国际标准

ISO/IEC

27701

第一版

2019-08

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

参考编号

ISO/IEC 27701:2019

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门系统。属于 ISO 或 IEC 的国家机构通过各自组织成立的技术委员会参与国际标准的制定，以处理特定的技术活动领域。ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。与 ISO 和 IEC 联络的其他国际组织，政府和非政府组织也参加了这项工作。

ISO/IEC 指令第 1 部分中描述了用于开发本文件的流程以及打算用于进一步维护的流程。特别是，应注意不同类型文档所需的不同批准标准。本文件是根据 ISO/IEC 指令第 2 部分的编辑规则起草的（请参见 www.iso.org/directives）。

请注意，本文件的某些内容可能是专利权的主题。ISO 和 IEC 对识别任何或所有此类专利权概不负责。在文档开发流程中确定的任何专利权的详细信息将在“简介”和/或 ISO 收到的专利声明清单中（请参见网址 www.iso.org/patents）或 IEC 收到的专利声明清单（请参见 http://patents.iec.ch）。

本文件中使用的任何商标名称都是为了方便用户而提供的信息，并非构成认可。

有关标准的自愿性质的解释，与合格评定相关的 ISO 特定术语和表达的含义，以及有关 ISO 在贸易技术壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请参见 iso.org/iso/foreword.html。

该文件由联合技术委员会 ISO/IEC JTC 1，信息技术，小组委员会 SC 27，安全技术准备。

对本文件的任何反馈或问题应直接发送给用户的国家标准机构。这些机构的完整清单可以在下面找到 www.iso.org/members.html。

引言

0.1 总则

几乎每个组织都处理个人识别信息（PII）。此外，处理的 PII 的数量和种类正在增加，一个组织需要与其他组织合作处理 PII 的情况也在增加。在 PII 处理过程中保护隐私是一种社会需要，也是世界各国专门立法和/或法规的主题。

ISO/IEC 27001 中定义的信息安全管理系统（ISMS）旨在允许添加特定于部门的要求，而无需开发新的管理系统。ISO 管理体系标准，包括特定部门的标准，旨在能够单独实施或作为一个综合管理体系 实施。

PII 保护的要求和指南根据组织环境而不同，特别是在国家立法和/或法规存在的情况下。ISO/IEC 27001 要求理解并考虑到这一背景。本文档包括映射到：

—ISO/IEC 29100 中定义的隐私框架和原则；

—ISO/IEC27018；

—ISO/IEC 29151；和

—欧盟通用数据保护条例。

然而，这些可能需要解释为考虑到当地立法和/或法规。

本文件可供 PII 控制者（包括联合 PII 控制者）和 PII 处理者（包括使用分包 PII 处理者和像分包商一样给 PII 处理者处理 PII ）使用。

符合本文件要求的组织将生成其如何处理 PII 的书面证据。此类证据可用于促进与业务合作伙伴达成 协议，其中 PII 的处理是相互关联的。这也有助于与其他利益相关者的关系。如果需要，将本文件与 ISO/IEC 27001 结合使用，可提供对该证据的独立验证。

本文件最初为 ISO/IEC 27552。

0.2 与其他管理体系标准的兼容性

本文件采用 ISO 开发的框架，以提高其管理体系标准之间的一致性。

本文件使组织能够使其 PIMS 与其他管理体系标准的要求保持一致或集成。

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

1. 范围

本文件规定了建立、实施、维护和持续改进隐私信息管理体系（PIMS）的要求，并提供了指南，其形式是对组织范围内隐私管理的 ISO/IEC 27001 和 ISO/IEC 27002 的扩展。

本文件规定了与 PIMS 相关的要求，并为负责 PII 处理的 PII 控制者和 PII 处理者提供了指导。

本文件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，它们是使用 ISMS 处理 PII 的 PII 控制者和/或 PII 处理者。

2. 规范性引用文件

以下文件在正文中的引用方式应使其部分或全部内容构成本文件的要求。凡是注日期的引用文件，只有引用的版本适用。凡是不注日期的引用文件，其最新版本（包括任何修改件）适用。

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

ISO/IEC 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 - 信息安全实践指南*

ISO/IEC 29100, *信息技术 - 安全技术-隐私框架*

3. 术语和定义

在本文件中，ISO/IEC 27000、ISO/IEC 29100 和以下给出的术语和定义适用。

国际标准化组织和国际电工委员会在下列地址维护用于标准化的术语数据库：

—ISO 在线浏览平台：https://www.ISO.org/obp

—可在 http://www.electropedia.org 上获得 IEC Electropedia

3.1. 联合 PII 控制者

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

3.2. 隐私信息管理体系

信息安全管理体系，解决因处理 PII 而可能受到影响的隐私保护问题

4. 总则

4.1. 文件的结构

这是与 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013 相关的行业特定文件。

本文件着重于符合 ISO/IEC 27001:2013 要求的 PIMS。本文件扩展了 ISO/IEC 27001:2013 的要求，以考虑到 PII 主体的隐私保护，除信息安全外，PII 主体的隐私可能受到 PII 处理的影响。为了更好地理解，包含了实施指南和其他有关需求的信息。

第 5 条给出了 PIMS 的具体要求和 ISO/IEC 27001 中有关信息安全要求的其他信息，适用于作为 PII 控制者或 PII 处理者的组织。

注 1：为完整起见，第 5 条包含了包含 ISO/IEC 27001:2013 要求的每个条款的子条款，即使没有 PIMS 特定要求或其他信息。

第 6 条为作为 PII 控制者或 PII 处理者的组织提供了有关 ISO/IEC 27002 中信息安全控制的 PIMS 特定指南和其他信息，以及 PIMS 特定指南。

注 2：为完整起见，第 6 条包含 ISO/IEC 27002:2013 中包含目标或控制的每个条款的子条款，即使没有 PIMS 特定指南或其他信息。

第 7 条为 PII 控制者提供额外的 ISO/IEC 27002 指南，第 8 条为 PII 处理者提供额外的 ISO/IEC 27002 指南。

附录 A 列出了作为 PII 控制者的组织的 PIMS 特定控制目标和控制（无论其是否使用 PII 处理者，以及是否与另一个 PII 控制者联合行动）。

附录 B 列出了作为 PII 处理者的组织的 PIMS 特定控制目标和控制（无论其是否将 PII 处理分包给单独的 PII 处理者，包括作为 PII 处理者分包商的 PII 处理）。

附录 C 包含 ISO/IEC 29100 的对应关系。

附录 D 列出了本文件中的控制措施与欧盟通用数据保护条例的对应关系。

附录 E 包含 ISO/IEC 27018 和 ISO/IEC 29151 的对应关系。

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。

4.2. ISO/IEC 27001:2013 要求的应用

表 1 给出了本文件中与 ISO/IEC 27001 相关的 PIMS 具体要求的位置

表 1—PIMS 的位置—实施 ISO/IEC 27001:2013 中控制的具体要求和其他信息

ISO/IEC 27001:2013	标题	本文件中的子	评论
4	组织环境	5.2	附加要求
5	领导	5.3	无 PIMS 特定要求
6	规划	5.4	附加要求
7	支持	5.5	无 PIMS 特定要求
8	运行	5.6	无 PIMS 特定要求
9	绩效评价	5.7	无 PIMS 特定要求
10	改进	5.8	无 PIMS 特定要求

注：即使没有 PIMS 的具体要求，根据 5.1 对“信息安全”的扩展解释始终适用。

4.3. ISO/IEC 27002:2013 指南的应用

表 2 给出了本文件中与 ISO/IEC 27002 相关的 PIMS 具体要求的位置

表 2—PIMS 的位置—实施 ISO/IEC 27002:2013 中控制的具体要求和其他信息

ISO/IEC 27001:2013 中的条款	标题	本文件中的子条款	评论
5	信息安全策略	6.2	附加要求
6	信息安全组织	6.3	附加要求
7	人力资源安全	6.4	附加要求
8	资产管理	6.5	附加要求
9	访问控制	6.6	附加要求
10	密码	6.7	附加要求
11	物理和环境安全	6.8	附加要求
12	运行安全	6.9	附加要求
13	通信安全	6.10	附加要求
14	系统获取、开发和维护	6.11	附加要求
15	供应商关系	6.12	附加要求
16	信息安全事件管理	6.13	附加要求
17	业务连续性管理的信息安全方面	6.14	无 PIMS 特定要求
18	符合性	6.15	附加要求

注：即使没有 PIMS 的具体要求，根据 6.1 对“信息安全”的扩展解释始终适用。

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（如 PII 控制者的客户）签订合同的组织；

注 1：这可能是一个联合控制的组织的情况。

注 2：在本文件中，与组织的企业对客户关系中的个人被称为“PII 主体”。

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

c) 与分包商签订 PII 处理合同的 PII 处理者（如分包 PII 分包商的客户）。

注 3：在第 6 条中提及“客户”的情况下，相关规定可适用于上下文 a）、b）或 c）。

注 4：如果第 7 条和附录 A 中提到“客户”，则相关规定适用于背景 a）。

注 5：如果第 8 条和附录 B 中提到“客户”，则关系条款可适用于背景 b）和/或 c）。

5. 与 ISO/IEC 27001 相关的 PIMS 具体要求

5.1. 总则

提及“信息安全”的 ISO/IEC 27001:2013 的要求应扩展到保护可能受 PII 处理影响的隐私。

注：在实践中，如果 ISO/IEC 27001:2013 中使用了“信息安全”，则“信息安全与隐私”适用（见附录 F）。

5.2. 组织背景

5.2.1. 理解组织和组织背景

ISO/IEC 27001:2013，4.1 的附加要求是：

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

组织应确定与信息技术环境相关的外部和内部因素，这些因素影响其实现信息管理系统预期结果的能力。例如，这些可以包括：

—适用的隐私立法；

—适用法规；

—适用的司法裁决；

—适用的组织背景、管理、策略和程序；

—适用的行政决定；

—适用的合同要求。

当组织同时扮演两个角色（如 PII 控制者和 PII 处理者）时，应确定单独的角色，每个角色都是一组单独的控制对象。

注：组织的角色对于 PII 处理的每个实例都可能不同，因为它取决于由谁决定处理的目的和方法。

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：

组织应在其相关方（见 ISO/IEC 27001:2013，4.2）中包括与 PII 处理相关的利益方或责任方，包括 PII 主体。

注 1：其他相关方包括客户（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 处理相关的要求可由法律法规要求、合同义务和自我强加的组织目标确定。ISO/IEC 29100 中规定的隐私原则为 PII 的处理提供了指导。

注 3：作为证明符合组织义务的一个要素，一些相关方可以期望组织符合特定标准，如本文件规定的管理体系和/或任何相关规范。这些缔约方可以要求独立审计遵守这些标准。

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：由于根据 5.1 对“信息安全”的扩展解释，确定信息管理系统的范围可能需要修改信息安全管理系统的范围。

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 ISO/IEC 27001:2013 第 4 条至第 10 条的要求（根据第 5 条的要求扩展）建立、实施、维护和持续改进 PIMS。

5.3. 领导

5.3.1. 领导和承诺

ISO/IEC 27001:2013，5.1 中规定的要求和 5.1 中规定的解释适用。

5.3.2. 方针

ISO/IEC 27001:2013，5.2 中规定的要求和 5.2 中规定的解释适用。

5.3.3. 组织的角色、责任和权限

ISO/IEC 27001:2013，5.3 中规定的要求和 5.3 中规定的解释适用。

5.4. 规划

5.4.1. 应对风险和机遇的措施

5.4.1.1. 总则

ISO/IEC 27001:2013，6.1.1 中规定的要求和 5.1 中规定的解释适用。

5.4.1.2. 信息安全风险评估

ISO/IEC 27001:2013，6.1.2 中规定的要求适用于以下改进。ISO/IEC 27001:2013，6.1.2 c）1）修订如下：

组织应采用隐私风险评估程序，在 PIMS 范围内识别与 PII 处理相关的风险。

组织应确保在整个风险评估过程中，适当管理信息安全和 PII 保护之间的关系。

注：组织可以采用综合信息安全与隐私风险评估流程，也可以采用两个独立的流程来评估信息安全和与 PII 处理相关的风险。

ISO/IEC 27001:2013，6.1.2 d）1）修订如下：

如果上述 ISO/IEC 27001:2013，6.1.2 c）中确定的风险得以实现，组织应评估对组织和 PII 主体造成的潜在后果。

5.4.1.3. 信息安全风险处置

ISO/IEC 27001:2013，6.1.3 中规定的要求适用于以下改进。

ISO/IEC 27001:2013，6.1.3 c)修订如下：

应将 ISO/IEC 27001:2013 6.1.3 b）中确定的控制与附录 A 和/或附录 b 和 ISO/IEC 27001:2013 附录 A 中的控制进行比较，以验证没有遗漏任何必要的控制。

在评估 ISO/IEC 27001:2013 附录 A 中的控制目标和控制措施在风险处理中的适用性时，控制目标和控制措施应同时考虑信息安全风险和与 PII 处理相关的风险，包括 PII 主体的风险。

ISO/IEC 27001:2013，6.1.3 d)修订如下：

制定适用性声明，其中包括：

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

—选择的合理性说明；

—是否实施了必要的控制措施；和

—根据组织对其角色的确定（见 5.2.1），对附录 A 和/或附录 B 和 ISO/IEC 27001:2013，附

录 A 中任何控制删减的合理性说明。

并非所有附录中列出的控制目标和控制都需要包含在 PIMS 实施中。删减的理由可以包括风险评估认为不需要控制的情况，以及法律和/或法规（包括适用于 PII 委托人的法规）不要求（或受例外情况的 影响）的情况。

5.4.2. 信息安全目标及其实现规划

ISO/IEC 27001:2013，6.2 中规定的要求和 5.1 中规定的解释适用。

5.5. 支持

5.5.1. 资源

ISO/IEC 27001:2013，7.1 中规定的要求和 5.1 中规定的解释适用。

5.5.2. 能力

ISO/IEC 27001:2013，7.2 中规定的要求和 5.1 中规定的解释适用。

5.5.3. 意识

ISO/IEC 27001:2013，7.3 中规定的要求和 5.1 中规定的解释适用。

5.5.4. 沟通

ISO/IEC 27001:2013，7.4 中规定的要求和 5.1 中规定的解释适用。

5.5.5. 成文信息

5.5.5.1. 总则

ISO/IEC 27001:2013，7.5.1 中规定的要求和 5.1 中规定的解释适用。

5.5.5.2. 创建和更新

ISO/IEC 27001:2013，7.5.2 中规定的要求和 5.1 中规定的解释适用。

5.5.5.3. 文件化信息的控制

ISO/IEC 27001:2013，7.5.3 中规定的要求和 5.1 中规定的解释适用。

5.6. 运行

5.6.1. 运行规划和控制

ISO/IEC 27001:2013，8.1 中规定的要求和 5.1 中规定的解释适用。

5.6.2. 信息安全风险评估

ISO/IEC 27001:2013，8.2 中规定的要求和 5.1 中规定的解释适用。

5.6.3. 信息安全风险处置

ISO/IEC 27001:2013，8.3 中规定的要求和 5.1 中规定的解释适用。

5.7. 绩效评价

5.7.1. 监视、测量、分析和评价

ISO/IEC 27001:2013，9.1 中规定的要求和 5.1 中规定的解释适用。

5.7.2. 内部审核

ISO/IEC 27001:2013，9.2 中规定的要求和 5.1 中规定的解释适用。

5.7.3. 管理评审

ISO/IEC 27001:2013，9.3 中规定的要求和 5.1 中规定的解释适用。

5.8. 改进

5.8.1. 不符合及纠正措施

ISO/IEC 27001:2013，10.1 中规定的要求和 5.1 中规定的解释适用。

5.8.2. 持续改进

ISO/IEC 27001:2013，10.2 中规定的要求和 5.1 中规定的解释适用。

6. ISO/IEC 27002 相关的 PIMS 特定指南

6.1. 总则

ISO/IEC 27002:2013 中提到“信息安全”的要求应扩展到保护隐私，因为隐私可能受到 PII 处理的影响。

注 1：在实践中，如果 ISO/IEC 27002:2013 中使用了“信息安全”，则“信息安全与隐私”适用（见附录 F）。

所有控制目标和控制措施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：除非第 6 条中的具体规定另有说明，或由组织根据适用的司法管辖区确定，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

ISO/IEC 27002:2013，5.1.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 5.1.1 信息安全策略的附加实施指南为：

通过制定单独的隐私策略，或者通过增加信息安全策略，组织应制定一份声明，说明对遵守适用的 PII 保护法律和/或法规以及组织与其合作伙伴、分包商和适用的第三方（客户、供应商等）之间商定 的合同条款的支持和承诺在他们之间分配责任。

ISO/IEC 27002:2013 第 5.1.1 条信息安全策略的附加其他信息：

任何处理 PII 的组织，无论是 PII 控制者还是 PII 处理者，在制定和维护信息安全策略期间，都应考虑适用的 PII 保护立法和/或法规。

6.2.1.2. 信息安全策略的评审

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

6.3. 信息安全组织

6.3.1. 内部组织

6.3.1.1. 信息安全角色和责任

ISO/IEC 27002:2013，6.1.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 6.1.1 信息安全角色和责任的附加实施指南为：

组织应指定一个联络点，供客户处理 PII 时使用。当组织是 PII 控制者时，为 PII 主体指定一个处理其 PII 的联络点（见 7.3.2）。

组织应指定一名或多名人员负责制定、实施、维护和监督组织范围的管理和隐私计划，以确保遵守与处理 PII 相关的所有适用法律法规。

负责人应酌情：

—独立并直接向组织的适当管理层报告，以确保对隐私风险的有效管理；

—参与管理与 PII 处理相关的所有问题；

—精通数据保护立法、法规和实践；

—作为监管机构的联络点；

—向组织的最高管理层和员工告知他们在处理 PII 方面的义务；

—就组织进行的隐私影响评估提供建议。

注：在某些司法管辖区，此类人员被称为数据保护官员，该官员定义何时需要此类职位，以及他

们的职位和角色。这个职位可以由工作人员来完成，也可以外包。

6.3.1.2. 信息安全角色和责任

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

6.3.1.3. 与职能机构的联系

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

6.3.1.4. 与特定相关方的联系

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

6.3.1.5. 项目管理中信息安全

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

6.3.2. 移动设备和远程工作

6.3.2.1. 移动设备策略

ISO/IEC 27002:2013，6.2.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 6.2.1 移动设备策略的附加实施指南为：

组织应确保移动设备的使用不会导致 PII 受损。

6.3.2.2. 远程工作

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

6.4. 人力资源安全

6.4.1. 任用前

6.4.1.1. 审查

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

6.4.1.2. 任用条款及条件

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

6.4.2. 任用中

6.4.2.1. 管理责任

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

6.4.2.2. 信息安全意识、教育和培训

ISO/IEC 27002:2013，7.2.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 7.2.2 信息安全意识和教育和培训的附加实施指南为：

应采取措施，包括提高事故报告意识，以确保相关工作人员意识到可能对组织造成的后果（如法律后果、业务和品牌损失或声誉损害）、对工作人员（如纪律后果）和 PII 主体（如物质、材料和情感后 果）违反隐私或安全规则和程序，特别是那些处理个人隐私的规则和程序。

注：此类措施可包括对有权使用 PII 的人员进行适当的定期培训。

6.4.2.3. 违规处理过程

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

6.4.3. 任用的终止和变更

6.4.3.1. 任用的终止和变更和责任

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

6.5. 资产管理

6.5.1. 有关资产的责任

6.5.1.1. 资产清单

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

6.5.1.2. 资产的所属关系

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

6.5.1.3. 资产可接受使用

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

6.5.1.4. 资产归还

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

6.5.2. 信息的分级

6.5.2.1. 信息的分级

ISO/IEC 27002:2013，8.2.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 8.2.1 信息的分级的附加实施指南为：

组织的信息分类系统应该明确地将 PII 作为其实现方案的一部分。在整个分类系统中考虑 PII 对于理解组织过程（如类型、特殊类别）、存储 PII 的位置以及 PII 可以通过的系统是不可或缺的。

6.5.2.2. 信息的标记

ISO/IEC 27002:2013，8.2.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 8.2.2 信息的标记的附加实施指南为：

组织应确保其控制下的人员了解 PII 的定义，即如何识别 PII 信息。

6.5.2.3. 资产的处理

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

6.5.3. 介质处理

6.5.3.1. 移动介质的管理

ISO/IEC 27002:2013，8.3.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 8.3.1 移动介质的管理的附加实施指南为：

组织应记录任何使用可移动介质和/或设备存储 PII 的情况。在可行的情况下，组织应使用在存储 PII 时允许进行加密的可移动的物理介质和/或设备。只有在不可避免的情况下才应使用未加密的介质，并 且在使用未加密的介质和/或设备的情况下，组织应实施程序和补偿控制（如防篡改包装），以降低 PII 的风险。

ISO/IEC 27002:2013 第 8.3.1 节“可移动介质管理”的附加其他信息如下：

在组织的物理范围之外使用的可移动介质容易丢失、损坏和不适当的访问。加密可移动介质为 PII 增加了一个保护级别，如果可移动介质受到损害，可降低安全和隐私风险。

6.5.3.2. 介质的处理

ISO/IEC 27002:2013，8.3.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 8.3.2 介质的处理的附加实施指南为：

在处置存储 PII 的可移动介质时，应在记录的信息中包括安全处置程序，并实施以确保先前存储的 PII 不可访问。

6.5.3.3. 物理介质的转移

ISO/IEC 27002:2013，8.3.3 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 8.3.3 物理介质的转移的附加实施指南为：

如果使用物理介质传输信息，则应建立一个系统来记录包含 PII 的传入和传出物理介质，包括物理介质的类型、授权发件人/收件人、日期和时间以及物理介质的数量。在可能的情况下，应采取加密等其他措施，以确保数据只能在目的地访问，而不能在传输中访问。

组织在离开其场所前，应将含有 PII 的物理介质置于授权程序之下，并确保除授权人员外，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 通常不可访问的一种可能措施是对相关 PII 进行加密，并将解密能力限制在经授权的人员。

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

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

6.6.1.2. 网络和网络服务的访问

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

6.6.2. 用户访问管理

6.6.2.1. 用户注册和注销

ISO/IEC 27002:2013，9.2.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 9.2.1 用户注册和注销的附加实施指南为：

管理或操作处理 PII 的系统和服务的用户的注册和注销程序应解决这些用户的用户访问控制受到损害的情况，例如密码或其他用户注册数据的损坏或损害（例如，由于无意泄露）。

对于处理 PII 的系统和服务，组织不应向用户重新颁发任何已停用或过期的用户 ID。

在组织将 PII 处理作为一项服务提供的情况下，客户可以负责用户 ID 管理的某些或所有方面。此类情况应包含在文件信息中。

一些管辖区对与处理 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。在这些管辖区内运作的组织应考虑到这些要求的遵守情况。

6.6.2.2. 用户访问供给

ISO/IEC 27002:2013，9.2.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 9.2.2 用户访问供给的附加实施指南为：

本组织应保持一份准确、最新的记录，记录为经授权访问信息系统和其中所含 PII 的用户创建的用户配置文件。此配置文件包含有关该用户的一组数据，包括用户 ID，这些数据是实现提供授权访问的已标识技术控制所必需的。

实现个人用户访问 IDs 的适宜配置系统，以识别谁访问 PII 和他们进行的添加、删除或改变。作为对该组织的保护。使用者也受到保护，因为他们能够确定他们所处理的事项以及他们没有处理的事项。

在组织将 PII 处理作为一项服务提供的情况下，客户可以负责访问管理的某些或所有方面。在适当的情况下，组织应向客户提供执行访问管理的方法，例如通过提供管理或终止访问的管理权限，此类情况应包含在记录的信息中。

6.6.2.3. 特许访问权管理

ISO/IEC 27002:2013，9.2.3 中规定的控制、实施指南和其他信息适用。

6.6.2.4. 用户的秘密鉴别信息管理

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

6.6.2.5. 用户访问权的评审

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

6.6.2.6. 访问权的移除或调整

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

6.6.3. 用户责任

6.6.3.1. 秘密鉴别信息的使用

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

6.6.4. 系统和应用访问控制

6.6.4.1. 信息访问限制

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

6.6.4.2. 安全登陆规程

ISO/IEC 27002:2013，9.4.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 9.4.2 安全登陆规程的附加实施指南为：

在客户要求的情况下，组织应为客户控制下的任何用户帐户提供安全登录程序的能力。

6.6.4.3. 口令管理系统

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

6.6.4.4. 特权实用程序的使用

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

6.6.4.5. 程序源代码的访问控制

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

6.7. 密码

6.7.1. 密码控制

6.7.1.1. 密码控制的使用策略

ISO/IEC 27002:2013，10.1.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 10.1.1 密码控制的使用策略的附加实施指南为：

一些司法管辖区可能要求使用加密技术来保护特定种类的个人识别信息，如健康数据、居民注册号码、护照号码和驾驶执照号码。

组织应向客户提供有关在何种情况下使用加密技术保护 PII 进程的信息。组织还应该向客户提供有关其提供的任何功能的信息，这些功能可以帮助客户应用他们自己的加密保护。

6.7.1.2. 密钥管理

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

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

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

6.8.1.2. 物理入口控制

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

6.8.1.3. 办公室、房间和设施的安全保护

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

6.8.1.4. 外部和环境威胁的安全防护

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

6.8.1.5. 在安全区域工作

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

6.8.1.6. 交接区

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

6.8.2. 设备

6.8.2.1. 设备安置和保护

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

6.8.2.2. 支持性设施

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

6.8.2.3. 布缆安全

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

6.8.2.4. 设备维护

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

6.8.2.5. 资产的移动

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

6.8.2.6. 组织场所外的设备与资产安全

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

6.8.2.7. 设备的安全处置或再利用

ISO/IEC 27002:2013，11.2.7 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 11.2.7 设备的安全处置或再利用的附加实施指南为：

组织应确保，每当重新分配存储空间时，以前驻留在该存储空间上的任何 PII 都不可访问。

在删除信息系统中保存的 PII 时，性能问题可能意味着显式删除该 PII 是不切实际的。这就产生了另一个用户可以访问 PII 的风险。这种风险应通过具体的技术措施加以避免。

为了安全处置或重复使用，包含可能包含 PII 的存储介质的设备应视为包含 PII。

6.8.2.8. 无人值守的用户设备

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

6.8.2.9. 清理桌面和屏幕策略

ISO/IEC 27002:2013，11.2.9 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 11.2.9 清理桌面和屏幕策略的附加实施指南为：

组织应将硬拷贝材料（包括 PII）的创建限制在满足确定的处理目的所需的最低限度。

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

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

6.9.1.2. 变更管理

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

6.9.1.3. 容量管理

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

6.9.1.4. 开发，测试运行环境的分离

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

6.9.2. 恶意软件防范

6.9.2.1. 恶意软件的控制

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

6.9.3. 备份

6.9.3.1. 信息备份

ISO/IEC 27002:2013，12.3.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 12.3.1 信息备份的附加实施指南为:

组织应制定一项策略，以满足对 PII 的备份、恢复和修复的要求（可作为总体信息备份策略的一部分），以及擦除为满足备份要求而保留在信息中的 PII 的任何进一步要求（如合同和/或法律要求）。

PII 在这方面的具体责任取决于客户。组织应确保已将有关备份的服务限制告知客户。

当组织明确向客户提供备份和修复服务时，组织应向客户提供有关其在 PII 备份和修复方面的能力的明确信息。

有些管辖区域对 PII 的备份频率、备份的审查和测试频率或 PII 的恢复程序提出了具体要求。在这些管辖区内运营的组织应证明符合这些要求。

有时可能由于系统故障、攻击或灾难而需要恢复 PII。当 PII 被恢复时（通常是从备份介质中

恢复），需要有过程来确保 PII 被恢复到一个可以保证完整性或 PII 的状态，和/或 PII 不准确和/或不完整性被 识别的状态，并有过程来解决这些问题（可能涉及 PII 主体）。 组织应该有一个程序和一个记录，PII 修复工作。PII 修复工作的日志至少应包含：

—修复负责人姓名；

—对修复的 PII 的描述。

一些管辖区规定了 PII 修复工作日志的内容。组织应该能够记录对修复日志内容的任何适用的司法管辖区特定要求的遵守情况。这些审议的结论应列入文件资料。

本文件中适用于分包 PII 处理的控制措施（见 6.5.3.3、6.12.1.2）涵盖了使用分包商存储已处理 PII 的复制或备份副本。如果发生与备份和恢复相关的物理介质传输，本文档（6.10.2.1）中的控制也将对此 进行说明。

6.9.4. 日志和监视

6.9.4.1. 事态日志

ISO/IEC 27002:2013，12.4.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 12.4.1 事态日志的附加实施指南为：

应建立一个流程，使用连续、自动化的监测和警报流程审查事件日志，或者在应以规定的、有文件记录的周期进行此类审查的情况下手动审查事件日志，以识别违规行为并提出补救措施。

在可能的情况下，事件日志应记录对 PII 的访问，包括谁、何时、访问哪个 PII 主体的 PII，以及由于事件而进行的更改（添加、修改或删除）（如果有）。

当多个服务提供者参与提供服务时，可以在实施本指南时扮演不同或共享的角色。这些角色应该明确定义并包含在文档信息中，并且应该处理提供者之间关于任何日志访问的协议。

PII 处理者实施指南：

组织应定义有关是否、何时以及如何向客户提供或由客户使用日志信息的标准。这些标准应提供给客户。

当组织允许其客户访问由组织控制的日志记录时，组织应实施适当的控制，以确保客户只能访问与该客户活动相关的记录，不能访问与其他客户活动相关的任何日志记录，并且不能修改任何方式的日志。

6.9.4.2. 日志信息的保护

ISO/IEC 27002:2013，12.4.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 12.4.2 日志信息的保护的附加实施指南为：

记录的日志信息（例如，安全监视和操作诊断）可以包含 PII。应采取控制访问等措施（见 ISO/IEC 27002:2013，9.2.3），以确保记录的信息仅按预期使用。

应建立一个程序，最好是自动的，以确保记录的信息按照保留计划中的规定被删除或取消标识（见 7.4.7）。

6.9.4.3. 管理员和操作员日志

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

6.9.4.4. 时钟同步

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

6.9.5. 运行软件控制

6.9.5.1. 运行系统的软件安装

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

6.9.6. 技术方面的脆弱性管理

6.9.6.1. 技术方面脆弱性的管理

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

6.9.6.2. 软件安装限制

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

6.9.7. 信息系统审计的考虑

6.9.7.1. 信息系统审计的控制

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

6.10. 通信安全

6.10.1. 网络安全管理

6.10.1.1. 网络控制

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

6.10.1.2. 网络服务的安全

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

6.10.1.3. 网络中的隔离

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

6.10.2. 信息传输

6.10.2.1. 信息传输策略和规程

ISO/IEC 27002:2013，13.2.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 13.2.1 信息传输策略和规程的附加实施指南为：

组织应考虑规程，以确保与 PII 处理相关的规则在系统内外（如适用）得到执行。

6.10.2.2. 信息传输协议

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

6.10.2.3. 电子消息发送

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

6.10.2.4. 保密或不泄露协议

ISO/IEC 27002:2013，13.2.4 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 13.2.4 保密或不泄露协议的附加实施指南为：

本组织应确保在其控制下、可接触 PII 的个人负有保密义务。保密协议，无论是合同的一部分还是单独的，都应规定应遵守义务的期限。

当组织是 PII 处理者时，组织、其员工和代理之间以任何形式签订的保密协议应确保员工和代理遵守有关数据处理和保护的策略和程序。

6.11. 系统获取、开发和维护

6.11.1. 信息系统的安全要求

6.11.1.1. 信息安全要求分析和说明

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

6.11.1.2. 公共网络上应用服务的安全保护

ISO/IEC 27002:2013，14.1.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 14.1.2 公共网络上应用服务的安全保护的附加实施指南为：

组织应确保通过不受信任的数据传输网络传输的 PII 被加密以进行传输。

不受信任的网络可以包括公共互联网和组织运行控制之外的其他设施。

注：在某些情况下（例如，电子邮件的交换），不受信任的数据传输网络系统的固有特性可能要求公开某些报头或流量数据以进行有效传输。

6.11.1.3. 应用服务事物的保护

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

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

ISO/IEC 27002:2013，14.2.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 14.2.1 安全的开发策略的附加实施指南为：

系统开发和设计策略应包括根据对 PII 主体的义务和/或任何适用的法律和/或法规以及组织执行的处理类型，为组织处理 PII 需求提供指导。第 7 条和第 8 条为 PII 的处理提供了控制考虑，这有助于制 定系统设计中的隐私策略。

设计隐私和默认隐私的策略应考虑以下方面：

a) 软件开发生命周期中 PII 保护和隐私原则实施指南（见 ISO/IEC 29100）；

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

c) 项目里程碑内的 PII 保护检查点；

d) 所需的隐私和 PII 保护知识；

e) 默认情况下最小化 PII 处理。

6.11.2.2. 系统变更控制规程

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

6.11.2.3. 运行平台变更后对应用的技术评审

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

6.11.2.4. 软件包变更的限制

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

6.11.2.5. 系统安全工程原则

ISO/IEC 27002:2013，14.2.5 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 14.2.5 系统安全工程原则的附加实施指南为：

与 PII 处理相关的系统和/或组件的设计应遵循按设计隐私和默认隐私的原则，并预期和促进相关控制的实施（如第 7 条和第 8 条所述，分别针对 PII 控制者和 PII 处理者），特别是而在这些系统中，PII 的处理仅限于为确定 PII 的处理目的所必需的内容（见 7.2）。

例如，处理 PII 的组织应确保，基于相关管辖权，在指定的时间段后处理 PII。处理 PII 的系统，其设计方式应便于此删除要求。

6.11.2.6. 安全的开发环境

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

6.11.2.7. 外包开发

ISO/IEC 27002:2013，14.2.7 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 14.2.7 外包开发的附加实施指南为：

设计隐私和默认隐私的相同原则（见 6.11.2.5）应适用于外包信息系统（如适用）。

6.11.2.8. 系统安全测试

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

6.11.2.9. 系统验收测试

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

6.11.3. 测试数据

6.11.3.1. 测试数据的保护

ISO/IEC 27002:2013，14.3.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 14.3.1 测试数据的保护的附加实施指南为：

PII 不应用于测试目的；应使用假 PII 或合成 PII。在无法避免使用 PII 进行测试的情况下，应实施与生产环境中使用的 PII 相同的技术和组织措施，以将风险降至最低。如果此类同等措施不可行，则应进行风险评估，并用于通知选择适当的缓解控制措施。

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

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

6.12.1.2. 在供应商协议中强调安全

ISO/IEC 27002:2013，15.1.2 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 15.1.2 在供应商协议中强调安全的附加实施指南为：

组织应在与供应商的协议中详细说明是否处理了 PII，以及供应商需要满足的最低技术和组织措施，以便组织履行其信息安全和 PII 保护义务（见 7.2.6 和 8.2.1）。

供应商协议应在组织、其合作伙伴、其供应商及其适用的第三方（客户、供应商等）之间明确分配责任，同时考虑到处理的 PII 类型。

组织与其供应商之间的协议应提供一种机制，以确保组织支持和管理对所有适用法律和/或法规的遵守。协议应要求客户接受独立审计的合规性。

注：出于审计目的，可考虑遵守相关和适用的安全和隐私标准，如 ISO/IEC 27001 或本文件。

PII 处理者实施指南：

组织应在与任何供应商的合同中规定，PII 仅按照其指示进行处理。

6.12.1.3. 信息与通信技术供应链

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

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评审

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

6.12.2.2. 供应商服务的变更管理

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

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

ISO/IEC 27002:2013，16.1.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 16.1.1 责任和规程的附加实施指南为：

作为整个信息安全事件管理过程的一部分，组织应建立识别和记录违反 PII 的责任和程序。此外，组织应建立与向被要求方通报 PII 违规行为（包括此类通知的时间）和向当局披露有关的责任

和程序，同时考虑到适用的法律和/或法规。

有些行政管辖区域对违约反应（包括通知）规定了具体条例。在这些管辖区内运营的组织应确保能够证明其遵守了这些法规。

6.13.1.2. 报告信息安全事态

ISO/IEC 27002:2013，16.1.2 中规定的控制、实施指南和其他信息适用。

6.13.1.3. 报告信息安全弱点

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

6.13.1.4. 信息安全事态的评估和决策

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

6.13.1.5. 信息安全事件的响应

ISO/IEC 27002:2013，16.1.5 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 16.1.5 信息安全事件的响应的附加实施指南为：

PII 控制者实施指南：

涉及 PII 的事件应触发组织的审查，作为其信息安全事件管理流程的一部分，以确定是否发生了涉及 PII 的需要响应的违规行为。 事态不一定会引发这样的审查。

注 1：信息安全事态不一定导致未经授权访问 PII 或任何存储 PII 的组织设备或设施的实际或重大可能性。这些攻击包括但不限于对防火墙或边缘服务器的 ping 和其他广播攻击、端口扫描、登录尝试 失败、拒绝服务攻击和数据包嗅探。

当发生违反 PII 时，响应程序应包括相关通知和记录。

有些行政管辖域规定了何时应将违约行为通知监管机构，何时应将违约行为通知 PII 主体的情况。

通知应该清楚，并且可以是必需的。

注 2：通知可包含以下详细信息：

—可以获得更多信息的联络点；

—违约的描述和可能的后果；

—对违规行为的描述，包括相关人员的数量以及相关记录的数量；

—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，则应保存一份记录，记录中应包含足够的信息，以便为监管和/或法医目的提供报告，例如：

—事件描述；

—时间段；

—事件的后果；

—报告人姓名；

—事件报告人；

—为解决事件而采取的措施（包括负责人和恢复的数据）；

—事件导致 PII 不可用、丢失、披露或变更的事实。

如果发生了涉及 PII 的违规行为，记录还应包括对 PII 受损的描述（如果已知）；如果执行了通知，则应包括为通知 PII 主体、监管机构或客户而采取的步骤。

PII 处理者实施指南：

涉及 PII 违约通知的条款应构成组织与客户之间合同的一部分。合同应规定组织将如何提供必要的信息，以便客户履行其通知有关当局的义务。此通知义务不适用于客户或 PII 主体或其负责的系统组件 内造成的违约。合同还应规定通知响应时间的预期限制和外部强制限制。

在某些司法管辖区中，PII 处理者应当通知 PII 控制者，在不存在不适当的延迟（即尽快）的情况下，最好是一旦发现 PII 控制者就可以采取适当的行动。

如果发生涉及 PII 的违规行为，则应保存一份记录，记录中应包含足够的信息，以便为监管和/或法庭目的提供报告，例如：

—事件描述；

—时间段；

—事件的后果；

—报告人姓名；

—事件报告人；

—为解决事件而采取的措施（包括负责人和恢复的数据）；

—事件导致 PII 不可用、丢失、披露或变更的事实。

如果发生了涉及 PII 的违规行为，记录还应包括 PII 泄露的描述（如果知道）；如果执行了通知，则应包括为通知客户和/或监管机构而采取的步骤。

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

6.13.1.6. 从信息安全事件中学习

ISO/IEC 27002:2013，16.1.6 中规定的控制、实施指南和其他信息适用。

6.13.1.7. 证据的收集

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

6.14. 业务连续性管理的信息安全方面

6.14.1. 信息安全的连续性

6.14.1.1. 规划信息安全连续性

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

6.14.1.2. 实现信息安全连续性

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

6.14.1.3. 验证、评审和评价信息安全连续性

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

6.14.2. 冗余

6.14.2.1. 信息处理设施的可用性

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

6.15. 符合性

6.15.1. 符合法律和合同要求

6.15.1.1. 适用的法律和合同要求的识别

ISO/IEC 27002:2013，18.1.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 18.1.1 是适用的法律和合同要求的识别的附加实施指南为：

组织应确定与 PII 处理相关的任何潜在法律制裁（可能是由于遗漏了一些义务），包括直接从当地监管机构处的巨额罚款。在某些司法管辖区，本文件等国际标准可用于构成组织与客户之间合同的基础，概述各自的安全、隐私和 PII 保护责任。合同条款可为违反这些责任时的合同制裁提供依据。

6.15.1.2. 知识产权

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

6.15.1.3. 记录的保护

ISO/IEC 27002:2013，18.1.3 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 18.1.3 是记录的保护的附加实施指南为：

可能需要审查当前和历史的策略和程序（例如，在客户争议解决和监管机构调查的情况下）。

组织应在其保留计划（见 7.4.7）规定的期限内保留其隐私策略和相关程序的副本。这包括在更新这些文档时保留以前的版本。

6.15.1.4. 隐私和个人可识别信息保护

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

6.15.1.5. 密码控制规则

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

6.15.2. 信息安全评审

6.15.2.1. 信息安全的独立评审

ISO/IEC 27002:2013，18.2.1 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 18.2.1 信息安全的独立评审的附加实施指南为：

如果一个组织作为 PII 处理者，且个别客户审核不切实际或可能增加安全风险，则该组织应在签订合同之前和合同期间向客户提供，独立的证据，证明信息安全是按照组织的策略和程序实施和操作的。组织选择的相关独立审计，如果涵盖预期用户的需求，并且结果以足够透明的方式提供，通常应是满足客户审查组织处理操作的兴趣的可接受方法。

6.15.2.2. 符合安全策略和标准

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

6.15.2.3. 技术符合性评审

ISO/IEC 27002:2013，18.2.3 和以下附加指南中规定的控制、实施指南和其他信息适用。

ISO/IEC 27002:2013 中 18.2.3 技术符合性评审的附加实施指南为：

作为安全策略和标准合规性技术审查的一部分，组织应包括审查与处理 PII 相关的工具和组件的方法。

这可以包括：

—持续监控，以验证仅允许进行处理；和/或

—特定的渗透或脆弱性测试（例如，去识别的数据集可以接受主动入侵者测试，以验证去识别方法是否符合组织要求。

7. 附加 ISO/IEC 27002 PII 控制者指南

7.1. 总则

第 6 条中的指南和本条中的附加内容为 PII 控制者创建了 PIMS 特定指南。本条中记录的实施指南与附件 A 中列出的控制措施有关。

7.2. 收集和处理条件

目标：确定并证明处理是合法的，根据适用的司法管辖区有法律依据，目的明确合法。

7.2.1. 确定并记录目的

控制

组织应确定并记录处理 PII 的具体目的。

实施指南

组织应确保 PII 主体了解处理其 PII 的目的。组织有责任清楚地记录并传达给 PII 主体。如果不明确说明处理的目的，就不能给予充分的同意和选择。

处理 PII 目的的文件应足够清晰和详细，以便在提供给 PII 主体的所需信息中使用（见 7.3.2）。这包括获得同意所需的信息（见 7.2.3），以及策略和程序的记录（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描述 PII 处理目的的术语。

7.2.2. 确定法律依据

控制

组织应确定、记录并遵守为确定目的处理 PII 的相关法律依据。

实施指南

有些行政管辖域要求本组织能够证明在处理之前已适当确立了处理的合法性。

处理 PII 的法律依据包括：

—PII 主体同意；

—合同的履行；

—遵守法律义务；

—保护 PII 主体的切身利益；

—执行为公众利益而进行的任务；

—PII 控制者的合法权益。

组织应记录每个 PII 处理活动的依据（见 7.2.8）。

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

无论何时根据 PII 的性质（如健康信息）或相关 PII 主体（如与儿童有关的 PII）定义了 PII 的特 殊类别，组织都应将这些类别的 PII 包括在其分类方案中。

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

使用特殊类别的 PII 也可以受到更严格的控制。

更改或扩展 PII 处理目的可能需要更新和/或修订法律依据。还可能需要获得 PII 主体的额外同意。

7.2.3. 确定何时以及如何获得同意

控制

组织应确定并记录一个过程，以证明是否、何时以及如何从 PII 负责人处获得处理 PII 的同意。

实施指南

除非有其他合法理由，否则处理 PII 可能需要征得同意。组织应明确记录何时需要获得同意以及获得同意的要求。将处理的目的与是否以及如何获得同意的信息相关联是有用的。

有些行政管辖区对如何收集和记录同意有具体要求（例如，不与其他协议捆绑在一起）。此外，某些类型的数据收集（例如科学研究）和某些类型的 PII 主体（例如儿童）可能会受到额外的要求。本 组织应考虑到这些要求，并记录同意机制如何满足这些要求。

7.2.4. 获得并记录同意

控制

组织应根据文件化的流程获得并记录 PII 主体的同意。

实施指南

组织应获得并记录 PII 主体的同意，以便在要求时提供所提供同意的详细信息（例如，提供同意的时 间、PII 主体的身份和同意声明）。

在同意程序之前提交给 PII 主体的信息应遵循 7.3.3 中的指导。

同意应为：

—自由给予；

—关于处理目的的具体规定；以及

—易于理解和清晰。

7.2.5. 隐私影响评估

控制

当 PII 的新处理或 PII 的现有处理改变时，组织应评估是否需要并实施适当的隐私影响评估。

实施指南

PII 处理为 PII 主体产生风险。这些风险应通过隐私影响评估进行评估。有些司法管辖区规定了必须进行隐私影响评估的案例。标准可以包括对 PII 主体产生法律影响的自动决策、大规模处理特殊类别的 PII（如与健康有关的信息、种族或人种、政治观点、宗教或哲学信仰、工会成员资格、遗传数据或生物测定数据），或系统地监测大规模的公共区域。

组织应确定完成隐私影响评估所需的要素。其中可以包括处理的 PII 类型、PII 的存储位置和

传输位置的列表。在这种情况下，数据流程图和数据图也会很有帮助（请参见 7.2.8，了解可告知隐私影响或其他风险评估的 PII 处理记录的详细信息）。

其他信息

与 PII 处理相关的隐私影响评估指南见 ISO/IEC 29134。

7.2.6. 与 PII 处理者的合同

控制

组织应与其使用的任何 PII 处理者签订书面合同，并应确保其与 PII 处理者签订的合同涉及附件 B 中 适当控制措施的实施。

实施指南

组织与代表其处理 PII 的任何 PII 处理者之间的合同应要求 PII 处理者实施附件 B 中规定的适当控制，同时考虑信息安全风险评估过程（见 5.4.1.2）和 PII 处理者处理 PII 的范围（见 6.12）。默认情况下， 附件 B 中规定的所有控制应视为相关。如果组织决定不要求 PII 处理者实施附件 B 中的控制，则应证 明其被排除在外（见 5.4.1.3）。

合同可以以不同的方式定义各方的责任，但为了与本文件保持一致，应考虑所有控制措施，并将其包含在文件化信息中。

7.2.7. 联合 PII 控制者

控制

组织应与任何 PII 联合控制者确定处理 PII 的各自角色和责任（包括 PII 保护和安全要求）。

实施指南

应以透明的方式确定 PII 处理的角色和责任。

这些角色和责任应记录在合同或任何类似的约束性文件中，其中包含联合处理 PII 的条款和条件。在某些法域，这种协议称为数据共享协议。

共同 PII 控制者协议可以包括（此列表既不确定也不详尽）：

—PII 共享/联合 PII 控制者关系的目的；

—确定属于联合 PII 控制者关系的组织（PII 控制者）；

—根据协议共享和/或转让和处理的 PII 类别；

—加工操作概述（如转移、使用）；

—各自角色和职责的描述；

—负责实施 PII 保护的技术和组织安全措施；

—PII 违约时的责任定义（例如，谁将在何时通知共有信息）；

—保留和/或处置 PII 的条款；

—不遵守本协议的责任；

—如何履行对 PII 主体的义务；

—如何向 PII 主体提供涵盖联合 PII 控制人之间安排本质的信息；

—PII 主体如何获取其有权接收的其他信息；以及

—PII 主体的联络点。

7.2.8. 与处理 PII 相关的记录

控制

组织应确定并安全保存必要的记录，以支持其处理 PII 的义务。

实施指南

维护 PII 处理记录的一种方法是拥有组织执行的 PII 处理活动的库存或列表。此类清单可包括：

—处理类型；

—处理目的；

—对 PII 和 PII 主体（如儿童）类别的描述；

—已披露或将披露 PII 的接收者类别，包括第三国或国际组织的接收者；

—技术和组织安全措施的一般说明；以及

—隐私影响评估报告。

这样的库存应该有一个所有者，他对其准确性和完整性负责。

7.3. 对 PII 主体的义务

目标：确保向 PII 主体提供有关其 PII 处理的适当信息，并履行与 PII 处理相关的对 PII 主

体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

组织应确定并记录其对 PII 主体的法律、法规和业务义务，以处理其 PII，并提供履行这些义务的手段。

实施指南

对 PII 主体的义务和支持他们的方式因司法管辖区而异。

组织应确保他们提供适当的手段，以方便和及时的方式履行对 PII 主体的义务。应向 PII 主体提供明确的文件，说明对他们的义务在多大程度上得到履行，以及如何履行，并提供一个最新的联络点，以便他们能够处理他们的请求。

应以与收集 PII 和同意书类似的方式提供联络点（例如，如果 PII 是通过电子邮件或网站收集的，则联络点应通过电子邮件或网站，而不是电话或传真等替代方式）。

7.3.2. 确定 PII 主体的信息

控制

组织应确定并记录向 PII 主体提供的有关其 PII 处理和此类规定时间的信息。

实施指南

组织应确定何时向 PII 主体提供信息（例如，在处理之前、在要求提供信息后的一定时间内等）和提供信息类型的法律、法规和/或业务要求。

根据要求，这些信息可以采取通知的形式。可提供给 PII 主体的信息类型示例如下：

—有关处理目标的信息；

—PII 控制者或其代表的联系方式；

—有关处理的法律依据的信息；

—如果不是直接从 PII 主体处获得 PII 的信息；

—关于 PII 规定是法定要求还是合同要求的信息，以及在适当情况下，未能提供 PII 的可能后果；

—7.3.1 中确定的对 PII 主体的义务，以及 PII 主体如何从中受益的信息，特别是关于访问、

修改、

—更正、请求擦除、接收其 PII 副本和反对处理的信息；

—关于 PII 委托人如何撤回同意的信息；

—关于 PII 转移的信息；

—接收者类别信息；

—关于 PII 保留期的信息；

—关于使用基于 PII 自动处理的自动决策的信息；

—关于提出申诉的权利和如何提出申诉的信息；

—有关提供信息的频率的信息（例如“及时”通知、组织定义的频率等。

如果处理 PII 的目的发生变化或扩展，组织应提供最新信息。

7.3.3. 向 PII 主体提供信息

控制

组织应向 PII 主体提供明确且易于访问的信息，以识别 PII 控制者并描述其 PII 的处理。

实施指南

组织应以及时、简明、完整、透明、易懂和易于获取的形式，向 PII 主体提供第 7.3.2 条中详细说明的信息，并酌情使用清晰明了的语言向目标受众提供。

在适当情况下，应在收集 PII 时提供信息。它也应该是永久性的。

注：图标和图像可以通过提供预期处理的视觉概述来帮助 PII 主体。

7.3.4. 提供修改或撤回同意的机制

控制

组织应为 PII 主体提供修改或撤回其同意的机制。

实施指南

组织应随时告知 PII 主体其撤回同意相关的权限（可能因司法管辖权不同而有所不同），并提供这样做的机制。用于撤回的机制取决于制度；应尽可能与用于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书，撤回同意书的机制应该是相同的，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。

有些行政管辖区对 PII 委托人何时以及如何修改或撤回其同意施加限制。

组织应以记录同意书本身的类似方式记录撤回或更改同意书的任何请求。

任何同意的变更都应通过适当的系统传播给授权用户和相关第三方。

组织应该定义一个响应时间，请求应该根据它来处理。

附加信息

当撤回对特定 PII 处理的同意时，通常应视为撤回前进行的所有 PII 处理适当，但此类处理的结果不应用于新的处理。例如，如果 PII 主体撤回其配置文件的同意，则不应进一步使用或咨询其配置文件。

7.3.5. 为 PII 处理提供反对机制

控制

组织应该为 PII 主体提供一种机制，以反对其 PII 的处理。

实施指南

有些行政管辖区为 PII 主体提供了反对处理其 PII 的权利。受此类行政管辖区的法律和/或法规约束的组织应确保其实施适当措施，使 PII 主体能够行使这项权利。

组织应记录与 PII 主体对处理的异议相关的法律和法规要求（例如，与直接营销目的的 PII 处理相关的异议）。组织应向委托人提供有关在这些情况下反对的能力的信息。反对的机制可能不同，

但应与提供的服务类型一致（例如，在线服务应在线提供此功能）。

7.3.6. 访问、更正和/或删除

控制

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

实施指南

本组织应实施策略、程序和/或机制，使 PII 主体能够在收到请求时，在没有不当延误的情况下获得、纠正和删除其 PII。

组织应该定义一个响应时间，请求应该根据它来处理。

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

注：由 7.5.3 中指定的控件生成的记录可以在这方面提供帮助。

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

有些行政管辖区对 PII 主体请求更正或删除其 PII 的时间和方式施加限制。组织应确定适用的这些限制，并随时了解这些限制的最新情况。

7.3.7. PII 控制者通知第三方的义务

控制

组织应将与共享 PII 有关的任何修改、撤回或反对通知与之共享 PII 的第三方，并实施适当的策略、程序和/或机制。

实施指南

本组织应采取适当步骤，考虑到现有技术，向第三方通报与共享 PII 有关的任何修改或撤回同意或反对。有些行政管辖区强制要求将这些行动通知这些第三方。

组织应确定并保持与第三方的积极沟通渠道。相关职责可分配给负责其操作和维护的人员。当通知第三方时，组织应监测其收到信息的确认情况。

注：由于对 PII 主体的义务而产生的变更可包括修改或撤回同意、更正请求、删除或处理限制，

或根据 PII 主体的要求对处理 PII 提出异议。

7.3.8. 提供已处理的 PII 副本

控制

组织应能够提供一份在 PII 主体要求时处理的 PII 副本。

实施指南

组织应提供一份以 PII 主体可访问的结构化、常用格式处理的 PII 副本。

一些行政管辖区定义了这样的情况，即组织应提供以允许移植到 PII 主体或收件人 PII 控制者（通常是结构化的、常用的和机器可读的）的格式处理的 PII 副本。

组织应确保提供给 PII 主体的任何 PII 副本都与该 PII 主体具体相关。

如果根据保留和处置策略（如 7.4.7 所述）已删除所请求的 PII，则 PII 控制者应通知 PII 主体已删除所请求的 PII。

如果组织不再能够识别 PII 主体（例如，由于去识别过程），组织不应寻求（重新）识别 PII 主体，因为实施此控制的唯一原因。然而，在某些行政管辖区中，合法请求可能要求 PII 主体提供额外信息，以便重新识别和随后披露。

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

7.3.9. 处理请求

控制

组织应定义并记录处理和响应 PII 主体合法请求的策略和程序。

实施指南

合法的请求可以包括请求处理的 PII 副本，或提出投诉的请求。

有些行政管辖区允许组织在某些情况下收取费用（例如过度或重复的请求）。

请求应在适当的定义响应时间内处理。

有些行政管辖区根据请求的复杂性和数量来定义响应时间，以及将 PII 主体通知任何延迟的要求。应在隐私策略中定义适当的响应时间。

7.3.10. 自动化决策

控制

组织应确定并解决由于组织所做的决定而产生的对 PII 主体的义务，包括法律义务，这些决定仅基于与 PII 相关的自动处理 PII 主体。

实施指南

一些行政管辖区定义了对 PII 主体的具体义务，当基于 PII 的自动化处理的决策显著影响它们时，例如通知自动决策的存在，允许 PII 主体反对这样的决策，和/或获得人为干预。

注：在某些行政管辖区，PII 的某些处理不能完全自动化。

在这些行政管辖区内运作的组织应考虑到遵守这些义务。

7.4. 设计隐私和默认隐私

目标：确保流程和系统的设计使收集和处理（包括使用、披露、保留、传输和处置）限于为确定的目的所必需的内容。

7.4.1. 限制收集

控制

组织应将 PII 的收集限制在与确定的目的相关、成比例和必要的最低限度。

实施指南

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

默认的隐私意味着，在 PII 的收集和处理中存在任何可选性时，每个选项应在默认情况下被禁用，并且仅由 PII 主体的显式选择启用。

7.4.2. 限制处理

控制

组织应将 PII 的处理限制在对所确定的目的而言是充分、相关和必要的。

实施指南

应通过信息安全与隐私策略（见 6.2）以及采用和遵守的书面程序来管理对 PII 处理的限制。

PII 的处理，包括：

—披露；

—PII 储存期；以及

—能够访问他们的 PII。

默认情况下，应限制在与所确定的目的相关的最小必要范围内。

7.4.3. 准确度和质量

控制

组织应确保并记录在 PII 的整个生命周期内，PII 的准确性、完整性和最新性，这是处理 PII 的目的所必需的。

实施指南

组织应实施策略、程序和/或机制，以尽量减少 PII 处理过程中的不准确。还应制定策略、程序和/或机制，以应对不准确的 PII。这些策略、程序和/或机制应包含在文件化信息中（例如，通过技术系统配置等），并应在整个 PII 生命周期中应用。

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

组织应定义并记录数据最小化目标，以及使用何种机制（如取消标识）来实现这些目标。

实施指南

组织应确定收集和处理的特定 PII 和 PII 数量相对于确定的目的是如何受到限制的。这可以包括使用去识别或其他数据最小化技术。

已识别的目的（见 7.2.1）可能需要处理未被取消识别的 PII，在这种情况下，组织应能够描述此类处理。

在其他情况下，所确定的目的不需要处理原始的 PII，而已被取消识别的 PII 的处理可以足以实现所 确定的目的。在这些情况下，组织应定义并记录 PII 需要与 PII 主体关联的程度，以及设计用于处理 PII 的机制和技术，以便实现去识别和/或 PII 最小化目标。

用于最小化 PII 的机制因处理类型和用于处理的系统而异。组织应记录用于实现数据最小化的

任何机制（技术系统配置等）。

如果对已识别数据的处理足以达到目的，组织应记录旨在及时实现组织设定的已识别目标的任何机制（技术系统配置等）。例如，删除与 PII 主体相关联的属性就足以让组织实现其确定的目的。在其他情况下，可以使用其他去识别技术，例如泛化（例如舍入）或随机化技术（例如噪声添加）来实现足 够程度的去识别。

注 1：有关去识别技术的更多信息，请参考 ISO/IEC 20889。

注 2：对于云计算，ISO/IEC 19944 提供了数据标识限定符的定义，这些限定符可用于分类数据标识

PII 主体或将 PII 主体与 PII 中的一组特征关联的程度。

7.4.5. 处理结束时 PII 去识别和删除

控制

一旦原始 PII 不再需要用于识别的目的，组织应删除 PII，或以不允许识别或重新识别 PII 主体的形式提交。

实施指南

组织应建立机制，在预期没有进一步处理时删除 PII。或者，只要产生的去识别数据不能合理地允许重新识别 PII 主体，就可以使用一些去识别技术。

7.4.6. 临时文件

控制

组织应确保在规定的记录期内，按照记录程序处理因处理 PII 而创建的临时文件（如删除或销毁）。

实施指南

组织应定期检查未使用的临时文件是否在标识的时间段内被删除。

其他信息

信息系统可以在正常运行过程中创建临时文件。这些文件是特定于系统或应用程序的，但可以包括与数据库更新和其他应用程序软件操作相关联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，但在某些情况下无法删除它们。这些文件保留使用的时间并不总是确定的，但是“垃圾收集”过程应该识别相关文件并确定自上次使用以来的时间。

7.4.7. 保留

控制

组织保留 PII 的时间不应超过处理 PII 所需的时间。

实施指南

组织应制定并维护其保留信息的保留时间表，同时考虑到保留 PII 的时间不超过必要的时间。此类时间表应考虑法律、法规和业务要求。当这些需求发生冲突时，需要做出业务决策（基于风险评估），并记录在适当的时间表中。

7.4.8. 处置

控制

组织应具有处置 PII 的文件化策略、程序和/或机制。

实施指南

PII 处置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，在生成的物理介质的粒度上，或在电子介质上恢复删除信息的能力上）。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 相关联的元数据以及存储 PII 的介质的物理特性。

7.4.9. 传输控制

控制

组织应将通过数据传输网络传输（例如发送给另一个组织）的 PII 置于适当的控制之下，以确保数据达到其预期目的地。

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（包括保留审核日志），以确保在不损害正确收件人的情况下传输 PII。

7.5. PII 共享、转移和披露

目标：确保流程和系统的设计使收集和处理（包括使用、披露、保留、传输和处置）限于为确定的目的所必需的内容。

7.5.1. 确定行政管辖区之间 PII 转移的依据

控制

组织应确定并记录各行政管辖区之间 PII 转移的相关依据。

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行政管辖区或国际组织（以及数据的来源地）。组织应记录对这些要求的遵守情况，作为转移的依据。

有些行政管辖区可能要求由指定的监督机构审查信息转让协议。在这些管辖区内运作的组织应了解任何此类要求。

注：如果转让发生在特定行政管辖区内，则发送人和接收人的适用法律和/或法规相同。

7.5.2. PII 可以转移到的国家和国际组织

控制

该组织应详细说明和记录可能向哪些国家和国际组织转移 PII。

实施指南

应向客户提供正常操作中 PII 可能转移到的国家和国际组织的身份。应包括使用分包 PII 处理产生的国家的身份。应根据 7.5.1 考虑所包括的国家。

在正常业务之外，还可能发生应执法机关要求进行的移交案件，而这些案件的国家身份不能事先说明，或适用的司法管辖区为保护执法调查的机密性而禁止移交（见 7.5.1、8.5.4 和 8.5.5）。

7.5.3. PII 转移记录

控制

组织应记录 PII 向第三方或从第三方转移的情况，并确保与第三方合作，以支持未来与 PII 主体义务相关的请求。

实施指南

记录可以包括由于 PII 控制者管理其义务而修改的 PII 从第三方转移或转移到第三方以执行来自 PII 主体的合法请求，包括删除 PII 的请求（例如，在同意撤回后）。

组织应该有一个定义这些记录保留期的策略。

组织应通过仅保留严格需要的信息，将数据最小化原则应用于传输记录。

7.5.4. 向第三方披露 PII 的记录

控制

组织应记录向第三方披露的 PII，包括披露的 PII 内容、披露对象和时间。

实施指南

PII 可以在正常操作过程中披露。应记录这些披露。

对第三方的任何额外披露，如因合法调查或外部审计而产生的披露，也应记录在案。记录应包括披露的来源和作出披露的权力来源。

8. 附加 ISO/IEC 27002 PII 处理者指南

8.1. 总则

第 6 条中的指南和本条中的附加内容为 PII 处理者创建了 PIMS 特定指南。本条中记录的实施指南与附件 B 中列出的控制措施有关。

8.2. 收集和处理条件

目标：确定并证明处理是合法的，根据适用的司法管辖区有法律依据，目的明确合法。

8.2.1. 客户协议

控制

在相关情况下，组织应确保处理 PII 的合同涉及组织在协助客户履行义务方面的作用（考虑到处理的性质和组织可获得的信息）。

实施指南

组织与客户之间的合同应包括以下内容（视客户的角色而定）（PII 控制者或 PII 处理者）（此列表既不确定也不详尽）：

—设计隐私和默认隐私（见 7.4、8.4）；

—实现处理的安全性；

—向监管机构通知涉及 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）；以及

—如果需要事先与相关 PII 保护机构协商，PII 处理机构应保证提供协助。

有些行政管辖区要求合同应包括处理的标的物和期限、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

组织应确保代表客户处理的 PII 仅用于客户书面说明中所述的目的。

实施指南

组织与顾客之间的合同应包括但不限于服务所要达到的目标和时限。

为了达到客户的目的，可能有技术上的原因使组织能够确定处理 PII 的方法，符合客户的一般指示，但没有客户的明确指示。例如，为了有效地利用网络或处理能力，可能需要根据 PII 主体的某些特性分配特定的处理资源。

组织应允许客户验证其是否符合目的规范和限制原则。这也确保组织或其任何分包商不会出于客户书面指示中所述目的以外的其他目的处理任何 PII。

8.2.3. 营销和广告使用

控制

未经相关 PII 主体事先同意，组织不得将根据合同处理的 PII 用于营销和广告目的。组织不应将提供这种同意作为接受服务的条件。

实施指南

记录 PII 处理者遵守客户合同要求的情况，特别是在计划营销和/或广告的情况下。

组织不应坚持在未获得 PII 主体的明确同意的情况下纳入营销和/或广告用途。

注：此控制是对 8.2.2 中更多通用控制的补充，不会替换或以其他方式取代它。

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，则应通知客户。

实施指南

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

8.2.5. 客户义务

控制

组织应向客户提供适当的信息，以便客户能够证明其遵守了其义务。

实施指南

客户所需的信息可以包括组织是否允许并有助于客户或客户授权或同意的其他审计员进行的审计。

8.2.6. 与处理 PII 相关的记录

控制

组织应确定并保持必要的记录，以证明其对代表客户进行的 PII 处理的义务（如适用合同所规定）的遵守。

实施指南

有些行政管辖区可能要求组织记录以下信息：

—代表每个客户进行的处理类别；

—转让给第三国或国际组织；以及

—技术和组织安全措施的一般说明。

8.3. 对 PII 主体的义务

目标：确保向 PII 主体提供有关其 PII 处理的适当信息，并履行与 PII 处理相关的对 PII 主体的任何其他适用义务。

8.3.1. 对 PII 主体的义务

控制

组织应向客户提供履行其与 PII 主体相关义务的手段。

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。这些义务可以包括客户使用组织的服

务来履行这些义务的事项。例如，这可以包括及时纠正或删除 PII。

如果客户依赖组织提供信息或技术措施以便履行对 PII 主体的义务，则应在合同中规定相关信息或技术措施。

8.4. 设计的隐私和默认的隐私

目标：确保设计的过程和系统能够将 PII 的收集和处理（包括使用、披露、保留、传输和处置）限制在为确定的目的所必需的范围内。

8.4.1. 临时文件

控制

组织应确保在规定的记录期内，按照记录程序处理因处理 PII 而创建的临时文件（如删除或销毁）。

实施指南

组织应定期核查未使用的临时文件是否在确定的时间内被删除。

其他信息

信息系统可以在正常运行过程中创建临时文件。这些文件是特定于系统或应用程序的，但可以包括与数据库更新和其他应用程序软件操作相关联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，但在某些情况下无法删除它们。这些文件保留使用的时间并不总是确定的，但是“垃圾收集”过程应该识别相关文件并确定自上次使用以来的时间。

8.4.2. PII 的返还、转让或处置

控制

组织应提供以安全方式返还、转移和/或处置 PII 的能力。它还应该向客户提供其策略。

实施指南

作为某个时间点，可能需要以某种方式处理 PII。这可能涉及将 PII 返还给客户、将其转移给另一个组织或 PII 控制者（例如，由于合并）、删除或以其他方式销毁、取消识别或存档。应以安全的方式管理 PII 的返还、转移和/或处置能力。

组织应提供必要的保证，以允许客户确保根据合同处理的 PII（由组织及其任何分包商）从其存储的任何地方删除，包括为备份和业务连续性的目的，只要这些 PII 不再需要用于确定的目的顾客。

组织应制定并实施与 PII 处置相关的策略，并应在客户要求时向其提供该策略。

策略应涵盖在合同终止后处置 PII 之前的 PII 保留期，以保护客户不因合同意外失效而丢失 PII。

注：根据保留原则（见 7.4.7），本控制和指南也具有相关性。

8.4.3. PII 的传输控制

控制

组织应将通过数据传输网络传输的 PII 置于适当的控制之下，以确保数据达到其预期目的地。

实施指南

需要控制 PII 的传输，通常是通过确保只有授权人员才能访问传输系统，并遵循适当的流程（包括保留审计数据），以确保 PII 在不损害正确收件人的情况下传输。传输控制要求可包含在 PII 处理者-客户合同中。

如果没有与传输相关的合同要求，则可以在传输前听取客户的建议。

8.5. PII 共享、转移和披露

目标：确定是否按照适用的义务分享、转让给其他司法管辖区或第三方和/或披露 PII，并记录。

8.5.1. 行政管辖区间 PII 转移的基础

控制

组织应及时通知客户在司法管辖区之间进行 PII 转移的依据以及这方面的任何预期变更，以便客户有能力反对此类变更或终止合同。

实施指南

不同司法管辖区之间的 PII 转移可能受到法律和/或法规的约束，具体取决于 PII 将转移到的司法管辖区或组织（以及 PII 的来源地）。组织应记录这些要求的遵守情况，作为转移的依据。

组织应通知客户任何 PII 转移，包括转移到：

—供应商；

—其他各方；

—其他国家或国际组织。

如有变更，组织应按约定的时间提前通知顾客，使顾客有能力对变更提出异议或终止合同。

组织和客户之间的协议可以有这样的条款：组织可以在不通知客户的情况下实施变更。在这些情况下，应设定此转移的限制（例如，组织可以在不通知客户的情况下更改供应商，但不能将 PII 转移到其他国家）。

在 PII 国际转让的情况下，应确定示范合同条款、有约束力的公司规则或跨境隐私规则等协议、涉及的国家和适用这些协议的情况。

8.5.2. PII 可以转移到的国家和国际组织

控制

该组织应详细说明和记录可能向哪些国家和国际组织转移 PII。

实施指南

应向客户提供正常运行中 PII 可能转移到的国家和国际组织的身份。应包括使用分包 PII 处理产生的国家的身份。应根据 8.5.1 考虑所包括的国家。

在正常业务之外，还可能发生应执法机关要求进行的移交案件，而这些案件的国家身份不能事先说明，或适用的司法管辖区禁止此类案件，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

组织应记录向第三方披露的 PII，包括向谁和何时披露的 PII。

实施指南

PII 可在正常操作过程中披露。应记录这些披露。对第三方的任何额外披露，如因合法调查或外部审计而产生的披露，也应记录在案。记录应包括披露的来源和作出披露的权力来源。

8.5.4. PII 披露请求通知

控制

组织应将任何具有法律约束力的 PII 披露请求通知客户。

实施指南

该组织可收到具有法律约束力的 PII 披露要求（例如，来自执法机关）。在这些情况下，组织应在商定的时间范围内并根据商定的程序（可包括在客户合同中）将任何此类请求通知客户。

在某些情况下，具有法律约束力的请求包括要求该组织不向任何人通报这一事件（一个可能禁止

披露的例子是刑法禁止保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

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

实施指南

与实施控制相关的详细信息可包含在客户合同中。

这类请求可来自若干来源，包括法院、法庭和行政当局。它们可能来自任何司法管辖区。

8.5.6. 用于处理 PII 的分包商的披露

控制

组织应在使用前向客户披露任何使用分包商处理 PII 的情况。

实施指南

客户合同中应包括使用分包商处理 PII 的规定。

披露的信息应包括使用分包的事实和相关分包商的名称。披露的信息还应包括分包商可以向其传输数据的国家和国际组织（见 8.5.2）以及分包商有义务履行或超过组织义务的方式（见 8.5.7）。

如果分包商信息的公开披露被评估为增加超出可接受范围的安全风险，则应根据保密协议和/或客户的要求进行披露。应该让客户知道信息是可用的。

这与 PII 可以转移的国家名单无关。在任何情况下，都应向客户披露该清单，以便他们通知相应的 PII 主体。

8.5.7. 聘请分包商处理 PII

控制

组织应仅根据客户合同雇佣分包商处理 PII。

实施指南

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

这可以是客户合同中适当条款的形式，也可以是具体的“一次性”协议。

组织应与代表其进行 PII 处理的任何分包商签订书面合同，并应确保其与分包商签订的合同涉及附件 B 中适当控制措施的实施。

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

合同可以以不同的方式定义各方的责任，但为了与本文件保持一致，应考虑所有控制措施，并将其包含在文件化信息中。

8.5.8. 处理 PII 分包商的变更

控制

在获得一般书面授权的情况下，组织应通知客户关于增加或更换分包商以处理 PII 的任何预期变更，从而使客户有机会反对此类变更。

实施指南

如果组织更改了其分包部分或全部 PII 处理的组织，则在新分包商处理 PII 之前，需要客户的书面授权进行更改。这可以是客户合同中适当条款的形式，也可以是具体的“一次性”协议。

附录 A

规范

PIMS 特定参考控制目标和控制（PII 控制）

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

表 A.1 中列出的附加或修改的控制目标和控制直接来源于本文件中定义的目标和控制，并与本文件中定义的目标和控制保持一致，并将与 5.4.1.3 中改进的 ISO/IEC 27001:2013，6.1.3 结合使用。

并非本附录中列出的所有控制目标和控制都需要包含在 PIMS 实施中。适用性声明中应包括排除任何控制目标的理由（见 5.4.1.3）。排除的理由可以包括风险评估认为不需要控制的情况，以及适用法律 和/或法规不要求控制的情况。

注：本附件中的条款编号与第 7 条中的条款编号有关。

表 A.1——控制目标和控制

A.7.2 **收集和处理条件** **目标：** **确定并记录处理是合法的，根据适用的行政管辖区具有法律依据，并且具有明确的和合法的目的。**		
A.7.2.1	**确定并记录目的**	控制： **组织应确定并记录处理 PII 的具体目标。**
A.7.2.2	**确定法律依据**	控制： **组织应确定、记录并遵守为确定的目标处理 PII 的相关法律依据。**
A.7.2.3	**确定何时以及如何获得同意**	控制： **组织应确定并记录一个过程，以证明是否、何时以及如何从 PII 主体处获得处理 PII 的同意。**
A.7.2.4	**获得并记录同意**	控制： **组织应根据文件化的过程，获得并记录 PII 主体的同意。**
A.7.2.5	**隐私影响评估**	控制： **当 PII 的新处理或 PII 的现有处理改变时，组织应评估是否需要并实施适当的隐私影响评估。**

A.7.2.6	与 PII 处理者的合同	控制： 组织应与使用的任何 PII 处理者签订书面合同，并应确保其与 PII 处理者签订的合同涉及附录 B 中适当控制措施的实施。
A.7.2.7	联合 PII 控制者	控制： 组织应与任何 PII 联合控制员确定处理 PII 的各自角色和责任（包括 PII 保护和安全要求）。
A.7.2.8	与处理 PII 相关的记录	控制： 组织应确定并安全保存必要的记录，以支持其处理 PII 的义务。
A.7.3 对 PII 主体的义务 目标： 确保向 PII 主体提供有关其 PII 处理的适当信息，并履行与 PII 处理相关的对 PII 主体的任何其他适用义务。		
A.7.3.1	确定和履行对 PII 主体的义务	控制： 组织应确定并记录其对 PII 主体在处理其 PII 过程中的法律、法规和业务义务，并提供履行这些义务的手
A.7.3.2	确定 PII 主体的信息	控制： 组织应确定并记录向 PII 主体提供的有关其 PII 处理和此类规定时间的信息。
A.7.3.3	向 PII 主体提供信息	控制： 组织应向 PII 主体提供明确且易于访问的信息，以识别 PII 控制者并描述其 PII 的处理。
A.7.3.4	提供修改或征得同意的机制	控制： 组织应为 PII 主体提供修改或撤回其同意的机制。
A.7.3.5	为 PII 处理提供对象机制	控制： 组织应提供一种机制，使 PII 主体反对其 PII 的处理。
A.7.3.6	访问、更正和/或删除	控制： 组织应实施策略、程序和/或机制，以履行其对 PII 主体访问、纠正和/或删除其 PII 的义务。
A.7.3.7	PII 控制者通知第三方的义务	控制： 组织应将与共享 PII 有关的任何修改、撤回或反对通知与之共享 PII 的第三方，并实施适当的策略、程序和/或机制。

A.7.3.8	提供已处理的 PII 副本	控制： 当 PII 主体要求时，组织应能够提供一份处理过的 PII 副本。
A.7.3.9	处理请求	控制： 组织应定义并记录处理和响应 PII 主体合法请求的政策和程序。
A.7.3.10	自动化决策	控制： 组织应确定并解决由组织作出的与 PII 主体有关的决定所产生的对 PII 主体的义务，包括法律义务，这些决定仅基于 PII 的自动处理。
A.7.4 设计的隐私和默认的隐私 目标： 确保过程和系统的设计使收集和处理（包括使用、披露、保留、传输和处置）限于为确定的目的所必需的内容。		
A.7.4.1	限制收集	控制： 组织应将 PII 的收集限制在与确定的目的相关、成比例和必要的最低限度。
A.7.4.2	限制处理	控制： 组织应将 PII 的处理限制在为确定的目的而充分、相关和必要的范围内。
A.7.4.3	准确度和质量	控制： 组织应确保并记录在 PII 的整个生命周期内，PII 的准确性、完整性和最新性，这是处理 PII 的目的所必需的。
A.7.4.4	PII 最小化目标	控制： 组织应定义并记录数据最小化目标，以及使用何种机制（如取消标识）来实现这些目标。
A.7.4.5	处理结束时 PII 去识别和删除	控制： 组织应删除 PII 或以不允许识别或重新识别 PII 主体的形式提交 PII，只要原始 PII 不再需要用于识别的目的。

A.7.4.6	临时文件	控制： 组织应确保在规定的文件期限内，按照文件化程序处理因处理 PII 而创建的临时文件（如删除或销毁）。
A.7.4.7	保留	控制： 组织不得保留 PII 超过处理 PII 所需的时间。
A.7.4.8	处置	控制： 组织应具有处置 PII 的文件化策略、程序和/或机制。
A.7.4.9	传输控制	控制： 组织应将通过数据传输网络传输（例如发送给另一组织）的 PII 置于设计用于确保数据达到其预期目的地的适当控制之下。
A.7.5 共享、转让和披露 目标： 确定 PII 是否被共享、转移至其他司法管辖区或第三方和/或根据适用义务披露，并记录。		
A.7.5.1	确定行政管辖区之间 PII 转移的依据	控制： 组织应确定并记录辖区间 PII 转移的相关依据。
A.7.5.2	PII 可以转移到的国家和国际组织	控制： 该组织应详细说明和记录 PII 可能转移到的国家和国际组织。
A.7.5.3	PII 转移记录	控制： 组织应记录向第三方或从第三方转移 PII 的情况，并确保与第三方合作，以支持未来有关 PII 主体义务的请求。
A.7.5.4	向第三方披露 PII 的记录	控制： 组织应记录向第三方披露的 PII，包括披露的 PII 内容、披露对象和时间。

附录 B

规范

PIMS 特定参考控制目标和控制（PII 处理者）

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

表 B.1 中列出的附加或修改的控制目标和控制直接来源于本文件中定义的目标和控制，并与本文件中定义的目标和控制保持一致，并将与 5.4.1.3 中改进的 ISO/IEC 27001:2013，6.1.3 结合使用.

并非本附录中列出的所有控制目标和控制都需要包含在 PIMS 实施中。适用性声明中应包括排除任何控制目标的理由（见 5.4.1.3）。排除的理由可以包括风险评估认为不需要控制的情况，以及适用法律和/或法规不要求控制的情况

注：本附件中的条款编号与第 8 条中的条款编号有关。

表 B.1——控制目标和控制

B.8.2 收集和处理条件 目标： 确定并记录处理是合法的，根据适用的行政管辖区具有法律依据，并且具有明确的和合法的目的。		
B.8.2.1	客户协议	控制： 在相关情况下，组织应确保处理 PII 的合同涉及组织在协助客户履行义务方面的作用（考虑到处理的性质和组织可获得的信息）。
B.8.2.2	组织的目的	控制： 组织应确保代表客户处理的 PII 仅用于客户书面指示中所述的目的。
B.8.2.3	营销和广告使用	控制： 未经相关 PII 主体事先同意，组织不得将根据合同处理的 PII 用于营销和广告目的。该组织不得将提供这种同意作为接受服务的条件。
B.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，则应通知客户。

B.8.2.5	客户义务	控制： 组织应向客户提供适当的信息，使客户能够证明其履行了义务。
B.8.2.6	与处理 PII 相关的记录	控制： 组织应确定并保持必要的记录，以证明其对代表客户进行的 PII 处理的义务（如适用合同所规定）的遵守。
B.8.3 对 PII 主体的义务 目标： 确保向 PII 主体提供有关其 PII 处理的适当信息，并履行与 PII 处理相关的对 PII 主体的任何其他适用义务。		
B.8.3.1	对 PII 主体的义务	控制： 组织应向客户提供履行其与 PII 主体有关的义务的手段。
B.8.4 设计的隐私和默认的隐私 目标： 确保过程和系统的设计使收集和处理 PII（包括使用、披露、保留、传输和处置）限于为确定的目的所必需的内容。		
B.8.4.1	临时文件	控制： 组织应确保在规定的文件期限内，按照文件程序处理因处理 PII 而创建的临时文件（如删除或销毁）。
B.8.4.2	PII 的返还、转让或处置	控制： 组织应提供以安全方式返还、转移和/或处置 PII 的能力。它还应向客户提供其策略。
B.8.4.3	传输控制	控制： 组织应将通过数据传输网络传输的 PII 置于适当的控制之下，以确保数据达到预期目的地。
B.8.5 PII 共享、转让和披露 目标： 确定 PII 是否被共享、转移至其他司法管辖区或第三方和/或根据适用义务披露，并记录。		
B.8.5.1	行政管辖辖区间 PII 转移的依据	控制： 组织应及时通知客户各行政管辖区之间 PII 转移的依据以及这方面的任何预期变更，以便客户有能力反对此类变更或终止合同。

B.8.5.2	PII 可以转移到的国家和国际组织	控制： 该组织应详细说明和记录可能向其转移 PII 的国家和国际组织。
B.8.5.3	向第三方披露 PII 的记录	控制： 组织应记录向第三方披露的 PII，包括向谁和何时披露的 PII。
B.8.5.4	PII 披露请求通知	控制： 组织应将任何具有法律约束力的PII 披露请求通知客户。
B.8.5.5	具有法律约束力的 PII 披露	控制： 组织应拒绝任何不具法律约束力的PII 披露请求，在进行任何 PII 披露之前咨询相应的客户，并接受相应客户授权的任何合同约定的PII 披露请求。
B.8.5.6	披露用于处理 PII 的分包商	控制： 组织应在使用前向客户披露任何使用分包商处理 PII 的情况。
B.8.5.7	聘请分包商处理 PII	控制： 组织应只根据客户合同聘用分包商处理 PII。
B.8.5.8	处理 PII 的分包商的变更	控制： 在获得一般书面授权的情况下，组织应通知客户关于增加或更换分包商以处理 PII 的任何预期变更，从而 使客户有机会反对此类变更。

附录 C

信息

IEC29100 的对应关系

表 C.1 和 C.2 给出了本文件规定与 ISO/IEC 29100 隐私原则之间的指示性映射。它以一种纯粹的指示性方式展示了如何遵守本文件的要求和控制与 ISO/IEC 29100 中规定的一般隐私原则相关

表 C.1——PII 控制者和 ISO/IEC 29100 的控制映射

隐私原则	PII 控制者相关控制
1. 同意与选择	A.7.2.1 确定并记录目的 A.7.2.2 确定法律依据 A.7.2.3 确定何时以及如何获得同意 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 提供修改或撤回同意的机制 A.7.3.5 提供拒绝处理的机制 A.7.3.7 PII 控制者的义务和第三方
2. 目标合法性和规范性	A.7.2.1 确定并记录目的 A.7.2.2 确定法律依据 A.7.2.5 隐私影响评估 A.7.3.2 确定 PII 主体的信息 A.7.3.3 向 PII 主体提供信息 A.7.3.10 自动化决策
3. 收集限制	A.7.2.5 隐私影响评估 A.7.4.1 限制收集
4. 数据最小化	A.7.4.2 限制处理 A.7.4.4 PII 最小化目标 A.7.4.5 处理结束时 PII 去识别和删除

5. 使用、保留和披露限制	A.7.4.4 PII 最小化目标 A.7.4.5 处理结束时 PII 去识别和删除 A.7.4.6 临时文件 A.7.4.7 保留 A.7.4.8 处置 A.7.5.1 确定国际 PII 转移的依据 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、透明和通知	A.7.3.2 确定 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/或删除 A.7.3.8 提供已处理的 PII 副本 A.7.3.9 处理请求
9. 责任	A.7.2.6 与 PII 处理者的合同 A.7.2.7 联合控制者 A.7.2.8PII 与处理 PII 相关的记录 A.7.3.9 处理请求 A.7.5.1 确定国际 PII 转移的依据 A.7.5.2 PII 可以转移到的国家和组织 A.7.5.3 PII 的记录和转移
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 的控制映射

ISO/IEC 29100 隐私原则	PII 处理者相关控制
1. 同意与选择	B.8.2.5 客户义务
2.目标合法性和规范性	B.8.2.1 客户协议 B.8.2.2 组织的目标 B.8.2.3 营销和广告使用 B.8.2.4 侵权指令 B.8.3.1 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、透明和通知	B.8.5.6 用于处理 PII 的分包商的披露 B.8.5.7PII 聘请分包商处理 PII B.8.5.8 处理 PII 分包商变更
8. 个人参与和访问	B.8.3.1 PII 主体的义务
9. 责任	B.8.2.6 与处理 PII 相关的记录 B.8.4.2 PII 的返还、转让或处置 B.8.5.1 确定国际 PII 转移的依据 B.8.5.2 PII 可以转移到的国家和组织
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

信息

与通用数据保护条例的对应关系

本附录给出了本文条款与《欧洲联盟通用数据保护条例》第 5 至 49 条（第 43 条除外）之间的指示性映射。它说明了如何遵守本文的要求和控制，可以相关的履行 GDPR 的义务。

然而，这纯粹是指示性的，根据本文件，各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 结构与 GDPR 条款的映射

本文件的子条款	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)
5.2.3	(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)©
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)
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)，
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)
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)

附录 E

信息

与 ISO/IEC 27018 和 ISO/IEC 29151 的对应关系

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

表 E.1 给出了本文件规定与 ISO/IEC 27018 和 ISO/IEC 29151 隐私原则之间的指示性映射。它说明了本文件的要求和控制如何与 ISO/IEC 27018 和/或 ISO/IEC 29151 中的规定有一些对应关系

这纯粹是指示性的，不应假定规定之间的给定联系意味着等同。

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

本文件的子条款	IEC 27018 的子条款	ISO/IEC 29151 的子条款
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	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

附录 F

信息

如何将 ISO/IEC 27701 应用于 ISO/IEC 27001 和 ISO/IEC 27002

F.1 如何运用此文件

本文件以 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013 为基础，并扩展了其要求和指南，以便除信息安全外，还考虑到可能受 PII 处理影响的 PII 主体的隐私保护。这意味着，如果在 ISO/IEC 27001 或 ISO/IEC 27002 中使用“信息安全”一词，则“信息安全与隐私”应适用。

表 F.1 给出了术语“信息安全”的扩展映射，以便将其应用于本文件。

表 F.1——隐私信息安全术语扩展的映射

ISO/IEC 27001	本文件（扩展）
信息安全	信息安全与隐私
信息安全策略	信息安全与隐私策略
信息安全管理	信息安全与隐私信息管理
信息安全管理体系(ISMS)	隐私信息管理体系（PIMS）
信息安全目标	信息安全与隐私目标
信息安全性能	信息安全与隐私性能
信息安全要求	信息安全与隐私要求
信息安全风险	信息安全与隐私风险
信息安全风险评估	信息安全与隐私风险评估
信息安全风险处置	信息安全与隐私风险处置

基本上，在处理 PII 时，将本文档应用于保护 PII 主体的隐私有三种情况：

1) 按原样应用安全标准：参考标准按原样应用，延长上述条款。因此，引用标准不重复，只引用相应的条款。

2) 附加到安全标准：参考标准适用于附加的隐私特定要求或实施指南。

3) 完善安全标准：参考标准由隐私特定要求或实施指南进行完善。

F.2 安全标准改进示例

本条描述了 5.4.1.2 如何应用于 ISO/IEC 27001:2013，6.1.2。

在考虑到处理 PII 时对 PII 主体隐私的保护时，ISO/IEC 27001:2013，6.1.2 将用下面的下划线文本进行修改：

6.1.2 信息安全风险评估

组织应定义并应用信息安全与隐私风险评估流程，该流程应：

a) 建立并维护信息安全与隐私风险标准，包括

   1) **风险接受标准；以及**

   2) 执行信息安全与隐私风险评估的标准；

b) 确保重复的信息安全与隐私风险评估产生一致、有效和可比的结果；

c) **识别信息安全与隐私风险：**

   1) 应用信息安全与隐私风险评估流程，识别与信息安全与隐私信息管理体系范围内信息的机密性、完整性和可用性丧失相关的风险；以及

   2) **识别风险责任人；**

d) **分析信息安全与隐私风险；**

   1) 评估 6.1.2 c）中确定的风险实现时可能产生的潜在后果；

   2) 评估 6.1.2 c）1）中确定的风险发生的现实可能性

   3) 确定风险等级；

e) **评估信息安全与隐私风险：**

   1) 将风险分析结果与 6.1.2 a 中确定的风险标准进行比较

   2) 对分析的风险进行优先级排序，以便进行风险处理。

组织应保留有关信息安全与隐私风险评估过程的书面信息。

Bibliography （参考文献）

[1] ISO/IEC 19944, I*nformation 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 mamagement*

- 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 29184, *Information technology - Security techniques -Guidelines for online privacy notices and consent*