ISO IEC 27701-2025 中文版

信息安全、网络安全和隐私保护——隐私信息管理系统 — 要求和指导

信息安全、网络安全和隐私 - 隐私管理系统 - 要求和建议

国际 标准

ISO/IEC 27701 标准

再版

2025-10

受版权保护的文档

C ISO/IEC 2025 标准

ISO版权局

CP 401-Ch.de 布兰多内特 8

CH-1214 游标，日内瓦

电话：+41227490111

Email:copyright@iso.org

网站： www.iso.org

出版于瑞士

目录

页面

前言 V
介绍 ..... 六
1 范围 1
2 规范性参考文献 1
3 术语、定义和缩写 1
4 组织背景 4
4.1 了解组织及其背景 4
4.2 了解相关方的需求和期望 5
4.3 确定隐私信息管理体系的范围 5
4.4 隐私信息管理系统 6
5 领导力 6
5.1 领导力和承诺 6
5.2 隐私政策 6
5.3 角色、职责和权限 7
6 规划 7
6.1 应对风险和机遇的行动 7
6.1.1 一般规定 7
6.1.2 隐私风险评估员 7
6.1.3 隐私风险处理 8
6.2 隐私目标和实现这些目标的计划 9
6.3 变更规划 10
7 **支持器** 10
7.1 资源 10
7.2 能力 10
7.3 感知者 10
7.4 沟通 10
7.5 记录信息 11
7.5.1 一般规定 11
7.5.2 创建和更新记录的信息 11
7.5.3 记录信息的控制 11
8 歌剧tion 12
8.1 运营规划与控制 12
8.2 隐私风险评估员 12
8.3 隐私风险处理 12
9 绩效评估 12
9.1 监测、测量、分析与评价 12
9.2 内部审计 13

9.2.1 一般规定 13
9.2.2 内部审计方案 13
9.3 管理审查 13
9.3.1 一般规定 13
9.3.2 管理审查 13
9.3.3 管理审查结果 14
10 改进者 14
10.1 持续改进 14
10.2 不合格项和纠正措施 14
11 关于附件的进一步资料 14
附件A（规范性）PIMS参考控制目标和PII控制者和PII的控制处理器 15

附件B（规范性） PII控制器和PII处理器的实施指南 21
附录 C（信息性）与 ISO/IEC 2910 的映射 51
附件 D（信息性）与《通用数据保护条例》的映射 53
附录E（信息性）与ISO/IEC 27018和ISO/IEC2915的映射 56
附录 F（信息性）与 ISO/IEC 27701：2019 的对应关系 58
书目 64

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体系。作为 ISO 或 IEC 成员的国家机构通过各自组织设立的技术委员会参与国际标准的制定，以处理特定的技术活动领域。ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。其他国际组织，包括政府和非政府组织，与 ISO 和 IEC 联络，也参与了这项工作。

用于制定本文件的程序以及用于进一步维护的程序在 ISO/IEC 指令第 1.In 部分中进行了描述，特别是应注意不同类型文件所需的不同批准标准。本文档是根据 ISO/IEC 指令第 2 部分的编辑规则起草的（参见 www.iso.org/directives 或 www.iec.ch/members experts/refdocs）。

ISO 和 IEC 提请注意，本文件的实施可能涉及使用 （a） 专利。ISO 和 IEC 对任何与此相关的任何主张专利权的证据、有效性或适用性不持任何立场。截至本文件发布之日，ISO 和 IEC 尚未收到实施本文件可能需要的 （a） 专利通知。但是，请注意实施者，这可能不代表最新信息，这些信息可以从 www.iso.org/patents 和 https://patents.iec.ch 提供的专利数据库中获得 。 ISO 和 IEC 不负责识别任何或所有此类专利权。

本文档中使用的任何商品名称都是为方便用户而提供的信息，不构成认可。

有关标准自愿性质的解释、与合格评定相关的ISO特定术语和表述的含义，以及有关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 。 在 IEC 中，see www.iec.ch/understanding-standards。

本文件由联合技术委员会 ISO/IEC JTC 1，信息技术，*SC* 27 *小组，信息安全，网络安全和隐私保护*，与欧洲标准化委员会 （CEN） 技术委员会 CEN/CLC/JTC 13，网络安全和数据保护合作，根据 ISO 和 CEN 之间的技术合作协议（维也纳协议）编写。

第二版取消并取代了经过技术修订的第一版（ISO/IEC 27701：2019）。

主要变化如下：

一 该文件已重新起草为独立的管理体系标准。

对本文档的任何反馈或问题都应直接咨询用户的国家标准机构。这些机构的完整列表可以在 www.iso.org/members.html 和

www.iec.ch/national-committees .

介绍

0.1 一般

几乎每个组织都会处理个人身份信息（PII）。此外，处理的PII数量和类型也在增加，组织需要与其他组织合作处理PII的情况也在增加。在处理PII的背景下保护隐私是一项社会需求，也是全球范围内专门法律要求的主题。

本文档包括映射到：

— ISO/IEC 29100 中定义的隐私框架和原则;

— ISO/IEC 27018;

— ISO/IEC 29151;

— 欧盟通用数据保护条例。

注意：这些映射可以解释为考虑当地法律要求。

本文档可供PII控制者（包括联合PII控制者）和PII处理者（包括使用分包PII处理器的控制者以及作为 PII 处理者的分包商处理 PII 的处理者）使用。

通过遵守本文档中的要求，组织可以生成其如何处理PII处理的证据。此类证据可用于促进与业务合作伙伴达成协议，其中PII的处理是相互相关的。这也有助于与其他相关方建立关系。使用本文件可以对该证据进行独立验证。

0.2 与其他管理体系标准的兼容性

本文件应用 ISO 制定的框架，以提高其管理体系标准之间的一致性。

本文件使组织能够将其隐私信息管理体系（PIMS）与其他管理体系标准的要求保持一致或集成，特别是与ISO/IEC 27001中规定的信息安全管理体系保持一致或集成。

信息安全、网络安全和隐私保护——隐私信息管理体系——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系统 （PIMS） 的要求。

还提供了指导，以协助实施本文件中的要求。

本文档适用于对 PII 处理负有责任和问责的个人身份信息 （PII） 控制者和 PII 处理者。

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。

2 规范性参考文献

以下文件在正文中引用的方式是，其部分或全部内容构成本文件的要求。对于注明日期的参考文献，仅适用引用的版本。对于未注明日期的参考文献，适用参考文件的最新版本（包括任何修订）。

ISO/IEC 29100，信息技术—安全技术—隐私框架

3 术语、定义和缩写

就本文档而言，ISO/IEC 29100 和以下条款和定义适用。ISO 和 IEC

在以下地址维护术语数据库以用于标准化：

一 ISO在线浏览平台：可在 https://www.iso.org/obp

一 IEC 电子百科：可在 https://www.electropedia.org/

3.1

组织

具有自身职能的个人或群体，具有实现其目标的责任、权力和关系 （3.6）

条目注1：组织的概念包括但不限于个体经营者、公司、公司、商所、企业、当局、合伙企业、慈善机构或机构，或其部分或组合，无论是否注册成立，公共或私人。

条目注2：如果组织是较大实体的一部分，则术语“组织”仅指较大实体中属于隐私信息管理系统范围内的部分（3.23）。

3.2

利害关系方

个人或组织 （3.1） 可能影响、受决定或活动影响或认为自己受到决定或活动的影响

3.3

高层管理人员

在最高级别指挥和控制组织（3.1）的个人或一群人

条目注1：高层管理人员有权在组织内下放权力和提供资源。

注2：如果管理体系（3.4）的范围仅涵盖组织的一部分，则高层管理人员指那些指挥和控制组织该部分的人。

3.4

管理体系

组织（3.1）的一组相互关联或相互作用的元素，以制定政策（3.5）和目标（3.6）以及实现这些目标的流程（3.8）

条目注1：管理系统可以处理单个学科或多个学科。

条目注2：管理体系要素包括组织的结构、角色和职责、规划和运营。

3.5

政策

组织的意图和方向（3.1）由其高层管理人员正式表达（3.3）

3.6

目的

要取得的成果

条目注1：目标可以是战略性的、战术性的或作战性的。

条目注2：目标可以涉及不同的学科（例如金融、健康与安全、环境）。例如，它们可以是组织范围内的，也可以是特定于项目、产品或流程的（3.8）。

条目注3：目标可以用其他方式表达，例如作为预期结果、目的、作标准、隐私目标或使用具有相似含义的其他词语（例如目的、目标或目标）。

条目注4：在隐私信息管理体系（3.23）的背景下，隐私目标是由组织设定（3.1），与隐私政策（3.5）保持一致，以达到具体效果。

3.7

风险

不确定性的影响

条目注 1：效果是与预期的偏差——积极或消极。

条目注 2：不确定性是与事件、其后果或可能性相关的信息、理解或知识的缺乏状态，甚至是部分的。

条目注3：风险通常以潜在事件和后果或这些事件和后果的组合为特征。

条目注 4：风险通常以事件的后果（包括情况的变化）和相关发生可能性的组合来表示。

3.8

过程

使用或转换输入以交付结果的相互关联或交互的活动集

注1：一个过程的结果是称为输出、产品还是服务，取决于引用的上下文。

3.9

能力

应用知识和技能以达到预期结果的能力

3.10

记录信息

需要由组织控制和维护的信息 （3.1） 及其包含该信息的媒介

条目注 1：记录的信息可以采用任何格式和媒体，也可以来自任何来源。

条目注2：记录信息可以参考：

— 管理体系（3.4），包括相关流程（3.8）；

— 为组织运作而创建的信息（文档）；

— 取得成果的证据（记录）。

3.11

性能

可衡量的结果

条目注 1：性能可以与定量或定性结果有关。

条目注 2：绩效可以与管理活动、流程 （3.8）、产品、服务、系统或 *组织 （3.1） 有关*。

3.12

持续改进

用于提高性能的经常性活动 （3.11）

3.13

有效性

计划活动的实现和计划成果的实现程度

3.14

要求

陈述的需要或期望，通常是暗示的或强制性的

条目的注释 1：“一般隐含”是指组织 （3.1） 和相关方 （3.2）
的习惯或惯例是隐含所考虑的需求或期望。

条目注2：指定要求是指在文件化信息（3.10）中说明的要求。

3.15

整合

满足要求（3.14）

3.16

不合格

未满足要求 （3.14）

3.17

纠正措施

消除不合格原因的行动 （3.16） 并防止再次发生

3.18

审计

系统和独立的过程 （3.8）获取证据并客观评估以确定满足审计标准的程度

条目注1：审计可以是内部审计（第一方）或外部审计（第二方或第三方），也可以是联合审计（结合两个或多个学科）。

条目注 2：内部审计由组织本身 （3.1） 或由外部方代表其进行。

条目注3：“审核证据”和“审核标准”在ISO 19011中定义。

3.19

测量

过程（3.8）确定一个值

3.20

监测

确定系统、进程（3.8）或活动的状态

条目注1：要确定状态，可能需要检查、监督或批判性观察。

3.21

联合 PII 控制器

个人身份信息 （PII） 控制者，用于确定您与一个或多个其他 PII 控制者共同处理 PII 的目的和方式

3.22

客户

个人或组织 （3.1）能够或确实收到为该个人或组织准备或要求的产品或服务

示例消费者 、客户、最终用户、零售商、来自内部流程的产品或服务的接收者 （3.8），

受益人和购买者。

条目注 1：客户可以是组织内部的，也可以是组织外部的。

条目注 2：客户可以是与 PII 控制者签订合同的组织、与 PII 处理者签订合同的 PII 管理员或与分包商签订 PIIprocessing 合同的 PII 处理者。

3.23

隐私信息管理系统

PIMS

管理系统（3.4 ），解决可能受到个人身份信息处理影响的隐私保护问题

3.24

信息安全计划

一套政策 （3.5）、目标 （3.6） 和流程 （3.8） 旨在管理组织 （3.1） 资产的风险 （3.7），以确保信息的机密性、完整性和可用性

条目注1：例如，信息安全计划可以是信息安全管理体系，例如基于ISO/IEC 27001的信息安全管理体系。

3.25

适用性声明

所有必要控制措施的文件以及纳入或排除此类控制措施的理由

4 组织背景

4.1 了解组织及其背景

组织应确定与其目的相关并影响其实现其隐私信息管理系统预期结果的能力的外部和内部问题。

该组织应确定气候变化是否是一个相关问题。

该组织应确定其是充当 PII 控制者（包括作为联合 PII 控制者）还是作为 PII 处理者。

该组织应确定与其背景相关并影响其实现其 PIMS 预期成果的能力的外部和内部问题。

一 适用的隐私立法;

一 适用法规;

一、适用的司法判决;

一 适用的组织环境、治理、政策和程序;

一 适用的行政决定;

一 适用的合同要求。

如果组织同时担任两个角色（即 PII 控制者和 PII 处理者），则应确定单独的角色，每个角色都是一组单独控制的主题。

注 2：对于 PII 处理的每个实例，组织的作用可能不同，因为这取决于谁决定处理的目的和方式。

4.2 了解相关方的需求和期望

组织应确定：

一 与隐私信息管理系统相关的利害关系人;

一 这些利害关系人的相关要求;

一 这些要求中的哪一项将通过隐私信息管理系统得到满足。注1 相关方可以有与气候变化相关的要求。

该组织应将与 PII 处理相关的利益或责任的各方包括在其利益相关方中，包括 PII 委托人。

注 2：其他相关方可以包括客户、监管机构、其他 PII 控制者、PII 处理者及其分包商。

根据组织的角色，“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 3：这可能是作为联合 PII 控制者的组织的情况。

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

c） 与分包商签订 PII 处理合同的 PII 处理者（例如，您的分包 PII 处理者的客户）。

注4
在商业协会（例如，在消费者、员工、供应商、访客关系中）处理其个人信息的个人在本文档中称为“PII 委托人”。

注 5：与 PII 处理相关的要求可以由法律和监管要求、合同义务和自我强加的组织目标确定。ISO/IEC 29100 中规定的隐私原则提供了有关 PII 处理的指导。

注
6：为了证明符合组织的义务，一些相关方可以期望组织符合特定标准，例如本文档中规定的管理体系或任何相关规范集。这些各方可以要求经过独立审计的符合这些标准。

4.3 确定隐私信息管理体系的范围

组织应确定隐私信息管理系统的边界和适用性，以确定其范围。

在确定此范围时，组织应考虑：

— 4.1 中提到的外部和内部问题;

— 4.2 中提到的要求。

范围应作为书面信息提供。

在确定 PIMS 的范围时，组织应包括 PII 的处理。

4.4 隐私信息管理系统

组织应根据本文件的要求建立、实施、维护和持续改进隐私信息管理系统，包括所需的流程及其交互。

5 领导力

5.1 领导力和承诺

最高管理层应通过以下方式展示对隐私信息管理系统的领导力和承诺：

— 确保制定隐私政策（见 5.2）和隐私目标（见 6.2）并与组织的战略方向相一致;

- 确保将隐私信息管理系统要求集成到组织的业务流程中;

- 确保隐私信息管理系统所需的资源可用;

— 传达有效隐私信息管理和遵守隐私信息管理体系要求的重要性;

——确保隐私信息管理系统达到预期效果;

— 指导和支持人员为隐私信息管理系统的有效性做出贡献;

— 促进持续改进;

— 支持其他相关角色以展示他们的领导力，因为它应用了他们的责任领域。

注：本文档中对“业务”的提及可以广义地解释为指对组织存在的目的至关重要的那些活动。

5.2 隐私政策

最高管理层应制定隐私政策，包括：

a） 适合组织的宗旨;

b） 提供设定隐私目标的框架;

c） 包括满足适用要求的承诺;

d） 包括对持续改进隐私信息管理系统的承诺。隐私政策应：

——作为记录信息提供;

——在组织内部进行沟通;

——酌情提供给相关方。

5.3 角色、职责和权限

最高管理层应确保在组织内分配和传达相关角色的职责和权限。

最高管理层应分配以下责任和权限：

a） 确保隐私信息管理体系符合本文件的要求;

b） 向最高管理人员报告隐私信息管理体系的绩效。

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般规定

在规划隐私信息管理系统时，组织应考虑 4.1 中提到的问题和 4.2 中提到的要求，并确定需要解决的风险和机遇：

— 保证隐私信息管理系统能够达到其预期效果;

— 防止或减少不良影响;——

实现持续改进。

组织应计划：

a） 应对这些风险和机遇的行动;

b）如何

— 将这些行动整合并实施到其隐私信息管理体系流程中;——评估这些行动的有效性。

6.1.2 隐私风险评估

组织应定义并应用隐私风险评估流程，以：

a） 建立并维护隐私风险标准，包括：

1）风险接受标准;和

2）进行隐私风险评估的标准;

b） 确保重复的隐私风险评估产生一致、有效和可比的结果;

c） 识别隐私风险：

1）隐私信息管理体系范围内与隐私保护和信息安全风险相关的;和

2）确定风险所有者;

d）分析以下隐私风险：

1）评估如果 c）1） 中确定的风险成为现实，对组织和 PII 负责人造成的潜在后果;

2）评估c）1）中确定的风险发生的现实可能性和

3）确定风险水平;

e） 评估以下隐私风险：

1）将风险分析结果与a）中确定的风险标准进行比较;和

2）优先考虑分析的风险进行风险处理。

组织应保留有关隐私风险评估过程的书面信息。

注意有关隐私风险评估过程的更多信息，请参阅 ISO/IEC 27557。

6.1.3 隐私风险处理

组织应定义并应用隐私风险处理流程，以处理与 PII 处理相关的风险，包括 PII 委托人的风险，包括 PII 的安全性，具体方式：

a） 考虑风险评估结果，选择适当的隐私风险处理方案;

b） 确定实施所选隐私风险处理选项所需的所有控制措施;

注1 组织可以根据需要设计控制措施或从任何来源识别它们。

c） 确定并记录本组织实施的信息安全计划， 包括适当的安全控制措施;

信息安全计划至少应解决以下问题：

—信息安全风险管理;

——信息安全政策;

一 信息安全组织;——人力资源安全;

一、资产管理;—门禁;

一、运营安全;

—网络安全管理;——发展安全;

一、供应商管理;

一、事件管理;

——信息安全连续性;——
信息安全审查;

一 密码学;和

——物理和环境安全。

注 2：ISO/IEC 27002 提供了可能的信息安全控制措施的列表。如果信息安全计划基于 ISO/IEC 27001，则可以查阅 ISO/IEC 27002，以确保不会忽视必要的信息安全控制。

d）将上文b）和c）中确定的控制措施与附件A中的控制措施进行比较 _
，并核实没有遗漏任何必要的控制措施;

注3：附件A载有可能的隐私控制措施清单。 可以查阅附件A，以确保没有必要的隐私控制被忽视了。

注 4：附件 A 中列出的隐私控制并不详尽，如果需要，可以包括额外的隐私控制。

注 5：在考虑 PII 处理的安全性时，组织可以以综合方式解决信息安全和隐私问题，例如将信息安全和隐私风险评估结合起来，或者作为具有重叠领域的独立实体。

e） 制作一份适用性声明，其中包括：

——必要的控制（见 b），c] 和 d]];

— 纳入它们的理由;

— 是否实施必要的控制;和

——将任何控制措施排除在附件A之外的理由。

没有必要包括附件A中列出的所有控制措施。
例如，如果风险评估认为控制措施不必要，或者不受适用法律要求（包括适用于 PII 委托人的法律要求）的涵盖（或受例外情况的约束），则可以排除控制措施。

f） 制定隐私风险处理方案;

g） 获得隐私风险所有者对隐私风险处理方案的批准并接受您的剩余隐私风险;和

h）
考虑附件B中关于实施b）和c]中确定的控制措施的指导意见。组织应保留有关隐私风险处理过程的书面信息。

6.2 隐私目标和实现这些目标的计划

组织应在相关职能和级别建立隐私目标。

隐私目标应：

a）与隐私政策一致（见 5.2）；

b） 是可衡量的（如果可行）；

c） 考虑适用的要求;

d）被监控;

e） 被沟通;

f） 酌情更新;

g）作为记录信息提供。

在规划如何实现其隐私目标时，组织应确定：

— 将要做什么;

— 将需要哪些资源;

— 谁来负责;

— 何时完成;

——如何评估结果。

6.3 变更规划

当组织确定需要对隐私信息管理系统进行变更时，应有计划地进行变更。

7 客户支持

7.1 资源

该组织应确定并提供建立、实施、维护和持续改进隐私信息管理系统所需的资源。

7.2 能力

该组织应：

— 确定在其控制下从事影响其隐私信息管理绩效的人员的必要能力;

- 确保这些人在适当的教育、培训或经验的基础上胜任;

— 在适用的情况下，采取行动获得必要的能力，并评估所采取行动的有效性。

应提供适当的书面信息作为能力的证据。

注
适用的行动可以包括，例如：向现有受雇人员提供培训、指导或重新分配;或雇用或签订合格人员的合同。

7.3 意识

在组织控制下从事工作的人员应了解：

— 隐私政策（见 5.2）;

— 它们对隐私信息管理系统有效性的贡献，包括提高隐私绩效的好处;

— 不符合隐私信息管理体系要求的影响。

7.4 沟通

组织应确定与隐私信息管理系统相关的内部和外部通信，包括：

— 它将传达什么;

一、何时沟通;

— 与谁沟通;

— 如何沟通。

7.5 记录信息

7.5.1 一般规定

组织的隐私信息管理系统应包括：

a） 本文件要求的书面信息;

b） 组织确定为隐私信息管理系统有效性所必需的书面信息。

注意：隐私信息管理系统的记录信息范围可能因组织而异，原因如下：

一 组织规模及其活动类型、流程、产品和服务;

一 过程及其相互作用的复杂性;

一 人的能力。

7.5.2 创建和更新记录的信息

在创建和更新记录信息时，组织应确保适当：

——标识和描述（例如标题、日期、作者或参考号）；

—格式（例如语言、软件版本、图形）和媒体（例如纸质、电子）；

——审查和批准适用性和充分性。

7.5.3 记录信息的控制

隐私信息管理系统和本文档所需的书面信息应受到控制，以确保：

a） 随时随地可用且适合使用;

b） 它受到充分保护（例如，防止机密性丢失、使用不当或完整性丧失）。

为了控制记录在案的信息，该组织应在适用的情况下开展以下活动：

一 分发、访问、检索和使用;

一 储存和保存，包括保持易读性;

一 对变更的控制（例如版本控制）；

一 保留和处置。

组织确定为隐私信息管理体系规划和运营所必需的外部来源的书面信息，应适当地识别并加以控制。

注意 访问可能意味着关于仅查看记录信息的权限或查看和更改记录信息的权限和权限的决定。

8 手术

8.1 运营规划和控制

组织应通过以下方式规划、实施和控制满足要求所需的流程，并实施第 6 条中确定的行动：

— 制定流程标准；

— 按照标准对过程实施控制。

应在必要的范围内提供书面信息，以便确信这些过程已按计划进行。

组织应控制计划内的变更并审查意外变更的后果，必要时采取行动减轻任何不利影响。

组织应确保外部提供的与隐私信息管理系统相关的流程、产品或服务受到控制。

8.2 隐私风险评估

组织应按计划的时间间隔或在提议或发生重大变更时进行隐私风险评估，同时考虑到 6.1.2 a）中规定的标准。

组织应保留隐私风险评估结果的书面信息。

8.3 隐私风险处理

组织应实施隐私风险处理计划。

组织应保留隐私风险处理结果的书面信息。

9 绩效评估

9.1 监测、测量、分析与评价

组织应确定：

— 需要监测和测量的内容；

— 监测、测量、分析和评价方法（如适用），确保结果有效；

— 何时应进行监测和测量；

— 监测测量结果应当进行分析和评价。应提供书面信息作为结果的证据。

组织应评估隐私绩效和隐私信息管理系统的有效性。

9.2 内部审计

9.2.1 一般规定

组织应按计划的时间间隔进行内部审计，以提供有关隐私信息管理系统是否：

a） 符合：

一 组织自身对其隐私信息管理体系的要求;——本文件的要求;

b）得到有效实施和维护。

9.2.2 内部审计方案

该组织应规划、建立、实施和维护（一个）审计计划，包括频率、方法、职责、规划要求和报告。

在制定内部审计计划时，组织应考虑相关流程的重要性和以往审计的结果。

该组织应：

a） 确定每次审核的审核目标、标准和范围;

b） 选择审计师并进行审计，以确保审计过程的客观性和公正性;

c） 确保向相关管理人员报告审计结果。

应提供书面资料，作为审计方案执行情况和审计结果的证据。

9.3 管理审查

9.3.1 一般规定

最高管理层应按计划定期审查组织的隐私信息管理系统，以确保其持续适用性、充分性和有效性。

9.3.2 管理审查投入

管理审查应包括：

a） 先前管理审查的行动状态;

b） 与隐私信息管理系统相关的外部和内部问题的变化;

c） 与隐私信息管理系统相关的相关方的需求和期望的变化;

d） 有关隐私信息管理系统性能的信息，包括以下趋势：

——不合格和纠正措施;

——监测和测量结果;

一、审核结果;

e] 持续改进的机会。

9.3.3 管理评审结果

管理审查的结果应包括与持续改进机会和隐私信息管理系统任何需要更改的必要性相关的决定。

应提供书面信息作为管理审查结果的证据。

10 改进

10.1 持续改进

本组织应不断改进隐私信息管理系统的适用性、充分性和有效性。

10.2 不合格项和纠正措施

当发生不合格时，组织应：

a） 对不合格项做出反应，并在适用的情况下：

——采取行动控制和纠正它;

——处理后果;

b）评估是否需要采取行动消除不合格的原因，以免在其他地方再次发生或发生，方法是：

——审查不合格项;

一、确定不合格的原因;

——确定是否存在或可能发生类似的不合格项;

c） 实施任何需要的行动;

d）审查所采取的任何纠正措施的有效性;

e] 如有必要，对隐私信息管理系统进行更改。

纠正措施应适合遇到的不合格项的影响。

书面信息应作为以下证据：

——不合格项的性质和采取的任何后续行动;

一 任何纠正措施的结果。

11 关于附件的进一步资料

附录 C 包含本文档的规定与 ISO/IEC 29100 中的隐私原则之间的映射。

附件 D 包含本文档中控制措施与《欧盟通用数据保护条例》的映射。

附件E 包含本文档规定与ISO/IEC 27018和ISO/IEC 29151规定的映射。

附录 F 显示了本版 ISO/IEC 27701 与上一版 （ISO/IEC 27701：2019） 中的控制措施之间的对应关系。

附件A
（规范性）

PIM 参考控制目标以及 PII 控制器和 PII 处理器的控制

本附件旨在供充当 PII 控制者或 PII 处理者或两者的组织使用。

没有必要将本附件中列出的所有控制目标和控制措施纳入 PIMS 实施中。在适用性说明中应列明排除任何控制目标的理由[见6.1.3 e]]。排除的理由可以包括风险评估认为没有必要控制措施，以及适用法律要求不要求（或受例外情况限制）的控制措施。

表A.1适用于PII控制器，表A.2适用于PII处理器，表A.3涉及PII控制器和PII处理器的信息安全控制。

注：表A.1、A.2和A.3中“控制参考”下的提文参考附件B中的等效条款编号（例如，控制A.1.2.2的指导意见见B.1.2.2）。

表 A.1 — PII 控制器的控制目标和控制

收集和处理的条件 目的：证明处理是合法的，具有适用司法管辖区的法律依据，具有明确 定义和合法的目的。		
控制 参考	控制标题	控制
答 1.2.2	识别和 文档用途	该组织应确定并记录处理 PII 的具体目的。
答 1.2.3	确定法律依据	组织应确定、记录并能够证明 遵守为确定目的处理 PII 的相关法律依据。
答 1.2.4	确定何时以及如何 须征得同意	该组织应确定并记录其 可以证明是否、何时以及如何获得 PII 委托人对处理 PII 的同意。
答 1.2.5	获取并记录同意	组织应根据记录的流程获得并记录 PII 负责人的同意。
答 1.2.6	隐私影响评估	每当计划对 PII 进行新的处理或对现有的 PII 处理进行更改时，组织应评估是否需要，并在适当的情况下实施隐私影响评估。
答 1.2.7	与 PII 程序签订的合同	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 处理者的合同涉及附件 A 中适当控制措施的实施（见 表A.2）。
答 1.2.8	联合 PII 控制器	该组织应与任何联合 PII 控制者确定处理 PII（包括 PII 保护和安全要求）的各自角色和职责。

答 1.2.9	与处理 PII 相关的记录	该组织应确定并安全地维护必要的记录，以支持其处理 PII 的义务。

表 A.1（续）

对 PII 委托人的义务		
目标：确保向 PII 委托人提供有关其 PII 处理的适当信息，并履行与处理其 PII 相关的 PII 委托人的任何其他适用义务。		
答 1.3.2	确定和履行对 PII 原则的义务	组织应确定并记录其法律、监管 以及与处理其 PII 相关的对 PII 委托人的业务义务，并提供履行这些义务的手段。
答 1.3.3	确定 PII 主体的信息	组织应确定并记录信息以供 向 PII 委托人提供有关其 PII 的处理及其提供时间的信息。
答 1.3.4	向 PII 负责人提供信息	组织应向 PII 负责人提供清晰且易于访问的信息，以识别 PII 控制者并描述其 PII 的处理。
答 1.3.5	提供修改或撤回同意的机制	组织应为 PII 主事人提供修改或撤回其同意的机制。
答 1.3.6	提供反对 PII 的机制 加工	该组织应为 PII 负责人提供一种机制，以监督其 PII 的处理。
答 1.3.7	访问、更正或删除	组织应实施政策、程序或机制 履行其对 PII 委托人访问、更正或删除其 PII 的义务。
答 1.3.8	PII 控制者通知第三方的义务	组织应将与共享 PII 相关的任何修改、撤销或异议通知与之共享 PII 相关的第三方，并实施适当的政策、程序或 这样做的机制。
答 1.3.9	提供已处理的 PII 副本	当 PII 负责人要求时，组织应能够提供一份已处理的 PII 副本。
答 1.3.10	处理请求	该组织应制定并记录处理和响应 PII 原则的合法请求的政策和程序。
答 1.3.11	自动化决策	该组织应确定因 PII 委托人做出的决定而产生的义务，包括法律义务 仅基于 PII 的自动化处理与 PII 主体相关的组织，并能够展示它如何 穿上这些义务。
隐私设计和默认隐私		
目标：确保流程和系统的设计使 PII 的收集和处理（包括使用、披露、保留、传输和处置）仅限于确定目的所需的范围。		
答 1.4.2	限制收集	组织应将 PII 的收集限制在与已确定目的相关、相称和必要的最低限度。
答 1.4.3	限制处理	该组织应将 PII 的处理限制在对已确定目的充分、相关和必要的处理范围内。
答 1.4.4	准确性和质量	组织应确保并记录 PII 在 PII 的整个生命周期中，根据处理目的所需的准确性、完整性和最新性。
答 1.4.5	PII 最小化目标	组织应定义并记录数据最小化目标 jectives 以及使用哪些机制（例如去标识化）来实现这些目标。
答 1.4.6	PII 去标识化和删除结束时 加工	一旦原始 PII 不再需要用于确定的目的，组织应立即删除 PII 或以不允许识别或重新识别 PII 主体的形式呈现。

答 1.4.7	临时文件	组织应确保在指定的、有记录的记录内按照记录程序处理（例如删除或销毁）处理（例如删除或销毁）处理因处理 PII 而创建的临时文件 时期。

表 A.1（续）

答 1.4.8	保留	组织保留 PII 的时间不得超过处理 PII 目的所需的时间。
答 1.4.9	处理	该组织应有记录在案的 PII 处置政策、程序或机制。
答 1.4.10	PII 传输控制	组织应对通过数据传输网络传输（例如发送到另一个机构）的 PII 进行适当的控制，以确保数据到达其预定目的地。
PII 共享、传输和披露 目的：确定 PIIis 是否共享、转让给其他司法管辖区或第三方或根据适用义务披露，并记录何时。		
答 1.5.2	确定司法管辖区之间 PII 传输的依据	该组织应确定并记录在司法管辖区之间传输 PII 的相关依据。
答 1.5.3	国家和国际 PII 可以转移到的组织	该组织应具体说明并记录 PIII 可能转让给的国家和跨国组织。
答 1.5.4	PII 转移记录	该组织应记录与第三方之间的 PII 传输，并确保与这些方合作，以支持未来与对 PII 委托人的义务相关的请求。
答 1.5.5	向第三方披露个人身份信息的记录	该组织应记录向第三方披露 PII 的情况，包括向谁披露以及何时披露了哪些 PII。

表 A.2 — PII 处理器的控制目标和控制

收集和处理的条件 目的：证明处理是合法的，具有适用司法管辖区的法律依据，并具有明确定义和合法的目的。		
控制 参考	控件标题	控制
答2.2.2	客户 协议	在相关情况下，该组织应确保与 流程 PII 涉及组织在协助履行客户义务方面的作用（考虑到处理的性质和组织可用的信息）。
答2.2.3	组织宗旨	组织应确保代表 客户仅出于客户文档说明中表达的目的进行处理。
答 2.2.4	营销和 广告使用	组织不得将根据合同处理的 PII 用于营销和广告目的，而无需证明 事先获得相应 PII 委托人的同意。该组织不得将提供此类同意作为接受服务的条件。
答2.2.5	侵权指令	如果组织认为程序指示违反了适用的法律要求，则应通知客户。
答 2.2.6	客户 义务	组织应向客户提供适当的信息，以便客户能够证明合规性 履行他们的义务。

答 2.2.7	与处理 PII 相关的记录	该组织应确定并维持必要的重新 支持证明其遵守代表客户处理 PII 的义务（如适用合同中规定的那样）。
对 PII 委托人的义务 目标：确保向 PII 委托人提供有关其 PII 处理的适当信息，并履行与处理其 PII 相关的 PII 委托人的任何其他适用义务。		
答 2.3.2	遵守对 PII 委托人的义务	该组织应为客户提供履行其与 PII 委托人相关的义务的手段。

表A.2（续）

隐私设计和默认隐私 目标：确保流程和系统的设计使 PII 的收集和处理（包括使用、披露、保留、传输和处置）仅限于确定目的所需的范围。		
答 2.4.2	临时文件	组织应确保创建为 处理 PII 的结果在指定的记录期限内按照记录在案的程序进行处置（例如删除或销毁）。
答 2.4.3	归还、转让或处置 PII	该组织应能够以安全的方式归还、转让或处置 PII。它还应将其政策提供给 客户。
答 2.4.4	PII 传输控制	组织应对通过数据传输网络传输的个人身份信息进行适当的控制，以确保 数据到达其预期目的地。
PII 共享、传输和披露 目的：确定 PII 是否共享、转让给其他司法管辖区或第三方，或根据适用义务披露，以及何时记录。		
答2.5.2	司法管辖区之间 PII 传输的依据	组织应及时告知客户 司法管辖区之间 PII 传输的依据以及这方面的任何预期更改，以便客户可以反对此类 更改或终止合同。
答2.5.3	国家和国际 PII 可以转移到的组织	该组织应具体说明并记录这些国家和 PII 可以转移到的跨国组织。
答2.5.4	向第三方披露个人身份信息的记录	组织应记录向第三方披露 PII，包括向谁披露、何时披露。
答2.5.5	PII 披露请求的通知	组织应将任何具有法律约束力的 PII 披露请求通知客户。
答2.5.6	具有法律约束力的 PII 披露	组织应拒绝任何不具有法律约束力的 PII 披露请求，事先咨询相应客户 进行任何 PII 披露，并接受相应客户授权的任何合同约定的 PII 披露要求。
答 2.5.7	披露用于处理 PII 的分包商	在使用之前，组织应向客户披露是否使用任何子协议来处理 PII。
答2.5.8	委托分包商处理个人身份信息	组织只能聘请分包商根据客户合同处理 PII。
答2.5.9	分包商更改为程序 PII	在获得一般书面授权的情况下，组织应将有关 增加或更换分包商来处理 PII，从而让客户有机会反对此类更改。

表 A.3 — PII 控制器和 PII 处理器的控制目标和控制

PII 控制器和处理器的安全注意事项 目的：确保个人信息处理的安全性。		
控制 参考	控件标题	控制

答 3.3	信息安全政策	与 PII 处理相关的信息安全政策应由管理层定义、批准、发布、传达给 并得到相关人员和相关利益相关人士的认可 各方，并按计划的时间间隔进行审查，如果发生重大变化。
答 3.4	信息安全角色和 职责	应根据组织需要定义和分配与个人信息识别过程相关的信息安全角色和职责 。

表A.3（续）

答 3.5	信息分类	应根据组织的信息安全需求对信息进行分类，同时考虑 PII，基于 保密性、完整性、可用性和相关利害关系方要求。
答 3.6	信息标签	应根据以下规定制定和实施一套适当的信息标记程序，以配合个人身份信息 本组织采用的信息分类方案。
答 3.7	信息传递	与以下相关的信息传输规则、程序或协议 组织内部以及组织与其他组织之间的所有类型的传输设施都应处理 PII 各方。
答 3.8	身份管理	应管理与 PII 处理相关的身份的整个生命周期。
答3.9	访问权限	应在 根据组织的特定主题访问控制政策和规则。
答 3.10	在供应商协议中解决信息安全问题	应根据供应商关系的类型，制定与 PII 处理相关的相关信息安全要求并与 每个供应商达成一致。
答3.11	信息安全事件管理规划和 制备	组织应规划和准备管理信息 通过定义、建立和沟通事件管理流程、角色和 责任。
答 3.12	信息安全事件的应对	对与个人信息识别相关的信息安全事件的响应应按照记录在案的程序进行。
答 3.13	法律、法定、监管和合同要求	相关法律、法定、监管和合同要求 应记录与 PII 处理相关的信息安全以及组织满足这些要求的方法 并且该文档保持最新。
答3.14	保护记录	应保护与 PII 处理相关的记录免遭丢失、破坏、篡改、未经授权的访问 和未经授权的发布。
答 3.15	信息安全独立审查	组织管理信息安全的方法 与 PII 处理及其实施相关的人员、流程和技术，应按计划的时间间隔或发生 重大变化时独立审查。
答 3.16	遵守信息安全政策、规则和标准	遵守组织的信息安全政策， 应定期审查与 PII 处理相关的特定主题政策、规则和标准。
答 3.17	信息安全意识、教育和培训	组织人员及相关利害关系人应接受适当的信息安全意识教育，并 培训，并定期更新组织的信息安全政策、特定主题的政策和程序，与其工作 职能相关，因为它们与 PII 处理有关。
答3.18	保密或保密协议	应确定、记录、定期审查并由人员和其他相关人员签署反映组织保护 PII 需求的保密或保密协议 有意。
答3.19	清晰的办公桌和清晰的屏幕	清晰的纸张和可移动存储介质的桌面规则和清晰 应确定并适当执行信息处理设施的筛选规则。

答3.20	存储介质	具有PII的存储介质应按照组织的分类方案和处理要求，在其获取、使用、运输和处置的整个生命周期中进行管理。

表A.3（续）

答3.21	安全处置或重复使用设备	包含带有 PII 的存储介质的设备项目应符合 经过验证，以确保在处置或重复使用之前已删除或安全覆盖任何敏感数据和许可软件。
答3.22	用户终结点设备	存储在用户端点设备上、由用户端点设备处理或通过用户端点设备访问的 PII 应受到保护。
答3.23	安全身份验证	应根据信息访问限制实施与个人身份信息处理相关的安全认证技术和程序。
答 3.24	信息备份	应维护个人身份信息的备份副本，以及与个人身份信息处理相关的软件和系统，并定期进行测试。
答：3.25	伐木	应生成、存储、保护和分析记录与 PII 处理相关的活动、异常、故障和其他相关事件的日志。
答3.26	密码学的使用	应制定和实施有效使用与个人身份信息处理相关的密码学的规则，包括加密密钥管理。
答3.27	安全的开发生命周期	应制定并适用与个人身份信息处理相关的软件和系统安全开发规则。
答3.28	应用程序安全要求	在开发或获取应用程序时，应确定、指定和批准与 PII 处理相关的信息安全要求。
答3.29	安全系统架构和工程原理	应建立、记录、维护和适用于任何与处理 PII 相关的工程安全系统的原则 信息系统开发活动。
答：3.30	外包开发	该组织应指导、监督和审查与外包 PII 处理系统开发相关的活动。
答3.31	测试信息	应适当选择、保护和管理与PII处理相关的测试信息。

附件B

（规范性）

PII 控制器和 PII 处理器的实现指南

B.1 PII 控制器的实施指南

B.1.1 总则

本条款为 PII 控制器提供了 PIMS 指南，该指南与表 A.1 中列出的控件有关。

B.1.2 收集和处理的条件

B.1.2.1 目标

证明处理是合法的，具有适用司法管辖区的法律依据，并具有明确定义和合法的目的。

B.1.2.2 确定和记录目的

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 委托人了解处理其 PII 的目的。组织有责任清楚地记录这一点并将其传达给 PII 负责人。如果没有明确说明处理目的，就无法充分给予同意和选择。

处理 PII 目的的文档应足够清晰和详细，以便将其用作提供给 PII 委托人的信息的一部分（见 B.1.3.3）。该文档应包括获得同意所需的信息（见 B.1.2.4），以及政策和程序的书面信息（见 B.1.2.9）。

其他信息

在云计算服务的部署中，ISO/IEC 19944-1中的分类法和定义有助于提供描述PII处理目的的术语。

B.1.2.3 确定法律依据

控制

组织应确定、记录并能够证明遵守为确定目的处理 PII 的相关法律依据。

实施指南

一些司法管辖区要求组织能够证明在处理之前已正式确定处理的合法性。

处理 PII 的法律依据可以包括：

— PII 委托人的同意；

——履行合同;

一 遵守法律义务;

——保护 PII 委托人的切身利益;

一 执行为公共利益而执行的任务;——PII
控制者的合法利益。

组织应记录每项 PII 处理活动的这一基础（参见 B.1.2.9）。

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 主体在保护隐私方面的义务相平衡。

每当根据 PII 的性质（例如健康信息）或相关 PII 负责人（例如与儿童相关的 PII）定义特殊类别的 PII 时，组织都应将这些类别的 PII 纳入其分类方案中。

属于这些类别的 PII
分类可能因司法管辖区而异，并且适用于不同类型业务的不同监管制度也可能有所不同，因此组织应了解适用于正在执行的 PII 处理的分类。

使用特殊类别的 PII 也可能受到更严格的控制。

更改或扩展 PII 的处理目的可能需要更新或修订法律依据。它还可能需要获得 PII 委托人的额外同意。

B.1.2.4 确定何时以及如何获得同意

控制

组织应确定并记录一个流程，通过该流程可以证明是否、何时以及如何获得 PII 委托人对处理 PII 的同意。

实施指南

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。将处理目的与是否以及如何获得同意的信息相关联可能会很有用。

注意：法律要求可能适用。

一些司法管辖区对如何收集和记录同意有特定要求（例如，不与其他协议捆绑在一起）。此外，某些类型的数据收集（例如用于科学研究）和某些类型的 PII
主体（例如儿童）可能需要遵守其他要求。该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。

B.1.2.5 征得并记录同意

控制

组织应根据记录的流程获得并记录 PII 负责人的同意。

实施指南

组织应获得并记录 PII
主体的同意，以便它可以根据所提供同意的请求提供详细信息（例如，提供同意的时间、您的 PII
主体的身份和同意声明）。

在同意流程之前交付给 PII 委托人的信息应遵循

B.1.3.4.

同意书应为：

——白白给予;

一 具体处理目的;和

一 明确明确。

B.1.2.6 隐私影响评估

控制

组织应评估是否需要，并在计划对 PII 进行新的处理或更改现有的 PII 处理时实施隐私影响评估。

实施指南

PII 处理会给 PII 委托人带来风险。这些风险应通过隐私影响评估来评估。一些司法管辖区定义了强制进行隐私影响评估的案件。标准可以包括对 PII 委托人产生法律效力的自动决策、对特殊类别的 PII（例如与健康相关的信息、种族或民族血统、政治观点、宗教或哲学信仰、工会成员资格、遗传数据或生物识别数据）的大规模处理，或对公共可访问区域进行大规模系统监控。

组织应确定完成隐私影响评估所需的要素。这些可以包括处理的 PII 类型列表、PII 的存储位置和传输位置。在这种情况下，数据流图和数据映射也很有帮助。

注意：有关 PII 处理的书面信息的详细信息，请参阅 B.1.2.9，这些信息可以为隐私影响或其他风险评估提供信息。

其他信息

有关与 PII 处理相关的隐私影响评估的指南，请参阅 ISO/IEC 29134。

B.1.2.7 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 处理者的合同涉及表 A.2 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 处理者实施表 A.2 中规定的适当控制措施，同时考虑到信息安全风险评估流程（见 6.1.2）和 PII 处理者执行的 PII 处理范围。默认情况下，表 A.2 中指定的所有控件都应假定为相关。如果组织决定不需要 PII 处理器实施表 A.2 中的控制措施，则应证明排除其的合理性（见 6.1.3）。

合同可以以不同的方式定义各方的责任，但是，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记录的信息中。

B.1.2.8 联合 PII 控制器

控制

组织应与任何联合 PII 控制者一起确定处理 PII（包括 PII 保护和安全要求）的各自角色和职责。

实施指南

应以透明的方式确定处理 PII 的角色和责任。

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

联合 PII 控制者协议可以包括：

一 PII共享/共同PII控制者关系的目的;

一 属于联合 PIIcontroller 关系的组织（PIIcontrollers）的身份;

一 协议项下共享或转让和处理的个人信息类别;

一 处理作概述（例如传输、使用）;

一 描述各自的角色和职责;

一 负责实施个人信息保护的技术和组织安全措施;

一 PII 泄露时的责任定义（例如谁将通知、何时通知、相互信息）;

一 个人身份信息的保留或处置条款;

——不遵守协议的责任;——如何履行对 PII
委托人的义务;

——如何向 PII 主事人提供涵盖联合 PII 控制者之间安排本质的信息;

——PII 委托人如何获得他们有权获得的其他信息;和

一 PII 负责人的联系点。

B.1.2.9 与处理 PII 相关的记录

控制

组织应确定并安全地维护必要的记录，以支持其处理 PII 的义务。

实施指南

可以通过组织执行的 PII 处理活动的清单或列表来维护 PII 处理的记录信息。此类清单可以包括：

一 加工类型;

一 处理目的;

一 个人身份信息和个人身份信息主体（例如儿童）的类别描述;

一 已经或将要向其披露个人身份信息的接收者类别，包括第三国或国际组织的接收者;

一 技术和组织安全措施的一般说明;和

一 隐私影响评估报告。

这样的清单应该有一个负责其准确性和完整性的所有者。

B.1.3 对主要 PII 的义务

B.1.3.1 目标

确保向 PII 委托人提供有关其 PII 处理的适当信息，并履行与处理其 PII 相关的 PII 委托人的任何其他适用义务。

B.1.3.2 确定和履行对 PII 委托人的义务

控制

组织应确定并记录其对 PII 委托人与处理其 PII 相关的法律、监管和业务义务，并提供履行这些义务的方法。

实施指南

对 PII 委托人的义务以及支持他们的手段因司法管辖区而异。

组织应确保他们提供适当的方法，以可访问且及时的方式履行对 PII 委托人的义务。应向 PII 委托人提供明确的文件，描述履行对他们的义务的程度以及如何履行，以及他们可以解决其请求的最新联系点。

联系点的提供方式应与收集 PII 和同意的方式类似（例如，如果通过电子邮件或网站收集 PI，则联系点应通过电子邮件或网站，而不是电话或传真等替代方式）。

B.1.3.3 确定 PII 主体的信息

控制

组织应确定并记录要向 PII 负责人提供的有关其 PII 处理及其提供时间的信息。

实施指南

组织应确定向 PII 委托人提供信息的法律、法规或业务要求（例如，在处理之前，在请求后的特定时间内）以及要提供的信息类型。

根据要求，此信息可以采取通知的形式。可以向 PII 委托人提供的信息类型的示例包括：

——有关处理目的的信息（见 B.1.2.2）；

一 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（参见B.1.2.3）；

一 个人信息来源信息，如果不是直接从个人信息主体处获得的;

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

— B.1.3.2 中确定的有关对 PII 委托人的义务的信息，以及 PII 委托人如何从中受益，特别是关于访问、修改、更正、请求删除、接收其 PII 副本和反对处理;

——有关 PII 委托人如何撤回同意的信息（参见 B.1.3.5）；

一 个人信息转移信息;

——有关 PII 接收者或接收者类别的信息;

- 有关 PII 保留期限的信息;

- 有关使用基于 PII 自动处理的自动决策的信息;——

关于提出投诉的权利以及如何提出投诉的信息;

一 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）。

如果 PII 的处理目的发生变化或扩展，组织应提供更新信息。

B.1.3.4 向 PII 负责人提供信息

控制

组织应向 PII 负责人提供清晰且易于访问的信息，以识别您的 PII 控制者并描述其 PII 的处理。

实施指南

组织应以及时、简洁、完整、透明、易懂且易于访问的形式，使用适合目标受众的清晰易懂的语言，向 PII 负责人提供 B.1.3.3 中详述的信息。

在适当的情况下，应在收集个人身份信息时提供信息。它还应该是永久可访问的。

注意：图标和图像可以通过直观地概述预期处理来帮助 PII 主体。

B.1.3.5 提供修改或撤回同意的机制

控制

组织应为 PII 委托人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 负责人他们与撤回同意相关的权利（可能因司法管辖区而异），并提供这样做的机制。用于提款的机制取决于系统;它应与尽可能获得同意的机制保持一致。例如，如果同意是通过电子邮件或网站收集的，撤回同意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，这可能包括在某些情况下限制您的 PII 控制者删除 PII。

一些司法管辖区对 PII 委托人何时以及如何修改或撤回其同意施加限制。

组织应以与记录同意本身类似的方式记录任何撤回或更改同意的请求。

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。

组织应定义响应时间，并应根据该响应时间处理请求。

其他信息

当撤回对特定 PII 处理的同意时，通常应将撤回前对 PII 进行的所有处理视为适当，但此类处理的结果不应

用于新加工。例如，如果 PII 主体撤回了对分析的同意，则不应进一步使用或查阅其个人资料。

B.1.3.6 提供反对个人身份信息处理的机制

控制

组织应为 PII 负责人提供一种机制，以反对处理其 PII

实施指南

一些司法管辖区为 PII 委托人提供了反对处理其 PII 的权利。受此类司法管辖区法律要求约束的组织应能够证明他们如何确保保留行使此权利的 PII 委托人的记录。

组织应记录与 PII 负责人对处理的异议相关的法律和监管要求（例如，与出于直接营销目的处理 PII 有关的异议）]。您的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。反对机制可能会有所不同，但应与所提供的服务类型一致（e.g.online 服务应在线提供此功能）。

B.1.3.7 访问、更正或删除

控制

组织应实施政策、程序或机制，以履行其对 PII 委托人访问、更正或删除其 PII 的义务。

实施指南

组织应实施政策、程序或机制，使 PII 负责人能够在要求时访问、更正和删除其 PII，并且不得无故拖延。

组织应定义响应时间，并应根据该响应时间处理请求。

任何更正或删除都应通过系统或授权用户传播，并应传递给 PII 已传输给的第三方（见 B.1.3.8）。

注意 B.1.5.4 中指定的控制措施生成的记录信息可以在这方面提供帮助。

组织应实施政策、程序或机制，以便在 PII 委托人对数据的准确性或更正存在争议时使用。这些政策、程序或机制应包括告知 PII 委托人进行了哪些更改，以及无法进行更正的原因（在这种情况下）。

一些司法管辖区对 PII 委托人何时以及如何请求更正或删除其 PII 施加了限制。该组织应及时了解此类限制。

B.1.3.8 PII 控制者通知第三方的义务

控制

组织应将与共享 PII 相关的任何修改、撤销或反对通知与之共享 PII 的第三方，并实施适当的政策、程序或机制。

实施指南

组织应采取适当措施，牢记现有技术，将任何修改或撤回同意或与共享 PII 相关的异议通知第三方。

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，组织应监控其对收到信息的确认。

注意 因对 PII 委托人的义务而产生的变更可能包括修改或撤回同意、请求更正、删除或限制处理，或根据 PII 委托人的要求反对处理 PII。

B.1.3.9 提供已处理的 PII 副本

控制

组织应能够提供 PII 主体请求时处理的 PII 副本。

实施指南

组织应提供 PII 的副本，该副本以结构化、常用的 PII 主体可访问的格式进行处理。

一些司法管辖区定义了组织应提供处理后的 PII 副本的情况，其格式允许移植到 PII 主体或接收者 PII 控制者（通常是结构化的、常用的和机器可读的）。

组织应确保提供给 PII 委托人的任何 PII 副本都与该 PII 委托人具体相关。

如果请求的 PII 已根据保留和处置策略（如 B.1.4.8 中所述）被删除，则 PII 控制者应通知 PII 主体请求的 PII 已被删除。

如果组织不再能够识别 PII 主体（e.g.as 去标识化过程的结果），则组织不应仅以实施此控制为由寻求（重新）识别 PII 主体。然而，在某些司法管辖区，合法请求可能需要 PII 委托人提供额外信息，以便重新识别和随后披露。

在技术上可行的情况下，应 PII 委托人的请求，应有可能将 PII 的副本从一个组织直接传输到另一个组织。

B.1.3.10 处理请求

控制

组织应定义并记录处理和响应 PII 委托人的合法请求的政策和程序。

实施指南

合法请求可以包括请求提供已处理的 PII 副本或提出投诉的请求。

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）。

请求应在定义的适当响应时间内处理。

一些司法管辖区根据请求的复杂性和数量以及通知 PII 委托人任何延迟的要求来定义响应时间。应在隐私政策中定义适当的响应时间。

B.1.3.11 自动决策

控制

组织应确定组织仅基于 PII 自动处理的与 PII 委托人相关的决策而对 PII 委托人承担的义务，包括法律义务，并能够证明其如何履行这些义务。

实施指南

一些司法管辖区在仅基于 PII 自动处理的决策对 PII 委托人产生重大影响时，定义了对 PII 委托人的具体义务，例如通知自动决策的存在，允许 PII 委托人反对此类决策，或获得人为干预。

注意：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该能够证明他们如何考虑遵守这些义务的情况。

B.1.4 隐私设计和默认隐私

B.1.4.1 目标

确保流程和系统的设计使 PII 的收集和处理（包括使用、披露、保留、传输和处置）仅限于确定目的所必需的范围。

B.1.4.2 限制收集

控制

组织应将 PII 的收集限制在与已确定目的相关、相称和必要的最低限度。

实施指南

组织应将 PII 的收集限制在与已确定的目的相关的充分、相关和必要的范围内。这包括限制组织间接收集的 PII 数量（例如通过网络日志、系统日志）。

默认隐私意味着，如果 PII 的收集和处理存在任何可选性，则默认情况下应禁用每个选项，并且只能通过显式选择 PII 主体来启用。

B.1.4.3 极限处理

控制

组织应将 PII 的处理限制在对您确定的目的而言是充分、相关和必要的。

实施指南

应通过信息安全和隐私政策（见 5.2）以及采用和合规的书面程序来管理 PII 的处理。

默认情况下，PII 的处理应限制在相对于已确定的目的所需的最低限度。此处理包括：

——披露；

——PII 存储期限;和

一 谁可以访问他们的 PII。

B.1.4.4 准确性和质量

控制

组织应确保并记录 PII 在 PII 的整个生命周期中尽可能准确、完整和最新，以满足其处理目的。

实施指南

组织应实施政策、程序或机制，以尽量减少其处理的 PII 中的不准确之处。还应该制定政策、程序或机制来应对不准确的个人身份信息的情况。这些政策、程序或机制应包含在记录的信息中（例如通过技术系统配置），并应适用于整个 PII 生命周期。

其他信息

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

B.1.4.5 个人身份信息最小化目标

控制

组织应定义并记录数据最小化目标以及使用哪些机制（例如去标识化）来实现这些目标。

实施指南

组织应确定相对于已确定的目的，收集和处理的特定 PII 和 PII 数量如何受到限制。这可以包括使用去标识化或其他数据最小化技术。

已识别的目的（见 B.1.2.2）可能需要处理尚未去标识化的 PII，在这种情况下，组织应该能够描述此类处理。

在其他情况下，识别的目的不需要对原始PII进行处理，对已去标识化的PII进行处理就足以实现识别的目的。在这些情况下，组织应定义并记录 PII 应与 PII 委托人相关联的程度，以及旨在处理 PII 的机制和技术，以便实现去标识化和 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。组织应记录用于实施数据最小化的任何机制（例如技术系统配置）。

如果处理去识别化数据足以满足这些目的，组织应记录旨在及时实施组织设定的去识别化目标的任何机制（例如技术系统配置）。例如，删除与 PII 主体相关的属性足以使组织实现其确定的目的。在其他情况下，可以使用其他去标识化技术，例如泛化（例如舍入）或随机化技术（例如噪声添加）来实现足够的去标识化水平。

注1 有关去标识化技术的更多信息，请参阅 ISO/IEC 20889。

注 2：对于云计算，ISO/IEC 19944-1 提供了数据识别限定符的定义，可用于对数据识别 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。

B.1.4.6 处理结束时的PII去标识化和删除

控制

一旦原始 PII 不再需要用于确定的目的，组织应立即删除 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

组织应具有在预计不会进行进一步处理时擦除 PII 的机制。或者，可以使用一些去标识化技术，只要生成的去标识化数据不能合理地允许重新识别 PII 主体。

B.1.4.7 临时文件

控制

组织应确保在规定的记录期限内按照记录在案的程序处置（例如删除或销毁）处理因处理 PII 而创建的临时文件。

实施指南

组织应定期检查未使用的临时文件是否在确定的时间段内被删除。

其他信息

信息系统可以在其正常运行过程中创建临时文件。此类文件特定于系统或应用程序，但可以包括文件系统回滚日志和与数据库更新和其他应用程序软件作相关的临时文件。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。这些文件保持使用的时间长度并不总是确定性的，但“垃圾回收”过程应该识别相关文件并确定自上次使用它们以来已经过去了多长时间。

B.1.4.8 保留

控制

组织保留 PII 的时间不应超过处理 PII 的目的所需的时间。

实施指南

组织应为其保留的信息制定和维护保留时间表，同时考虑到保留 PII 的时间不超过必要的时间的要求。此类时间表应考虑法律、法规和业务要求。如果这些要求发生冲突，则应做出业务决策（基于风险评估）并记录在适当的时间表中。

B.1.4.9 处置

控制

该组织应有记录在案的 PII 处置政策、程序或机制。

实施指南

PII 处置技术的选择取决于许多因素，因为处置技术的属性和结果不同（e.g.in 生成的物理介质的粒度，或恢复电子介质上已删除信息的能力）。选择适当的处置技术时要考虑的因素包括但不限于要处置的 PII 的性质和范围、是否存在与 PII 相关的元数据以及存储 PII 的介质的物理特征。

B.1.4.10 PII 传输控制

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期目的地。

实施指南

应控制 PII 的传输，通常通过确保只有授权个人才能访问传输系统，并遵循适当的流程（包括保留审计日志）来确保 PII 不会泄露地传输给正确的接收者。

B.1.5 PII共享、传输和披露

B.1.5.1 目标

确定 PII 是否共享、传输给其他司法管辖区或第三方，或根据适用义务披露 PII 并记录何时。

B.1.5.2 确定司法管辖区之间 PII 传输的依据

控制

该组织应确定并记录在司法管辖区之间传输 PII 的相关依据。 **实施指南**

PII 传输可能受到法律要求的约束，具体取决于数据要传输到的司法管辖区或国际组织（以及数据的来源）。该组织应记录遵守此类要求的情况，作为转移的依据。

一些司法管辖区可以要求信息传输协议由指定的监管机构进行审查。在此类司法管辖区运营的组织应了解任何此类要求。

注意：如果转账发生在特定司法管辖区内，则对发件人和收件人适用的法律要求是相同的。

B.1.5.3 个人身份信息可以转移到的国家和国际组织

控制

该组织应具体说明并记录 PII 可能转移到的国家和国际组织。

实施指南

应向客户提供在正常作中可能将 PII 转移到的国家和国际组织的身份。由你而生的国家的身份

应包括使用分包的 PII 处理。应结合 **B.1.5.2** 考虑所包括的国家。

在正常业务之外，可能会有应法律当局的要求进行的转移，但无法事先指定国家的身份，或者适用的司法管辖区可以禁止这种转移，以保护执法调查的机密性（见 B.1.5.2、B.2.5.5 和 B.2.5.6）。

B.1.5.4 个人身份信息转移记录

控制

该组织应记录与第三方之间的 PII 传输，并确保与这些方合作，以支持未来与对 PII 委托人的义务相关的请求。

实施指南

记录可以包括从第三方传输的 PII，该 PII 因 PII 控制者管理其义务而被修改，或传输给第三方以执行 PII 委托人的合法请求，包括删除 PII 的请求（例如在撤回同意后）。

组织应制定定义这些记录保留期限的策略。

组织应将数据最小化原则应用于传输记录，仅保留绝对需要的信息。

B.1.5.5 向第三方披露个人身份信息的记录

控制

组织应记录向第三方披露 PII 的情况，包括向谁披露了哪些 PII、何时披露了 PII。

实施指南

PII 可以在正常运营期间披露。这些披露应被记录下来。向第三方披露的任何额外信息，例如法律调查或外部审计引起的信息，也应记录在案。记录应包括披露的来源和进行披露的当局的来源。

B.2 PII 处理器的实施指南

B.2.1 总则

本条款为 PII 处理器提供了 PIMS 指南，该指南与表 A.2 中列出的控制有关。

B.2.2 收集和处理的条件

B.2.2.1 目标

证明处理是合法的，具有适用司法管辖区的法律依据，并具有明确定义和合法的目的。

B.2.2.2 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履行客户义务方面的作用（考虑到处理的性质和组织可用的信息）。

实施指南

组织与客户之间的合同应包括以下方面，在相关的情况下，取决于客户的角色（即 PII 控制者或 PII 处理者）：

——隐私设计和默认隐私（参见 B.1.4 和 B.2.4）；

—实现加工的安全性;

— 向监管机构通报涉及 PII 的违规行为;

— 向客户和 PII 委托人通报涉及 PII 的违规行为;

一 进行隐私影响评估;和

一 如果需要事先与相关 PII 保护机构协商，则保证 PII 处理者提供帮助。

一些司法管辖区要求合同包括处理的标的物和持续时间、处理的性质和目的、PII 的类型和 PII 委托人的类别。

B.2.2.3 本组织的宗旨

控制

组织应确保仅出于客户书面说明中表达的目的而代表客户处理的 PII。

实施指南

组织与客户之间的合同应包括但不限于服务要实现的目标和时间范围。

为了实现客户的目的，可能存在技术原因，说明组织应该确定处理 PII 的方法，与客户的一般指示一致，但没有客户的明确指示。例如，为了有效利用网络或处理能力，可能需要根据PII主体的某些特征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客户书面说明中表达的目的以外的其他目的处理 PII。

B.2.2.4 营销和广告使用

控制

在未证明事先获得相应 PII 委托人的同意的情况下，组织不应将根据合同处理的 PII 用于营销和广告目的。该组织不应将提供此类同意作为接受服务的条件。

实施指南

应记录 PII 处理者是否符合客户的合同要求，尤其是在计划进行营销或广告的情况下。

在未公平获得 PII 委托人的明确同意的情况下，组织不应坚持包含营销或广告用途。

注意：此控件是对 B.2.2.3 中更通用的控件的补充，不会取代或以其他方式取代它。

B.2.2.5 侵权指令

控制

如果组织认为处理指令违反了适用的法律要求，则应通知客户。

实施指南

组织验证指令是否违反法律要求的能力可能取决于您的技术背景、指令本身以及组织与客户之间的合同。

B.2.2.6 客户义务

控制

组织应向客户提供适当的信息，以便客户能够证明遵守其义务。

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以其他方式同意的其他审计员进行的审计。

B.2.2.7 与处理 PII 相关的记录

控制

组织应确定并维护必要的记录，以证明其遵守代表客户处理 PII 的义务（如适用合同中规定）。

实施指南

某些司法管辖区可以要求组织记录以下信息：

一 类代为每个客户进行的加工;

一 向第三国或国际组织转移;和

一 技术和组织安全措施的一般说明。

B.2.3 对主要 PII 的义务

B.2.3.1 目标

确保向 PII 委托人提供有关其 PII 处理的适当信息，并履行与处理其 PII 相关的 PII 委托人的任何其他适用义务。

B.2.3.2 遵守对 PII 委托人的义务

控制

组织应为客户提供遵守其与 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法律要求或合同来定义。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，这可以包括及时更正或删除 PII。

客户依赖组织获取信息或技术措施以促进履行对个人信息识别委托人的义务的，应在合同中明确相关信息或技术措施。

B.2.4 隐私设计和默认隐私

B.2.4.1 目标

确保流程和系统的设计使 PII 的收集和处理（包括使用、披露、保留、传输和处置）仅限于确定目的所必需的范围。

B.2.4.2 临时文件

控制

组织应确保在规定的记录期限内按照记录在案的程序处置（例如删除或销毁）处理因处理 PII 而创建的临时文件。

实施指南

组织应定期验证未使用的临时文件是否在确定的时间段内被删除。

其他信息

信息系统可以在其正常运行过程中创建临时文件。此类文件特定于系统或应用程序，但可以包括文件系统回滚日志和与数据库更新和其他应用程序软件作相关的临时文件。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。这些文件保持使用的时间长度并不总是确定性的，但“垃圾回收”过程应该识别相关文件并确定自上次使用它们以来已经过去了多长时间。

B.2.4.3 个人身份信息的归还、转让或处置

控制

组织应该能够以安全的方式归还、转移或处置 PII。它还应该向客户提供其策略。

实施指南

在某个时间点，可能需要以某种方式处理 PII。这可能涉及将您的 PII 返回给客户、将其传输给另一个组织或 PII 控制者（e.g.as 合并的结果）、删除或以其他方式销毁它、去标识化或存档它。应以安全的方式管理个人身份信息的归还、转移或处置能力。

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 从存储的任何地方（由组织及其任何分包商）删除，包括出于备份和业务连续性的目的，一旦客户确定的目的不再需要它们。

组织应制定和实施有关 PII 处置的政策，并应在客户要求时向客户提供此政策。

保单应涵盖合同终止后处置个人信息之前的保留期，以保护客户不会因合同意外失效而丢失个人信息。

注意：这种控制和指导也与保留原则相关（见 B.1.4.8）。

B.2.4.4 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，这些控制旨在确保数据到达其预期目的地。

实施指南

应控制 PII 的传输，通常通过确保只有授权个人才能访问传输系统，并遵循适当的流程（包括保留审计数据）以确保 PII 在不损害的情况下传输给正确的接收者。传输控制的要求可以包含在 PII 处理器与客户之间的合同中。

如果没有与传输相关的合同要求，则在传输前征求客户的建议可能是合适的。

B.2.5 个人信息共享、转让和披露

B.2.5.1 目标

确定 PII 是否共享、传输给其他司法管辖区或第三方，或根据适用义务披露 PII 并记录何时。

B.2.5.2 司法管辖区之间个人身份信息转移的依据

控制

组织应及时告知客户司法管辖区之间 PII 传输的依据以及这方面的任何预期更改，以便客户可以反对此类更改或终止合同。

实施指南

司法管辖区之间的 PII 传输可能受到法律要求的约束，具体取决于 PII 要转移到的司法管辖区或组织（以及其来源）。该组织应记录遵守此类要求的情况，作为转移的依据。

组织应将任何 PII 的传输通知客户，包括传输到：

一、供应商;

一 其他当事人;

一 其他国家或国际组织。

如有变更，组织应按照约定的时间提前通知客户，以便客户有能力反对此类变更或终止合同。

组织与客户之间的协议可以包括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，应设定此限额的限制（例如，组织可以在不通知客户的情况下更换供应商，但不能将 PII 转移到其他国家/地区）。

在PII的国际传输中，应确定合同条款范本、具有约束力的公司规则或跨境隐私规则等协议，涉及的国家和此类协议的适用情况。

B.2.5.3 个人身份信息可以转移到的国家和国际组织

控制

该组织应具体说明并记录 PII 可能转移到的国家和国际组织。

实施指南

应向客户提供在正常作中可能将 PII 转移到的国家和国际组织的身份。应包括因使用分包 PII 处理而产生的国家/地区的身份。应结合B.2.5.2考虑所包括的国家。

在正常业务之外，可能会有应法律当局的要求进行的转移，但无法事先指定国家/地区的身份，或者适用的司法管辖区可以禁止这种转移，以保护执法调查的机密性（见 B.1.5.2、B.2.5.5 和 B.2.5.6）。

B.2.5.4 向第三方披露个人信息的记录

控制

组织应记录向第三方披露 PII，包括向谁披露了哪些 PII、何时披露。

实施指南

PII
可以在正常运营期间披露。这些披露应被记录下来。向第三方披露的任何额外信息，例如法律调查或外部审计引起的信息，也应记录在案。记录应包括披露的来源和进行披露的当局的来源。

B.2.5.5 个人身份信息披露请求的通知

控制

组织应通知客户任何具有法律约束力的 PII 披露请求。

实施指南

组织可以收到具有法律约束力的 PII
披露请求（例如来自法律当局）。在这些情况下，组织应在约定的时间范围内并按照可包含在客户合同中的商定程序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得将该事件通知任何人。可能禁止披露的一个例子是刑法禁止对法律调查保密。

B.2.5.6 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 披露之前咨询相应客户，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

与控制实施相关的详细信息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。

B.2.5.7 披露用于处理个人身份信息的分包商

控制

在使用之前，组织应向客户披露是否使用任何分包商来处理 PII。

实施指南

客户合同中应包含使用分包商处理个人身份信息的条款。

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 B.2.5.3），以及分包商有义务履行或超过该组织义务的方式（见 B.2.5.8）。

如果评估公开披露分包商信息会使安全风险超出可接受的限度，则应根据保密协议或应客户要求进行披露。您的客户应该知道这些信息是可用的。

这不涉及可以转移 PII
的国家/地区列表。在所有情况下，都应向客户披露该列表，以便他们能够通知适当的 PII 负责人。

B.2.5.8 委托分包商处理个人身份信息

控制

组织应仅聘请分包商根据客户合同处理 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
之前需要获得客户的书面授权。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。

组织应与代表其用于 PII
处理的任何分包商签订书面合同。该组织应确保其与分包商的合同涉及表A.2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表 A.2
中规定的适当控制措施，同时考虑到信息安全风险评估流程（见 6.1.2）和 PII 处理者执行的 PII
处理范围。默认情况下，表 A.2
中指定的所有控件都应假定为相关。如果您的组织决定不要求分包商实施表 A.2
的控制，则应证明将其排除在外的合理性。

合同可以以不同的方式定义各方的责任，但是，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记录的信息中。

B.2.5.9 处理 PII 的分包商变更

控制

在获得一般书面授权的情况下，组织应告知客户有关添加或更换分包商处理 PII
的任何预期变更，从而让客户有机会反对此类变更。

实施指南

如果组织更改了将其部分或全部 PII 处理分包的组织，则在新分包商处理 PII 之前，需要获得客户的书面授权才能进行更改。这可以是客户合同中适当的条款或特定的“一次性”协议的形式。

B.3 PII控制器和PII处理器的实施指南

B.3.1 目标

确保PII处理的安全性。

B.3.2 总则

本条款为 PII 控制器和 PII 处理器提供了 PIMS 指南，这与表 A.3 中列出的控制有关。除非表 A.3 中的具体规定另有说明或组织确定，否则相同的指南适用于 PII 控制者和 PII 处理者。

B.3.3 信息安全政策

控制

应定义与 PII 处理相关的信息安全政策，由管理层批准，发布，向相关人员和相关利益相关方传达并得到认可，并按计划的时间间隔进行审查，如果发生重大变化。

实施指南

通过制定单独的隐私政策或通过增强信息安全政策，组织应出具一份声明，以支持和承诺遵守适用于 PII 保护的法律要求以及组织与其合作伙伴、其分包商和适用的第三方（客户、供应商等），应明确分配他们之间的责任。

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于 PII 保护的法律要求。

B.3.4 信息安全角色和职责

控制

应根据组织需求定义和分配与 PII 处理相关的信息安全角色和职责。

实施指南

组织应指定一个联系人，供客户在处理 PII 方面使用。当组织是 PII 控制者时，应为 PII 委托人指定一个联系人，以处理其 PII（参见 B.1.3.4）。

组织应任命一名或多名负责制定、实施、维护和监控组织范围的治理和隐私计划的人员，以确保遵守有关 PII 处理的所有适用法律要求。

负责人应在适当的情况下：

——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；

——参与与 PII 处理相关的所有问题的管理；

——成为数据保护立法、监管和实践方面的专家;

— 充当监管部门的联络点;

— 告知组织的高层管理人员和员工他们在处理 PII 方面的义务;

— 就组织进行的隐私影响评估提供建议。

注意：某些司法管辖区将此人称为数据保护官。司法管辖区定义何时需要这种地位，以及它们的立场和作用。该职位可以由工作人员或外包。

B.3.5 信息分类

控制

应根据组织的信息安全需求对信息进行分类，同时考虑 PII，基于机密性、完整性、可用性和相关利益相关方的要求。

实施指南

组织的信息分类方案应明确将 PII 视为其实施的方案的一部分。在整体分类方案中考虑 PII 对于了解组织处理哪些 PII（例如类型、特殊类别）、此类 PII 存储在哪里以及它可以流经的系统至关重要。

B.3.6 信息标签

控制

应根据组织采用的信息分类方案制定和实施一套考虑个人身份信息的信息标签程序。

实施指南

组织应确保其控制下的人员了解 PII 的定义以及如何识别 PII 信息。

B.3.7 信息传输

控制

组织内部以及组织与其他方之间的所有类型的传输设施都应制定与处理 PII 相关的信息传输规则、程序或协议。

实施指南

组织应考虑确保在系统内外执行与 PII 处理相关的规则的程序（如适用）。

B.3.8 身份管理

控制

应管理与 PII 处理相关的身份的整个生命周期。

实施指南

管理或作处理 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泄露（e.g.as 无意中泄露的结果）。

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

如果组织将 PII 处理作为服务提供，客户可以负责用户 ID
管理的部分或全部方面。此类情况应包含在记录的信息中。

一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证的检查频率提出了具体要求。在这些司法管辖区运营的组织应考虑遵守这些要求。

B.3.9 访问权限

控制

应根据组织的特定主题访问控制政策和规则，配置、审查、修改和删除与 PII 处理相关的 PII 和其他相关资产的访问权限。

实施指南

该组织应保留为有权访问信息系统的用户创建的用户配置文件及其中包含的个人身份信息的准确、最新记录。每个配置文件都包含有关用户的一组数据，包括用户
ID，这些数据是实施提供授权访问的已识别技术控制所必需的。

实施单个用户访问 ID 使适当配置的系统能够识别谁访问了 PII 以及他们进行了哪些添加、删除或更改。除了保护组织外，用户还受到保护，因为他们可以识别他们已经处理的内容和未处理的内容。

如果组织提供 PII
处理即服务，客户可以负责访问管理的部分或全部方面。在适当的情况下，组织应为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信息中。

B.3.10 在供应商协议中处理信息安全问题

控制

应根据供应商关系的类型，制定与 PII 处理相关的相关信息安全要求并与每个供应商达成一致。

实施指南

组织应在与供应商的协议中具体说明是否处理 PII，以及供应商为履行其信息安全和 PII 保护义务而需要满足的最低技术和组织措施（参见 B.1.2.7 和 B.2.2.2）。

供应商协议应明确分配组织、其合作伙伴、供应商及其相关第三方（客户、供应商等）之间的责任。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，以确保您的组织支持和管理遵守所有适用的法律要求。协议应要求经过独立审计的合规性，并被客户接受。

注意 出于此类审核目的，可以考虑符合相关且适用的安全标准，例如 ISO/IEC 27001。

如果组织的角色是 PII 处理者，则组织应在与任何供应商签订的合同中规定，仅根据其指示处理 PII。

B.3.11 信息安全事件管理规划和准备

控制

组织应通过定义、建立和传达事件管理流程、角色和职责来规划和准备管理与 PII
处理相关的信息安全事件。

实施指南

作为整个信息安全事件管理流程的一部分，组织应建立识别和记录 PII
违规行为的责任和程序。此外，组织应制定与通知相关方 PII
违规行为（包括此类通知的时间）和向当局披露相关的责任和程序，同时考虑到适用的法律要求。

一些司法管辖区对违规响应（包括通知）实施了具体规定。在这些司法管辖区运营的组织应确保他们了解并记录他们如何遵守这些法规。

B.3.12 信息安全事件的应对

控制

对与 PII 处理相关的信息安全事件的响应应按照记录的程序进行。

PII 控制器的实现指南

作为其信息安全事件管理流程的一部分，涉及 PII
的事件应触发组织的审查，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审查。

注1：信息安全事件不一定会导致实际或极有可能未经授权访问 PII 或组织存储 PII
的任何设备或设施。这些攻击可能包括但不限于对防火墙或边缘服务器的 ping
和其他广播攻击、端口扫描、登录尝试失败、拒绝服务攻击和数据包嗅探。

当发生个人身份信息泄露时，应对程序应包括相关通知和记录。

一些司法管辖区定义了应将违规行为通知相关监管机构以及应通知 PII 委托人的情况。

通知应该很清楚。

注 2：通知可以包含以下详细信息：

— 可以获取更多信息的联系点;

— 对违规行为的描述和可能的后果;

— 对违规行为的描述，包括有关个人的人数以及有关记录的数量;

— 已采取或计划采取的措施。

注 3：有关安全事件管理的信息，请参阅 ISO/IEC 27035 系列。

如果发生涉及 PII
的违规行为，则应保存记录，其中包含足够的信息，以便为监管或取证目的提供报告，例如：

— 事件描述;

一、时间段;

——事件的后果;

一、记者姓名;

一 向谁报告了该事件;

一 为解决事件而采取的步骤（包括负责人和恢复的数据）;

一 事件导致 PII 不可用、丢失、披露或更改的事实。

如果发生涉及 PII 的违规行为，记录还应包括对被泄露的 PII 的描述（如果已知）。如果使用了通知，还应记录通知 PII 委托人、监管机构或客户所采取的步骤。

PII 处理器的实施指南

涉及 PII 的违规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向您提供客户履行通知有关当局的义务所需的信息。此通知义务不适用于由客户或 PII 委托人造成的违规行为，也不适用于他们负责的系统组件内部的违规行为。合同还应定义通知响应时间的预期和外部规定的限制。

在某些司法管辖区，PII 处理者应立即通知 PII 控制者存在违规行为（一旦发现 i.e.as 立即），以便 PII 控制者可以采取适当的行动。

如果发生涉及 PII 的违规行为，则应保存记录，其中包含足够的信息，以便为监管或取证目的提供报告，例如：

一 事件的描述;——时间段;

一 事件的后果;

一、记者姓名;

一 向谁报告了该事件;

一 为解决事件而采取的步骤（包括负责人和恢复的数据）;——事件导致 PII 不可用、丢失、披露或更改的事实。

如果发生涉及 PII 的违规行为，记录还应包括对被泄露的 PII 的描述（如果已知）;如果使用了通知，则通知客户或您的监管机构所采取的步骤。

在某些司法管辖区，适用的法律要求可能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。

B.3.13 法律、法定、监管和合同要求

控制

应记录与 PII 处理相关的信息安全相关的法律、法定、法规和合同要求，以及组织满足这些要求的方法，并保持本文档的最新状态。

实施指南

该组织应确定与 PII 处理相关的任何潜在法律制裁（可能因错过某些义务而导致），包括直接来自当地监管机构的巨额罚款。

在某些司法管辖区，本文档等国际标准可用于构成组织与客户之间合同的基础，概述了各自的安全、隐私和 PII 保护责任。合同条款可以为违反这些责任时的合同制裁提供依据。

B.3.14 记录保护

控制

应保护与 PII 处理相关的记录免遭丢失、破坏、篡改、未经授权的访问和未经授权的发布。

实施指南

可能需要审查当前和历史的政策和程序（e.g.in 客户争议解决和监管机构调查的案例）。

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程序的副本（参见 B.1.4.8）。这包括在更新这些文档的先前版本时保留它们。

B.3.15 信息安全独立审查

控制

组织管理与 PII 处理及其实施相关的信息安全的方法，包括人员、流程和技术，应按计划的时间间隔或在发生重大变化时独立审查。

实施指南

如果组织充当 PII 处理者，并且单个客户审计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限内向客户提供独立证据，证明信息安全是根据组织的政策和程序实施和运营的。由组织选择的相关独立审计通常应该是满足客户审查组织处理作的利益的可接受方法，如果它涵盖了预期用户的需求，并且结果是否以足够透明的方式提供。

B.3.16 遵守信息安全政策、规则和标准

控制

应定期审查与 PII 处理相关的组织信息安全政策、特定主题政策、规则和标准的遵守情况。

实施指南

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

— 持续监测，以验证是否只进行允许的处理;或

— 特定的渗透或漏洞测试（例如，去识别化的数据集可以接受有动机的入侵者测试以验证去识别化方法是否符合组织要求）。

B.3.17 信息安全意识、教育培训

控制

组织人员及相关利害关系人应接受适当的信息安全意识教育培训，并定期更新组织信息安全

政策、特定主题的政策和程序，与其工作职能相关，因为它们与 PII 处理相关。

实施指南

应采取措施，包括提高对事件报告的认识，以确保相关工作人员了解违反隐私或安全规则和程序可能产生的后果，尤其是那些处理个人身份信息的规则和程序。其中包括违反隐私或安全规则和程序对组织造成的后果（例如法律后果、业务和品牌损失或声誉受损）、对员工的后果（例如纪律处分后果）和对 PII 主体的后果（例如身体、物质和情感后果），尤其是那些涉及 PII 处理的规则和程序。

注：此类措施可以包括对有权访问 PII 的人员进行适当的定期培训。

B.3.18 保密或保密协议

控制

应确定、记录、定期审查并由人员和其他相关相关方签署反映组织保护 PII 需求的保密或保密协议。

实施指南

该组织应确保在其控制下运营并有权访问 PII 的个人承担保密义务。保密协议，无论是合同的一部分还是单独的，都应规定应遵守义务的时间长度。

当组织是 PII 处理者时，无论以何种形式，组织、其员工及其代理人之间都应确保员工和代理人遵守有关数据处理和保护的政策和程序。

B.3.19 清晰的办公桌和清晰的屏幕

控制

应为文件和可移动存储介质制定清晰的案头规则，为信息处理设施制定清晰的屏幕规则，并适当执行。

实施指南

组织应将包括 PII 在内的硬拷贝材料的创建限制在实现已确定的处理目的所需的最低限度。

B.3.20 存储介质

控制

具有PII的存储介质应按照组织的分类方案和处理要求，在其获取、使用、运输和处置的整个生命周期中进行管理。

实施指南

组织应记录用于存储 PII 的可移动媒体或设备的任何使用。在可行的情况下，组织应在存储 PII 时使用允许加密的可移动物理介质或设备。仅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或设备的情况下，组织应实施程序和补偿控制（例如防篡改包装）以降低 PII 的风险。

在处置存储 PII 的可移动介质时，应在记录的信息中包含安全处置程序并实施，以确保以前存储的 PII 无法访问。

如果使用物理介质进行信息传输，应建立系统来记录包含个人身份信息的传入和传出物理介质，包括物理介质的类型、授权发送者、授权接收者、日期和时间以及物理介质的数量。在可能的情况下，应实施加密等额外措施，以确保数据只能在目的地访问，而不是在传输过程中访问。

组织应在离开其场所之前对包含 PII
的物理介质进行授权程序，并确保除授权人员外的任何人都无法访问 PII。

注意：确保离开组织场所的物理介质上的 PII 通常无法访问的一种可能措施是加密相关 PII
并将解密功能限制为授权人员。

在组织物理范围之外的可移动介质很容易丢失、损坏和不当访问。加密可移动媒体增加了对 PII 的保护级别，从而在可移动媒体受到损害时降低安全和隐私风险。

B.3.21 安全处置或重复使用设备

控制

应验证包含具有 PII
存储介质的设备项目，以确保在处置或重复使用之前已删除或安全覆盖任何敏感数据和许可软件。

实施指南

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 都无法访问。

关于删除信息系统中保存的 PII，性能问题可能意味着显式擦除该 PII
是不切实际的。这会产生其他用户可以访问 PII 的风险。应通过具体的技术措施来避免这种风险。

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被视为包含 PII。

B.3.22 用户端点设备

控制

应保护存储在用户端点设备上、由用户端点设备处理或通过用户端点设备访问的 PII。

实施指南

组织应确保移动设备的使用不会导致 PII 泄露。

B.3.23 安全认证

控制

应根据信息访问限制实施与 PII 处理相关的安全身份验证技术和程序。

实施指南

如果客户需要，组织应为客户控制下的任何用户帐户提供安全登录过程的功能。

B.3.24 信息备份

控制

应维护 PII 的备份副本以及与 PII 处理相关的软件和系统并定期测试。

实施指南

组织应制定一项政策，解决 PII 的备份、恢复和恢复要求（可以作为整体信息备份策略的一部分）以及删除为备份要求而持有的信息中包含的 PII 的任何进一步要求（例如合同或法律要求）。

这方面的 PII 特定职责可能取决于客户。组织应确保已告知客户有关备份的服务限制。

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

一些司法管辖区对 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。在这些司法管辖区运营的组织应证明遵守这些要求。

在某些情况下，可能需要恢复 PII，可能是由于系统故障、攻击或灾难。当 PII 恢复（通常从备份介质）时，应制定流程以确保将 PII 恢复到可以保证 PII 完整性的状态，或者识别 PII 不准确或不完整性并制定流程来解决它们（可能涉及 PII 主体）。

组织应该有一个 PII 恢复工作的程序和日志。PII 恢复工作的日志至少应包含：

——负责修复的人员的姓名；

一 恢复的 PII 的描述。

一些司法管辖区规定了 PII 恢复工作的日志内容。组织应该能够记录对还原日志内容的任何此类要求的遵守情况。这种审议的结论应列入书面资料。

本文档中适用于分包 PII 处理的控制措施涵盖了使用分包商存储已处理的 PII 的复制或备份副本（参见 B.3.10、B.3.20）。在与备份和恢复相关的物理介质传输发生的情况下，本文档中的控制措施也涵盖了这一点（参见 B.3.7）。

B.3.25 日志记录

控制

应生成、存储、保护和分析记录与 PII 处理相关的活动、异常、故障和其他相关事件的日志。

实施指南

应制定一个流程，使用连续、自动化的监控和警报流程来审查事件日志，或者手动执行此类审查，并按指定的、记录的周期执行此类审查，以识别违规行为并提出补救措施。

在可能的情况下，事件日志应记录对 PII 的访问，包括谁、何时、哪个 PII 主体的 PII 被访问，以及由于事件而进行了哪些（如果有）更改（例如添加、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以有不同或共享的角色。应明确定义这些角色并将其包含在记录的信息中，并且应解决提供商之间对任何日志访问的协议。

例如，为安全监控和作诊断而记录的日志信息可以包含 PII。应采取控制访问等措施，以确保记录的信息仅按预期使用。

应制定一个程序，最好是自动程序，以确保按照保留时间表的规定删除或去识别化记录的信息（见B.1.4.8）。

PII 处理器的实施指南

组织应定义有关是否、何时以及如何向客户提供日志信息或可供客户使用的标准。这些标准应提供给客户。

如果组织允许其客户访问组织控制的日志记录，则组织应实施适当的控制措施，以确保客户：

一 只能访问与该客户活动相关的记录;

一 无法访问任何与其他客户活动相关的日志记录;和

一 不能以任何方式修改日志。

B.3.26 密码学的使用

控制

应定义和实施有效使用与个人身份信息处理相关的密码学的规则，包括加密密钥管理。

实施指南

一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加密技术来保护其处理的PII的情况的信息。组织还应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自己的加密保护。

B.3.27 安全的开发生命周期

控制

应制定并应用与个人身份信息处理相关的软件和系统的安全开发规则。

实施指南

系统开发和设计的政策应包括根据对PII委托人的义务或任何适用的法律要求以及组织执行的处理类型，对组织处理 PII 需求的指导。

有助于隐私设计和默认隐私的策略应考虑以下方面：

a） 关于 PII 保护和在软件开发生命周期中实施隐私原则（参见 ISO/IEC 29100）的指南;

b） 设计阶段的隐私和 PII 保护要求，可以基于隐私风险评估或隐私影响评估的输出（见 B.1.2.6）;

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]，最小化对PII的处理。

B.3.28应用程序安全要求

控制

在开发或获取应用程序时，应确定、指定和批准与 PII 处理相关的信息安全要求。

实施指南

组织应确保通过不受信任的数据传输网络传输的 PII 经过加密以进行传输。

不受信任的网络可能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公开一些标头或流量数据才能有效传输。

B.3.29 安全系统架构和工程原则

控制

应建立、记录、维护和应用于任何信息系统开发活动的与处理 PII 相关的工程安全系统的原则。

实施指南

与 PII 处理相关的系统或组件应遵循设计隐私和默认隐私原则进行设计，并预测和促进相关控制的实施（分别如 B.1 和 B.2 中针对 PII 控制者和 PII 处理者所述），特别是在这些系统中收集和处理 PII 仅限于确定目的所需的范围PII 的处理（see B.1.2.2）。

例如，处理 PII 的组织应确保在指定期限后处理 PII。处理该 PII 的系统应以促进此删除要求的方式设计。

注意 ：法律要求可能适用。

B.3.30 外包开发

控制

该组织应指导、监控和审查与外包 PII 处理系统开发相关的活动。

实施指南

如果适用，应将设计隐私和默认隐私的相同原则（见B.3.29）应用于外包信息系统。

B.3.31 测试信息

控制

应适当选择、保护和管理与 PII 处理相关的测试信息。

实施指南

个人身份信息不应用于测试目的;应使用false或合成PII。在无法避免将 PII 用于测试目的的情况下，应实施与生产环境中使用的技术和组织措施相当的技术和组织措施，以最大限度地降低风险。如果这种等效措施不可行，则应进行风险评估，并用于确定选择适当的缓解控制措施。

附件C

（信息丰富）

映射到 ISO/IEC 29100

表 C.1 和 C.2 给出了本文档的规定与 ISO/IEC 29100 中的隐私原则之间的指示性映射。表 C.1 和 C.2 以纯粹的指示性方式显示了符合本文档的要求和控制措施如何与 ISO/IEC 29100 中规定的一般隐私原则相关。表 C.1 和 C.2 中的交叉引用与表 A.1 至 A.3 中引用的控制措施相对应。

表 C.1 - PII 控制器和 ISO/IEC29100 的控件映射

ISO/IEC29100 的隐私原则	PII 控制器的相关控件
1.同意与选择（ISO/IEC 29100：2024,6.2）	A.1.2.2 识别和记录目的 A.1.2.3 确定法律依据 A.1.2.4 确定何时以及如何获得同意A.1.2.5 获得同意并记录在案 A.1.2.6 隐私影响评估 A.1.3.5 提供修改或撤回同意的机制 A.1.3.6 提供反对个人信息处理的机制 A.1.3.8 PII 控制者通知第三方的义务
2.目的合法性和规范（ISO/IEC 29100：2024,6.3）	A.1.2.2 确定并记录目的A.1.2.3 确定合法依据 A.1.2.6 隐私影响评估 A.1.3.3 确定 PII 委托人的信息A.1.3.4 向 PII 委托人提供信息 A.1.3.11 自动决策
3.采集限制（ISO/IEC 29100：2024,6.4）	A.1.2.6 隐私影响评估A.1.4.2 限制收集
4.数据最小化（ISO/IEC 29100：2024,6.5）	A.1.4.3 极限处理 A.1.4.5 个人身份信息最小化目标 A.1.4.6 处理结束时的PII去标识化和删除
5.使用、保留和披露限制（ISO/IEC 29100：2024,6.6）	A.1.4.5 个人身份信息最小化目标 A.1.4.6 处理结束时的PII去标识化和删除A.1.4.7 临时文件 A.1.4.8 保留 A.1.4.9 处置 A.1.5.2 确定司法管辖区之间PII传输的依据A.1.5.5 向第三方披露

	PII的记录
6.精度和质量（ISO/IEC 29100：2024,6.7）	A.1.4.4 准确性和质量
7.公开、透明和通知（ISO/IEC 29100：2024,6.8）	A.1.3.3 确定 PII 主体的信息A.1.3.4 向 PII 主体提供信息
8.个人参与和访问（ISO/IEC 29100：2024,6.9）	A.1.3.2 确定和履行对 PII 委托人的义务A.1.3.4 向 PII 委托人提供信息 A.1.3.7 访问、更正或删除 A.1.3.9 提供已处理的 PII 副本A.1.3.10 处理请求

表C.1（续）

ISO/IEC29100 的隐私原则	PII 控制器的相关控件
9. 问责制（ISO/IEC 29100：2024,6.10）	A.1.2.7 与 PII 处理者的合同 A.1.2.8 联合 PII 控制器 A.1.2.9 与处理个人身份信息相关的记录 A.1.3.10 处理请求 A.1.5.2 确定司法管辖区之间个人身份信息传输的依据 A.1.5.3 可以转交个人信息的国家和国际组织 A.1.5.4 PII转移记录
10. 信息安全（ISO/IEC 29100：2024,6.11）	A.1.2.7 与PII处理者的合同A.1.4.10 PII传输控制
11. 隐私合规（ISO/IEC 29100：2024,6.12）	A.1.2.6 隐私影响评估

表C.2 - PII处理器和ISO/IEC 29100控制的映射

ISO/IEC29100 的隐私原则	PII 处理器的相关控制
1. 同意和选择（ISO/IEC 29100：2024,6.2）	A.2.2.6 客户义务
2. 用途合法性和规范（ISO/IEC29100：2024,6.3）	A.2.2.2 客户协议 A.2.2.3 本组织的宗旨 A.2.2.4 营销和广告使用A.2.2.5 侵权指令 A.2.3.2 遵守对太平委托人的义务
3. 采集限制（ISO/IEC 29100：2024,6.4）	不适用
4. 数据最小化（ISO/IEC 29100：2024,6.5）	A.2.4.2 临时文件
5. 使用、保留和披露限制（ISO/IEC29100：2024,6.6）	A.2.5.4 向第三方披露个人信息的记录A.2.5.5 个人信息披露请求的通知 A.2.5.6 具有法律约束力的 PII 披露
6. 精度和质量（ISO/IEC 29100：2024,6.7）	不适用
7. 公开、透明、通知（ISO/IEC 29100：2024,6.8）	A.2.5.7 披露用于处理 PII 的分包商A.2.5.8 委托分包商处理PII A.2.5.9 处理PII的分包商变更
8. 个人参与和访问（ISO/IEC 29100：2024,6.9）	A.2.3.2 遵守对太平委托人的义务

9. 问责制（ISO/IEC 29100：2024,6.10）	A.2.2.7 与处理 PII 相关的记录 A.2.4.3 个人身份信息的返还、转让或处置 A.2.5.2 司法管辖区之间PII转移的依据 A.2.5.3 个人身份信息可以转让给的国家和国际组织
10. 信息安全（ISO/IEC 29100：2024,6.11）	A.2.4.4 PII 传输控制
11. 隐私合规性（ISO/IEC 29100：2024,6.12）	A.2.2.6 客户义务

附件D

（信息丰富）

与《通用数据保护条例》的映射

表 D.1 给出了本文件规定与欧盟《通用数据保护条例》第 5 条至第 49 条（第 43 条除外）之间的指示性映射。[16可 D.1 显示了遵守本文档的要求和控制措施如何与履行 GDPR 的义务相关。

注意：此表纯粹是指示性的。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 - 本文档与 GDPR 文章的映射

本文件的子条款	相关 GDPR 文章
4.1	(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）、（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)
4.2	（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）
4.3	(32)(2)
4.4	(32)(2)
6.1.2	(32)(1)（b），（32）（2）
6.1.3	〔32〕（1）（b），（32）（2）
5.2	(24)(2)
5.3	(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）
B.3.5	(5)（1）f），（32）（2）
B.3.6	(5)（1）f）
B.3.7	(5)（1）f）

B.3.9	(5) (1) f)
B.3.10	(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)
B.3.11	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)
B.3.12	(33) (1)、(33) (2)、(33) (3) (a)、(33) (3) (b)、(33) (3) (c)、(33) (3) (d)、(33) (4)、(33) (5)、(34) (1)、(34) (2)
B.3.13	(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)
B.3.14	(5)(2),(24)(2)
B.3.15	(32)(1) (d)，(32) (2)
B.3.16	(32)(1) (d)，(32) (2)
B.3.17	(39)(1) (二)
B.3.18	(5) (1) f)、(28) (3) (b)、(38) (5)
B.3.19	(5) (1) f)
B.3.20	(5) (1) f)，(32) (1) (a)

表D.1（续）

本文件的子条款	相关 GDPR 文章
B.3.21	(5)（1）f）
B.3.22	(5)（1）f）
B.3.23	(5)（1）f）
B.3.24	(5)（1）f），（32）（1）（C）
B.3.25	(5)（1）f）
B.3.26	(32)(1)（一）
B.3.27	(25)(1)
B.3.28	(5)（1）f），（32）（1）（a）
B.3.29	(25)(1)
B.3.31	(5)（1）f）
B.1.2.2	(5)(1)（b），（32）（4）
B.1.2.3	（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）
B.1.2.4	(8)(1),(8)(2)
B.1.2.5	(7)（1）、（7）（2）、（9）（2）（a）
B.1.2.6、	(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）
B.1.2.7	(5)（2）、（28）（3）（e）、（28）（9）
B.1.2.8	(26)(1),(26)(2),(26)(3)
B.1.2.9	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)
B.1.3.2	(12)(2)

B.1.3.3	(11) (2)、(13) (3)、(13) (1) (a)、(13) (1) (b)、(13) (1) (c)、(13) (1) (d)、(13) (e)、(13) (4)、(14) (1) (a)、(14) (b)、(14) (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)
B.1.3.4	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
B.1.3.5	(7) (3)、(13) (2) (c)、(14) (2) (d)、(18) (1) (a)、(18) (1) (b)、(18) (1) (c)、(18) (1) (d)
B.1.3.6	(13)(2) (b)、(14) (2) (c)、(21) (1)、(21) (2)、(21) (2)、(21) (3)、(21) (5)、(21) 6)
B.1.3.7、	(5) (1) (d)、(13) (2) (b)、(14) (2) (c)、(16)、(17) (1) (a)、(17) (1) (b)、(17) (c)、(17) (1) (d)、(17) (e)、(17) (1) (f)、(17) (2)
B.1.3.8	(19)
B.1.3.9	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
B.1.3.10	(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)
B.1.3.11	(13)(2) (f)，(14) (2) (g)，(22) (1)，(22) (3)
B.1.4.2	(5)(1) (b)，(5) (1) (c)
B.1.4.3	(25)(2)
B.1.4.4	(5)(1) (四)
B.1.4.5	(5)(1) (c)，(5) (1) (e)
B.1.4.6	(5)(1) (C)、(5) (1) (e)、(6) (4) (e)、(11) (1)、(32) (1) (a)
B.1.4.7	(5) (1) c)
B.1.4.8	(13)(2) (a)，(14) (2) (a)

表D.1（续）

本文件的子条款	相关 GDPR 文章
B.1.4.9	(5)（1）f）
B.1.4.10	(5)（1）f）
B.1.5.阿拉伯数字	(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）（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）（1）、（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）
B.1.5.3	(15)（2），（30）（1）（e）
B.1.5.4	(30)(1)（戊）
B.1.5.5	(30)(1)（四）
B.2.2.2	(28)（3）f）、（28）（3）（e）、（28）（9）、（35）（1）
B.2.2.3	(5)(1)（a）、（5）（1）（b）、（28）（3）（a）、（29）、（32）（4）
B.2.2.4	(7)(4)
B.2.2.5	(28)(3)（八）
B.2.2.6	(28)(3)（八）
B.2.2.7	(30)（3）、（30）（4）、（30）（5）、（30）（2）（a）、（30）（2）（b）
B.2.3.2	(15)（3）、（17）（2）、（28）（3）（e）
B.2.4.2	(5)(1)（三）
B.2.4.3	(28)(3)（g），（30）（1）f）
B.2.4.4	(5)（1）f）
B.2.5.2	（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）
B.2.5.3	(30)（2）c）
B.2.5.4	(30)(1)（四）
B.2.5.5	(28)(3)（一）
B.2.5.6	(48)

B. 2. 5. 7	(28) (2), (28) (4)
B. 2. 5. 8	(28) （2）， （28） （3） （d）
B. 2. 5. 9	(28) (2)

附件E
（信息丰富）

映射到 ISO/IEC 27018 和 ISO/IEC 29151

ISO/IEC 27018 为充当 PII 处理器和提供公共云服务的组织提供了更多信息。ISO/IEC 29151 为 PII 控制器处理 PII 提供了额外的控制和指导。

表 E.1 给出了本文档规定与 ISO/IEC 27018 和 ISO/IEC29151 规定之间的指示性映射。它显示了本文档的要求和控制措施如何与 ISO/IEC 27018 或 ISO/IEC 29151 的规定相对应。

表E.1所示的映射纯粹是指示性的;这些条款之间的给定联系并不意味着它们是等同的。

表E.1 - ISO/IEC 27701与ISO/IEC 27018和ISO/IEC29151的映射

本文档中的子条款	ISO/IEC27018 中的子条款	ISO/IEC29151 中的子条款
4	不适用	不适用
5	不适用	不适用
6	不适用	不适用
7	不适用	不适用
8	不适用	不适用
9	不适用	不适用
10	不适用	不适用
B.3.2	不适用	不适用
B.3.3，B.3.4，B.3.5，B.3.6，B.3.7，B.3.8，B.3.9，B.3.10，B.3.11，B.3.12，B.3.13，B.3.14，B.3.15，B.3.16	5.1, 5.2, 5.12, 5.13, 5.14, 5.16, 5.18, 5.20, 5.24, 5.26, 5.31, 5.33, 5.35, 5.36，A.10.1，A.10.2，A.11.8，A，11,9，A.11.10，A.11.11	5.1, 5.2, 5.12, 5.13, 5.14, 5.16, 5.18, 5.22, 5.24, 5.26, 5.31, 5.33, 5.35, 5.36
B.3.17，B.3.18	6.3, 6.6，A11.1	6.3, 6.6
B.3.19，B.3.20，B.3.21	7.7, 7.10, 7.14，A.11.2，A.11.4，A.11.5，A.11.13，	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.10, 7.14
B.3.22，B.3.23，B.3.24，B.3.25，B.3.26，B.3.27，B.3.28，	8.1, 8.5, 8.13, 8.15, 8.24, 8.25, 8.26, 8.27, 8.30, 8.33，A.11.6	8.1, 8.13, 8.15, 8.24, 8.25, 8.26, 8.27, 8.30, 8.33

B.3.29，B.3.30，B.3.31		
B.1.2.2	不适用	答.4
B.1.2.3	不适用	答 4.1
B.1.2.4	不适用	答 3.1
B.1.2.5	不适用	答 3.1
B.1.2.6	不适用	答.11.2
B.1.2.7	不适用	答 11.3
B.1.2.8	不适用	不适用
B.1.2.9	不适用	8.15
B.1.3.2	不适用	答.10
B.1.3.3	不适用	答 9.2
B.1.3.4	不适用	答.9

表1（续）

B.1.3.5	不适用	答 3.2
B.1.3.6	不适用	答 3.2
B.1.3.7	不适用	A.10.1，A.10.2
B.1.3.8	不适用	答 10.2
B.1.3.9	不适用	答 10.1
B.1.3.10	不适用	答 10.1
B.1.3.11	不适用	不适用
B.1.4.2	不适用	答 5
B.1.4.3	不适用	答 7.1
B.1.4.4	不适用	答.8
B.1.4.5	不适用	答.6
B.1.4.6	不适用	答 7.1
B.1.4.7	不适用	答 7.2
B.1.4.8	不适用	答 7.1
B.1.4.9	不适用	答7.14
B.1.4.10	不适用	不适用
B.1.5.2	不适用	答.13.2
B.1.5.3	不适用	答.13.2
B.1.5.4	不适用	答.13.2
B.1.5.5	不适用	答 7.4
B.2.2.2	不适用	不适用
B.2.2.3	答 3.1	不适用
B.2.2.4	答 3.2	不适用
B.2.2.5	不适用	不适用
B.2.2.6	不适用	不适用
B.2.2.7	不适用	答 7.4
B.2.3.2	答 2.1	不适用
B.2.4.2	答.5.1	答 7.2
B.2.4.3	答.10.3	答 11.3
B.2.4.4	答.12.2	不适用
B.2.5.2	不适用	A.4.1，A.13.2

B.2.5.3	答 12.1	答.13.2
B.2.5.4	答 6.2	答 7.4
B.2.5.5	答 6.1	答7.3
B.2.5.6	答 6.1	答7.3
B.2.5.7	答8.1	答7.5
B.2.5.8	答8.1	不适用
B.2.5.9	答8.1	不适用

附件F

（信息丰富）

与 ISO/IEC 27701：2019 的对应关系

本附件的目的是为当前正在使用该文档并希望过渡到此新版本的组织提供与本文档先前版本（ISO/IEC 27701：2019）的向后兼容性。

表 F.1 提供了附录 A 中规定的控制措施与 ISO/IEC 27701：2019 中规定的控制措施的对应关系。“N/A”标识本文档中未包含的控件。新“标识 ISO/IEC 27701：2019 中未包含的控件。

表 F.1 — 本文档中的控制措施与 ISO/IEC 27701：2019 中的控制措施之间的对应关系

ISO/IEC27701 控制标识符	国际标准化标准/ IEC 27701：2019 控制标识符	控制名称
答 3.3	6.2.1.1,6.2.1.2	信息安全政策
答 3.4	6.3.1.1	信息安全角色和职责
不适用	6.3.1.2	职责分离
不适用	6.4.2.1	管理职责
不适用	6.3.1.3	与当局联系
不适用	6.3.1.4	与特殊兴趣团体联系
不适用	新增功能	威胁情报
不适用	6.3.1.5,6.11.1.1	项目管理中的信息安全
不适用	6.5.1.1,6.5.1.2	信息和其他相关资产的清单
不适用	6.5.1.3,6.5.2.3	信息和其他相关资产的可接受使用
不适用	6.5.1.4	资产返还
答 3.5	6.5.2.1	信息分类
答 3.6	6.5.2.2	信息标签
答 3.7	6.10.2.1、6.10.2.2、6.10.2.3	信息传递
不适用	6.6.1.1,6.6.1.2	存取控制
答 3.8	6.6.2.1	身份管理

不适用	6.6.2.4,6.6.3.1, 6.6.4.3	身份验证信息
答3.9	6.6.2.2,6.6.2.5, 6.6.2.6	访问权限
答 3.10	6.12.1.1 6.12.1.2	在供应商协议中解决信息安全问题
不适用	6.12.1.3	管理ICT供应链中的信息安全
不适用	6.12.2.1,6.12.2.2	供应商服务的监控、审查和变更管理
不适用	新增功能	使用云服务的信息安全
不适用	6.13.1.1	信息安全事件管理规划和准备
答3.11	6.13.1.4	信息安全事件的评估和决策
答 3.12	6.13.1.5	信息安全事件应对
不适用	6.13.1.6	从信息安全事件中吸取教训

表 F.1（续）

ISO/IEC 27701 控制标识符	国际标准化标准/ IEC 27701：2019 控制标识符	控制名称
不适用	6.13.1.7	证据收集
不适用	6.14.1.1、6.14.1.2、 6.14.1.3	中断期间的信息安全
不适用	新增功能	为业务连续性准备ICT
答 3.13	6.15.1.1,6.15.1.5	法律、法定、监管和合同要求
不适用	6.15.1.2	知识产权
答3.14	6.15.1.3	保护记录
不适用	6.15.1.4	隐私和 PII 保护
答 3.15	6.15.2.1	信息安全独立审查
答 3.16	6.15.2.2,6.15.2.3	遵守信息安全政策、规则和标准
不适用	6.9.1.1	记录在案的作程序
不适用	6.4.1.1	筛分
不适用	6.4.1.2	雇佣条款和条件
答 3.17	6.4.2.2	信息安全意识、教育培训
不适用	6.4.2.3	纪律处分程序
不适用	6.4.3.1	终止或变动后的责任
答3.18	6.10.2.4	保密或保密协议
不适用	6.3.2.2	远程工作
不适用	6.13.1.2,6.13.1.3	信息安全事件报告
不适用	6.8.1.1	物理安全边界
不适用	6.8.1.2,6.8.1.6	实体入口
不适用	6.8.1.3	确保办公室、房间和设施的安全
不适用	新增功能	物理安全监控
不适用	6.8.1.4	防范物理和环境威胁
不适用	6.8.1.5	在安全区域工作
答3.19	6.8.2.9	清晰的办公桌和清晰的屏幕
不适用	6.8.2.1	设备选址和保护
不适用	6.8.2.6	外部资产的安全性

答3.20	6.5.3.1,6.5.3.2, 6.5.3.3,6.8.2.5	存储介质
不适用	6.8.2.2	支持公用事业
不适用	6.8.2.3	布线安全
不适用	6.8.2.4	设备维护
答3.21	6.8.2.7	安全处置或重复使用设备
答3.22	6.3.2.1,6.8.2.8	用户终结点设备
不适用	6.6.2.3	特权访问权限
不适用	6.6.4.1	信息访问限制
不适用	6.6.4.5	访问源代码
答3.23	6.6.4.2	安全身份验证
不适用	6.9.1.3	容量管理
不适用	6.9.2.1	防恶意软件
不适用	6.9.6.1	技术漏洞管理
不适用	新增功能	配置管理

表F.1（续）

ISO/IEC 27701 控制标识符	国际标准化标准/ IEC 27701：2019 控制标识符	控制名称
不适用	新增功能	信息删除
不适用	新增功能	数据屏蔽
不适用	新增功能	数据泄露预防
答 3.24	6.9.3.1	信息备份
不适用	6.14.2.1	信息处理设施的冗余
答：3.25	6.9.4.1,6.9.4.2, 6.9.4.3	伐木
不适用	新增功能	监测活动
不适用	6.9.4.4	时钟同步
不适用	6.6.4.4	使用特权公用事业计划
不适用	6.9.5.1,6.9.6.2	在作系统上安装软件
不适用	6.10.1.1	网络安全
不适用	6.10.1.2	网络服务安全
不适用	6.10.1.3	网络隔离
不适用	新增功能	Web 过滤
答3.26	6.7.1.1,6.7.1.2	密码学的使用
答3.27	6.11.2.1	安全的开发生命周期
答3.28	6.11.1.2,6.11.1.3	应用程序安全要求
答3.29	6.11.2.5	安全系统架构和工程原理
不适用	新增功能	安全编码
不适用	6.11.2.8,6.11.2.9	开发和验收中的安全测试
答：3.30	6.11.2.7	外包开发
不适用	6.9.1.4,6.11.2.6	开发、测试和生产环境分离
不适用	6.9.1.2,6.11.2.2, 6.11.2.3,6.11.2.4	变更管理
答3.31	6.11.3.1	测试信息
不适用	6.9.7.1	在审计测试期间保护信息系统

表 F.2 提供了 ISO/IEC 27701：2019 第 6
条中规定的控制措施与本文档中规定的控制措施的对应关系。N/A“标识本文档中未包含的控件。

表 F.2 - ISO/IEC 27701：2019 中的控制与本文档中的控制之间的对应关系

国际标准化标准/ IEC27701：2019 控制标识符	ISO/IEC27701 控制标识符	控制名称符合 ISO/IEC 27701：2019
6.2.1.1	答 3.3	信息安全政策
6.2.1.2	答 3.3	信息安全政策的审查
6.3.1.1	答 3.4	内部安全角色和职责
6.3.1.2	不适用	职责分离
6.3.1.3	不适用	与当局联系
6.3.1.4	不适用	与特殊兴趣团体联系
6.3.1.5	不适用	项目管理中的信息安全
6.3.2.1	答3.22	移动设备政策
6.3.2.2	不适用	远程办公

表F.2（续）

国际标准化标准/IEC27701：2019 控制标识符	ISO/IEC27701 控制标识符	控制名称符合 ISO/IEC 27701：2019
6.4.1.1	不适用	筛分
6.4.1.2	不适用	雇佣条款和条件
6.4.2.1	不适用	管理职责
6.4.2.2	答 3.17	信息安全意识、教育培训
6.4.2.3	不适用	纪律处分程序
6.4.3.1	不适用	终止或改变雇佣责任
6.5.1.1	不适用	资产清单
6.5.1.2	不适用	资产所有权
6.5.1.3	不适用	可接受的资产用途
6.5.1.4	不适用	资产返还
6.5.2.1	答 3.5	信息分类
6.5.2.2	答 3.6	信息标签
6.5.2.3	不适用	资产处理
6.5.3.1	答3.20	可移动媒体的管理
6.5.3.2	答3.20	媒体的处置
6.5.3.3	答3.20	物理介质传输
6.6.1.1	不适用	访问控制策略
6.6.1.2	不适用	访问网络和网络服务
6.6.2.1	答 3.8	用户注册和注销
6.6.2.2	答3.9	用户访问预配
6.6.2.3	不适用	特权访问权限的管理
6.6.2.4	不适用	用户的秘密认证信息管理
6.6.2.5	答3.9	用户访问权限审查
6.6.2.6	答3.9	删除或调整访问权限
6.6.3.1	不适用	使用密钥认证信息
6.6.4.1	不适用	信息访问限制
6.6.4.2	答3.23	安全登录过程
6.6.4.3	不适用	密码管理系统

6.6.4.4	不适用	使用特权公用事业计划
6.6.4.5	不适用	对程序源代码的访问控制
6.7.1.1	答3.26	关于使用加密控制的政策
6.7.1.2	答3.26	密钥管理
6.8.1.1	不适用	物理安全边界
6.8.1.2	不适用	物理进入控制
6.8.1.3	不适用	确保办公室、房间和设施的安全
6.8.1.4	不适用	防范外部和环境威胁
6.8.1.5	不适用	在安全区域工作
6.8.1.6	不适用	送货和装货区
6.8.2.1	不适用	设备选址和保护
6.8.2.2	不适用	支持公用事业
6.8.2.3	不适用	布线安全
6.8.2.4	不适用	设备维护
6.8.2.5	不适用	资产移除

表F.2（续）

国际标准化标准/IEC27701：2019 控制标识符	ISO/IEC27701 控制标识符	控制名称符合 ISO/IEC 27701：2019
6.8.2.6	不适用	场外设备和资产的安全
6.8.2.7	答3.21	安全处置或重复使用设备
6.8.2.8	答3.22	无人值守用户设备
6.8.2.9	答3.19	清晰的办公桌和清晰的屏幕政策
6.9.1.1	不适用	记录作程序
6.9.1.2	不适用	变更管理
6.9.1.3	不适用	容量管理
6.9.1.4	不适用	开发、测试和运营环境的分离
6.9.2.1	不适用	针对恶意软件的控制
6.9.3.1	答 3.24	信息备份
6.9.4.1	答：3.25	事件日志记录
6.9.4.2	答：3.25	日志信息保护
6.9.4.3	答：3.25	管理员和操作员日志
6.9.4.4	不适用	时钟同步
6.9.5.1	不适用	在作系统上安装软件
6.9.6.1	不适用	技术漏洞管理
6.9.6.2	不适用	软件安装限制
6.9.7.1	不适用	信息系统审计控制
6.10.1.1	不适用	网络控制
6.10.1.2	不适用	网络服务中的安全性
6.10.1.3	不适用	网络中的隔离
6.10.2.1	答 3.7	信息传输政策和程序
6.10.2.2	答 3.7	信息转让协议
6.10.2.3	答 3.7	电子消息传递
6.10.2.4	答3.18	保密或保密协议
6.11.1.1	不适用	信息安全需求分析与规范
6.11.1.2	答3.28	保护公共网络上的应用程序服务
6.11.1.3	答3.28	保护应用程序服务事务

6.11.2.1	答3.27	安全开发策略
6.11.2.2	不适用	系统变更控制过程
6.11.2.3	不适用	作平台变更后应用技术审查
6.11.2.4	不适用	对软件包的更改限制
6.11.2.5	答3.29	安全系统工程原则
6.11.2.6	不适用	安全的开发环境
6.11.2.7	答：3.30	外包开发
6.11.2.8	不适用	系统安全测试
6.11.2.9	不适用	系统验收测试
6.11.3.1	答：3.30	保护测试数据
6.12.1.1	答 3.10	供应商关系信息安全政策
6.12.1.2	答 3.10	解决供应商协议中的安全性问题
6.12.1.3	不适用	信息通信技术供应链
6.12.2.1	不适用	对供应商服务的监控和审查
6.12.2.2	不适用	管理供应商服务的变更

表F.2（续）

国际标准化标准/IEC27701：2019 控制标识符	ISO/IEC27701 控制标识符	控制名称符合 ISO/IEC 27701：2019
6.13.1.1	不适用	职责和程序
6.13.1.2	不适用	报告信息安全事件
6.13.1.3	不适用	报告信息安全漏洞
6.13.1.4	答3.11	信息安全事件的评估和决策
6.13.1.5	答 3.12	信息安全事件应对
6.13.1.6	不适用	从信息安全事件中吸取教训
6.13.1.7	不适用	证据收集
6.14.1.1	不适用	规划信息安全连续性
6.14.1.2	不适用	实施信息安全连续性
6.14.1.3	不适用	验证、更新和评估信息安全连续性
6.14.2.1	不适用	信息处理设施的可用性
6.15.1.1	答 3.13	确定适用的立法和合同要求
6.15.1.2	不适用	知识产权
6.15.1.3	答3.14	保护记录
6.15.1.4	不适用	隐私和个人身份信息保护
6.15.1.5	答 3.13	加密控制的监管
6.15.2.1	答 3.15	信息安全独立审查
6.15.2.2	答 3.16	遵守安全策略和标准
6.15.2.3	答 3.16	技术合规性审查

书目

[1] *ISO 19011，管理体系审核指南*

[2] ISO/IEC19944-1，云计算与分布式平台——数据流、数据类别和数据使用——第一部分：基础

[3] ISO/IEC 19944-2，云计算和分布式平台——数据流、数据类别和数据使用——第2部分：应用和可扩展性指南

[4] ISO/IEC 20889，隐私增强数据去标识化术语和技术分类

[5] ISO/IEC 27001，信息安全、网络安全和隐私保护——信息安全管理体系——要求

[6] ISO/IEC 27002，信息安全、网络安全和隐私保护——信息安全控制

[7] ISO/IEC 27005，信息安全、网络安全和隐私保护——信息安全风险管理指南

[8] ISO/IEC 27018，信息安全、网络安全和隐私保护——作为 PII 处理器的公共云中个人身份信息（PII）保护指南

[9] ISO/IEC 27035（所有部分），信息技术—信息安全事件管理

[10] ISO/IEC 27557，信息安全、网络安全和隐私保护——ISO 31000：2018在组织隐私风险管理中的应用

[11] ISO/IEC 29101：2018，信息技术—安全技术—隐私架构框架

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

[13] ISO/IEC 29151，信息技术 - 安全技术 - 个人身份信息保护行为准则

[14] ISO/IEC 29184，信息技术 - 在线隐私声明和同意

[15] ISO 31000，风险管理——指南

[16] 欧洲议会和理事会的通用数据保护条例（EU）-Regulation（EU）2016/79

国际集成电路 35.030

价格基于 64 页