国际标准

ISO/IEC 27701

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

参考编号
ISO/IEC 27701:2019（E）

内容

页

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。

用于指定本标准以及进一步维护本标准的规程在ISO/IEC导则第1部分中有所描述。不同类型标准所需的不同批准准则应特别注意。本标准是根据ISO/IEC导则第2部分的编辑规则起草的（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.

0 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，也是全世界立法和/或监管的主题。

ISO/IEC 27001中定义的信息安全管理体系（ISMS）被设计成可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;和

-欧盟通用数据保护条例。

但是，这些可能需要考虑到当地的立法和/或法规。

本标准可供PII控制者（包括联合PII控制者）和PII处理者（包括使用分包的PII处理者和作为分包商处理PII的PII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商业伙伴的协议，其中PII的处理是相互关联的。这也可以帮助与其他利益相关者建立关系。如果需要，可以将本文档与ISO/IEC 27001结合使用，对该证据进行独立验证。

本标准最初是作为ISO/IEC 27552开发的。

0.2 与其他管理体系的兼容性

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。

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

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 规范性引用文献

文中提到了以下文件，其中部分或全部内容构成了本标准的要求。凡是注日期的引用文件，只有引用的版本适用于本标准；凡是不注日期的引用文件，其最新版本（包括任何修改）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 - 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

出于本标准的目的，ISO/IEC 27000和ISO/IEC 29100中给出的术语和定义适用。

ISO和IEC在以下网址中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

IEC Electropedia： http://www.electropedia.org/

3.1 联合PII控制者

决定与一个或多个PII控制者联合处理PII的目的和方式的PII控制者。

3.2 隐私信息管理体系PIMS

在处理PII过程中应对可能潜在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相关的特定领域的标准。

本标准专注于PIMS领域的要求。遵守本标准的基础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，以考虑到可能潜在受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的要求时相关的PIMS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是如此。

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是如此。

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控制者的组织的PIMS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处理者的组织的PIMS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欧盟通用数据保护法规的映射。

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

附录F.解释了如何在处理PII时将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给出了本标准中与ISO/IEC 27001相关的PIMS特定要求的位置。

表1 – PIMS的特定要求的位置和实施ISO/IEC 27001:2013中控制的其他信息

ISO/IEC 27001:2013中的条款	标题	本标准中的子条款	备注
4	组织环境	5.2	补充要求
5	领导	5.3	没有特定于PIMS的要求
6	规划	5.4	补充要求
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	绩效评价	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　　5.1中“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。

表2 - PIMS特定指南的位置和实施在ISO/IEC 27002：2013中控制的其他信息

ISO / IEC 27002:2013中的条款	标题	本标准中的子条款	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	系统的获取，开发和维护	6.11	补充指南
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　6.1中“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 顾客

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　组织作为联合控制者的的情况。

注2　与组织建立企业对消费者（B2C）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子处理者的客户）。

注3　第6章中提到的“客户”，相关条款可适用于a），b）或 c）的语境中。

注4　第7章和附录A中提到的“客户”，相关条款可适用于a）的语境中。

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）的语境中。

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”的要求应扩展到针对可能受PII处理而产生潜在影响的隐私保护。

注　　在实践中，在ISO/IEC 27001:2013中使用“信息安全”时，相当于“信息安全和隐私”（见附录F.）.

5.2 组织环境

5.2.1 理解组织及其环境

ISO/IEC 27001:2013，4.1 的补充要求是：

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起作用（例如PII控制者和PII处理者），则应确定单独的角色，每个角色都应作为一系列独立控制的对象。

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的补充要求是：

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，有利益关系或负有责任的各方，以及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　作为证明对组织义务合相符合的一个要素，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。这些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的补充要求是：

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的补充要求是：

组织应根据在本标准第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

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

5.3.2 方针

ISO/IEC 27001:2013，5.2中陈述的要求以及本标准5.1中的解释说明适用。

5.3.3 组织角色，职责和权限

ISO/IEC 27001:2013，5.3中陈述的要求以及本标准5.1中的解释说明适用。

5.4 规划

5.4.1 应对风险和机会的措施

5.4.1.1 总则

ISO/IEC 27001:2013,6.1.1中陈述的要求以及本标准5.1中的解释说明适用。

5.4.1.2 信息安全风险评估

ISO/IEC 27001:013,6.1.2中陈述的要求以及下列改进内容适用。

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 c）中识别的风险可能发生，组织应评估其对组织和PII主体的潜在后果。

5.4.1.3 信息安全风险处置

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

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，处理PII的风险以及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

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

5.5 支持

5.5.1 资源

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

5.5.2 能力

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

5.5.3 意识

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

5.5.4 沟通

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

5.5.5 文件记录信息

5.5.5.1 总则

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

5.5.5.2 创建和更新

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

5.5.5.3 文件记录信息的控制

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

5.6 运行

5.6.1 运行的规划和控制

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

5.6.1 信息安全风险评估

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

5.6.2 信息安全风险处理

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

5.7 绩效评价

5.7.1 监测，测量，分析和评价

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

5.7.2 内部审核

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

5.7.3 管理评审

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

5.8 改进

5.8.1 不符合和纠正措施

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

5.8.2 持续改进

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

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

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适用：

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政策，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

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 信息安全角色和职责

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适用：

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

组织应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，负责人应：

— 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

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

6.3.1.5 项目管理中的信息安全

ISO/IEC 27002:2013,6.1.5中规定的控制，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中规定的控制，实施指南和其他信息以及以下补充指南适用。

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

组织应确保移动设备的使用不会导致PII的损害。

6.3.2.2 远程工作

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

6.4.1.2 任用条款和条件

ISO/IEC 27002:2013,7.1.2中规定的控制，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中规定的控制，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中规定的控制，实施指南和其他信息以及以下补充指南适用：

ISO/IEC 27002：2013，7.2.2，信息安全意识、教育和培训的补充实施指南是：

应采取措施，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

ISO/IEC 27002:2013,7.2.3中规定的控制，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 任用终止或变更的责任

ISO/IEC 27002:2013,7.3.1中规定的控制，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 资产的可接受使用

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 信息分级

6.5.2.1 信息的分级

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适用：

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应明确将PII视为其实施方案的一部分。在整个分类系统中考虑PII对于理解组织处理什么样的PII（例如种类，特殊类别），以及存储此类PII的位置以及它可以通过哪系统流通是不可或缺的。

6.5.2.2 信息的标记

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适用。

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

组织应确保其控制下的人员了解PII的定义以及如何识别PII信息。

6.5.2.3 资产的处理

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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，组织应使用在存储PII时允许加密可移动物理介质和/或设备。未加密的介质仅应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，组织应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，损坏和不当访问。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

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适用。

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形成文件的信息中，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

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适用：

6.5.3.4 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，则应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，应实施其他措施（如加密），以确保数据只能在目的地而非传输途中被访问。

组织应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程序，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

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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应解决用户对其的访问控制受到损害的情况，例如密码泄漏或其他用户注册数据收到侵害（例如，无意泄露的情况）。

对于处理PII的系统和服务，组织不应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，客户可以负责用户ID管理的一些或所有方面。此类情况应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

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适用：

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

组织应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。

通过设置单独的用户访问ID，可以使适当配置系统识别访问PII的用户以及他们所做的添加，删除或更改。除了保护组织外，用户还可以通过识别他们已处理的内容以及未处理的内容来获得保护。

在组织将PII处理作为服务提供的情况下，客户可以负责访问管理的一些或所有方面。在适当的情况下，组织应向客户提供执行访问管理的方法，例如通过提供管理权限来管理或终止访问。此类情况应包括在文件化信息中。

6.6.2.3 特定访问权管理

ISO/IEC 27002:2013,9.3.3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 系统和应用程序访问控制

6.6.4.1 信息访问限制

ISO/IEC 27002:2013中规定的控制，实施指南和其他信息适用。

6.6.4.2 安全登录规程

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适用：

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，组织应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

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

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。

组织应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。组织还应向客户提供相应的信息以帮助客户应用自己的加密保护。

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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：

组织应确保每当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，性能问题可能意味着明确删除该PII是不切实际的。这会产生另一个用户可以访问PII的风险。应通过具体的技术措施避免这种风险。

为了安全处置或再利用，可能包含PII的存储介质的设备应该被视为包含PII。

6.8.2.8 无人值守的用户设备

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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：

组织应将包含PII的硬拷贝材料的创建限制在满足所识别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，测试和运行环境的分离

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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

组织应制定策略，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）以及删除备份信息中包含的PII信息的任何进一步要求（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。组织应确保已向客户通知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，组织应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应证明符合这些要求。

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）。

组织应该有PII恢复工作的规程和日志。至少，PII恢复的日志应包含：

— 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。组织应该能够记录恢复日志的适当内容以符合辖区特定要求。此类审议的结论应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

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适用：

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

应该建立一个流程来使用连续的，手动或自动化的监控和警报流程来审查事件日志。审查应以明确的，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）。

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

PII处理者的实施指南：

组织应定义关于客户是否，何时以及如何确保日志信息可用的标准。这些标准应该提供给客户。

如果组织允许其客户访问组织控制的日志记录，组织应实施适当的控制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

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适用：

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。应采取措施控制访问（参见ISO/IEC 27002:2013,9.2.3），以确保记录的信息仅按预期使用。

应建立一个程序，最好是自动程序，以确保按照保留计划删除或去识别化记录信息（参见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 运行软件的控制

6.9.5.1 在运行系统上安装软件

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 技术脆弱性管理

6.9.6.1 技术脆弱性的管理

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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：

组织应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。

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 保密或不泄漏协议

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适用：

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

组织应确保在其控制下，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间长度。

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

6.11 系统的获取，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 公共网络上的应用服务的安全保护

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

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：

组织应确保在不受信任的数据传输网络上传输的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需要暴露一些报头或业务数据以进行有效传输。

6.11.1.3 应用服务事务的保护

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中规定的控制，实施指南和其他信息以及以下补充指南均适用。

ISO/IEC 27002:2013,14.2.1C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应该包含组织对处理PII需求的指导， 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应该考虑以下几个方面：

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

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中规定的控制，实施指南和其他信息以及以下附加补充适用：

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/或组件应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的PII处理目的所必需的（见7.2）。

例如，处理PII的组织应确保根据相关管辖区在指定期限后处置PII。处理该PII的系统应该设计相应功能以便于实施删除操作来满足要求。

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。

6.11.2.7 外包开发

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适用。

ISO/IEC 27002:2013,14.2.7外贸开发的补充指南是：

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

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

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

PII不应用于测试目的；应使用假的或合成的PII。如果无法避免将PII用于测试目的，则应实施与生产环境中使用的等效技术和组织措施，以最大限度地降低风险。如果这种等效措施不可行，则应进行风险评估，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

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中规定的控制，实施指南和其他信息适用于以下补充指南适用：

ISO/IEC 27002:2013，5.1.2在供应商协议中强调安全的补充实施指南是：

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

供应商协议应在考虑处理的PII种类的情况下，明确地在组织，其合作伙伴，供应商和适当的第三方（客户，供应商等）之间分配责任。

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/或法规的遵守情况。协议应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：

组织应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

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审查

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中规定的控制，实施指南和其他信息适用于以下补充指南使用：

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，组织应建立识别及记录违反PII的责任和规程。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）和向当局披露相关的责任和程序。

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

6.13.1.2 报告信息安全事态

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

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

ISO/IEC 27002:2013的16.1.5，信息安全事件的响应的补充实施指南是：

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的事件应引发组织的评审，以确定是否发生了涉及需要响应的PII的违规行为。

事件不一定会触发此类评审。

注1　信息安全事件不一定以高概率导致未经授权访问PII或存储PII的任何组织设备或设施。这些可以包括但不限于对

防火墙或边缘服务器的ping攻击和其他广播攻击，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时，响应规程应包括相关通知和记录。

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

通知应该是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，应保留一份记录，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，该记录还应包括已泄露的PII描述（如果已知）;如果需要实施通知，应采取措施通知PII主体，监管机构或客户。

PII处理者的实施指南

涉及PII违约通知的规定应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主体引起的由其负责的系统组件的违规。合同还应定义预期和外部强制限制的通知响应时间。

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，应保留一份记录，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;

— 报告着的名字;

— 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，该记录还应包括已泄露的PII描述（如果已知）;如果执行了通知，则应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

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中规定的控制，实施指南和其他信息适用于以下补充指南：

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有关的任何潜在法律制裁（可能由于某些义务被遗漏而导致），包括直接来自当地监

管机构的巨额罚款。在某些司法管辖区，本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/ EC 27002:2013,18.1.3，中规定的控制，实施指南和其他信息适用于以下补充指南：

ISO/IEC 27002:2013的18.1.3，保护的记录的补充实施指南是：

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

组织应在其保留时间表中规定的期限内保留其隐私政策和相关规程的副本（请参阅7.4.7）。这包括在更新这些文档的先前版本时保留它们。

6.15.1.4 隐私和个人身份信息保护

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中规定的控制，实施指南和其他信息适用于以下补充指南：

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，并且个别客户审核不切实际或可能增加安全风险，组织应在订立合同之前，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。如果它涵盖预期用户的需求并且结果以足够透明的方式提供，组织选择的相关独立审核通常可以满足客户审核组织处理相关操作的关注点。

6.15.2.2 符合安全政策和标准

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中规定的控制，实施指南和其他信息以及以下补充指南适用：

ISO/IEC 27002:2013,18.2.3，技术符合性评审的补充指南是：

作为遵守安全策略和标准的技术评审的一部分，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：

— 持续监控以确认只进允许的处理可以实施;和/或

— 特定的渗透或漏洞测试（例如，去识别化数据集可以应对有动机的入侵测试，以验证去识别化方法是否符合组织要求的）。

7 针对PII控制者的补充ISO/IEC 27002指南

7.1 总论

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：根适用的司法管辖区要求，以明确界定的且合法的目的以及明确的法律为依据确定并记录相关处理是合法的。

7.2.1 识别并记录目的

控制

组织应识别并记录PII处理的特定目的。

实施指南

组织应确保PII主体了解其PII处理的目的。组织有责任向PII主体明确记录并传达此信息。如果没有明确说明处理目的，就不能充分给予准许和选择。

记载处理PII目的的文件应足够清晰和详细，以便可用于向PII主体提供的所需信息（见7.3.2）。这包括需要获得准许所需的信息（见7.2.3），以及政策和规程的记录（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 确定法律依据

控制

为了所识别的目的，组织应确定，记录并遵守处理PII的相关法律依据。

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的法律依据包括：

— PII主体的准许;

— 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。

组织应记录每个PII处理活动的法律依据（参见7.2.8）.

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

无论何时应根据PII的性质（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，且组织应在其分类方案中包括这些类别的PII。

属于这些类别的PII分类可能因司法管辖区而异，并且可能因适用于不同类型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准许。

7.2.3 确定何时以及如何获得准许

控制

组织应确定并记录一个过程，通过该过程，证明是否，何时以及如何从PII主体获得PII处理的准许。

实施指南

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

某些司法管辖区对如何收集和记录准许具有特定要求（例如，未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。组织应考虑此类要求并记录准许机制是如何满足这些要求的。

7.2.4 获得并记录准许

控制

组织应根据文件化的流程获得并记录PII主体的准许。

实施指南

组织应根据请求提供所需准许的详细信息，以便获得PII主体的准许（例如，提供准许的时间，PII主体的身份和准许声明）。

在准许过程之前提交给PII主体的信息应遵循在7.3.3的指导。

准许应该是：

— 自由地给予;

— 根据处理的目的而异;和

— 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，组织应评估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。应通过隐私影响评估来评估这些风险。某些司法管辖区定义了要求进行隐私影响评估的情况。标准可包括对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。

组织应确定完成隐私影响评估所必需的要素。这些可以包括已处理的PII类型的列表，存储PII的位置以及可以被传输到的位置。在这种情况下，数据流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，这些信息可以帮助通知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

组织应与其使用的任何PII处理者签订书面合同，合同应确保在附录B中规定的适当控制得到实施。

实施指南

组织与代表其处理PII的任何PII处理者之间签订的合同应要求实施附录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处理者执行的PII处理范围（见6.12）的考虑基础上。默认情况下，附录B中所有相关的控制都应备考虑。如果组织决定不要求PII处理者实现附录B中的某些控制，应明确不实施的理由。（见5.4.1.3）。

合同可以分别定义各自的责任，但为了与本标准持一致，应考虑所有控制并将其包含在文档化信息中。

7.2.7 联合PII控制者

控制

组织应确定与任何联合PII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的角色和责任应以透明方式确定。

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

联合PII控制者协议可以包括（此列表既不是最终的也不是详尽的）：

— PII共享/联合PII控制者关系的目的;

— 识别作为联合PII控制者关系中的组织（PII控制者）的身份;

— 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主体提供有关联合PII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;和

— 给PII主体的联络点。

7.2.8 与处理PII控制有关的记录

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已经或将要披露的接受者类别，包括第三国或国际组织的接受者;

— 技术和组织安全措施的通用描述;和

— 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

组织应确定并记录其对于PII主体的与PII处理其PII相关的法律，监的管义务，并提供履行这些义务的方式。

实施指南

PII主体的义务及其支持手段因司法管辖区而异。

组织应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。应向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。

联系点应以与收集PII和准许相似的方式提供（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 确定提供给PII主体的信息

控制

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。

实施指南

组织应确定法律，法规和/或业务要要以明确向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等）以及提供信息类型。

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主体如何撤回准许的信息;

— 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，组织定义的频率等）。

如果更改或扩展PII处理的目的，组织应提供最新信息。

7.3.3 向PII主体提供信息

控制

组织应向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

组织应向PII主体提供7.3.2中的详细信息。并要求使用清晰明了的语言，以及时，简洁，完整，透明，易懂和易于访问的形式，明确的目标受众以向PII主体提供。

在适当的情况下，应在收集PII时提供信息。它也应该是永久可访问的。

注　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　提供修改或撤销准许的机制

控制

组织应为PII主体提供修改或撤销其准许的机制。

实施指南

组织应告知PII主体其可在任何时间撤销准许（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;它应该与获得准许的机制保持一致。例如，如果通过电子邮件或网站收集准许，则撤销它时机制应该与其相同，而不是电话或传真等替代解决方案。

修改准许可以包括对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准许施加了限制

组织应以与记录准许相类似的方式记录撤回或更改准许的任何请求

任何准许的更改应传达到适当的系统，授权用户和相关第三方。

组织应该定义响应时间，并且应该根据它来处理请求。

附加信息

当撤销对特定PII处理的准许时，通常应认为在撤回之前进行的所有PII处理都是适当的，但这种处理的结果不应用于新处理。例如，如果PII主体撤回其对概况信息的准许，则不应进一步使用或咨询其概况信息。

7.3.5　提供反对PII处理的机制

控制

组织应为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/或法规约束的组织应确保他们采取适当措施使PII主体能够行使这一权利。

组织应记录与PII主体反对处理相关的法律和监管要求（例如，反对准对PII处理以直接营销为目的而使用）。组织应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，但应与所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/或擦除

控制

组织应实施政策，程序和/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

组织应实施策略，程序和/或机制，以使PII主体能够在没有不当延迟的情况下获取，纠正和擦除其PII。

组织应该定义响应时间，并且应该根据它来处理请求。

任何更正或擦除都应通过系统和/或授权用户传达，并应传递给PII已传递到的第三方。

注　由7.5.3相关规定产生的控制可以在这方面提供帮助。

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

某些司法管辖区对PII主体何时以及如何要求更正或擦除其PII施加限制。组织应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

组织应通知共享PII的第三方有关共享PII的任何修改，撤回或异议，并实施适当的政策，流程和/或机制予以实现。

实施指南

组织应该应用适当技术，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。

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

注　对PII主体的义务所产生的变更可包括修改或撤销准许，纠正请求，删除或处理限制，或对PII主体要求的关于PII处理的异议。

7.3.8　提供PII处理者的副本

控制

当PII主体要求是，组织应该能够提供其处理的PII的副本。

实施指南

组织应提供PII的副本，该副本以PII主体可访问的结构化，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一些组织应提供PII副本的情况，这些情况要求以允许PII主体或接收方PII控制者可移植性的格式提供（通常是结构化的，常规的和机器可读的）。

组织应确保提供给PII主体的任何PII副本仅与该PII主体相关。

如果已根据保留和处置政策（如7.4.7中所述），所请求的PII已经被删除了，PII控制者应通知PII主体已经删除了所请求的PII。

如果组织不再能够识别PII主体（例如，由于去识别化过程），组织不应仅以此为理由寻求（重新）识别PII主体。但是，在某些司法管辖区，合法请求可能要求从PII主体请求其他信息，以便重新识别和随后的披露。

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

组织应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）。

请求应在适当的定义响应时间内处理。

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

7.3.10 自动决策的制定

控制

组织应识别并明确对于PII主体的义务（包括法律义务），这些义务是由组织做出的决定产生且基于PII主体有关的PII自动处理。

实施指南

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

注：在某些司法管辖区，某些PII处理无法完全自动化。

在这些司法管辖区运营的组织应考虑到这些义务。

7.4 设计的隐私和默认的隐私

目标：确保设计流程和系统，使收集和处理（包括使用，披露，保留，传输和处置）仅限于所识别目的所必需的。

7.4.1 限制收集

控制

组织应将PII的收集限制在与所识别目的相关性，比例和必要性的最小值。

实施指南

组织应将PII的收集限制在与所识别目的充分的，相关的和必要的范围内。这包括限制组织间接收集的PII数量（例如，通过Web日志，系统日志等）。

默认的隐私意味着，如果有收集和处理已存在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主体的明确选择来启用。

7.4.2 限制处理

控制

组织应将PII的处理限制在对于所识别的目的而言是足够，相关和必要的处理。

实施指南

限制PII的处理应通过信息安全和隐私政策进行管理（见6.2），同时应建立文件化的流程以满足其选择以及合规。

PII的处理包括：

— 披露;

— PII存储期;和

— 谁能够访问他们的PII;

应默认限制为相对于所识别目的所需的最小值。

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

组织应实施政策，程序和/或机制，以尽量减少其处理的PII中的不准确性。还应该有政策，程序和/或机制来应对不准确的PII实例。这些政策，程序和/或机制应包含在记录的信息中（例如通过技术系统配置等），并应适用于整个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

组织应定义和记录数据最小化目标，以及使用哪些机制（例如去识别化）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数量相对于所识别目的是如何受限的。这可以包括使用去识别化或其他数据最小化技术。

所识别的目的（见7.2.1）可以要求处理尚未被识别的PII，在这种情况下，组织应该能够描述这种处理。

在其他情况下，所识别的目的不需要处理原始PII，并且已经去识别化的PII的处理足以实现所识别的目的。

在这些情况下，组织应定义并记录PII需要与PII主体相关联的程度，以及用于处理PII的机制和技术，这样去标识化和/或PII最小化的目标得以实现。

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

如果处理去识别化数据足以达到目的，组织应定时记录旨在实现组织设定的去识别目标的任何机制（技术系统配置等）。例如，删除与PII主体相关联的属性可足以使组织实现其所识别化的目的。在其他情况下，可以使用其他去识别技术，例如泛化（例如四舍五入）或随机化技术（例如，噪声添加）来实现足够的去识别化水平。

注1：有关去识别化技术的更多信息，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符的定义，可用于对数据识别为PII主体或将PII主体与PII中的一组特征相关联的程度进行分类。

7.4.5 PII在处理结束时去识别化和删除

控制

一旦原始PII不再需要用于所识别的目的，组织应该删除PII或以不允许识别或重新识别PII主体的形式呈现它。

实施指南

组织应该有机制在没有预期进一步处理时删除PII。或者，可以使用一些去识别化技术以达到去识别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

组织应确保按照在指定期限的文件化处理规程（例如删除或销毁），来由于处理PII而创建的临时文件。

实施指南

组织应定期检查在指定的时间段内未使用的临时文件已被删除。

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。此类文件特定于系统或应用程序，但可包括与数据库更新和其他应用程序软件操作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总是确定的，但“垃圾收集”程序应识别相关文件并确定自上次使用以来已经存在多长时间。

7.4.7 保留

控制

组织不应保留PII的时间超过处理PII目的所需的时间。

实施指南

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

表中记录。

7.4.8 处置

控制

组织应具有处置PII的文件化策略，规程序和/或机制。

实施指南

PII处理技术的选择取决于许多因素，因为处置技术的性质和结果不同（例如，由此得到的物理介质的粒度，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

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

实施指南

需要控制PII的传输，通常是通过确保只有经过授权的个人可以访问传输系统，并遵循适当的流程（包括保留审核日志）来确保PII的传输不会损害正确的接收者。

7.5 PII共享，传输和披露

目标：确定是否并记录何时共享PII，传输到其他司法管辖区或第三方和/或根据适用义务披露。

7.5.1 识别司法管辖区之间PII传输的基础

控制

组织应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）。组织应记录对作为传输基础的要求的遵守情况。

某些司法管辖区可以要求指定的监管机构审查信息转让协议。在这些司法管辖区运营的组织应了解任何此类要求。

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

7.5.2 PII可以传输至的国家和国际组织

控制

组织应指定并记录PII可以传输至的国家和国际组织。

实施指南

在正常运营中，PII可能被传输至的国家和国际组织的身份应该对用户可用。应包括使用分包PII处理产生的国家的身份。所包含国家的考虑应涉及7.5.1。

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

7.5.3 PII传输的记录

控制

组织应记录PII向第三方的传输，并确保与各方的合作。作为对PII主体的义务，组织应支持PII主体未来的请求。

实施指南

记录可以包括来自第三方传输的PII，而该PII由于PII控制者具有管理义务而被修改，或转让给第三方以实施来自PII主体的合法请求，包括删除PII的请求（例如，在准许撤回后）。

组织应该有一个策略来定义这些记录的保留期间。

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的PII披露，包括已披露的PII，向谁和在何时披露。

实施指南

PII可以在正常操作过程中披露。应记录这些披露。还应记录对第三方的任何其他披露，例如合法调查或外部审核所产生的披露。记录应包括披露的来源和进行披露的批准来源。

8 针对PII处理者的补充ISO/IEC 27002指南

8.1 总则

第6条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

组织应在相关时确保处理PII的合同能够明确组织在客户义务辅助方面的作用（应考虑处理的性质和对组织

可用的信息）。

实施指南

组织与客户之间的合同应包括以下相关内容，并取决于客户的角色（PII控制者或PII处理者）（此列表既不是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）;和

— 如果需要事先应与相关PII保护机构进行协商，以确定PII处理者需要提供的协助。

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

组织应确保代表客户处理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达到的目标和时间范围。

为了实现客户的目的，可能存在技术原因，比如组织确定处理PII的方法是否合适，与客户的通用指令一致而不是客户的专门指令。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任何分包商不会出于其他目的而仅出于客户书面说明中所表达的目的来处理PII。

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，组织不应使用合同下处理的PII进行营销和广告。组织不应将提供此类准许作为接收服务的条件。

实施指南

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

如果未经PII主体明确同意，组织不应坚持包含营销和/或广告用途。

注　此控件是对通用控制8.2.2的补充，而不是替换或者取代。

8.2.4 侵权指令

控制

如果在组织看来，处理指令违反了适用法律和/或法规，组织应通知客户。

实施指南

组织验证指令是否违反法律和/或法规的能力取决于技术背景，指令本身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，以便客户证明其履行义务。

实施指南

客户所需的信息可包括组织是否允许客户或由客户授权或以其他方式准许的其他审核员进行的审核。

8.2.6 与处理PII有关的记录

控制

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

实施指南

某些司法管辖区可要求组织记录以下信息：

— 代表每个客户进行的处理类别;

— 传输到第三国或国际组织;和

— 技术和组织安全措施的通用描述。

8.3 对于PII主体的义务

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。

8.3.1 对于PII主体的义务

控制

组织应为客户提供遵守与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。这些义务包括客户使用组织服务来履行的义务。例如，这可以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促进履行对PII主体的义务，则应在合同中规定相关信息或技术措施。

8.4 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）仅限于所识别目的的所必需的。

8.4.1 临时文件

控制

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

实施指南

组织应定期验证在指定的时间段内未使用的临时文件已被删除。

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。此类文件特定于系统或应用程序，但可包括与数据库更新和其他应用程序软件操作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总是确定的，但“垃圾收集”程序应识别相关文件并确定自上次使用以来已经存在多长时间。

8.4.2 退回，传输或处置PII

控制

组织应提供以安全的方式退回，传输和/或处置PII的能力。它还应该向客户提供其政策。

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退回给客户，将其传输给另一个组织或PII控制者（例如，由于合并），删除或以其他方式销毁，去识别化或存档。应以安全的方式管理退回，传输和/或处置PII的能力。

组织应提供必要的保证，以使客户能够确保根据合同，处理的PII（由组织及其任何分包商）已从存储的场所删除，包括为了备份和业务连续性的场所。当它们不再为客户所识别的目的所必需，应立即执行删除。

组织应制定并实施有关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后处置之前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

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

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。传输控制的要求可以包含在PII处理与客户的合同中。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：确定是否并记录何时共享PII，传输到其他司法管辖区或第三方和/或根据适用义务披露PII。

8.5.1 管辖区之间PII传输的基础

控制

组织应及时告知客户管辖区之间的PII传输的法律基础以及此方面的任何预期更改，以便客户能够反对此类更改或终止合同。

实施指南

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（以及它来自何处）。组织应记录对于传输的法律基础的要求的遵守情况。

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

组织与客户之间的协议可以包含组织可以在不通知客户的情况下实施更改的条款。在这些情况下，应设置此限制范围（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）。

在国际传输PII的情况下，应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，以及在相关国家中于此类似的情况的有关协议。

8.5.2 PII可以传输至的国家和国际组织

控制

组织应指定并记录PII可能会被传输至的国家和国际组织。

实施指南

在正常运营中，PII可能被传输至的国家和国际组织的身份应该对用户公开。应包括使用分包PII处理产生的国家身份。所包含的国家的考虑应涉及8.5.1。

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

8.5.3 向第三方披露PII的记录

控制

组织应记录向第三方的PII披露，包括已披露的PII，向谁和何时披露。

实施指南

PII可以在正常操作过程中公开。应记录这些披露。还应记录对第三方的任何其他披露，例如合法调查或外部审核所产生的披露。记录应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

组织应通知客户任何具有法律约束力的披露PII的请求。

实施指南

组织可能收到具有法律约束力的披露PII的请求（例如来自执法机构）。在这些情况下，组织应在约定的时间范围内并根据商定的规程（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任何人（可能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

组织应拒绝任何不具有法律约束力的PII披露请求，在进行任何PII披露之前应询问客户，并接受那些已经通过客户授权且记录在合同中的纰漏请求。

实施指南

与控制实施相关的细节可以包含在客户合同中。

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

8.5.6 处理PII的分包商的披露

控制

在使用之前组织向客户告知使用分包商以处理PII的情况。

实施指南

使用分包商处理PII的规定应包括在客户合同中。

披露的信息应涵盖在合同中，合同中应包括分包商的使用的事实以及相关分包商的名称。披露的信息还应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）以及分包商有义务履行或被强制实施的超越组织义务的手段（见8.5.7）.

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

这与PII可以传输至的国家名单无关。该清单应在传达给客户，且在任何情况下允许他们通知相应PII主体。

8.5.7 分包商处理PII的参与

控制

组织应仅根据客户合同聘请分包商处理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，也可以是特定的“一次性”协议。

组织应与其用于代表其进行PII处理的任何分包商签订书面合同，并应确保其与分包商的合同涉及实施在附录B中相应的控制措施。

组织与代表其处理PII的任何分包商之间的合同应要求分包商实施附录B中相应的控制措施。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中指定的所有控制应该被认为是相关的。如果组织决定不要求分包商实施附录B中的某个控制，应证明它被排除在外的正确定。

合同可以分别定义每个相关方的责任，但为了与本标准保持一致，应考虑所有控制并将其包含在记录的信息中。

8.5.8 分包商处理PII的变更

控制

在获得通用书面授权的情况下，组织应将有关添加或更换处理PII的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

如果组织更改处理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更改。这可以是客户合同中适当条款的形式，也可以是特定的“一次性”协议。

附录A

（规范性附录）

PIMS特定的参考控制目标和控制（PII控制者）

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。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。

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。

表A.1 - 控制目标和控制

A.7.2收集和处的理条件 目标：根适用的司法管辖区要求，以明确界定的且合法的目的以及明确的法律为依据确定并记录相关处理是合法的。		
A.7.2.1	识别并记录目的	控制 组织应识别并记录PII处理的特定目的。
A.7.2.2	确定法律依据	控制 为了所识别的目的，组织应确定，记录并遵守处理PII的相关法律依据。
A.7.2.3	确定何时以及如何获得准许	控制 组织应确定并记录一个过程，通过该过程，证明是否，何时以及如何从PII主体获得PII处理的准许。
A.7.2.4	获得并记录准许	控制 组织应根据文件化的流程获得并记录PII主体的准许。
A.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，组织应评估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	控制 组织应与其使用的任何PII处理者签订书面合同，合同应确保在附录B中规定的适当控制得到实施。

表A.1（续）

A.7.2.7	联合PII控制者	控制 组织应确定与任何联合PII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	处理PII控制有关的记录	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。
A.7.3对PII主体的义务 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。		
A.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于PII主体的与PII处理其PII相关的法律，监的管义务，并提供履行这些义务的方式
A.7.3.2	确定提供给PII主体的信息	控制 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	控制 组织应向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	提供修改或撤销准许的机制	控制 组织应为PII主体提供修改或撤销其准许的机制。
A.7.3.5	提供反对PII处理的机制	控制 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/或擦除	控制 组织应实施政策，程序和/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。
A.7.3.7	PII控制者告知第三方的义务	控制 组织应通知共享PII的第三方有关共享PII的任何修改，撤回或异议，并实施适当的政策，流程和/或机制予以实现。
A.7.3.8	提供PII处理者的副本	控制 当PII主体要求是，组织应该能够提供其处理的PII的副本。
A.7.3.9	处理请求	控制 组织应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	自动决策的制定	控制 组织应识别并明确对于PII主体的义务（包括法律义务），这些义务是由组织做出的决定产生且基于PII主体有关的PII自动处理。

表A.1（续）

A.7.4设计的隐私和默认的隐私 目标：确保设计流程和系统，使收集和处理（包括使用，披露，保留，传输和处置）仅限于所识别目的所必需的		
A.7.4.1	限制收集	控制 组织应将PII的收集限制在与所识别目的的相关性，比例和必要性的最小值。
A.7.4.2	限制处理	控制 组织应将PII的处理限制在对于所识别的目的而言是足够，相关和必要的处理。
A.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。
A.7.4.4	PII最小化目标	控制 组织应定义和记录数据最小化目标，以及使用哪些机制（例如去识别化）来实现这些目标。
A.7.4.5	PII在处理结束时的去识别化和删除	控制 一旦原始PII不再需要用于所识别的目的，组织应该删除PII或以不允许识别或重新识别PII主体的形式呈现它。
A.7.4.6	临时文件	控制 组织应确保按照在指定期限的文件化处理规程（例如删除或销毁），来由于处理PII而创建的临时文件。
A.7.4.7	保留	控制 组织不应保留PII的时间超过处理PII目的所需的时间。
A.7.4.8	处置	控制 组织应具有处置PII的文件化策略，规程序和/或机制。
A.7.4.9	PII传输	控制 组织应对通过数据传输网络传输（例如发送到另一个组织）的PII进行适当的控制，以确保数据到达其预定目的地。
A.7.5 PII共享，传输和披露 目标：确定是否并记录何时共享PII，传输到其他司法管辖区或第三方和/或根据适用义务披露。		
A.7.5.1	识别司法管辖区之间PII传输的基础	控制 组织应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	控制 织应指定并记录PII可以传输至的国家和国际组织。

表A.1（续）

A.7.5.3	PII传输的记录	控制 组织应记录PII向第三方的传输，并确保与各方的合作。作为对PII主体的义务，组织应支持PII主体未来的请求。
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的PII披露，包括已披露的PII，向谁和在何时披露。

附录B.

（规范性附录）

PIMS特定的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的并与之一致，并在ISO/IEC 27001:2013,6.1.3的优化内容5.4.1.3的情景下使用。

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。

表B.1 - 控制目标和控制

B.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。		
B.8.2.1	客户协议	控制 组织应在相关时确保处理PII的合同能够明确组织在客户义务辅助方面的作用（应考虑处理的性质和对组织可用的信息）。
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	控制 没有事先获得相应PII主体的同意，组织不应使用合同下处理的PII进行营销和广告。组织不应将提供此类准许作为接收服务的条件。
B.8.2.4	侵权指令	控制 如果在组织看来，处理指令违反了适用法律和/或法规，组织应通知客户。
B.8.2.5	顾客义务	控制 组织应向客户提供适当的信息，以便客户证明其履行义务。

表B.1（续）

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，以支持证明其代表客户处理PII的义务（如适用的合同中所规定的那样）。
B.8.3对PII负责人的义务 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。		
B.8.3.1	对PII主体的义务	控制 组织应向客户提供履行与PII原则相关的义务的方法。
B.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）仅限于所识别目的所必需的。		
B.8.4.1	临时文件	控制 组织应确保在指定的记录期内按照文件化程序处理（例如删除或销毁）由于处理PII而创建的临时文件。
B.8.4.2	退回，传输或处置PII	控制 组织应提供以安全的方式退回，传输和/或处置PII的能力。它还应该向客户提供其政策。
B.8.4.3	PII传输控制	控制 组织应对通过数据传输网络传输的PII进行适当的控制，以确保数据到达其预定目的地。
B.8.5 PII共享，传输和披露 目标：确定是否并记录何时共享PII，传输到其他司法管辖区或第三方和/或根据适用义务披露PII。		
B.8.5.1	管辖区之间PII传输的基础	控制 组织应及时告知客户管辖区之间的PII传输的法律基础以及此方面的任何预期更改，以便客户能够反对此类更改或终止合同。
B.8.5.2	PII可以被传输至的国家和国际组织	控制 组织应指定并记录PII可能会被传输至的国家和国际组织。
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	控制 组织应通知客户任何具有法律约束力的披露PII的请求。

表B.1（续）

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有法律约束力的PII披露请求，在进行任何PII披露之前应询问客户，并接受那些已经通过客户授权且记录在合同中的纰漏请求。
B.8.5.6	处理PII的分包商的披露	控制 在使用之前组织向客户告知使用分包商以处理PII的情况。
B.8.5.7	分包商处理PII的参与	控制 组织应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	控制 在获得通用书面授权的情况下，组织应将有关添加或更换处理PII的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。

附录C

（信息提供）

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。本附录以纯粹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控制者的控制和ISO/IEC 29100的映射

ISO/IEC 29100的隐私原则	PII控制者的相关控制
1.准许和选择	A.7.2.1 识别并记录目的 A.7.2.2 确定法律基础 A.7.2.3 确定何时以及如何获得准许 A.7.2.4 获得并记录准许 A.7.2.5 隐私影响评估 A.7.3.4 提供修改或撤销准许的机制 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 确定法律基础 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
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 PII在处理结束时的去识别化和删除
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在处理结束时的去识别化和删除 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

表C.1（续）

ISO / IEC 29100的隐私原则	PII控制者的相关控制措施
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处理者的副本 A 7.3.9 处理请求
9.问责	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传输的记录
10.信息安全	A 7.2.6 与PII处理者的合同 A 7.4.9 PII传输
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的隐私原则	PII处理者的相关控制措施
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的分包商的披露 B.8.5.7 分包商处理PII的参与 B.8.5.8 分包商处理PII的变更
8.个人参与和访问	B.8.3.1 对于PII主体的义务
9.问责	B.8.2.6 与处理PII有关的记录 B.8.4.2 退回，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可以被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.

（信息提供）
与GDPR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到GDPR的映射

本标准的章节	GDPR章节
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)

表*D.1（续）*

本标准的章节	GDPR章节
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)

表*D.1（续）*

本标准的章节	GDPR章节
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.

(信息提供)

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。

本附录是指示性的，不应该假设具有映射关系的条款之间意味着等同。

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

本标准的条款	ISO/IEC 27018中的子条款	ISO/IEC 29151中的子条款
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

表*E.1（续）*

本标准的条款	ISO/IEC 27018中的子条款	ISO/IEC 29151中的子条款
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

表*E.1（续）*

本标准的条款	ISO/IEC 27018中的子条款	ISO/IEC 29151中的子条款
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.

(信息提供)

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

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	本标准（扩展）
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准则，包括：

1) 风险接受准则;和

2) 执行信息安全和隐私风险评估的准则;

b) 确保重复的信息安全和隐私风险评估产生一致的，有效的和可比较的结果;

c) 识别信息安全和隐私风险：

1) 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体系范围内的信息的机密性，完整性和可用性损失有关的风险;和

2) 识别风险责任人;

d) 分析信息安全和隐私风险;

1) 评估6.1.2 c）中确定的风险发生后，可能导致的潜在后果;

2) 评估6.1.2 c）1）中确定的风险发生的可能性;和

3) 确定风险级别;

e) 评估信息安全和隐私风险：

1) 将风险分析结果与6.1.2 a）中确定的风险准则进行比较;和

2) 为风险处置排序已经分析风险的优先级。

组织应保留有关信息安全和隐私风险评估过程的文件化信息。

参考书目

[1] ISO / IEC 19944，信息技术 - 云计算 - 云服务和设备：数据流，数据分类和数据使用

[2] ISO/IEC 20889，隐私增强数据去识别化术语和分类技术

[3] ISO/IEC 27005，信息技术 - 安全技术 - 信息安全风险管理

[4] ISO/IEC 27018，信息技术 - 安全技术 –作为PII处理者在公有云中个人可识别信息（PII）的保护实践准则

[5] ISO/IEC 27035-1，信息技术 - 安全技术 - 信息安全事件管理 - 第1部分：事件管理原则

[6] ISO/IEC 29101，信息技术 - 安全技术 - 隐私结构框架

[7] ISO/IEC 29134，信息技术 - 安全技术 - 隐私影响评估指南

[8] ISO/IEC 29151，信息技术 - 安全技术 – 个人可识别信息保护的实践准则

[9] ISO/IEC/DIS 29184，信息技术 - 安全技术 - 在线隐私通知和准许的指南