类型列表，存储 PII 的位置，以及可以传输到的位置。在这种情况下，数据流程图和数据地图也很有用（参见 7.2.8 可获得记录以及处理 PII 的详细信息，这些信息可以帮助隐私影响或其他风险评估）。
- **其他信息**：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 处理者的合同

- **控制**：组织宜与 PII 处理者签订书面合同，合同宜确保在附录 B 中规定的适当控制措施得以实施。
- **实施指南**：代表组织处理 PII 的 PII 处理者和组织之间签订的合同，宜要求实施附录 B 中适当控制，这需要建立在信息安全风险评估过程（见 5.4.1.2）和 PII 处理者执行范围（见 6.12）的基础上进行考虑。默认情况下，附录 B 中所有相关的控制都宜被考虑。如果组织决定不要求 PII 处理者实施附录 B 中的某些控制，宜明确不实施的理由（见 5.4.1.3）。合同可以分别定义各自的责任，但为了与本标准保持一致，宜考虑所有控制并将其包含在文档化信息中。

7.2.7 PII 联合控制者

- **控制**：组织宜确定与任何 PII 联合控制者处理 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 的角色和责任宜以透明的方式确定，这些角色和责任宜记录在合同或各种类似的有约束力的文件中，其中宜包含 PII 被联合处置的条款和条件。在某些司法管辖区，此类协议称为数据共享协议。PII 联合控制者协议可以包括（此列表既不是最终的也不是详尽的）：PII 共享 / PII 联合控制者关系的目的；识别 PII 联合控制者关系中的组织（PII 控制者）身份；根据协议分享和 / 或传输和处理的 PII 类别；处理操作概述（例如传

输，使用）；各自的角色和责任的描述；负责实施 PII 保护的技术和组织安全措施；在 PII 违约的情况下责任的定义（例如，谁将通知，何时，相互信息）；PII 的保留和 / 或处置条款；不遵守协议的责任；如何履行对 PII 主体的义务；如何向 PII 主体提供有关 PII 联合控制者之间安排的本质信息；PII 主体如何获得他们有权获得的其他信息；给 PII 主体的联络点。

7.2.8 与处理 PII 有关的记录

- **控制**：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 PII 处理活动的清单或列表，这样的清单可以包括：处理类型；处理目的；PII 和 PII 主体类别的描述（例如儿童）；PII 曾经或将要披露 PII 的接收受者类别，包括第三国或国际组织的接收受者；技术和组织安全措施的通用描述；隐私影响评估报告。这样的清单应该由拥有者负责其准确性和完整性。

7.3 对 PII 主体的主要义务

目标：确保为 PII 主体提供有关其 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**：对于 PII 主体，组织宜确定并记录其应承担的与其处理 PII 相对应的法律、法规和业务义务，并提供履行这些义务的方式。
- **实施指南**：对 PII 主体承担的义务及其支持他们的方式因司法管辖区而异。组织宜确保他们提供适当的方式，以便及时、可行地履行对 PII 主体的义务。宜向 PII 主体提供明确的文件，说明对他们履行义务的程度，并提供最新的联系点以便 PII 主体提出他们的要求。联系点宜以与收集和准许 PII 相似的方式提供（例如，如果收集 PII 是通过电子邮件或网站，联系点也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**：组织宜确定并记录需要向 PII 主体提供的信息，这些信息宜与他们的 PII 处理和提供时间相关联。
- **实施指南**：组织宜确定法律、法规和 / 或业务要求以明确向 PII 主体提供信息的时间（例如，在处理之前，在请求之后的某个时间内回应等）以及所能提供的信息类型。根据要求，信息可以采用通知的形式。可以提供给 PII 主体的信息类型的示例如下：有关处理目的的信息；PII 控制者或其代表的联系方式；有关处理的合法依据的信息；如果不是直接从 PII 主体那里获得的话，获取 PII 地点的信息；提供 PII 是否是法定或合同要求的信息，以及在适当情况下，未提供 PII 的可能后果；有关对 PII 主体义务的信息，具体见 7.3.1 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 传输的信息；有关 PII 接收人或接收人类别的信息；有关 PII 保留期限的信息；有关基于 PII 自动化处理的自动决策使用的信息；有关提出投诉的权利以及如何提出投诉的信息；关于提供信息的频率的信息（例如“及时”通知），组织如果更改或扩展 PII 处理的目的，组织宜提供最新信息。

7.3.3 向 PII 主体提供信息

- **控制**：组织宜向 PII 主体提供清晰且易于访问的信息，以识别 PII 主体并描述如何处理其 PII。
- **实施指南**：组织宜根据目标受众，使用清晰明了的语言，以及时、简洁、完整、透明、可理解和易于访问的形式向 PII 主体提供 7.3.2 中详细介绍的信息。在适当的情况下，宜在收集 PII 时提供信息，它也宜是永久可访问的。
- **注**：以图标和图像的形式向 PII 主体提供预定处理的概要是有帮助的。

7.3.4 提供修改或撤销同意的机制

- **控制**：组织宜为 PII 主体提供修改或撤销其同意的机制。
- **实施指南**：组织宜告知 PII 主体其可在任何时间撤销同意（可能因司法管辖区而异）的权利，并提供相应的机制。用于撤销的机制因系统而异；它应该与获得同意的机制保持一致。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与其相同，而不是电话或传真等替代解决方案。修改同意可以包括对 PII 的处理施加限制，这可以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 主体何时以及如何修改或撤销其同意施加了限制。组织宜以与记录同意相类似的方式记录撤回或更改同意的任何请求。任何同意的变更宜传达到适当的系统，授权用户和相关第三方。组织宜定义响应时间，并且宜根据它来处理请求。
- **附加信息**：当撤销对特定 PII 处理的同意时，通常认为在撤回同意之前进行的所有 PII 处理都是适当的，但这种处理的结果不宜用于新处理。例如，如果 PII 主体撤回其对摘要信息的同意，则不宜进一步使用或咨询其摘要信息。

7.3.5 提供反对 PII 处理的机制

- **控制**：组织宜为 PII 主体提供一种机制，以反对其 PII 的处理。
- **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。受这些管辖区立法和 / 或法规约束的组织宜确保他们采取适当措施使 PII 主体能够行使这一权利。组织宜记录与 PII 主体反对处理相关的法律和法规要求（例如，反对以有关直接营销为目的的 PII 处理）。组织宜向主体提供有关在这些情况下反对能力的信息。反对的机制可能有所不同，但宜与所提供的服务类型一致（例如，在线服务宜在线提供此功能）。

7.3.6 访问、更正和 / 或删除

- **控制**：组织宜实施策略，规程和 / 或机制，以履行其对 PII 主体的义务，以访问，纠正和 / 或擦除其 PII。
- **实施指南**：组织宜实施策略，规程和 / 或机制，以使 PII 主体能够在没有不当延迟的情况下获取，纠正和擦除其 PII。组织宜定义请求响应时间，并且根据它来处理请求。任何更正或擦除都宜通过系统和 / 或授权用户传达，并传递给接收 PII 数据的第三方。
- **注**：由 7.5.3 相关规定产生的控制措施，在这方面提供帮助。当 PII 主体对数据的准确性或更正存在争议时，组织宜实施策略，规程和 / 或机制予以解决。这些策略，规程和 / 或机制宜包括告知 PII 主体所做的更改，以及无法进行更正的原因（在特定情况下）。某些司法管辖区对 PII 主体何时以及如何要求更正或擦除其 PII 施加限制。组织宜确定适用的这些限制，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**：组织宜通知共享 PII 的第三方针对共享 PII 数据的修改，撤回或异议，并实施适当的策略，流程和 / 或机制予以实现。
- **实施指南**：组织宜用适当技术，采取适当措施，通知第三方任何与共享 PII 有关的修改，撤销准许，或异议。某些司法管辖区强制要求向这些第三方通报这些行为。组织宜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，组织宜监控第三方的信息反馈。
- **注**：对 PII 主体义务的变更可包括：修改、撤销同意、纠正请求、删除、处置限制，或对 PII 主体要求而产生的异议。

7.3.8 提供 PII 处置的副本

- **控制**：当 PII 主体要求时，组织应该能够提供 PII 处置的副本。
- **实施指南**：组织宜提供 PII 的副本，该副本以 PII 主体可访问的、结构化的、常用格式呈现，并确保 PII 主体能够访问。某些司法管辖区定义了哪些组织宜提供 PII 副本的情况，这些情况要求：允许 PII 主体或接收 PII 信息的控制者，以可移植性的格式提供（通常是结构化的、常规的、机器可读的）。组织宜确保提供给 PII 主体的 PII 副本仅与该 PII 主体相关。根据保留和处置策略（如 7.4.7 中所述），所请求的 PII 如果已被删除，PII 控制者应通知 PII 主体。如果组织不再能够识别 PII 主体（例如，由于去标识化过程），组织不宜仅以此为理由寻求（重新）识别 PII 主体。但是，在某些司法管辖区，法律可能会要求从 PII 主体处获取其他信息，以便重新识别 PII 主体和随后的披露。如果技术上可行，应 PII 主体的要求，可将 PII 的副本从一个组织直接传输到另一个组织。

7.3.9 处理请求

- **控制**：组织宜定义和记录策略和规程，用于处理和响应来自 PII 主体的合法请求。

- **实施指南**：合理请求可包括处理 PII 副本的请求或提出投诉的请求。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）。请求宜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，以及向 PII 主体通知的延迟要求。宜在隐私策略中定义适当的响应时间。

7.3.10 自动决策

- **控制**：组织宜识别并明确对于 PII 主体的义务（包括法律义务），这些义务是由组织做出的 PII 自动处理的决定。
- **实施指南**：当 PII 自动处理的决策对 PII 主体产生重大影响时，某些司法管辖区定义了对 PII 主体应尽的义务，例如：通知 PII 主体自动决策机制的存在、允许 PII 主体反对此类自动决策机制和 / 或使用人为干预。
- **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宜考虑到这些义务。

7.4 默认隐私和设计的隐私

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）仅限于所识别目的所必需的。

7.4.1 限制收集

- **控制**：组织宜将 PII 的收集限制在与所识别目的相关性，成比例和必要的最小数量。
- **实施指南**：组织宜将 PII 的收集与所识别的使用目的匹配，限定在充分的、相关的、必要的范围内。这包括限制组织间接收集的 PII 数量（例如，通过网络日志，系统日志等）。隐私默认原则意味着：如果存在收集和处理 PII 的若干选项，则默认情况下，应禁用每个选项，并且仅通过 PII 主体的明确选择来逐个启用。

7.4.2 限制处理

- **控制**：组织宜将 PII 的处理与所识别的使用目的匹配，限定在充分的、相关的、必要的范围内。
- **实施指南**：限制 PII 的处理宜通过信息安全和隐私策略进行管理（见 6.2），同时宜建立文件化的规程以满足其选择以及合规。PII 的处理包括：披露、PII 存储期、谁能够访问他们的 PII；宜默认为相对于所识别的处理目的，所需处理的最小数量。

7.4.3 准确性和质量

- **控制**：在 PII 的整个生命周期中，组织应确保并记录相关信息，这些信息表明针对其被收集的目的，PII 是准确的，完整的和最新的。

- **实施指南**：组织应实施策略，规程和 / 或机制，以尽量减少其处理的 PII 中的不准确性。还宜有策略，规程和 / 或机制来响应不准确的 PII 实例。这些策略，规程和 / 或机制宜包含记录的要求（例如通过技术系统配置等），并宜适用于整个 PII 生命周期。
- **附加信息**：有关 PII 处理生命周期的更多信息，请参见 ISO/IEC 29101:2018，6.2。

7.4.4 PII 最小化目标

- **控制**：组织宜定义和记录数据最小化目标，以及使用哪些机制（例如去标识化）来实现这些目标。
- **实施指南**：组织宜确定收集和处理的 PII 类型、PII 数量，相对于所识别目的是如何受限的。这可以包括使用去标识化或其他数据最小化技术。所识别的目的（见 7.2.1）可以要求处理 PII 的去标识化信息，在这种情况下，组织应该能够描述这种处理。在某些情况下，识别出的目的是：不需要处理原始 PII，并且已经去标识化的 PII 处理足以满足所识别的目的。在这些情况下，组织应定义并记录 PII 需求与 PII 主体之间的关联程度，以及用于处理 PII 的机制和技术，实现去标识化和 / 或 PII 最小化的目标。用于最小化 PII 的机制取决于处理类型和处理系统。组织宜记录用于实现数据最小化的任何机制（技术系统配置等）。如果数据去标识化处理后足以达到目的，组织宜定时记录旨在满足去识别目标的实施机制（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去标识化目的。在某些情况下，可以使用其他去识别技术，例如泛化（例如四舍五入）或随机化技术（例如，噪声添加）来实现足够的去标识化水平。
- **注 1**：有关去标识化技术的更多信息，请参阅 ISO/IEC 20889。
- **注 2**：对于云计算，ISO/IEC 19944 提供了数据识别限定的定义，可用于 PII 主体、将 PII 主体与 PII 中的一组特征的关联程度进行分类识别。

7.4.5 PII 在处理结束时去标识化和删除

- **控制**：一旦原始 PII 不再需要用于所识别的目的，组织宜删除 PII，以不允许识别或需要重新识别 PII 主体的形式呈现它。
- **实施指南**：组织宜有机制在没有预期进一步处理时删除 PII。或者，可以使用一些去标识化技术以达到去标识化数据不能被利用，以重新识别 PII 主体。

7.4.6 临时文件

- **控制**：组织宜确保在指定的记录期内，按照记录的规程处置（例如擦除或销毁），因处理 PII 而创建的临时文件。
- **实施指南**：组织宜定期检查以确保在确定的时间内删除未使用的临时文件。
- **其他信息**：信息系统可以在正常的操作过程中创建临时文件。此类文件区别于系统或应用程序，但可包括：与数据库更新和应用操作程序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。这些文件保持使用的时间长度并不都是确定的，但“垃圾文件收集”规程宜识别相关文件，并确定自上次使用以来已经保存了多长时间。

7.4.7 保留

- **控制**：满足 PII 处理目的时间截止，组织不宜逾期保留 PII。
- **实施指南**：组织宜制定并维护其保留 PII 信息的时间表，同时考虑到保留 PII 不超过必要的要求。此类时间表宜考虑法律，法规和业务要求，如果组织保留数据与此类要求发生冲突，则需要做出业务决策（基于风险评估），并在时间表中记录。

7.4.8 处置

- **控制**：组织宜具有处置 PII 的文件化策略，规程和 / 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，物理介质的粒度，或在电子介质上恢复已删除信息的能力）。在选择适当的处置技术时要考虑的因素包括但不限于待处置的 PII 的性质和范围，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**：组织宜对数据传输网络传输（例如发送到另一个组织）的 PII 予以适当的控制，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可以访问传输系统，并遵循适当的流程（包括保留审核日志）来确保 PII 的传输不会损害正确的接收者。

7.5 PII 共享、转移和披露

目标：确定是否并记录何时共享，传输 PII 到其他司法管辖区、承担披露义务的第三方。

7.5.1 识别司法管辖区之间 PII 传输的基础

- **控制**：组织宜确定并记录管辖区之间 PII 传输的相关基础。
- **实施指南**：PII 传输可能受到法律和 / 或法规的约束，具体取决于数据将被传输到的管辖区域或国际组织（以及从何处传输）。组织宜记录满足传输基础要求的遵守情况。某些司法管辖区可能会指定监管机构审查信息转让协议。在这些司法管辖区运营的组织宜了解此类要求。
- **注**：如果传输发生在特定的司法管辖区内，发件人和收件人则均要准守该管辖区内适用的法律和 / 或法规。

7.5.2 PII 可以传输至的国家和国际组织

- **控制**：组织宜制定并记录 PII 可以传输的目的国、目的国际组织。
- **实施指南**：在正常运营中，应该向顾客提供：PII 可能被传输至的国家和国际组织的身份，宜包括 PII 分包处理国的身份。所包含的国家身份应考虑 7.5.1 的要求。在正常运营之外，传输可能会应执法机关要求或者被适用的司法管辖区禁止，对这些国家的身份不能提前指定，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**：组织宜记录 PII 向第三方的传输，并确保与各方的合作。作为对 PII 主体应尽的义务，组织宜支持 PII 主体未来的请求。
- **实施指南**：记录包括：传输 PII 的第三方、由于 PII 控制者履行管理义务而修改的 PII、转让给第三方以满足 PII 主体的合法请求、删除 PII 的请求（例如，在撤回同意后）。组织宜有一个策略来定义这些记录的保留期间。组织宜严格保留必要信息，将数据最小化原则应用于传输记录。

7.5.4 向第三方披露 PII 的记录

- **控制**：组织宜记录向第三方的 PII 披露，包括披露的 PII 内容、向谁、何时披露。
- **实施指南**：PII 可以在正常操作过程中披露。宜记录这些披露。还宜记录对第三方的任何其他披露，例如合法调查或外部审核所产生的披露。记录宜包括披露的来源和进行披露权力的来源。

8 针对 PII 处理者的附加 ISO/IEC 27002 指南

8.1 总则

第 6 章中的指南以及本章的补充指南为 PII 处理者创建了特定于 PIMS 的指南。本章中记述的关于控制的实施指南在附录 B 中都有列出。

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，以及明确界定的合法的目的，确定并记录处理是合法的。

8.2.1 客户协议

- **控制**：组织宜确保相关的 PII 处理合同能够解决：组织协助客户履行 PII 义务方面的作用（应考虑处理的性质和组织可利用的信息）。

- **实施指南**：组织与客户之间的合同宜包括以下相关内容，并取决于客户的角色（PII 控制者或 PII 处理者）（此列表既不是绝对的也不是详尽的）：设计的隐私和默认的隐私（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）；如果需要事先与相关 PII 保护机构进行磋商，则由 PII 处理者保证提供协助。某些司法管辖区要求合同包括处理的主要内容和持续时间，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**：组织宜确保代表客户处理 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实现的目标和时间表。为了满足客户目标，在没有客户的明确指示的前提下，组织需满足客户的通用指令，组织可以确定处理 PII 方法的最优技术方案。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。这也确保了组织或其分包商不会出于其他目的而处理 PII，除非客户有书面说明具备其他目的。

8.2.3 营销和广告使用

- **控制**：没有事先获得相应 PII 主体的同意，组织不宜使用根据合同处理的 PII 时，进行营销和广告。组织不宜将提供此类同意作为接收服务的条件。
- **实施指南**：宜记录 PII 处理者与客户合同的合规性要求，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**：此控制是对通用控制 8.2.2 的补充，而不是替换或者取代。

8.2.4 侵权指令

- **控制**：如果组织认为，处理指令违反了适用的法律和 / 或法规，组织应通知客户。
- **实施指南**：组织验证客户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、以及组织与客户之间的合同。

8.2.5 客户义务

- **控制**：组织宜向客户提供适当的信息，以便向客户证明其履行了义务。
- **实施指南**：客户所需的信息可包括组织是否允许客户参与、由客户授权或以其他方式同意的审核员进行审核，并为此做出贡献。

8.2.6 与处理 PII 有关的记录

- **控制**：组织宜确定并保持必要的记录，以证明其代表客户尽了 PII 处理的义务（如适用合同中的规定）。
- **实施指南**：某些司法管辖区可要求组织记录以下信息：代表每个客户进行处理的类别；传输到第三国或国际组织；技术和安全措施的通用描述。

8.3 对 PII 主体的义务

8.3.1 对 PII 主体的义务

- **控制**：组织宜为客户提供履行与 PII 主体相关的义务的方法。
- **实施指南**：PII 控制者的义务可以通过立法、法规和 / 或合同来定义。客户的这些义务可能通过使用组织服务来履行，例如包括及时纠正或删除 PII。如果客户依赖于组织的信息或技术措施来履行其对 PII 主体的义务，则宜在合同中规定相关信息或技术措施。

8.4 默认的隐私、设计的隐私

目标：确保流程和系统的设计能够使 PII 的收集和处理（包括使用、披露、保留、传输和处置）必需限于所识别目的用途。

8.4.1 临时文件

- **控制**：组织宜确保在指定的记录期内按照文件化规程处理（例如擦除或销毁）由于处理 PII 而创建的临时文件。
- **实施指南**：组织宜定期验证以确保在指定的时间内删除未使用的临时文件。
- **其他信息**：信息系统可以在正常的操作过程中创建临时文件。此类文件区别于系统或应用程序，但可包括：与数据库更新和应用操作程序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。这些文件保持使用的时间长度并不都是确定的，但 “垃圾文件收集” 规程宜识别相关文件，并确定自上次使用以来已经保存了多长时间。

8.4.2 回退、传输或处置 PII

- **控制**：组织宜提供以安全的方式回退、传输和 / 或处置 PII 的能力。它还宜向客户提供该策略。
- **实施指南**：在某个时间点，PII 可能需要以某种方式处置。这可能涉及将 PII 回退给客户，将其传输给另一个组织或 PII 控制者（例如，由于合并的结果），删除或以其他方式销毁，去标识化或存档。宜以安全的方式管理回退、传输和 / 或处置 PII 的能力。当 PII 被客户确定为不再是必需时，组织宜提供必要的保证使客户确信，根据合同要求处理的 PII（由组织及其任何分包商）已从存储的任何位置删除，包括为了满足备份和业务连续性的目

标。组织宜制定并实施有关 PII 处置的策略，并应在被要求时向客户提供此策略。该策略应涵盖合同终止至处置 PII 的保留期，以保护客户不会因合同失效而失去 PII。

- **注**：这种控制和指南也与保存原则相关（见 7.4.7）。

8.4.3 PII 传输控制

- **控制**：组织宜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才能访问传输系统，并遵循适当的流程（包括保留审核数据）来确保 PII 的传输不会损害正确的接收者。PII 传输控制的要求可以包含在与客户签署的合同中。如果没有与传输相关的合同要求，则在传输之前应听取客户的建议。

8.5 PII 共享、传输和披露

目标：确定是否共享 PII，何时将其转让给其他司法管辖区或第三方，和 / 或根据适用的义务披露，以及是否提供文件。

8.5.1 管辖区之间 PII 传输的基础

- **控制**：组织宜及时告知客户各管辖区之间的 PII 传输依据、以及此方面的预期变更，以便客户能够反对此类更改或终止合同。
- **实施指南**：各管辖区之间的 PII 传输可能受到法律和 / 或法规的约束，具体取决于 PII 要传输到的管辖区域或组织（及 PII 数据的来源方）。组织宜记录对于此类要求的遵守情况，以作为转移的基础。组织宜告知客户任何 PII 传输，包括传输到：供应商、其他方、其他国家或国际组织。如果发生变更，组织宜根据约定的时间提前通知客户，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变更的条款。宜设置此类情况限制在一定的范围内（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 传输到其他国家 / 地区）。在国际间传输 PII，宜识别诸如示范合同条款，具有约束力的公司规则或跨境隐私规则，以及在相关国家间签署的适用类似情况的协议。

8.5.2 PII 可以传输至的国家和国际组织

- **控制**：组织宜制定并记录 PII 可能会被传输的目的地国和目的国际组织。
- **实施指南**：在正常运营中，应该向顾客提供：PII 可能被传输至的国家和国际组织的身份，宜包括 PII 分包处理国的身份。所包含的国家的考虑宜涉及 8.5.1。在正常运营之外，传输可能会应执法机关要求或者被适用的司法管辖区禁止，对这些国家的身份不能提前指定，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**：组织宜记录向第三方的 PII 披露，包括已披露的 PII、向谁和何时披露。
- **实施指南**：PII 可以在正常操作过程中公开。宜记录这些披露。还宜记录对第三方的任何其他披露，例如合法调查或外部审核所产生的披露。记录宜包括披露的来源和进行披露的批准来源。

8.5.4 PII 披露请求的通知

- **控制**：组织宜通知客户任何具有法律约束力的 PII 披露请求。
- **实施指南**：组织可能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，组织宜在约定的时间范围内并根据商定的规程（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给任何人（禁止通知披露的一个例子是：根据刑法禁止通知，以维护执法调查的机密性）。

8.5.5 具有法律约束力的 PII 披露

- **控制**：组织宜拒绝任何不具有法律约束力的 PII 披露请求，在进行任何 PII 披露之前宜询问客户，并接受那些已经通过客户授权且记录在合同中的披露请求。
- **实施指南**：与控制实施相关的细节可以包含在客户合同中。此类请求可能有多个来源，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 处理 PII 分包商的披露

- **控制**：在使用分包商之前，组织宜向客户告知会使用分包商处理 PII 的情况。
- **实施指南**：使用分包商处理 PII 的相关约定宜包括在客户合同中。合同中宜披露拟使用分包商以及相关分包商的名称。披露的信息还宜包括分包商可以将数据传输至的国家和国际组织（见 8.5.2），以及分包商有义务达到或超过组织应尽义务的方式（见 8.5.7）。如果评估分包商信息的公开披露为不可接受风险，则宜根据保密协议和 / 或应客户要求进行披露。宜让客户知道他的要求是可获得的。这与 PII 可以传输至的国家名单无关。在任何情况下，都应向客户披露该清单，以便客户通知相应的 PII 主体。

8.5.7 分包商参与处理 PII

- **控制**：组织宜仅根据客户合同聘请分包商处理 PII。
- **实施指南**：如果组织将 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。可以是客户合同中的某一条款，也可以是特定的 “一次性” 协议。组织宜与代表其进行 PII 处理的任何分包商签订书面合同，并宜确保其与分包商的合同涉及附录 B 中相应控制措施的实施。组织与代表其处理 PII 的任何分包商之间的合同宜

要求分包商实施附录 B 中相应的控制措施。这些措施应考虑到信息安全风险评估过程（见 5.4.1.2）和 PII 处理者执行的 PII 处理范围（见 6.12）。默认情况下，附录 B 中指定的所有控制宜被认为是有价值的。如果组织决定不要求分包商实施附录 B 中的某个控制，宜证明它被排除在外的正确性。合同可以对各方的责任做出不同的定义，但为了与本标准保持一致，宜考虑标准中的所有控制措施并将其记载在书面信息中。

8.5.8 处理 PII 分包商的变更

- **控制**：在获得常规书面授权的情况下，组织宜将有关添加或更换处理 PII 分包商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**：如果组织更换处理 PII 的部分或全部的分包商，则在新分包商处理 PII 之前，需要对客户的书面授权进行变更。可以是客户合同中的某一条款，也可以是特定的“一次性”协议。

附录 A（规范性附录）针对 PII 控制者的 PIMS 特定的控制目标和控制措施

本附录提供作为 PII 控制者的组织使用，无论是否使用 PII 处理者。本附录作为 ISO/IEC 27001:2013，附录 A 的扩展。

表 A.1 中列出的补充或修改的控制目标和控制直接源自本文档中的定义并与之一致，并在 ISO/IEC 27001:2013，6.1.3 的优化内容 5.4.1.3 的情景下使用。

表 A.1 - 控制目标和控制

条款	控制目标	控制内容
A.7.2	收集和处理条件	目的：确定并记录该处理是合法的，具有适用司法管辖区的法律基础以及明确定义的合法目的。
A.7.2.1	识别和记录目的	组织宜识别并记录 PII 处理的特定目的。
A.7.2.2	确定合法的依据	组织宜确定，记录并遵守为确定目的而处理 PII 的相关合法依据。
A.7.2.3	确定何时和如何获得同意	组织宜确定并记录一个过程，通过该过程，可以证明是否，何时以及如何从 PII 主

		体获得 PII 处理的同意。
A.7.2.4	获取并记录同意	组织宜根据文件化的流程获得并记录 PII 主体的同意。
A.7.2.5	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，组织宜判别实施隐私影响评估的必要性，适当时予以实施。
A.7.2.6	与 PII 处理者的合同	组织宜与 PII 处理者签订书面合同，合同宜确保在附录 B 中规定的适当控制措施得以实施。
A.7.2.7	联合 PII 控制者	组织宜确定与任何 PII 联合控制者处理 PII（包括 PII 保护和安全要求）的各自角色和职责。
A.7.2.8	与处理 PII 有关的记录	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。
A.7.3	对 PII 主体的义务	目的：确保为 PII 主体提供有关其 PII 处理的适当信息，履行与处理其 PII 相关的 PII 主体的任何其他适用义务。
A.7.3.1	确定并履行对 PII 主体的义务	对于 PII 主体，组织宜确定并记录其应承担的与其处理 PII 相对应的法律、法规和业务义务，并提供履行这些义务的方式。
A.7.3.2	确定 PII 主体的信息	组织应确定并记录需要向 PII 主体提供的信息，这些信息应与他们的 PII 处理和提供时间相关。
A.7.3.3	向 PII 主体提供信息	组织宜向 PII 主体提供清晰且易于访问的信息，以识别 PII 主体并描述如何处理其 PII。
A.7.3.4	提供修改或撤销同意的机制	组织宜为 PII 主体提供修改或撤销其同意的机制。

A.7.3.5	提供反对 PII 处理的机制	组织应为 PII 主体提供一种机制，以反对其 PII 的处理。
A.7.3.6	访问、更正和 / 或删除	组织宜实施政策、规程和 / 或机制，以履行其对 PII 主体的义务，以访问、更正和 / 或擦除其 PII。
A.7.3.8	提供 PII 处置的副本	当 PII 主体要求时，组织应该能够提供 PII 处置的副本。
A.7.3.9	处理请求	组织宜定义和记录策略和规程，用于处理和响应来自 PII 主体的合法请求。
A.7.3.10	自动决策	组织宜识别并明确对于 PII 主体的义务（包括法律义务），这些义务是由组织做出的 PII 自动处理的决定。
A.7.4	默认的隐私、设计的隐私	目的：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）仅限于所识别目的所必需的。
A.7.4.1	限制收集	组织宜将 PII 的收集限制在与所识别目的相关性，成比例和必要的最小数量。
A.7.4.2	限制处理	组织宜将 PII 的处理与所识别的使用目的匹配，限定在充分的、相关的、必要的范围内。
A.7.4.3	准确性和质量	在 PII 的整个生命周期中，组织应确保并记录相关信息，这些信息表明针对其被收集的目的，PII 是准确的、完整的和最新的。
A.7.4.4	PII 最小化目标	组织宜定义和记录数据最小化目标，以及使用哪些机制（例如去标识化）来实现这些目标。
A.7.4.5	PII 在处理结束时去识别化和删除	一旦原始 PII 不再需要用于所识别的目的，组织宜删除 PII，以不允许识别或需要重新

		识别 PII 主体的形式呈现它。
A.7.4.6	临时文件	组织宜确保在指定的记录期内，按照记录的规程处置（例如擦除或销毁），因处理 PII 而创建的临时文件。
A.7.4.7	保留	满足 PII 处理目的时间截止，组织不宜逾期保留 PII。
A.7.4.8	处置	组织宜具有处置 PII 的文件化策略、规程和 / 或机制。
A.7.4.9	PII 传输控制	组织宜对数据传输网络传输（例如发送到另一个组织）的 PII 予以适当的控制，以确保数据到达预定目的地。
A.7.5	PII 共享、转移和披露	目的：确定是否并记录何时共享、传输 PII 到其他司法管辖区、承担披露义务的第三方。
A.7.5.1	识别司法管辖区之间 PII 传输的基础	组织宜确定并记录管辖区之间 PII 传输的相关基础。
A.7.5.2	PII 可以传输至的国家和国际组织	组织宜制定并记录 PII 可以传输的目的国、目的国际组织。
A.7.5.3	PII 转移的记录	组织宜记录 PII 向第三方的传输，并确保与各方的合作。作为对 PII 主体应尽的义务，组织宜支持 PII 主体未来的请求。
A.7.5.4	向第三方披露 PII 的记录	组织宜记录向第三方的 PII 披露，包括披露的 PII 内容、向谁、何时披露。

并非本附录中列出的所有控制目标和控制都必须包含在 PIMS 的实施中。排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）。排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（或不受其限制）的情况。

注：本附录中的条款编号与本标准中第 7 章相关子条款编号一致。

附录 B（规范性附录）针对 PII 处理者的 PIMS 特定的控制目标和控制措施

本附录供作为 PII 处理者的组织使用，无论是否使用 PII 分包商。本附录作为 ISO/IEC 27001:2013，附录 A 的扩展。

表 B.1 中列出的补充或修改的控制目标和控制直接源自本文档中的定义并与之一致，并在 ISO/IEC 27001:2013，6.1.3 的优化内容 5.4.1.3 的情景下使用。

表 B.1 - 控制目标和控制

条款	控制目标	控制内容
B.8.2	收集和处理的条件	目的：根据适用的司法管辖区的法律，以及明确界定的合法的目的，确定并记录处理是合法的。
B.8.2.1	客户协议	组织宜确保相关的 PII 处理合同能够解决：组织协助客户履行 PII 义务方面的作用（应考虑处理的性质和组织可利用的信息）。
B.8.2.2	组织的目的	组织宜确保代表客户处理 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	没有事先获得相应 PII 主体的同意，组织不宜使用根据合同处理的 PII 时，进行营销和广告。组织不宜将提供此类同意作为接收服务的条件。
B.8.2.4	侵权指令	如果组织认为，处理指令违反了适用的法律和 / 或法规，组织应通知客户。
B.8.2.5	顾客义务	组织宜向客户提供适当的信息，以便向客户证明其履行了义务。
B.8.2.6	与处理 PII 相关的记录	组织宜确定并保持必要的记录，以证明其代表客户尽了 PII 处理的义务（如适用合同中的规定）。
B.8.3	对 PII 主体的义务	目的：确保为 PII 主体提供有关其 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	组织宜为客户提供履行与 PII 主体相关的义务的方法。
B.8.4	默认的隐私、设计的隐私	目的：确保流程和系统的设计能够使 PII 的收集和处理（包括使用、披露、保留、传输和处置）必需限于所识别目的用途。
B.8.4.1	临时文件	组织宜确保在指定的记录期内按照文件化规程处理（例如擦除或销毁）由于处理 PII 而创建的临时文件。
B.8.4.2	回退、传输或处置 PII	组织宜提供以安全的方式回退、传输和 / 或处置 PII 的能力。它还宜向客户提供该策略。
B.8.4.3	PII 传输控制	组织宜对通过数据传输网络传输的 PII 进行适当的控制，以确保数据到达其预定目的地。
B.8.5	PII 共享、传输和披露	目的：根据适用的义务，确定是否共享 PII，何时将其转让给其他司法管辖区或第三方和 / 或披露，以及是否提供文件。
B.8.5.1	管辖区之间 PII 传输的基础	组织宜及时告知客户各管辖区之间的 PII 传输依据、以及此方面的预期变更，以便客户能够反对此类更改或终止合同。
B.8.5.2	PII 可以被传输至的国家和国际组织	组织宜制定并记录 PII 可能会被传输的目的地国和目的国际组织。
B.8.5.3	向第三方披露 PII 的记录	组织宜记录向第三方的 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	组织宜通知客户任何具有法律约束力的 PII 披露请求。
B.8.5.5	具有法律约束力的 PII 披露	组织宜拒绝任何不具有法律约束力的 PII 披露请求，在进行任何 PII 披露之前宜询问客户，并接受那些已经通过客户授权且记录在合同中的披露请

		求。
B.8.5.6	处理 PII 的分包商的披露	在使用分包商之前，组织宜向客户告知会使用分包商处理 PII 的情况。
B.8.5.7	分包商处理 PII 的参与	组织宜仅根据客户合同聘请分包商处理 PII。
B.8.5.8	分包商处理 PII 的变更	在获得常规书面授权的情况下，组织宜将有关添加或更换处理 PII 分包商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。

并非本附录中列出的所有控制目标和控制都必须包含在 PIMS 的实施中。排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）。排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（或不受其限制）的情况。

注：本附录中的条款编号与本标准中第 8 章相关子条款编号一致。

附录 C（资料）与 ISO/IEC 29100 的映射

表 C.1 和 C.2 给出本标准条款与 ISO/IEC 29100 隐私原则之间的映射关系。本附录以简洁的指示性方式就本标准的要求和控制的符合性如何与 ISO/IEC 29100 中规定的一般隐私原则给出了映射关系。

表 C.1 - PII 控制者和 ISO/IEC 29100 控制的映射

ISO/IEC 29100 隐私原则	PII 控制者的相关控制
1. 同意和选择	A.7.2.1 识别并记录目的；A.7.2.2 确定合法的依据；A.7.2.3 确定何时以及如何获得准许；A.7.2.4 获得并记录同意；A.7.2.5 隐私影响评估；A.7.3.4 提供修改或撤销同意的机制；A.7.3.5 提供反对 PII 处理的机制；A.7.3.7 PII 控制者告知第三方的义务
2. 目的合法性和规范	A.7.2.1 识别并记录目的；A.7.2.2 确定合法的依据；A.7.2.5 隐私影响评估；A.7.3.2 确定提供给 PII 主体的信息；A.7.3.3 向 PII 主体提供信息；A.7.3.10 自动决策的制定

3. 收集限制	A.7.2.5 隐私影响评估；A.7.4.1 限制收集；A.7.4.2 限制处理；A.7.4.4 PII 最小化目标
4. 数据最小化	A.7.4.4 PII 最小化目标；A.7.4.5 PII 在处理结束时去识别化和删除
5. 使用、保留和披露限制	A.7.4.4 PII 最小化目标；A.7.4.5 PII 在处理结束时去识别化和删除；A.7.4.6 临时文件；A.7.4.7 保留；A.7.4.8 处置；A.7.5.1 识别司法管辖区之间 PII 传输的基础；A.7.5.4 向第三方披露 PII 的记录
6. 准确性和质量	A.7.4.3 准确性和质量
7. 公开性、透明度和通知	A.7.3.2 确定提供给 PII 主体的信息；A.7.3.3 向 PII 主体提供信息
8. 个人参与和访问	A.7.3.1 确定并履行对 PII 主体的义务；A.7.3.3 向 PII 主体提供信息；A.7.3.6 访问、更正和 / 或擦除；A.7.3.8 提供 PII 处置的副本；A.7.3.9 处理请求
9. 问责制	A.7.2.6 与 PII 处理者的合同；A.7.2.7 联合 PII 控制者；A.7.2.8 与处理 PII 控制有关的记录；A.7.3.9 处理请求；A.7.5.1 识别司法管辖区之间 PII 传输的基础；A.7.5.2 PII 可以传输至的国家和国际组织；A.7.5.3 PII 转移的记录
10. 信息安全	A.7.2.6 与 PII 处理者的合同；A.7.4.9 PII 传输控制
11. 隐私合规	A.7.2.5 隐私影响评估

表 C.2 - PII 处理者和 ISO/IEC 29100 控制的映射

ISO/IEC 29100 隐私原则	PII 处理者的相关控制
1. 准许和选择	B.8.2.5 客户义务
2. 目的合法性和规范	B.8.2.1 客户协议；B.8.2.2 组织的目的；B.8.2.3 营销和广

	告使用；B.8.2.4 侵权指令；B.8.3.1 对于 PII 主体的义务
3. 收集限制	N/A
4. 数据最小化	B.8.4.1 临时文件
5. 使用、保留和披露限制	B.8.5.3 向第三方披露 PII 的记录；B.8.5.4 PII 披露请求的通知；B.8.5.5 具有法律约束力的 PII 披露
6. 准确性和质量	N/A
7. 公开性、透明度和通知	B.8.5.6 处理 PII 分包商的披露；B.8.5.7 分包商参与处理 PII；B.8.5.8 处理 PII 分包商的变更
8. 个人参与和访问	B.8.3.1 对 PII 主体的义务
9. 问责制	B.8.2.6 与处理 PII 有关的记录；B.8.4.2 回退、传输或处置 PII；B.8.5.1 管辖区之间 PII 传输的基础；B.8.5.2 PII 可以传输至的国家和国际组织
10. 信息安全	B.8.4.3 PII 传输控制
11. 隐私合规	B.8.2.5 客户义务

附录 D（资料）与通用数据保护条例的映射

本附录给出了本标准条款与欧盟通用数据保护条例中第 5 章至第 49 条之间（43 条除外）的映射关系。它显示了如果遵守了本标准的要求和控制措施与其履行 GDPR 的相关性。

但是，这纯粹是指示性的，根据本标准，组织有责任评估其法律义务并决定如何遵守这些义务。

表 D.1 - ISO/IEC 27701 与 GDPR 的映射

ISO/IEC 27701 条款	GDPR 条款
5.2.1	(24)(3),(25)(3),(28)(5),(28)(6),(28)(10),(32)(3),(40)(1),(40)(2)(a),(40)(2)(b),(40

	)(2)(c),(40)(2)(d),(40)(2)(e),(40)(2)(f),(40)(2)(g),(40)(2)(h),(40)(2)(i),(40)(2)(j),(40)(2)(k),(40)(3),(40)(4),(40)(5),(40)(6),(40)(7),(40)(8),(40)(9),(40)(10),(40)(11),(41)(1),(41)(2)(a),(41)(2)(b),(41)(2)(c),(41)(2)(d),(41)(3),(41)(4),(41)(5),(41)(6),(42)(1),(42)(2),(42)(3),(42)(4),(42)(5),(42)(6),(42)(7),(42)(8)
5.2.2	(31),(35)(9),(36)(1),(36)(2),(36)(3)(a),(36)(3)(b),(36)(3)(c),(36)(3)(d),(36)(3)(e),(36)(3)(f),(36)(5)
5.2.4、5.4.1.2	(32)(1)(b),(32)(2)
5.4.1.3	(32)(1)(b),(32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1),(27)(2)(a),(27)(2)(b),(27)(3),(27)(4),(27)(5),(37)(1)(a),(37)(1)(b),(37)(1)(c),(37)(2),(37)(3),(37)(4),(37)(5),(37)(6),(37)(7),(38)(1),(38)(2),(38)(3),(38)(4),(38)(5),(38)(6),(39)(1)(a),(39)(1)(b),(39)(1)(c),(39)(1)(d),(39)(1)(e),(39)(2)
6.3.2.1	(5)(1)(F)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f),(32)(2)
6.5.2.2	(5)(1)(F)
6.5.3.1	(5)(1)(f),(32)(1)(a)
6.5.3.2	(5)(1)(F)
6.5.3.3	(5)(1)(f),(32)(1)(a)
6.6.2.1	(5)(1)(F)
6.6.2.2	(5)(1)(F)
6.6.4.2	(5)(1)(F)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(F)

6.8.2.9	(5)(1)(F)
6.9.3.1	(5)(1)(f),(32)(1)(c)
6.9.4.1	(5)(1)(F)
6.9.4.2	(5)(1)(F)
6.10.2.1、6.10.2.4	(5)(1)(F)、(5)(1)(f),(28)(3)(b),(38)(5)
6.11.1.2、6.11.2.1	(5)(1)(f),(25)(1)、(25)(1),(32)(1)(a)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(F)
6.12.1.2	(5)(1)(f),(28)(1),(28)(3)(a),(28)(3)(b),(28)(3)(c),(28)(3)(d),(28)(3)(e),(28)(3)(f),(28)(3)(g),(28)(3)(h),(28)(2),(28)(3)(d),(28)(3)(e),(28)(3)(g),(28)(3)(h),(30)(2)(b),(32)(1)
6.13.1.1、6.13.1.5	(5)(1)(f),(33)(1),(33)(3)(a),(33)(3)(b),(33)(3)(c),(33)(3)(d),(33)(4),(33)(5),(34)(1),(34)(2),(34)(3)(a),(34)(3)(c),(34)(4)、(33)(1),(33)(3)(a),(33)(3)(b),(33)(3)(d),(32)(1)(b)
6.15.1.3	(5)(2),(24)(2)
6.15.2.1	(32)(1)(d),(32)(2)
6.15.2.3	(32)(1)(d),(32)(2)
7.2.1	(5)(1)(b),(32)(4)
7.2.2	(5),(6)(1)(a),(6)(1)(b),(6)(1)(c),(6)(1)(d),(6)(1)(e),(6)(1)(f),(6)(2),(6)(3),(6)(4)(a),(6)(4)(b),(6)(4)(c),(6)(4)(d),(6)(4)(e),(8)(1),(9)(1),(9)(2)(b),(9)(2)(c),(9)(2)(d),(9)(2)(e),(9)(2)(f),(9)(2)(g),(9)(2)(h),(9)(2)(i),(9)(2)(j),(9)(3),(9)(4),(17)(3)(a),(17)(3)(b),(17)(3)(c),(17)(3)(d),(17)(2),(18),(22),(22)(2)(a),(22)(2)(b),(22)(2)(c)
7.2.3	(8)(1),(8)(2)
7.2.4	(7)(1),(7)(2),(9)(2)(a)

7.2.5	(35)(1),(35)(2),(35)(3)(a),(35)(3)(b),(35)(3)(c),(35)(4),(35)(5),(35)(7)(a),(35)(7)(b),(35)(7)(c),(35)(7)(d),(35)(8),(35)(9),(35)(10),(35)(11),(36)(1),(36)(3)(a),(36)(3)(b),(36)(3)(c),(36)(3)(d),(36)(5)
7.2.6	(5)(2),(28)(3),(28)(9)
7.2.7	(26)(1),(26)(2),(26)(3)
7.2.8	(5)(2),(24)(1),(30)(1)(a),(30)(1)(b),(30)(1)(c),(30)(1)(d),(30)(1)(f),(30)(1)(g),(30)(3),(30)(4),(30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2),(13)(3),(13)(1)(a),(13)(1)(b),(13)(1)(c),(13)(1)(d),(13)(1)(e),(13)(1)(f),(13)(2),(13)(4),(14)(1)(a),(14)(1)(b),(14)(1)(f),(14)(2)(b),(14)(2)(e),(14)(2)(f),(14)(3)(a),(14)(3)(b),(14)(3)(c),(14)(4),(14)(5)(a),(14)(5)(b),(14)(5)(c),(14)(5)(d),(15)(1)(a),(15)(1)(b),(15)(1)(c),(15)(1)(d),(15)(1)(e)
7.3.3	(11)(2),(12)(1),(12)(7),(13)(3),(21)(4)
7.3.4	(7)(3),(13)(2),(14)(2),(18)(1)(a),(18)(1)(b),(18)(1)(c),(18)(1)(d)
7.3.5	(13)(2)(b),(14)(2)(c),(21)(1),(21)(2),(21)(3),(21)(5),(21)(6)
7.3.6	(15)(1)(a),(15)(1)(b),(15)(1)(c),(15)(1)(d),(16),(17)(1)(a),(17)(1)(b),(17)(1)(c),(17)(1)(d),(17)(2)
7.3.7	(19)
7.3.8	(15)(3),(15)(4),(20)(1),(20)(2),(20)(3),(20)(4)
7.3.9	(12)(3),(12)(4),(12)(5),(12)(6),(15)(1)(a),(15)(1)(b),(15)(1)(c),(15)(1)(d),(15)(1)(e),(15)(1)(f),(15)(1)(g),(15)(1)(h)
7.3.10	(13)(2)(f),(14)(2)(g),(22)(1),(22)(3)
7.4.1	(5)(1)(b),(5)(1)(c)
7.4.2	(25)(2)
7.4.3	(5)(1)(d)

7.4.4	(5)(1)(c),(5)(1)(e)
7.4.5	(5)(1)(c),(5)(1)(e),(6)(4)(e),(11)(1)
7.4.6	(5)(1)(c),(32)(1)(a)
7.4.7	(13)(2)(a),(14)(2)(a)
7.4.8	(5)(1)(F)
7.4.9	(5)(1)(F)
7.5.1	(15)(2),(44),(45)(1),(45)(2)(a),(45)(2)(b),(45)(2)(c),(45)(3),(45)(4),(45)(5),(45)(6),(45)(7),(45)(8)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f),(28)(3)(e),(28)(9),(35)(1)
8.2.2	(5)(1)(a),(5)(1)(b),(28)(3)(a),(29),(32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(H)
8.2.5	(28)(3)(H)
8.2.6	(30)(3),(30)(4),(30)(5),(30)(2)(a),(30)(2)(b)
8.3.1	(15)(3),(17)(2),(28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g),(30)(1)(f)
8.4.3	(5)(1)(F)
8.5.1	(44),(46)(1),(46)(2)(a),(46)(2)(b),(46)(2)(c),(46)(2)(d),(46)(2)(e),(46)(2)(f),(46)(3)(a),(46)(3)(b),(48),(49)(1)(a),(49)(1)(b),(49)(1)(c),(49)(1)(d),(49)(1)(e),(49)(1)(f),(49)(1)(g),(49)(2),(49)(3),(49)(4),(49)(5),(49)(6)

8.5.2	(30)(2)(c)
8.5.3	(30)(1)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2),(28)(4)
8.5.7	(28)(2),(28)(3)(d)
8.5.8	(28)(2)

附录 E（资料）与 ISO/IEC 27018 和 ISO/IEC 29151 的映射

ISO/IEC 27018 为充当 PII 处理者并提供公共云服务的组织提供了进一步的信息。ISO/IEC 29151 为 PII 控制者处理 PII 提供了额外的控制和指导。

表 E.1 给出了本标准条款与 ISO/IEC 27018 和 ISO/IEC 29151 规定之间的指示性映射。它说明了本标准的要求和控制如何与 ISO/IEC 27018 和 / 或 ISO/IEC 29151 的规定保持一致。

表 E.1 - ISO/IEC 27701 与 ISO/IEC 27018 和 ISO/IEC 29151 的映射

ISO/IEC 27701 条款	ISO/IEC 27018 子条款	ISO/IEC 29151 子条款
5.2	N/A	N/A
5.3	N/A	N/A
5.4	N/A	4.2
5.5	N/A	7.2.3
5.6	N/A	N/A
5.7	N/A	N/A

5.8	N/A	N/A
6.1	N/A	N/A
6.2	5.1.1	5
6.3	6.1.1	N/A
6.4	7.2.2	N/A
6.5.1	N/A	8.1
6.5.2	N/A	8.2
6.5.3	A.11.4、A.11.5	8.3
6.6.1	N/A	N/A
6.6.2	9.2.1、A.11.8、A.11.9、A.11.10	9.2
6.6.3	N/A	9.3
6.6.4	7.2.2、9.4.2	9.4
6.7	10.1.1	N/A
6.8.1	N/A	11.1
6.8.2	11.2.7、A.11.2、A.11.13	N/A
6.9.1	N/A	12.1
6.9.2	N/A	12.2
6.9.3	N/A	12.3
6.9.4	12.4.1、12.4.2	12.4
6.9.5	N/A	N/A

6.9.6	N/A	N/A
6.9.7	N/A	N/A
6.10.1	N/A	13.1
6.10.2	13.2.1、A.11.1	13.2
6.11.1	A.11.6	N/A
6.11.2	N/A	N/A
6.11.3	12.1.4	N/A
6.12.1	A.11.11	N/A
6.12.2	N/A	N/A
6.13	16.1.1、A.10.1	N/A
6.14	N/A	N/A
6.15.1	A.10.2	N/A
6.15.2	18.2.1	18.2
7.2.1	N/A	A.4
7.2.2	N/A	A.4.1
7.2.3	N/A	N/A
7.2.4	N/A	A.3.1
7.2.5	N/A	A.11.2
7.2.6	N/A	A.11.3
7.2.7	N/A	N/A
7.2.8	N/A	N/A

7.3.1	N/A	A.10
7.3.2	N/A	N/A
7.3.3	N/A	A.9
7.3.4	N/A	N/A
7.3.5	N/A	N/A
7.3.6	N/A	A.10.1
7.3.7	N/A	N/A
7.3.8	N/A	N/A
7.3.9	N/A	N/A
7.3.10	N/A	N/A
7.4.1	N/A	A.5
7.4.2	N/A	N/A
7.4.3	N/A	A.8
7.4.4	N/A	N/A
7.4.5	N/A	A.7.1
7.4.6	N/A	A.7.2
7.4.7	N/A	A.7.1
7.4.8	N/A	N/A
7.4.9	N/A	N/A
7.5.1	N/A	A.13.2
7.5.2	N/A	A.13.2

7.5.3	N/A	A.13.2
7.5.4	N/A	A.7.4
8.2.1	N/A	N/A
8.2.2	N/A	N/A
8.2.3	N/A	N/A
8.2.4	N/A	N/A
8.2.5	N/A	N/A
8.2.6	N/A	N/A
8.3.1	N/A	N/A
8.4.1	N/A	N/A
8.4.2	N/A	N/A
8.4.3	N/A	N/A
8.5.1	N/A	N/A
8.5.2	N/A	N/A
8.5.3	N/A	N/A
8.5.4	N/A	N/A
8.5.5	N/A	N/A
8.5.6	A.7.5	N/A
8.5.7	N/A	N/A
8.5.8	N/A	N/A

本附录是指示性的，不宜假设具有映射关系的条款之间意味着等同。

附录 F（资料）如何在 ISO/IEC 27001 和 ISO/IEC 27002 的基础上实施 ISO/IEC 27701

F.1 如何应用本标准

本标准基于 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013，并扩展了他们的要求和指南，除信息安全外，还考虑了可能受 PII 处理影响的 PII 主体的隐私保护。这意味着，在 ISO/IEC 27001 或 ISO/IEC 27002 中使用术语 “信息安全” 时，等同于使用 “信息安全和隐私”。

表 F.1 给出了信息安全术语的扩展映射关系，以便将其应用于此文件。

表 F.1 - 对信息安全术语与追加隐私扩展后术语的映射关系

ISO/IEC 27001	ISO/IEC 27701
信息安全	信息安全和隐私
信息安全策略	信息安全和隐私策略
信息安全管理	信息安全和隐私信息管理
信息安全管理体系（ISMS）	隐私信息管理体系（PIMS）
信息安全目标	信息安全和隐私目标
信息安全绩效	信息安全和隐私绩效
信息安全要求	信息安全和隐私要求
信息安全风险	信息安全和隐私风险
信息安全风险评估	信息安全和隐私风险评估
信息安全风险处理	信息安全和隐私风险处理

基本上，在处理 PII 时，有三种情况本文适用于保护 PII 主体的隐私：

1. 安全标准的应用原则如下：参考的标准适用于上述各条款的术语扩展。因此，不再重复引用标准，而是仅在各个条款中提及。

2. 安全标准的增加：引用标准适用于其他特定于隐私的要求或实施指南。
3. 优化安全标准：引用标准通过隐私特定要求或实施指南进行完善。

F.2 安全标准的改进示例

本节描述了 5.4.1.2 如何适用于 ISO/IEC 27001:2013，6.1.2。

在处理 PII 时，考虑到保护 PII 主体的隐私，ISO/IEC 27001:2013，6.1.2 将使用下面带下划线的文本进行修改：

6.1.2 信息安全风险评估

组织应定义并应用信息安全和隐私风险评估过程：

a) 建立并维护信息安全和隐私风险标准，包括：

1. 风险验收标准；和
2. 进行信息安全和隐私风险评估的标准；

b) 确保重复的信息安全和隐私风险评估产生一致、有效和可比较的结果；

c) 识别信息安全和隐私风险：

3. 应用信息安全和隐私风险评估过程，以识别与信息安全和隐私信息管理系统范围内的信息的机密性、完整性和可用性丧失相关的风险；和
4. 识别风险所有者；

d) 分析信息安全和隐私风险；

5. 评估 6.1.2 c) 中确定的风险实现后可能产生的后果；
6. 评估 6.1.2 c) 1) 中确定的风险发生的实际可能性；和
7. 确定风险等级；

e) 评估信息安全和隐私风险：

8. 将风险分析结果与 6.1.2 a) 中确定的风险标准进行比较；和
9. 优先分析风险处理的分析风险。

组织应保留有关信息安全和隐私风险评估过程的文档信息。

参考文献

[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

[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

BS ISO/IEC 27701:2019

INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

© ISO/IEC 2019 – All rights reserved

© ISO/IEC 2019 – All rights reserved

© ISO/IEC 2019 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2019 – All rights reserved

Introduction

0.1 General

Almost every organization processes Personally Identifiable Information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation and/or regulation all over the world.

The Information Security Management System (ISMS) defined in ISO/IEC 27001 is designed to permit the addition of sector specific requirements, without the need to develop a new Management System. ISO Management System standards, including the sector specific ones, are designed to be able to be implemented either separately or as a combined Management System.

Requirements and guidance for PII protection vary depending on the context of the organization, in particular where national legislation and/or regulation exist. ISO/IEC 27001 requires that this context be understood and taken into account. This document includes mapping to:

the privacy framework and principles defined in ISO/IEC 29100;

ISO/IEC 27018;

ISO/IEC 29151; and

the EU General Data Protection Regulation.

However, these can need to be interpreted to take into account local legislation and/or regulation.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

An organization complying with the requirements in this document will generate documentary evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other stakeholders. The use of this document in conjunction with ISO/IEC 27001 can, if desired, provide independent verification of this evidence.

This document was initially developed as ISO/IEC 27552.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its Management System Standards.

This document enables an organization to align or integrate its PIMS with the requirements of other Management System standards.

© ISO/IEC 2019 – All rights reserved

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

1 Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and ISO/IEC 29100 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

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

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

3.1
joint PII controller
PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers

© ISO/IEC 2019 – All rights reserved

3.2
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of PII

4 General

4.1 Structure of this document

This is a sector-specific document related to ISO/IEC 27001:2013 and to ISO/IEC 27002:2013.

This document focuses on PIMS-specific requirements. Compliance with this document is based on adherence to these requirements and with the requirements in ISO/IEC 27001:2013. This document extends the requirements of ISO/IEC 27001:2013 to take into account the protection of privacy of PII principals as potentially affected by the processing of PII, in addition to information security. For a better understanding, implementation guidance and other information regarding the requirements is included.

Clause 5 gives PIMS-specific requirements and other information regarding the information security requirements in ISO/IEC 27001 appropriate to an organization acting as either a PII controller or a PII processor.

NOTE 1 For completeness, Clause 5 contains a subclause for each of the clauses containing requirements in ISO/IEC 27001:2013, even in cases where there are no PIMS-specific requirements or other information.

Clause 6 gives PIMS-specific guidance and other information regarding the information security controls in ISO/IEC 27002 and PIMS-specific guidance for an organization acting as either a PII controller or a PII processor.

NOTE 2 For completeness, Clause 6 contains a subclause for each of the clauses containing objectives or controls in ISO/IEC 27002:2013, even in cases where there is no PIMS-specific guidance or other information.

Clause 7 gives additional ISO/IEC 27002 guidance for PII controllers, and Clause 8 gives additional ISO/IEC 27002 guidance for PII processors.

Annex A lists the PIMS-specific control objectives and controls for an organization acting as a PII controller, (whether it employs a PII processor or not, and whether acting jointly with another PII controller or not).

Annex B lists the PIMS-specific control objectives and controls for an organization acting as a PII processor (whether it subcontracts the processing of PII to a separate PII processor or not, and including those processing PII as subcontractors to PII processors).

Annex C contains a mapping to ISO/IEC 29100.

Annex D contains a mapping of the controls in this document to the European Union General Data Protection Regulation.

Annex E contains a mapping to ISO/IEC 27018 and ISO/IEC 29151.

Annex F explains how ISO IEC 27001 and ISO/IEC 27002 are extended to the protection of privacy when processing PII.

4.2 Application of ISO/IEC 27001:2013 requirements

Table 1 gives the location of PIMS-specific requirements in this document in relation to ISO/IEC 27001.

© ISO/IEC 2019 – All rights reserved

Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

4.3 Application of ISO/IEC 27002:2013 guidelines

Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013

Clause in ISO/IEC 27002:2013	Title	Subclause in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resource security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications security	6.10	Additional guidance
14	System acquisition, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management.	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

© ISO/IEC 2019 – All rights reserved

4.4 Customer

Depending on the role of the organization (see 5.2.1), "customer" can be understood as either:

a) an organization who has a contract with a PII controller (e.g. the customer of the PII controller);

NOTE 1 This can be the case of an organization which is a joint controller.

NOTE 2 An individual person in a business to consumer relationship with an organization is referred to as a "PII principal" in this document.

b) a PII controller who has a contract with a PII processor (e.g. the customer of the PII processor); or

c) a PII processor who has a contract with a subcontractor for PII processing (e.g. the customer of the subcontracted PII sub-processor).

NOTE 3 Where “customer” is referred to in Clause 6, the related provisions can be applicable in contexts a), b), or c).

NOTE 4 Where “customer” is referred to in Clause 7 and Annex A, the relation provisions are applicable in context a).

NOTE 5 Where “customer” is referred to in Clause 8 and Annex B, the relation provisions can be applicable in contexts b) and/or c).

5 PIMS-specific requirements related to ISO/IEC 27001

5.1 General

The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE In practice, where "information security" is used in ISO/IEC 27001:2013, "information security and privacy” applies instead (see Annex F).

5.2 Context of the organization

5.2.1 Understanding the organization and its context

A requirement additional to ISO/IEC 27001:2013, 4.1 is:

The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor.

The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include:

applicable privacy legislation;

applicable regulations;

applicable judicial decisions;

applicable organizational context, governance, policies and procedures;

applicable administrative decisions;

applicable contractual requirements.

 © ISO/IEC 2019 – All rights reserved

Where the organization acts in both roles (e.g. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

NOTE The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

5.2.2 Understanding the needs and expectations of interested parties

A requirement additional to ISO/IEC 27001:2013, 4.2 is:

The organization shall include among its interested parties (see ISO/IEC 27001:2013, 4.2), those parties having interests or responsibilities associated with the processing of PII, including the PII principals.

NOTE 1 Other interested parties can include customers (see 4.4), supervisory authorities, other PII controllers, PII processors and their subcontractors.

NOTE 2 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 3 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization be in conformity with specific standards, such as the Management System specified in this document, and/or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

5.2.3 Determining the scope of the information security management system

A requirement additional to ISO/IEC 27001:2013, 4.3 is:

When determining the scope of the PIMS, the organization shall include the processing of PII.

NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

5.2.4 Information security management system

A requirement additional to ISO/IEC 27001:2013, 4.4 is:

The organization shall establish, implement, maintain and continually improve a PIMS in accordance with the requirements of ISO/IEC 27001:2013 Clauses 4 to 10, extended by the requirements in Clause 5.

5.3 Leadership

5.3.1 Leadership and commitment

The requirements stated in ISO/IEC 27001:2013, 5.1 along with the interpretation specified in 5.1, apply.

5.3.2 Policy

The requirements stated in ISO/IEC 27001:2013, 5.2 along with the interpretation specified in 5.1, apply.

5.3.3 Organizational roles, responsibilities and authorities

The requirements stated in ISO/IEC 27001:2013, 5.3 along with the interpretation specified in 5.1, apply.

© ISO/IEC 2019 – All rights reserved

5.4 Planning

5.4.1 Actions to address risks and opportunities

5.4.1.1 General

The requirements stated in ISO/IEC 27001:2013, 6.1.1 along with the interpretation specified in 5.1, apply.

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:

ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows:

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

5.4.1.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions:

ISO/IEC 27001:2013, 6.1.3 c) is refined as follows:

The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted.

When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.

ISO/IEC 27001:2013, 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)];

justification for their inclusion;

whether the necessary controls are implemented or not; and

the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1).

Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary

© ISO/IEC 2019 – All rights reserved

by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to the PII principal.

5.4.2 Information security objectives and planning to achieve them

The requirements stated in ISO/IEC 27001:2013, 6.2 along with the interpretation specified in 5.1, apply.

5.5 Support

5.5.1 Resources

The requirements stated in ISO/IEC 27001:2013, 7.1 along with the interpretation specified in 5.1, apply.

5.5.2 Competence

The requirements stated in ISO/IEC 27001:2013, 7.2 along with the interpretation specified in 5.1, apply.

5.5.3 Awareness

The requirements stated in ISO/IEC 27001:2013, 7.3 along with the interpretation specified in 5.1, apply.

5.5.4 Communication

The requirements stated in ISO/IEC 27001:2013, 7.4 along with the interpretation specified in 5.1, apply.

5.5.5 Documented information

5.5.5.1 General

The requirements stated in ISO/IEC 27001:2013, 7.5.1 along with the interpretation specified in 5.1, apply.

5.5.5.2 Creating and updating

The requirements stated in ISO/IEC 27001:2013, 7.5.2 along with the interpretation specified in 5.1, apply.

5.5.5.3 Control of documented information

The requirements stated in ISO/IEC 27001:2013, 7.5.3 along with the interpretation specified in 5.1, apply.

5.6 Operation

5.6.1 Operational planning and control

The requirements stated in ISO/IEC 27001:2013, 8.1 along with the interpretation specified in 5.1, apply.

5.6.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 8.2 along with the interpretation specified in 5.1, apply.

5.6.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:2013, 8.3 along with the interpretation specified in 5.1, apply.

© ISO/IEC 2019 – All rights reserved

5.7 Performance evaluation

5.7.1 Monitoring, measurement, analysis and evaluation

The requirements stated in ISO/IEC 27001:2013, 9.1 along with the interpretation specified in 5.1, apply.

5.7.2 Internal audit

The requirements stated in ISO/IEC 27001:2013, 9.2 along with the interpretation specified in 5.1, apply.

5.7.3 Management review

The requirements stated in ISO/IEC 27001:2013, 9.3 along with the interpretation specified in 5.1, apply.

5.8 Improvement

5.8.1 Nonconformity and corrective action

The requirements stated in ISO/IEC 27001:2013, 10.1 along with the interpretation specified in 5.1, apply.

5.8.2 Continual improvement

The requirements stated in ISO/IEC 27001:2013, 10.2 along with the interpretation specified in 5.1, apply.

6 PIMS-specific guidance related to ISO/IEC 27002

6.1 General

The guidelines in ISO/IEC 27002:2013 mentioning "information security" should be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE 1 In practice, where "information security" is used in ISO/IEC 27002:2013, "information security and privacy" applies instead (see Annex F).

All control objectives and controls should be considered in the context of both risks to information security as well as risks to privacy related to the processing of PII.

NOTE 2 Unless otherwise stated by specific provisions in Clause 6, or determined by the organization according to applicable jurisdictions, the same guidance applies for PII controllers and PII processors.

6.2 Information security policies

6.2.1 Management direction for information security

6.2.1.1 Policies for information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 5.1.1 and the following additional guidance applies:

Additional implementation guidance for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is:

Either by the development of separate privacy policies, or by the augmentation of information security policies, the organization should produce a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and/or regulation and with the contractual terms agreed between the organization and its partners, its subcontractors and its

© ISO/IEC 2019 – All rights reserved

applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them.

Additional other information for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is:

Any organization that processes PII, whether a PII controller or a PII processor, should consider applicable PII protection legislation and/or regulation during the development and maintenance of information security policies.

6.2.1.2 Review of the policies for information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 5.1.2 applies:

6.3 Organization of information security

6.3.1 Internal organization

6.3.1.1 Information security roles and responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.1 and the following additional guidance applies:

Additional implementation guidance for 6.1.1, Information security roles and responsibilities, of ISO/IEC 27002:2013 is:

The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principals regarding the processing of their PII (see 7.3.2).

The organization should appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII.

The responsible person should, where appropriate:

- be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;
- be involved in the management of all issues which relate to the processing of PII;
- be expert in data protection legislation, regulation and practice;
- act as a contact point for supervisory authorities;
- inform top-level management and employees of the organization of their obligations with respect to the processing of PII;
- provide advice in respect of privacy impact assessments conducted by the organization.

NOTE Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced.

6.3.1.2 Segregation of duties

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.2 applies.

© ISO/IEC 2019 – All rights reserved

6.3.1.3 Contact with authorities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.3 applies.

6.3.1.4 Contact with special interest groups

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.4 applies.

6.3.1.5 Information security in project management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.5 applies.

6.3.2 Mobile devices and teleworking

6.3.2.1 Mobile device policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.2.1 and the following additional guidance applies.

Additional implementation guidance for 6.2.1, Mobile device policy, of ISO/IEC 27002:2013 is:

The organization should ensure that the use of mobile devices does not lead to a compromise of PII.

6.3.2.2 Teleworking

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.2.2 applies.

6.4 Human resource security

6.4.1 Prior to employment

6.4.1.1 Screening

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.1.1 applies.

6.4.1.2 Terms and conditions of employment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.1.2 applies.

6.4.2 During employment

6.4.2.1 Management responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.1 applies.

6.4.2.2 Information security awareness, education and training

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.2 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 7.2.2, Information security awareness, education and training, of ISO/IEC 27002:2013 is:

Measures should be put in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the organization (e.g. legal consequences, loss of business and brand or reputational damage), to the staff member (e.g. disciplinary consequences) and to the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

NOTE Such measures can include the use of appropriate periodic training for personnel having access to PII.

6.4.2.3 Disciplinary procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.3 applies.

6.4.3 Termination and change of employment

6.4.3.1 Termination or change of employment responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.3.1 applies.

6.5 Asset management

6.5.1 Responsibility for assets

6.5.1.1 Inventory of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.1 applies.

6.5.1.2 Ownership of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.2 applies.

6.5.1.3 Acceptable use of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.3 applies.

6.5.1.4 Return of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.4 applies.

6.5.2 Information classification

6.5.2.1 Classification of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.1 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 8.2.1, Classification of Information, of ISO/IEC 27002:2013 is:

The organization's information classification system should explicitly consider PII as part of the scheme it implements. Considering PII within the overall classification system is integral to understanding what PII the organization processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow.

6.5.2.2 Labelling of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.2 and the following additional guidance applies.

Additional implementation guidance for 8.2.2, labelling of information, of ISO/IEC 27002:2013 is:

The organization should ensure that people under its control are made aware of the definition of PII and how to recognize information that is PII.

6.5.2.3 Handling of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.3 applies.

6.5.3 Media handling

6.5.3.1 Management of removable media

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.1 and the following additional guidance applies:

Additional implementation guidance for 8.3.1, Management of removable media, of ISO/IEC 27002:2013 is:

The organization should document any use of removable media and/or devices for the storage of PII. Wherever feasible, the organization should use removable physical media and/or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media and/or devices are used, the organization should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII.

Additional other information for 8.3.1, Management of removable media, of ISO/IEC 27002:2013 is:

Removable media which is taken outside the physical confines of the organization is prone to loss, damage and inappropriate access. Encrypting removable media adds a level of protection for PII which reduces security and privacy risks should the removable media be compromised.

6.5.3.2 Disposal of media

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.2 and the following additional guidance applies.

Additional implementation guidance for 8.3.2, Disposal of media, of ISO/IEC 27002:2013 is:

Where removable media on which PII is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored PII will not be accessible.

6.5.3.3 Physical media transfer

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.3 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 8.3.3, Physical media transfer, of ISO/IEC 27002:2013 is:

If physical media is used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/ recipients, the date and time, and the number of physical media. Where possible, additional measures such as encryption should be implemented to ensure that the data can only be accessed at the point of destination and not in transit.

The organization should subject physical media containing PII before leaving its premises to an authorization procedure and ensure the PII is not accessible to anyone other than authorized personnel.

NOTE One possible measure to ensure PII on physical media leaving the organization's premises is not generally accessible is to encrypt the PII concerned and restrict decryption capabilities to authorized personnel.

6.6 Access control

6.6.1 Business requirements of access control

6.6.1.1 Access control policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.1.1 applies.

6.6.1.2 Access to networks and network services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.1.2 applies.

6.6.2 User access management

6.6.2.1 User registration and de-registration

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.1 and the following additional guidance applies:

Additional implementation guidance for 9.2.1, User registration and de-registration, of ISO/IEC 27002:2013 is:

Procedures for registration and de-registration of users who administer or operate systems and services that process PII should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

The organization should not reissue to users any de-activated or expired user IDs for systems and services that process PII.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of user ID management. Such cases should be included in the documented information.

Some jurisdictions impose specific requirements regarding the frequency of checks for unused authentication credentials related to systems that process PII. Organizations operating in these jurisdictions should take compliance with these requirements into account.

6.6.2.2 User access provisioning

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.2 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 9.2.2, User access provisioning, of ISO/IEC 27002:2013 is:

The organization should maintain an accurate, up-to-date record of the user profiles created for users who have been authorized access to the information system and the PII contained therein. This profile comprises the set of data about that user, including user ID, necessary to implement the identified technical controls providing authorized access.

Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the organization, users are also protected as they can identify what they have processed and what they have not processed.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of access management. Where appropriate, the organization should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information.

6.6.2.3 Management of privileged access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.3 applies:

6.6.2.4 Management of secret authentication information of users

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.4 applies.

6.6.2.5 Review of user access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.5 applies.

6.6.2.6 Removal or adjustment of access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.6 applies.

6.6.3 User responsibilities

6.6.3.1 Use of secret authentication information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.3.1 applies.

6.6.4 System and application access control

6.6.4.1 Information access restriction

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.1 applies.

6.6.4.2 Secure log-on procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.2 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 9.4.2, Secure log-on procedures, of ISO/IEC 27002:2013 is:

Where required by the customer, the organization should provide the capability for secure log-on procedures for any user accounts under the customer's control.

6.6.4.3 Password management system

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.3 applies.

6.6.4.4 Use of privileged utility programs

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.4 applies.

6.6.4.5 Access control to program source code

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.5 applies.

6.7 Cryptography

6.7.1 Cryptographic controls

6.7.1.1 Policy on the use of cryptographic controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.1 and the following additional guidance applies:

Additional implementation guidance for 10.1.1, Policy on the use of cryptographic controls, of ISO/IEC 27002:2013 is:

Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection.

6.7.1.2 Key management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.2 applies.

6.8 Physical and environmental security

6.8.1 Secure areas

6.8.1.1 Physical security perimeter

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.1 applies.

© ISO/IEC 2019 – All rights reserved

6.8.1.2 Physical entry controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.2 applies.

6.8.1.3 Securing offices, rooms and facilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.3 applies.

6.8.1.4 Protecting against external and environmental threats

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.4 applies.

6.8.1.5 Working in secure areas

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.5 applies.

6.8.1.6 Delivery and loading areas

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.6 applies.

6.8.2 Equipment

6.8.2.1 Equipment siting and protection

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.1 applies.

6.8.2.2 Supporting utilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.2 applies.

6.8.2.3 Cabling security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.3 applies.

6.8.2.4 Equipment maıntenance

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.4 applies.

6.8.2.5 Removal of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.5 applies.

6.8.2.6 Security of equipment and assets off-premises

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.6 applies.

© ISO/IEC 2019 – All rights reserved

6.8.2.7 Secure disposal or re-use of equipment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.7 and the following additional guidance applies:

Additional implementation guidance for 11.2.7, Secure disposal or re-use of equipment, of ISO/IEC 27002:2013 is:

The organization should ensure that, whenever storage space is re-assigned, any PII previously residing on that storage space is not accessible.

On deletion of PII held in an information system, performance issues can mean that explicit erasure of that PII is impractical. This creates the risk that another user can access the PII. Such risk should be avoided by specific technical measures.

For secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does contain PII.

6.8.2.8 Unattended user equipment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.8 applies.

6.8.2.9 Clear desk and clear screen policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.9 and the following additional guidance applies:

Additional implementation guidance for 11.2.9, Clear desk and clear screen policy, of ISO/IEC 27002:2013 is:

The organization should restrict the creation of hardcopy material including PII to the minimum needed to fulfil the identified processing purpose.

6.9 Operations security

6.9.1 Operational procedures and responsibilities

6.9.1.1 Documenting operating procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.1 applies.

6.9.1.2 Change management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.2 applies.

6.9.1.3 Capacity management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.3 applies.

6.9.1.4 Separation of development, testing and operational environments

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.4 applies.

© ISO/IEC 2019 – All rights reserved

6.9.2 Protection from malware

6.9.2.1 Controls against malware

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.2.1 applies.

6.9.3 Backup

6.9.3.1 Information backup

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies:

Additional implementation guidance for 12.3.1, Information backup, of ISO/IEC 27002:2013 is:

The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements.

PII-specific responsibilities in this respect can depend on the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup.

Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII.

Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should demonstrate compliance with these requirements.

There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal).

The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain:

the name of the person responsible for the restoration;

a description of the restored PII.

Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to document compliance with any applicable jurisdiction-specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information.

The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see 6.5.3.3, 6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1).

6.9.4 Logging and monitoring

6.9.4.1 Event logging

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.1 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 12.4.1, Event logging, of ISO/IEC 27002:2013 is:

A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event.

Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles should be clearly defined and included in the documented information, and agreement on any log access between providers should be addressed.

Implementation guidance for PII processors:

The organization should define criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria should be made available to the customer.

Where the organization permits its customers to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the customer can only access records that relate to that customer's activities, cannot access any log records which relate to the activities of other customers, and cannot amend the logs in any way.

6.9.4.2 Protection of log information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.2 and the following additional guidance applies:

Additional implementation guidance for 12.4.2, Protection of log information, of ISO/IEC 27002:2013 is:

Log information recorded for, for example, security monitoring and operational diagnostics, can contain PII. Measures such as controlling access (see ISO/IEC 27002:2013, 9.2.3) should be put in place to ensure that logged information is only used as intended.

A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (see 7.4.7).

6.9.4.3 Administrator and operator logs

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.3 applies.

6.9.4.4 Clock synchronization

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.4 applies.

6.9.5 Control of operational software

6.9.5.1 Installation of software on operational systems

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.5.1 applies.

© ISO/IEC 2019 – All rights reserved

6.9.6 Technical vulnerability management

6.9.6.1 Management of technical vulnerabilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.6.1 applies.

6.9.6.2 Restriction on software installation

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.6.2 applies.

6.9.7 Information systems audit considerations

6.9.7.1 Information systems audit controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.7.1 applies.

6.10 Communications security

6.10.1 Network security management

6.10.1.1 Network controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.1.1 applies.

6.10.1.2 Security in network services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.1.2 applies.

6.10.1.3 Segregation in networks

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.1.3 applies.

6.10.2 Information transfer

6.10.2.1 Information transfer policies and procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.1 and the following additional guidance applies:

Additional implementation guidance for 13.2.1, Information transfer policies and procedures, of ISO/IEC 27002:2013 is:

The organization should consider procedures for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable.

6.10.2.2 Agreements for information transfer

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.2 applies.

© ISO/IEC 2019 – All rights reserved

6.10.2.3 Electronic messaging

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.3 applies.

6.10.2.4 Confidentiality or non-disclosure agreements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.4 and the following additional guidance applies:

Additional implementation guidance for 13.2.4, Confidentiality or non-disclosure agreements, of ISO/IEC 27002:2013 is:

The organization should ensure that individuals operating under its control with access to PII are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to.

When the organization is a PII processor, a confidentiality agreement, in whatever form, between the organization, its employees and its agents should ensure that employees and agents comply with the policy and procedures concerning data handling and protection.

6.11 Systems acquisition, development and maintenance

6.11.1 Security requirements of information systems

6.11.1.1 Information security requirements analysis and specification

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.1 applies.

6.11.1.2 Securing application services on public networks

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.2 and the following additional guidance applies:

Additional implementation guidance for 14.1.2, Securing application services on public networks, of ISO/IEC 27002:2013 is:

The organization should ensure that PII that is transmitted over untrusted data transmission networks is encrypted for transmission.

Untrusted networks can include the public internet and other facilities outside of the operational control of the organization.

NOTE In some cases (e.g. the exchange of e-mail) the inherent characteristics of untrusted data transmission network systems can require that some header or traffic data be exposed for effective transmission.

6.11.1.3 Protecting application services transactions

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.3 applies.

6.11.2 Security in development and support processes

6.11.2.1 Secure development policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.1 and the following additional guidance applies.

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 14.2.1, Secure development policy, of ISO/IEC 27002:2013 is:

Policies for system development and design should include guidance for the organization's processing of PII needs, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization. Clauses 7 and 8 provide control considerations for processing of PII, which can be useful in developing policies for privacy in systems design.

Policies that contribute to privacy by design and privacy by default should consider the following aspects:

a) guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle;

b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment (see 7.2.5);

c) PII protection checkpoints within project milestones;

d) required privacy and PII protection knowledge;

e) by default minimize processing of PII.

6.11.2.2 System change control procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.2 applies.

6.11.2.3 Technical review of applications after operating platform changes

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.3 applies.

6.11.2.4 Restrictions of changes to software packages

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.4 applies.

6.11.2.5 Secure systems engineering principles

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.5 and the following additional guidance applies:

Additional implementation guidance for 14.2.5, Secure systems engineering principles, of ISO/IEC 27002:2013 is:

Systems and/or components related to the processing of PII should be designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls (as described in Clauses 7 and 8, for PII controllers and PII processors, respectively), in particular such that the collection and processing of PII in those systems is limited to what is necessary for the identified purposes of the processing of PII (see 7.2).

For example, an organization that processes PII should ensure that, based on the relevant jurisdiction, it disposes of PII after a specified period. The system that processes that PII should be designed in a way to facilitate this deletion requirement.

6.11.2.6 Secure development environment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.6 applies.

© ISO/IEC 2019 – All rights reserved

6.11.2.7 Outsourced development

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.7 and the following additional guidance applies.

Additional implementation guidance for 14.2.7, Outsourced development, of ISO/IEC 27002:2013 is:

The same principles (see 6.11.2.5) of privacy by design and privacy by default should be applied, if applicable, to outsourced information systems.

6.11.2.8 System security testing

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.8 applies.

6.11.2.9 System acceptance testing

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.9 applies.

6.11.3 Test data

6.11.3.1 Protection of test data

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.3.1 and the following additional guidance applies:

Additional implementation guidance for 14.3.1, Protection of test data, of ISO/IEC 27002:2013 is:

PII should not be used for testing purposes; false or synthetic PII should be used. Where the use of PII for testing purposes cannot be avoided, technical and organizational measures equivalent to those used in the production environment should be implemented to minimize the risks. Where such equivalent measures are not feasible, a risk-assessment should be undertaken and used to inform the selection of appropriate mitigating controls.

6.12 Supplier relationships

6.12.1 Information security in supplier relationships

6.12.1.1 Information security policy for supplier relationships

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.1 applies.

6.12.1.2 Addressing security within supplier agreements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.2 and the following additional guidance applies:

Additional implementation guidance for 15.1.2, Addressing security within supplier agreements, of ISO/IEC 27002:2013 is:

The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations (see 7.2.6 and 8.2.1).

© ISO/IEC 2019 – All rights reserved

Supplier agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) taking into account the type of PII processed.

The agreements between the organization and its suppliers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation and/or regulation. The agreements should call for independently audited compliance, acceptable to the customer.

NOTE For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001 or this document can be considered.

Implementation guidance for PII processors

The organization should specify in contracts with any suppliers that PII is only processed on its instructions.

6.12.1.3 Information and communication technology supply chain

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.3 applies.

6.12.2 Supplier service delivery management

6.12.2.1 Monitoring and review of supplier services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.2.1 applies.

6.12.2.2 Managing changes to supplier services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.2.2 applies.

6.13 Information security incident management

6.13.1 Management of information security incidents and improvements

6.13.1.1 Responsibilities and procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.1 and the following additional guidance applies:

Additional implementation guidance for 16.1.1, Responsibilities and procedures, of ISO/IEC 27002:2013 is:

As part of the overall information security incident management process, the organization should establish responsibilities and procedures for the identification and recording of breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and/or regulation.

Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations.

6.13.1.2 Reporting information security events

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.2 applies.

© ISO/IEC 2019 – All rights reserved

6.13.1.3 Reporting information security weaknesses

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.3 applies.

6.13.1.4 Assessment of and decisions on information security events

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.4 applies.

6.13.1.5 Response to information security incidents

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.5 and the following additional guidance applies:

Additional implementation guidance for 16.1.5, Response to information security incidents, of ISO/IEC 27002:2013 is:

Implementation guidance for PII controllers

An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place.

An event does not necessarily trigger such a review.

NOTE 1 An information security event does not necessarily result in actual, or the significant probability of, unauthorized access to PII or to any of the organization's equipment or facilities storing PII. These can include, but are not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

When a breach of PII has occurred, response procedures should include relevant notifications and records.

Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals.

Notifications should be clear and can be required.

NOTE 2 Notification can contain details such as:

a contact point where more information can be obtained;

a description of and the likely consequences of the breach;

a description of the breach including the number of individuals concerned as well as the number of records concerned;

measures taken or planned to be taken.

NOTE 3 Information on the management of security incidents can be found in the ISO/IEC 27035 series.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:

a description of the incident;

the time period;

the consequences of the incident;

the name of the reporter;

to whom the incident was reported;

© ISO/IEC 2019 – All rights reserved

the steps taken to resolve the incident (including the person in charge and the data recovered);

the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII principals, regulatory agencies or customers.

Implementation guidance for PII processors

Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the customer. The contract should specify how the organization will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible. The contract should also define expected and externally mandated limits for notification response times.

In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (i.e. as soon as possible), preferably, as soon as it is discovered so that the PII controller can take the appropriate actions.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:

a description of the incident;

the time period;

the consequences of the incident;

the name of the reporter;

to whom the incident was reported;

the steps taken to resolve the incident (including the person in charge and the data recovered);

the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify the customer and/or the regulatory agencies.

In some jurisdictions, applicable legislation and/or regulation can require the organization to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a breach involving PII.

6.13.1.6 Learning from information security incidents

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.6 applies.

6.13.1.7 Collection of evidence

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.7 applies:

© ISO/IEC 2019 – All rights reserved

6.14 Information security aspects of business continuity management

6.14.1 Information security continuity

6.14.1.1 Planning information security continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.1.1 applies.

6.14.1.2 Implementing information security continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.1.2 applies.

6.14.1.3 Verify, renew and evaluate information security continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.1.3 applies.

6.14.2 Redundancies

6.14.2.1 Availability of information processing facilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.2.1 applies.

6.15 Compliance

6.15.1 Compliance with legal and contractual requirements

6.15.1.1 Identification of applicable legislation and contractual requirements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.1 and the following additional guidance applies:

Additional other information for 18.1.1, Identification of applicable legislation and contractual requirements, of ISO/IEC 27002:2013 is:

The organization should identify any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority. In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

6.15.1.2 Intellectual property rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.2 applies.

6.15.1.3 Protection of records

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.3 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Additional implementation guidance for 18.1.3, Protection of records, of ISO/IEC 27002:2013 is:

Review of current and historical policies and procedures can be required (e.g. in the cases of customer dispute resolution and investigation by a supervisory authority).

The organization should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule (see 7.4.7). This includes retention of previous versions of these documents when they are updated.

6.15.1.4 Privacy and protection of personally identifiable information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.4 applies.

6.15.1.5 Regulation of cryptographic controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.5 applies.

6.15.2 Information security reviews

6.15.2.1 Independent review of information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.1 and the following additional guidance applies:

Additional implementation guidance for 18.2.1, Independent review of information security, of ISO/IEC 27002:2013 is:

Where an organization is acting as a PII processor, and where individual customer audits are impractical or can increase risks to security, the organization should make available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organization's policies and procedures. A relevant independent audit, as selected by the organization, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization's processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner.

6.15.2.2 Compliance with security policies and standards

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.2 applies.

6.15.2.3 Technical compliance review

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.3 and the following additional guidance applies:

Additional implementation guidance for 18.2.3, Technical compliance review, of ISO/IEC 27002:2013 is:

As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing those tools and components related to processing PII. This can include:

- ongoing monitoring to verify that only permitted processing is taking place; and/or
- specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements).

© ISO/IEC 2019 – All rights reserved

7 Additional ISO/IEC 27002 guidance for PII controllers

7.1 General

The guidance in Clause 6 and the additions in this clause create the PIMS-specific guidance for PII controllers. The implementation guidance documented in this clause relate to the controls listed in Annex A.

7.2 Conditions for collection and processing

Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.

7.2.1 Identify and document purpose

Control

The organization should identify and document the specific purposes for which the PII will be processed.

Implementation guidance

The organization should ensure that PII principals understand the purpose for which their PII is processed. It is the responsibility of the organization to clearly document and communicate this to PII principals. Without a clear statement of the purpose for processing, consent and choice cannot be adequately given.

Documentation of the purpose(s) for processing PII should be sufficiently clear and detailed to be usable in the required information to be provided to PII principals (see 7.3.2). This includes information necessary to obtain consent (see 7.2.3), as well as records of policies and procedures (see 7.2.8).

Other information

In the deployment of cloud computing services, the taxonomy and definitions in ISO/IEC 19944 can be helpful in providing terms for describing the purpose of the processing of PII.

7.2.2 Identify lawful basis

Control

The organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

Some jurisdictions require the organization to be able to demonstrate that the lawfulness of processing was duly established before the processing.

The legal basis for the processing of PII can include:

consent from PII principals;

performance of a contract;

compliance with a legal obligation;

protection of the vital interests of PII principals;

performance of a task carried out in the public interest;

legitimate interests of the PII controller.

The organization should document this basis for each PII processing activity (see 7.2.8).

The legitimate interests of the organization can include, for instance, information security objectives, which should be balanced against the obligations to PII principals with regards to privacy protection.

Whenever special categories of PII are defined, either by the nature of the PII (e.g. health information) or by the PII principals concerned (e.g. PII relating to children) the organization should include those categories of PII in its classification schemes.

The classification of PII that falls into these categories can vary from one jurisdiction to another and can vary between different regulatory regimes that apply to different kinds of business, so the organization needs to be aware of the classification(s) that apply to the PII processing being performed.

The use of special categories of PII can also be subject to more stringent controls.

Changing or extending the purposes for the processing of PII can require updating and/or revision of the legal basis. It can also require additional consent to be obtained from the PII principal.

7.2.3 Determine when and how consent is to be obtained

Control

The organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.

Implementation guidance

Consent can be required for processing of PII unless other lawful grounds apply. The organization should clearly document when consent needs to be obtained and the requirements for obtaining consent. It can be useful to correlate the purpose(s) for processing with information about if and how consent is obtained.

Some jurisdictions have specific requirements for how consent is collected and recorded (e.g. not bundled with other agreements). Additionally, certain types of data collection (for scientific research for example) and certain types of PII principals, such as children, can be subject to additional requirements. The organization should take into account such requirements and document how mechanisms for consent meet those requirements.

© ISO/IEC 2019 – All rights reserved

7.2.4 Obtain and record consent

Control

The organization should obtain and record consent from PII principals according to the documented processes.

Implementation guidance

The organization should obtain and record consent from PII principals in such a way that it can provide on request details of the consent provided (for example the time that consent was provided, the identification of the PII principal, and the consent statement).

The information delivered to the PII principal before the consent process should follow the guidance in 7.3.3.

The consent should be:

freely given;

specific regarding the purpose for processing; and

unambiguous and explicit.

7.2.5 Privacy impact assessment

Control

The organization should assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.

Implementation guidance

PII processing generates risks for PII principals. These risks should be assessed through a privacy impact assessment. Some jurisdictions define cases for which a privacy impact assessment is mandated. Criteria can include automated decision making which produces legal effects on PII principals, large scale processing of special categories of PII (e.g. health-related information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data or biometric data), or systematic monitoring of a publicly accessible area on a large scale.

The organization should determine the elements that are necessary for the completion of a privacy impact assessment. These can include a list of the types of PII processed, where the PII is stored and where it can be transferred. Data flow diagrams and data maps can also be helpful in this context (see 7.2.8 for details of records of the processing of PII that can inform a privacy impact or other risk assessment).

Other information

Guidance on privacy impact assessments related to the processing of PII can be found in ISO/IEC 29134.

7.2.6 Contracts with PII processors

Control

The organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

The contract between the organization and any PII processor processing PII on its behalf should require the PII processor to implement the appropriate controls specified in Annex B, taking account of the information security risk assessment process (see 5.4.1.2) and the scope of the processing of PII performed by the PII processor (see 6.12). By default, all controls specified in Annex B should be assumed as relevant. If the organization decides to not require the PII processor to implement a control from Annex B, it should justify its exclusion (see 5.4.1.3).

A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information.

7.2.7 Joint PII controller

Control

The organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.

Implementation guidance

Roles and responsibilities for the processing of PII should be determined in a transparent manner.

These roles and responsibilities should be documented in a contract or any similar binding document that contains the terms and conditions for the joint processing of PII. In some jurisdictions, such an agreement is called a data sharing agreement.

A joint PII controller agreement can include (this list is neither definitive nor exhaustive):

purpose of PII sharing / joint PII controller relationship;

identity of the organizations (PII controllers) that are part of the joint PII controller relationship;

categories of PII to be shared and/or transferred and processed under the agreement;

overview of the processing operations (e.g. transfer, use);

description of the respective roles and responsibilities;

responsibility for implementing technical and organizational security measures for PII protection;

definition of responsibility in case of a PII breach (e.g. who will notify, when, mutual information);

terms of retention and/or disposal of PII;

liabilities for failure to comply with the agreement;

how obligations to PII principals are met;

how to provide PII principals with information covering the essence of the arrangement between the joint PII controllers;

how PII principals can obtain other information they are entitled to receive; and

a contact point for PII principals.

7.2.8 Records related to processing PII

Control

The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

A way to maintain records of the processing of PII is to have an inventory or list of the PII processing activities that the organization performs. Such an inventory can include:

the type of processing;

the purposes for the processing;

a description of the categories of PII and PII principals (e.g. children);

the categories of recipients to whom PII has been or will be disclosed, including recipients in third countries or international organizations;

a general description of the technical and organizational security measures; and

a Privacy Impact Assessment report.

Such an inventory should have an owner who is responsible for its accuracy and completeness.

7.3 Obligations to PII principals

Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.

7.3.1 Determining and fulfilling obligations to PII principals

Control

The organization should determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.

Implementation guidance

Obligations to PII principals and the means to support them vary from one jurisdiction to another.

The organization should ensure that they provide the appropriate means to meet the obligations to PII principals in an accessible and timely manner. Clear documentation should be provided to the PII principal describing the extent to which the obligations to them are fulfilled and how, along with an up-to-date contact point where they can address their requests.

The contact point should be provided in a similar way to that used to collect PII and consent (e.g. if PII are collected by email or a website, the contact point should be by email or the website, not an alternative such as phone or fax).

7.3.2 Determining information for PII principals

Control

The organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.

Implementation guidance

The organization should determine the legal, regulatory and/or business requirements for when information is to be provided to the PII principal (e.g. prior to processing, within a certain time from when it is requested, etc.) and for the type of information to be provided.

© ISO/IEC 2019 – All rights reserved

Depending on the requirements, the information can take the form of a notice. Examples of types of information that can be provided to PII principals are:

information about the purpose of the processing;

contact details for the PII controller or its representative;

information about the lawful basis for the processing;

information on where the PII was obtained, if not obtained directly from the PII principal;

information about whether the provision of PII is a statutory or contractual requirement, and where appropriate, the possible consequences of failure to provide PII;

information on obligations to PII principals, as determined in 7.3.1, and how PII principals can benefit from them, especially regarding accessing, amending, correcting, requesting erasure, receiving a copy of their PII and objecting to the processing;

information on how the PII principal can withdraw consent;

information about transfers of PII;

information about recipients or categories of recipients of PII;

information about the period for which the PII will be retained;

information about the use of automated decision making based on the automated processing of PII;

information about the right to lodge a complaint and how to lodge such a complaint;

information regarding the frequency with which information is provided (e.g. "just in time" notification, organization defined frequency, etc.).

The organization should provide updated information if the purposes for the processing of PII are changed or extended.

7.3.3 Providing information to PII principals

Control

The organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.

Implementation guidance

The organization should provide the information detailed in 7.3.2 to PII principals in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience.

Where appropriate, the information should be given at the time of PII collection. It should also be permanently accessible.

NOTE Icons and images can be helpful to the PII principal by giving a visual overview of the intended processing.

7.3.4 Providing mechanism to modify or withdraw consent

Control

The organization should provide a mechanism for PII principals to modify or withdraw their consent.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

The organization should inform PII principals of their rights related to withdrawing consent (which may vary by jurisdiction) at any time, and provide the mechanism to do so. The mechanism used for withdrawal depends on the system; it should be consistent with the mechanisms used for obtaining consent when possible. For example, if the consent is collected by email or a website, the mechanism for withdrawing it should be the same, not an alternative solution such as phone or fax.

Modifying consent can include placing restrictions on the processing of PII, which can include restricting the PII controller from deleting the PII in some cases.

Some jurisdictions impose restrictions on when and how a PII principal can modify or withdraw their consent.

The organization should record any request to withdraw or change consent in a similar way to the recording of the consent itself.

Any change of consent should be disseminated, through appropriate systems, to authorized users and to relevant third parties.

The organization should define a response time and requests should be handled according to it.

Additional information

When consent for particular processing of PII is withdrawn, all the processing of PII performed before withdrawal should normally be considered as appropriate, but the results of such processing should not be used for new processing. For example, if a PII principal withdraws their consent for profiling, their profile should not be further used or consulted.

7.3.5 Providing mechanism to object to PII processing

Control

The organization should provide a mechanism for PII principals to object to the processing of their PII.

Implementation guidance

Some jurisdictions provide PII principals with a right to object to the processing of their PII. Organizations subject to the legislation and/or regulation of such jurisdictions should ensure that they implement appropriate measures to enable PII principals to exercize this right.

The organization should document the legal and regulatory requirements related to objections by the PII principals to processing (e.g. objection relating to the processing of PII for direct marketing purposes). The organization should provide information to principals regarding the ability to object in these situations. Mechanisms to object can vary, but should be consistent with the type of service provided (e.g. online services should provide this capability online).

7.3.6 Access, correction and/or erasure

Control

The organization should implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

The organization should implement policies, procedures and/or mechanisms for enabling PII principals to obtain access to, correct and erase of their PII, if requested and without undue delay.

The organization should define a response time and requests should be handled according to it.

Any corrections or erasures should be disseminated through the system and/or to authorized users, and should be passed to third parties (see 7.3.7) to whom the PII has been transferred.

NOTE Records generated by the control specified in 7.5.3 can help in this regard.

The organization should implement policies, procedures and/or mechanisms for use when there can be a dispute about the accuracy or correction of the data by the PII principal. These policies, procedures and/or mechanisms should include informing the PII principal of what changes were made, and of reasons why corrections cannot be made (where this is the case).

Some jurisdictions impose restrictions on when and how a PII principal can request correction or erasure of their PII. The organization should determine these restrictions as applicable and keep itself up-to-date about them.

7.3.7 PII controllers' obligations to inform third parties

Control

The organization should inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so.

Implementation guidance

The organization should take appropriate steps, bearing in mind the available technology, to inform third parties of any modification or withdrawal of consent, or objections pertaining to the shared PII. Some jurisdictions impose a legal requirement to inform these third parties of these actions.

The organization should determine and maintain active communication channels with third parties. Related responsibilities can be assigned to individuals in charge of their operations and maintenance. When informing third parties, the organization should monitor their acknowledgement of receipt of the information.

NOTE Changes resulting from the obligations to PII principals can include modification or withdrawal of consent, requests for correction, erasure, or restrictions on processing, or objections to the processing of PII as requested by the PII principal.

7.3.8 Providing copy of PII processed

Control

The organization should be able to provide a copy of the PII that is processed when requested by the PII principal.

Implementation guidance

The organization should provide a copy of the PII that is processed in a structured, commonly used, format accessible by the PII principal.

Some jurisdictions define cases where the organization should provide a copy of the PII processed in a format allowing portability to the PII principals or to recipient PII controllers (typically structured, commonly used and machine readable).

The organization should ensure that any copies of PII provided to a PII principal relate specifically to that PII principal.

© ISO/IEC 2019 – All rights reserved

Where the requested PII has already been deleted subject to the retention and disposal policy (as described in 7.4.7), the PII controller should inform the PII principal that the requested PII has been deleted.

In cases where the organization is no longer able to identify the PII principal (e.g. as a result of a de-identification process), the organization should not seek to (re-)identify the PII principals for the sole reason of implementing this control. However, in some jurisdictions, legitimate requests can require that additional information should be requested from the PII principal to enable re-identification and subsequent disclosure.

Where technically feasible, it should be possible to transfer a copy of the PII from one organization directly to another organization, at the request of the PII principal.

7.3.9 Handling requests

Control

The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals.

Implementation guidance

Legitimate requests can include requests for a copy of PII processed, or requests to lodge a complaint.

Some jurisdictions allow the organization to charge a fee in certain cases (e.g. excessive or repetitive requests).

Requests should be handled within the appropriate defined response times.

Some jurisdictions define response times, depending on the complexity and number of the requests, as well as requirements to inform PII principals of any delay. The appropriate response times should be defined in the privacy policy.

7.3.10 Automated decision making

Control

The organization should identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.

Implementation guidance

Some jurisdictions define specific obligations to PII principals when a decision based solely on automated processing of PII significantly affects them, such as notifying the existence of automated decision making, allowing for the PII principals to object to such decision making, and/or obtaining human intervention.

NOTE In some jurisdictions, some processing of PII cannot be fully automated.

Organizations operating in these jurisdictions should take compliance with these obligations into account.

7.4 Privacy by design and privacy by default

Objective: To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

© ISO/IEC 2019 – All rights reserved

7.4.1 Limit collection

Control

The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.

Implementation guidance

The organization should limit the collection of PII to what is adequate, relevant and necessary in relation to the identified purposes. This includes limiting the amount of PII that the organization collects indirectly (e.g. through web logs, system logs, etc.).

Privacy by default implies that, where any optionality in the collection and processing of PII exists, each option should be disabled by default and only enabled by explicit choice of the PII principal.

7.4.2 Limit processing

Control

The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.

Implementation guidance

Limiting the processing of PII should be managed through information security and privacy policies (see 6.2) along with documented procedures for their adoption and compliance.

Processing of PII, including:

the disclosure;

the period of PII storage; and

who is able to access their PII;

should be limited by default to the minimum necessary relative to the identified purposes.

7.4.3 Accuracy and quality

Control

The organization should ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.

Implementation guidance

The organization should implement policies, procedures and/or mechanisms to minimize inaccuracies in the PII it processes. There should also be policies, procedures and/or mechanisms to respond to instances of inaccurate PII. These policies, procedures and/or mechanisms should be included in the documented information (e.g. through technical system configurations, etc.) and should apply throughout the PII lifecycle.

Additional information

For further information on the PII processing life-cycle, see ISO/IEC 29101:2018, 6.2.

© ISO/IEC 2019 – All rights reserved

7.4.4 PII minimization objectives

Control

The organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.

Implementation guidance

Organizations should identify how the specific PII and amount of PII collected and processed is limited relative to the identified purposes. This can include the use of de-identification or other data minimization techniques.

The identified purpose (see 7.2.1) can require the processing of PII that has not been de-identified, in which case the organization should be able to describe such processing.

In other cases, the identified purpose does not require the processing of the original PII, and the processing of PII which has been de-identified can suffice to achieve the identified purpose. In these cases, the organization should define and document the extent to which the PII needs to be associated with the PII principal, as well as the mechanisms and techniques designed to process PII, such that the de-identification and/or PII minimization objectives are achieved.

Mechanisms used to minimize PII vary depending on the type of processing and the systems used for the processing. The organization should document any mechanisms (technical system configurations, etc.) used to implement data minimization.

In cases where processing of de-identified data is sufficient for the purposes, the organization should document any mechanisms (technical system configurations, etc.) designed to implement de-identification objectives set by the organization in a timely manner. For instance, the removal of attributes associated with PII principals can be sufficient to allow the organization to achieve its identified purpose. In other cases, other de-identification techniques, such as generalization (e.g. rounding) or randomization techniques (e.g. noise addition) can be used to achieve an adequate level of de-identification.

NOTE 1 For further information on de-identification techniques, refer to ISO/IEC 20889.

NOTE 2 For Cloud computing, ISO/IEC 19944 provides a definition of data identification qualifiers that can be used to classify the degree to which the data can identify a PII principal or associate a PII principal with a set of characteristics in the PII.

7.4.5 PII de-identification and deletion at the end of processing

Control

The organization should either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).

Implementation guidance

The organization should have mechanisms to erase the PII when no further processing is anticipated. Alternatively, some de-identification techniques can be used as long as the resulting de-identified data cannot reasonably permit re-identification of PII principals.

7.4.6 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

The organization should perform periodic checks that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.

7.4.7 Retention

Control

The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed.

Implementation guidance

The organization should develop and maintain retention schedules for information it retains, taking into account the requirement to retain PII for no longer than is necessary. Such schedules should take into account legal, regulatory and business requirements. Where such requirements conflict, a business decision needs to be taken (based on a risk assessment) and documented in the appropriate schedule.

7.4.8 Disposal

Control

The organization should have documented policies, procedures and/or mechanisms for the disposal of PII.

Implementation guidance

The choice of PII disposal techniques depends on a number of factors, as disposal techniques differ in their properties and outcomes (for example in the granularity of the resultant physical media, or the ability to recover deleted information on electronic media). Factors to consider when choosing an appropriate disposal technique include, but are not limited to, the nature and extent of the PII to be disposed of, whether or not there is metadata associated with the PII, and the physical characteristics of the media on which the PII is stored.

7.4.9 PII transmission controls

Control

The organization should subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of audit logs) to ensure that PII is transmitted without compromise to the correct recipients.

© ISO/IEC 2019 – All rights reserved

7.5 PII sharing, transfer, and disclosure

Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

7.5.1 Identify basis for PII transfer between jurisdictions

Control

The organization should identify and document the relevant basis for transfers of PII between jurisdictions.

Implementation guidance

PII transfer can be subject to legislation and/or regulation depending on the jurisdiction or international organization to which data is to be transferred (and from where it originates). The organization should document compliance to such requirements as the basis for transfer.

Some jurisdictions can require that information transfer agreements be reviewed by a designated supervisory authority. Organizations operating in such jurisdictions should be aware of any such requirements.

NOTE Where transfers take place within a specific jurisdiction, the applicable legislation and/or regulation are the same for the sender and recipient.

7.5.2 Countries and international organizations to which PII can be transferred

Control

The organization should specify and document the countries and international organizations to which PII can possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 7.5.1.

Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see 7.5.1, 8.5.4 and 8.5.5).

7.5.3 Records of transfer of PII

Control

The organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.

Implementation guidance

Recording can include transfers from third parties of PII which has been modified as a result of PII controllers' managing their obligations, or transfers to third parties to implement legitimate requests from PII principals, including requests to erase PII (e.g. after consent withdrawal).

The organization should have a policy defining the retention period of these records.

© ISO/IEC 2019 – All rights reserved

The organization should apply the data minimization principle to the records of transfers by retaining only the strictly needed information.

7.5.4 Records of PII disclosure to third parties

Control

The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

Implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

8 Additional ISO/IEC 27002 guidance for PII processors

8.1 General

The guidance in Clause 6 and the additions of this clause create the PIMS-specific guidance for PII processors. The implementation guidance documented in this clause relate to the controls listed in Annex B.

8.2 Conditions for collection and processing

Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.

8.2.1 Customer agreement

Control

The organization should ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization).

Implementation guidance

The contract between the organization and the customer should include the following wherever relevant, and depending on the customer's role (PII controller or PII processor) (this list is neither definitive nor exhaustive):

privacy by design and privacy by default (see 7.4, 8.4);

achieving security of processing;

notification of breaches involving PII to a supervisory authority;

notification of breaches involving PII to customers and PII principals;

conducting Privacy Impact Assessments (PIA); and

the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed.

Some jurisdictions require that the contract include the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of PII principals.

© ISO/IEC 2019 – All rights reserved

8.2.2 Organizatıon s purposes

Control

The organization should ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.

Implementation guidance

The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service.

In order to achieve the customer's purpose, there can be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the customer's express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific processing resources depending on certain characteristics of the PII principal.

The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. This also ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the documented instructions of the customer.

8.2.3 Marketing and advertising use

Control

The organization should not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization should not make providing such consent a condition for receiving the service.

Implementation guidance

Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing and/or advertising is planned.

Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals.

NOTE This control is in addition to the more general control in 8.2.2 and does not replace or otherwise supersede it.

8.2.4 Infringing instruction

Control

The organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.

Implementation guidance

The organization's ability to verify if the instruction infringes legislation and/or regulation can depend on the technological context, on the instruction itself, and on the contract between the organization and the customer.

8.2.5 Customer obligations

Control

The organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.

© ISO/IEC 2019 – All rights reserved

Implementation guidance

The information needed by the customer can include whether the organization allows for and contributes to audits conducted by the customer or another auditor mandated or otherwise agreed by the customer.

8.2.6 Records related to processing PII

Control

The organization should determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.

Implementation guidance

Some jurisdictions can require the organization to record information such as:

categories of processing carried out on behalf of each customer;

transfers to third countries or international organizations; and

a general description of the technical and organizational security measures.

8.3 Obligations to PII principals

Objective: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.

8.3.1 Obligations to PII principals

Control

The organization should provide the customer with the means to comply with its obligations related to PII principals.

Implementation guidance

A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion.

Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a contract.

8.4 Privacy by design and privacy by default

Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

© ISO/IEC 2019 – All rights reserved

8.4.1 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.

Implementation guidance

The organization should conduct periodic verification that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.

8.4.2 Return, transfer or disposal of PII

Control

The organization should provide the ability to return, transfer and/or disposal of PII in a secure manner. It should also make its policy available to the customer.

Implementation guidance

At some point in time, PII can need to be disposed of in some manner. This can involve returning the PII to the customer, transferring it to another organization or to a PII controller (e.g. as a result of a merger), deleting or otherwise destroying it, de-identifying it or archiving it. The capability for the return, transfer and/or disposal of PII should be managed in a secure manner.

The organization should provide the assurance necessary to allow the customer to ensure that PII processed under a contract is erased (by the organization and any of its subcontractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the identified purposes of the customer.

The organization should develop and implement a policy in respect to the disposal of PII and should make this policy available to customer when requested.

The policy should cover the retention period for PII before its disposal after termination of a contract, to protect the customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention principle (see 7.4.7).

8.4.3 PII transmission controls

Control

The organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of

© ISO/IEC 2019 – All rights reserved

audit data) to ensure that PII is transmitted without compromise to the correct recipients. Requirements for transmission controls can be included in the PII processor — customer contract.

Where no contractual requirements related to transmission are in place, it can be appropriate to take advice from the customer prior to transmission.

8.5 PII sharing, transfer, and disclosure

Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

8.5.1 Basis for PII transfer between jurisdictions

Control

The organization should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.

Implementation guidance

PII transfer between jurisdictions can be subject to legislation and/or regulation depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates). The organization should document compliance with such requirements as the basis for transfer.

The organization should inform the customer of any transfer of PII, including transfers to:

suppliers;

other parties;

other countries or international organizations.

In case of changes, the organization should inform the customer in advance, according to an agreed timeframe, so that the customer has the ability to object to such changes or to terminate the contract.

The agreement between the organization and the customer can have clauses where the organization can implement changes without informing the customer. In these cases, the limits of this allowance should be set (e.g. the organization can change suppliers without informing the customer, but cannot transfer PII to other countries).

In case of international transfer of PII, agreements such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the countries involved and the circumstances in which such agreements apply, should be identified.

8.5.2 Countries and international organizations to which PII can be transferred

Control

The organization should specify and document the countries and international organizations to which PII can possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 8.5.1.

© ISO/IEC 2019 – All rights reserved

Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see 7.5.1, 8.5.4 and 8.5.5).

8.5.3 Records of PII disclosure to third parties

Control

The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.

Implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

8.5.4 Notification of PII disclosure requests

Control

The organization should notify the customer of any legally binding requests for disclosure of PII.

Implementation guidance

The organization can receive legally binding requests for disclosure of PII (e.g. from law enforcement authorities). In these cases, the organization should notify the customer of any such request within agreed timeframes and according to an agreed procedure (which can be included in the customer contract).

In some cases, the legally binding requests include the requirement for the organization not to notify anyone about the event (an example of a possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

8.5.5 Legally binding PII disclosures

Control

The organization should reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.

Implementation guidance

Details relevant to the implementation of the control can be included in the customer contract.

Such requests can originate from several sources, including courts, tribunals and administrative authorities. They can arise from any jurisdiction.

8.5.6 Disclosure of subcontractors used to process PII

Control

The organization should disclose any use of subcontractors to process PII to the customer before use.

Implementation guidance

Provisions for the use of subcontractors to process PII should be included in the customer contract.

© ISO/IEC 2019 – All rights reserved

Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors. The information disclosed should also include the countries and international organizations to which subcontractors can transfer data (see 8.5.2) and the means by which subcontractors are obliged to meet or exceed the obligations of the organization (see 8.5.7).

Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the customer. The customer should be made aware that the information is available.

This does not concern the list of countries where the PII can be transferred. This list should be disclosed to the customer in all cases in a way that allows them to inform the appropriate PII principals.

8.5.7 Engagement of a subcontractor to process PII

Control

The organization should only engage a subcontractor to process PII according to the customer contract.

Implementation guidance

Where the organization subcontracts some or all of the processing of that PII to another organization, a written authorization from the customer is required prior to the PII processed by the subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific "one-off" agreement.

The organization should have a written contract with any subcontractors that it uses for PII processing on its behalf, and should ensure that their contracts with subcontractors address the implementation of the appropriate controls in Annex B.

The contract between the organization and any subcontractor processing PII on its behalf should require the subcontractor to implement the appropriate controls specified in Annex B, taking account of the information security risk assessment process (see 5.4.1.2) and the scope of the processing of PII performed by the PII processor (see 6.12). By default, all controls specified in Annex B should be assumed as relevant. If the organization decides to not require the subcontractor to implement a control from Annex B, it should justify its exclusion.

A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information.

8.5.8 Change of subcontractor to process PII

Control

The organization should, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

Implementation guidance

Where the organization changes the organization with which it subcontracts some or all of the processing of that PII, then written authorization from the customer is required for the change, prior to the PII processed by the new subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific "one-off" agreement.

© ISO/IEC 2019 – All rights reserved

Annex A
(normative)

PIMS-specific reference control objectives and controls (PII Controllers)

This annex is for use by organizations acting as PII controllers, with or without the use of PII processors. It extends ISO/IEC 27001:2013, Annex A.

The additional or modified control objectives and controls listed in Table A.1 are directly derived from and aligned with those defined in this document and are to be used in context with ISO/IEC 27001:2013, 6.1.3 as refined by 5.4.1.3.

Not all the control objectives and controls listed in this annex need to be included in the PIMS implementation. A justification for excluding any control objectives shall be included in the Statement of Applicability (see 5.4.1.3). Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the applicable legislation and/or regulation.

NOTE Clause numbers in this annex relate to the subclause numbers in Clause 7.

Table A.1 — Control objectives and controls

A.7.2 Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.		
A.7.2.1	Identify and document purpose	*Control* The organization shall identify and document the specific purposes for which the PII will be processed.
A.7.2.2	Identify lawful basis	*Control* The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.
A.7.2.3	Determine when and how consent is to be obtained	*Control* The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals
A.7.2.4	Obtain and record consent	*Control* The organization shall obtain and record consent from PII principals according to the documented processes.
A.7.2.5	Privacy impact assessment	*Control* The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.
A.7.2.6	Contracts with PII processors	*Control* The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.

© ISO/IEC 2019 – All rights reserved

Table A.1 *(continued)*

A.7.2.7	Joint PII controller	*Control* The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.
A.7.2.8	Records related to processing PII	*Control* The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.
A.7.3 Obligations to PII principals Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.		
A.7.3.1	Determining and fulfilling obligations to PII principals	*Control* The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.
A.7.3.2	Determining information for PII principals	*Control* The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.
A.7.3.3	Providing information to PII principals	*Control* The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.
A.7.3.4	Providing mechanism to modify or withdraw consent	*Control* The organization shall provide a mechanism for PII principals to modify or withdraw their consent.
A.7.3.5	Providing mechanism to object to PII processing	*Control* The organization shall provide a mechanism for PII principals to object to the processing of their PII.
A.7.3.6	Access, correction and/or erasure	*Control* The organization shall implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.
A.7.3.7	PII controllers' obligations to inform third parties	*Control* The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so.
A.7.3.8	Providing copy of PII processed	*Control* The organization shall be able to provide a copy of the PII that is processed when requested by the PII principal.
A.7.3.9	Handling requests	*Control* The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.
A.7.3.10	Automated decision making	*Control* The organization shall identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.

© ISO/IEC 2019 – All rights reserved

Table A.1 *(continued)*

A.7.4 Privacy by design and privacy by default		
Objective:		
To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
A.7.4.1	Limit collection	*Control* The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.
A.7.4.2	Limit processing	*Control* The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.
A.7.4.3	Accuracy and quality	*Control* The organization shall ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.
A.7.4.4	PII minimization objectives	*Control* The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.
A.7.4.5	PII de-identification and deletion at the end of processing	*Control* The organization shall either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).
A.7.4.6	Temporary files	*Control* The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
A.7.4.7	Retention	*Control* The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed.
A.7.4.8	Disposal	*Control* The organization shall have documented policies, procedures and/or mechanisms for the disposal of PII.
A.7.4.9	PII transmission controls	*Control* The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
A.7.5 PII sharing, transfer and disclosure		
Objective:		
To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.		
A.7.5.1	Identify basis for PII transfer between jurisdictions	*Control* The organization shall identify and document the relevant basis for transfers of PII between jurisdictions.
A.7.5.2	Countries and international organizations to which PII can be transferred	*Control* The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.

© ISO/IEC 2019 – All rights reserved

Table A.1 *(continued)*

A.7.5.3	Records of transfer of PII	*Control* The organization shall record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.
A.7.5.4	Records of PII disclosure to third parties	*Control* The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

© ISO/IEC 2019 – All rights reserved

Annex B
(normative)

PIMS-specific reference control objectives and controls (PII Processors)

This annex is for use by organizations acting as PII processors, with or without the use of PII subcontractors. It extends ISO/IEC 27001:2013, Annex A.

The additional or modified control objectives and controls listed in Table B.1 are directly derived from and aligned with those defined in this document and are to be used in context with ISO/IEC 27001:2013, 6.1.3 as refined by 5.4.1.3.

Not all the control objectives and controls listed in this annex need to be included in the PIMS implementation. A justification for excluding any control objectives shall be included in the Statement of Applicability (see 5.4.1.3). Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the applicable legislation and/or regulation.

NOTE Clause numbers in this annex relate to the subclause numbers in Clause 8.

Table B.1 — Control objectives and controls

B.8.2 Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.		
B.8.2.1	Customer agreement	*Control* The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).
B.8.2.2	Organization's purposes	*Control* The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
B.8.2.3	Marketing and advertising use	*Control* The organization shall not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.
B.8.2.4	Infringing instruction	*Control* The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.
B.8.2.5	Customer obligations	*Control* The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.

© ISO/IEC 2019 – All rights reserved

Table B.1 *(continued)*

B.8.2.6	Records related to processing PII	*Control* The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.
B.8.3 Obligations to PII principals Objective: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.		
B.8.3.1	Obligations to PII principals	*Control* The organization shall provide the customer with the means to comply with its obligations related to PII principals.
B.8.4 Privacy by design and privacy by default Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
B.8.4.1	Temporary files	*Control* The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
B.8.4.2	Return, transfer or disposal of PII	*Control* The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.
B.8.4.3	PII transmission controls	*Control* The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
B.8.5 PII sharing, transfer and disclosure Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.		
B.8.5.1	Basis for PII transfer between jurisdictions	*Control* The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.
B.8.5.2	Countries and international organizations to which PII can be transferred	*Control* The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.
B.8.5.3	Records of PII disclosure to third parties	*Control* The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.
B.8.5.4	Notification of PII disclosure requests	*Control* The organization shall notify the customer of any legally binding requests for disclosure of PII.

© ISO/IEC 2019 – All rights reserved

Table B.1 *(continued)*

B.8.5.5	Legally binding PII disclosures	*Control* The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.
B.8.5.6	Disclosure of sub-contractors used to process PII	*Control* The organization shall disclose any use of subcontractors to process PII to the customer before use.
B.8.5.7	Engagement of a subcontractor to process PII	*Control* The organization shall only engage a subcontractor to process PII according to the customer contract.
B.8.5.8	Change of subcon-tractor to process PII	*Control* The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

© ISO/IEC 2019 – All rights reserved

Annex C
(informative)

Mapping to ISO/IEC 29100

Table C.1 and C.2 give an indicative mapping between provisions of this document and the privacy principles from ISO/IEC 29100. It shows in a purely indicative manner how compliance to requirements and controls of this document relates to the general privacy principles specified in ISO/IEC 29100.

Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
1. Consent and Choice	A.7.2.1 Identify and document purpose A.7.2.2 Identify lawful basis A.7.2.3 Determine when and how consent is to be obtained A.7.2.4 Obtain and record consent A.7.2.5 Privacy impact assessment A.7.3.4 Provide mechanism to modify or withdraw consent A.7.3.5 Provide mechanism to object to processing A.7.3.7 PII controllers' obligations and third parties
2. Purpose legitimacy and specification	A.7.2.1 Identify and document purpose A.7.2.2 Identify lawful basis A.7.2.5 Privacy impact assessment A.7.3.2 Determining information for PII principals A.7.3.3 Providing information to PII principals A.7.3.10 Automated decision making
3. Collection limitation	A.7.2.5 Privacy impact assessment A.7.4.1 Limit collection
4. Data minimization	A.7.4.2 Limit processing A.7.4.4 PII minimization objectives A.7.4.5 PII de-identification and deletion at the end of processing
5. Use, retention and disclosure limitation	A.7.4.4 PII minimization objectives A.7.4.5 PII de-identification and deletion at the end of processing A.7.4.6 Temporary files A.7.4.7 Retention A.7.4.8 Disposal A.7.5.1 Identify basis for international PII transfer A.7.5.4 Records of PII disclosure to third parties
6. Accuracy and quality	A.7.4.3 Accuracy and quality
7. Openness, transparency and notice	A.7.3.2 Determining information for PII principals A.7.3.3 Providing information to PII principals

© ISO/IEC 2019 – All rights reserved

Table C.1 *(continued)*

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
8. Individual participation and access	A.7.3.1 Determining and fulfilling obligations to PII principals
	A.7.3.3 Providing copy of PII processed
	A.7.3.6 Access, correction and/or erasure
	A.7.3.8 Providing copy of PII processed
	A.7.3.9 Handling requests
9. Accountability	A.7.2.6 Contracts with PII processors
	A.7.2.7 Joint controller
	A.7.2.8 Records related to processing PII
	A.7.3.9 Handling requests
	A.7.5.1 Identify basis for international PII transfer
	A.7.5.2 Countries and organizations to which PII can be transferred
	A.7.5.3 Records and transfer of PII
10. Information Security	A.7.2.6 Contracts with PII processors
	A.7.4.9 PII transmission controls
11. Privacy compliance	A.7.2.5 Privacy impact assessment

Table C.2 — Mapping of controls for PII processors and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII processors
1. Consent and choice	B.8.2.5 Customer obligations
2. Purpose legitimacy and specification	B.8.2.1 Customer agreement
	B.8.2.2 Organization's purposes
	B.8.2.3 Marketing and advertising use
	B.8.2.4 Infringing instruction
	B.8.3.1 Obligations to PII principals
3. Collection limitation	N/A
4. Data minimization	B.8.4.1 Temporary files
5. Use, retention and disclosure limitation	B.8.5.3 Records of PII disclosure to third parties
	B.8.5.4 Notification of PII disclosure requests
	B.8.5.5 Legally binding PII disclosures
6. Accuracy and quality	N/A
7. Openness, transparency and notice	B.8.5.6 Disclosure of subcontractors used to process PII
	B.8.5.7 Engagement of a subcontractor to process PII
	B.8.5.8 Change of subcontractor to process PII
8. Individual participation and access	B.8.3.1 Obligations to PII principals
9. Accountability	B.8.2.6 Records related to processing PII
	B.8.4.2 Return, transfer or disposal of PII
	B.8.5.1 Identify basis for international PII transfer
	B.8.5.2 Countries and organizations to which PII can be transferred
10. Information security	B.8.4.3 PII transmission controls
11. Privacy compliance	B.8.2.5 Customer obligations

© ISO/IEC 2019 – All rights reserved

Annex D
(informative)

Mapping to the General Data Protection Regulation

This annex gives an indicative mapping between provisions of this document and Articles 5 to 49 except 43 of the General Data Protection Regulation of the European Union. It shows how compliance to requirements and controls of this document can be relevant to fulfil obligations of GDPR.

However, it is purely indicative and as per this document, it is the organizations responsibility to assess its legal obligations and decide how to comply with them.

Table D.1 — Mapping of ISO/IEC 27701 structure to GDPR articles

Subclause of this document	GDPR article
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)
6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)

© ISO/IEC 2019 – All rights reserved

Table D.1 *(continued)*

Subclause of this document	GDPR article
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)
6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)
7.3.3	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)

© ISO/IEC 2019 – All rights reserved

Table D.1 *(continued)*

Subclause of this document	GDPR article
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c), (5)(1)(e)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)
7.4.8	(5)(1)(f)
7.4.9	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)
8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)
8.5.8	(28)(2)

© ISO/IEC 2019 – All rights reserved

Annex E
(informative)

Mapping to ISO/IEC 27018 and ISO/IEC 29151

ISO/IEC 27018 gives further information for organizations acting as PII processors and providing public cloud services. ISO/IEC 29151 gives additional controls and guidance for the processing of PII by PII controllers.

Table E.1 gives an indicative mapping between provisions of this document and provisions from ISO/IEC 27018 and ISO/IEC 29151. It shows how requirements and controls of this document can have some correspondence with provisions from ISO/IEC 27018 and/or ISO/IEC 29151.

It is purely indicative and it should not be assumed that a given link between provisions means equivalence.

Table E.1 — Mapping of ISO/IEC 27701 to ISO/IEC 27018 and ISO/IEC 29151

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
5.2	N/A	N/A
5.3	N/A	N/A
5.4	N/A	4.2
5.5	N/A	7.2.3
5.6	N/A	N/A
5.7	N/A	N/A
5.8	N/A	N/A
6.1	N/A	N/A
6.2	5.1.1	5
6.3	6.1.1	N/A
6.4	7.2.2	N/A
6.5.1	N/A	8.1
6.5.2	N/A	8.2
6.5.3	A.11.4, A.11.5	8.3
6.6.1	N/A	N/A
6.6.2	9.2.1, A.11.8, A,11,9, A.11.10	9.2
6.6.3	N/A	9.3
6.6.4	7.2.2, 9.4.2	9.4
6.7	10.1.1	N/A
6.8.1	N/A	11.1
6.8.2	11.2.7, A.11.2, A.11.13	N/A
6.9.1	N/A	12.1
6.9.2	N/A	12.2
6.9.3	N/A	12.3
6.9.4	12.4.1, 12.4.2	12.4
6.9.5	N/A	N/A
6.9.6	N/A	N/A

© ISO/IEC 2019 – All rights reserved

Table E.1 *(continued)*

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
6.9.7	N/A	N/A
6.10.1	N/A	13.1
6.10.2	13.2.1, A.11.1	13.2
6.11.1	A.11.6	N/A
6.11.2	N/A	N/A
6.11.3	12.1.4	N/A
6.12.1	A.11.11	N/A
6.12.2	N/A	N/A
6.13	16.1.1, A.10.1	N/A
6.14	N/A	N/A
6.15.1	A.10.2	N/A
6.15.2	18.2.1	18.2
7.2.1	N/A	A.4
7.2.2	N/A	A.4.1
7.2.3	N/A	N/A
7.2.4	N/A	A.3.1
7.2.5	N/A	A.11.2
7.2.6	N/A	A.11.3
7.2.7	N/A	N/A
7.2.8	N/A	N/A
7.3.1	N/A	A.10
7.3.2	N/A	N/A
7.3.3	N/A	A.9
7.3.4	N/A	N/A
7.3.5	N/A	N/A
7.3.6	N/A	A.10.1
7.3.7	N/A	N/A
7.3.8	N/A	N/A
7.3.9	N/A	N/A
7.3.10	N/A	N/A
7.4.1	N/A	A.5
7.4.2	N/A	N/A
7.4.3	N/A	A.8
7.4.4	N/A	N/A
7.4.5	N/A	A.7.1
7.4.6	N/A	A.7.2
7.4.7	N/A	A.7.1
7.4.8	N/A	N/A
7.4.9	N/A	N/A
7.5.1	N/A	A.13.2
7.5.2	N/A	A.13.2
7.5.3	N/A	A.13.2
7.5.4	N/A	A.7.4

© ISO/IEC 2019 – All rights reserved

Table E.1 *(continued)*

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
8.2.1	N/A	N/A
8.2.2	A.3.1	N/A
8.2.3	A.3.2	N/A
8.2.4	N/A	N/A
8.2.5	N/A	N/A
8.2.6	N/A	N/A
8.3.1	A.2.1	N/A
8.4.1	A.5.1	N/A
8.4.2	A.10.3	N/A
8.4.3	A.12.2	N/A
8.5.1	N/A	N/A
8.5.2	A.12.1	N/A
8.5.3	A.6.2	N/A
8.5.4	A.6.1	N/A
8.5.5	A.6.1	N/A
8.5.6	A.8.1	A.7.5
8.5.7	A.8.1	N/A
8.5.8	A.8.1	N/A

© ISO/IEC 2019 – All rights reserved

Annex F
(informative)

How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

F.1 How to apply this document

This document is based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013 and extends their requirements and guidance to take into account, in addition to information security, the protection of privacy of PII principals as potentially affected by the processing of PII. That means, where the term "information security" is used in ISO/IEC 27001 or ISO/IEC 27002 "information security and privacy" applies instead.

Table F.1 gives the mapping of the extension of the term information security in order to apply it to this document.

Table F.1 — Mapping of the extension of the term information security by privacy

ISO/IEC 27001	This document (extension)
information security	information security and privacy
information security policy	information security and privacy policy
information security management	information security and privacy information management
information security management system (ISMS)	privacy information management system (PIMS)
information security objectives	information security and privacy objectives
Information security performance	information security and privacy performance
Information security requirements	information security and privacy requirements
information security risk	information security and privacy risk
information security risk assessment	information security and privacy risk assessment
information security risk treatment	information security and privacy risk treatment

Basically, there are three cases for applying this document to protection of privacy of PII principals when processing PII:

1) Application of security standards as is: The referring standards apply as it is with the extension of terms as listed above. Therefore, the referring standard is not repeated, but only referred to in respective clauses.

2) Additions to security standards: The referring standards apply with additional privacy-specific requirements or implementation guidance.

3) Refinement of security standards: The referring standards are refined by privacy-specific requirements or implementation guidance.

F.2 Example of refinement of security standards

This clause describes how 5.4.1.2 is applied to ISO/IEC 27001:2013, 6.1.2.

When taking into account the protection of privacy of PII principals when processing PII, ISO/IEC 27001:2013, 6.1.2, would be amended with the underlined text below:

© ISO/IEC 2019 – All rights reserved

6.1.2 Information security risk assessment

The organization shall define and apply an information security and privacy risk assessment process that:

a) establishes and maintains information security and privacy risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security and risk assessments;

b) ensures that repeated information security and privacy risk assessments produce consistent, valid and comparable results;

c) identifies the information security and privacy risks:

   1) apply the information security and privacy risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security and privacy information management system; and

   2) identify the risk owners;

d) analyses the information security and privacy risks;

   1) assess the potential consequences that would result if the risks identified in 6.1.2 c) were to materialize;

   2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

   3) determine the levels of risk;

e) evaluates the information security and privacy risks:

   1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

   2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security and privacy risk assessment process.

© ISO/IEC 2019 – All rights reserved

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*

© ISO/IEC 2019 – All rights reserved