国际标准

ISO/IEC 27701

信息安全、网络安全和隐私保护——隐私信息管理体系

——要求与指南

信息安全、网络安全与隐私保护——隐私信息管理体系—要求与建议

第二版2025-10

参考编号ISO/IEC
27701:2025(en)

版权保护文件

ISO版权办公室
CP 401·布兰东内街8号CH-1214 韦 尔
尼耶，日内瓦电话：+41227490111
电子邮箱：copyright@iso.org 网站：
www.iso.org

瑞士出版

目 录

页码

前言

国际标准化组织(ISO) 与国际电工委员会 (IEC) 共同构成全球标准化专业体系。作为ISO 或IEC 成员的国家机构，通过各组织为特定技术领域设立的技术委员会参与国际标准制定工作。 ISO 与IEC 技术委员会在共同关注领域开展协作。其他与ISO 和IEC 保持联络的国际组织(包括政府组织和非政府组织)也参与相关工作。

本文件的编制程序及其后续维护程序详见ISO/IEC指令第1部分。特别需要注意的是，不同类型的文件需满足不同的批准标准。本文件的起草遵循了ISO/IEC 指令第2部分的编辑规则(详见www. iso.org/directives 或www.iec.ch/members experts/refdocs)。

ISO 和IEC 提醒注意，实施本文件可能涉及使用一项或多项专利。ISO 和IEC对任何相关专利权主张的证据、、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涉及的专利通知。但需提醒实施者注意，此信息可能并非最新状态，最新专利信息可通过www.iso.org/patents 和 htts://patents.iec.ch 查 询 。ISO 和IEC 不承担识别任何或所有此类专利权利的责任。

本文件中使用的任何商标名称仅为方便用户而提供，并不构成推荐。

关于标准自愿性的说明、ISO特定术语及符合性评估相关表述的含义，以及ISO 在《技术性贸易壁垒协定》(TBT)中遵循世界贸易组织(WTO)原则的信息，请参阅www.iso.org/iso/foreword.html。在IEC 中，请参阅www.iec.ch/understanding-standards。

本文件由国际标准化组织/国际电工委员会联合技术委员会1 (JTC1) 下属信息技术分技术委员会27 (SC 27) _____ *信息安全、网络安全与隐私保护分技术委员会*，与欧洲标准化委员会 (CEN) 技术委员会CEN/CLC/JTC 13——网络安全与数据保护技术委员会共同编制，依据ISO与CEN 技术合作协议(维也纳协议)完成。

本第二版取代并废止了经技术修订的第一版 (ISO/IEC 27701:2019)。

主要变更如下：

一 本文件已重新编写为独立的管理体系标准。

关于本文件的任何反馈或疑问，请联系用户所在国家的国家标准机构。这些机构的完整列表可查阅 www. iso. org/ members. html 和 www.iec.ch/national-committees。

引 言

0.1概述

几乎所有组织都会处理个人身份信息 (PII)。 随着组织间协作处理PII 的情形日益增多，所处理PII 的数量与类型也在持续增长。在处理PII过程中保障隐私既是社会需求，也是全球专项法律要求的核心议题。

本文档包含以下映射关系：

— ISO/IEC29100 中定义的隐私框架和原则；

— ISO/IEC27018;

一 ISO/IEC29151;

— 欧盟《通用数据保护条例》。

注 这些映射可根据当地法律要求进行解释。

本文件适用于个人身份信息 (PII) 控制者(包括共同控制者)及处理者(包括使用分包处理者的控制者，以及作为处理者分包商的处理者)。

通过遵守本文件的要求，组织可生成其处理个人身份信息(PII) 方式的证据。此类证据可用于促进与业务伙伴的协议达成，尤其在双方均涉及PII处理时。这亦有助于维护与其他相关方的关系。采用本文件可为该证据提供独立验证。

0.2 与其他管理体系标准的兼容性

本文件采用ISO 制定的框架，旨在提升其管理体系标准间的协调性。

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进行协调或整合，特别是与ISO/IEC 27001中规定的信息安全管理体系相协调。

信息安全、网络安全与隐私保护——隐私信息管理体系——要求与指南

0 范 围

本文件规定了建立、实施、维护和持续改进隐私信息管理体系(PIMS) 的要求。

同时提供实施指南以协助落实本文件要求。

本文件适用于对个人身份信息 (PII) 处理负有责任和问责的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。

1 规 范 性 引 用

以下文件在本文中被引用，其部分或全部内容构成本文件的要求。对于带日期的引用，仅适用所引用的版本。对于不带日期的引用，适用被引文件的最新版本(包括任何修订)。

ISO/IEC 29100, 信息技术——安全技术——隐私框架

2 术 语 、 定 义 和 缩 写

为本文件之目的，除另有规定外，采用ISO/IEC 29100所载术语及定义。ISO 与IEC 在下列网址维护标准化用术语数据库：

—ISO 在线浏览平台：可访问https://www.iso.org/obp

—IEC Electropedia: 访问地址https://www.electropedia.org/

3.1
组织
具有自身职能、责任、权限及关系以实现其目标(3.6)的个人或群体

注1:组织的概念包括但不限于个体经营者、公司、企业、机构、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，无论公营还是私营。
注释2:若该组织隶属于更大实体，则"组织"仅指该实体中属于隐私信息管理体系(3.23)范围的部分。

3.2
相关方
能够影响、受影响或认为自己受某项决定或活动影响的个人或组织(3.1)。

3.3
最高管理层
在最高层级指导和控制组织的人或群体（3.1）

注1:最高管理层有权在组织内部授权并提供资源。

注2:若管理体系(3.4)的范围仅覆盖组织的部分领域，则最高管理层指该部分领域的决策控制者。

3.4
管理体系
组 织 （3.1）中相互关联或相互作用的要素集合，用于制定政策(3.5)和目标
(3.6)，以及实现这些目标的过程(3.8)

注1:管理体系可涉及单一领域或多个领域。

条目注释2:管理体系要素包括组织的结构、角色与职责、规划和运作。

3.5
政策
组 织 （3.1）的意图和方向，由其最高管理层(3.3)正式表达

3.6
目标
需达成的结果

注1:目标可分为战略目标、战术目标或操作目标。

条目注释2:目标可涉及不同领域(如财务、健康与安全、环境)。例如，目标可以是全 组织性的，也可以针对特定项目、产品或流程(3.8)。

注3:目标可通过其他形式表达，例如作为预期结果、宗旨、操作标准、隐私目标，或使用其他含义相近的词语(如宗旨、目标或指标)。

注4:在隐私信息管理体系(3.23)的背景下，隐私目标由组织(3.1)设定，
组织(3.1)根据隐私政策(3.5)制定，以实现特定结果。

3.7
风险
不确定性的影响

注1:效应是指与预期值的偏差。可能是正向或负向偏差。

注释2:不确定性是指对某事件、其后果或发生概率的信息、理解或认知存在不足的状态，即使这种不足是部分性的。

注3:风险通常通过潜在事件及其后果，或二者的组合来表征。

注4:风险通常通过事件后果(包括环境变化)与发生概率的组合来表述。

3.8
过程
一组相互关联或相互作用的活动，通过使用或转化投入来交付成果

注1:过程结果称作产出、产品或服务，取决于引用的语境。

3.9
能力
将知识和技能应用于实现预期结果的能力

3.10
文件化信息
组 织 (3.1) 需要控制和维护的信息及其载体

注1:文件化信息可以采用任何格式和介质，来自任何来源。注2:文件化信息可指:

一 *管理体系(3.4),包括相关过程(3.8);*

一 为组织运作而创建的信息(文件);

一 实现结果的证据(记录)。

3.11
绩效
可测量的结果

注1:绩效可涉及定量或定性发现。

条目注释2:绩效可涉及管理活动、流程(3.8)、产品、服务、系统或
组织(3.1)。

3.12
持续改进
为提升绩效而反复开展的活动(3.11)

3.13
有效性
计划活动实现及计划结果达成的程度

3.14
要求
明示、默示或强制性的需求或期望

注释1:“通常暗示”是指该组织(3.1)的惯例或普遍做法
相关方(3.2)应知悉，所考虑的需求或期望是隐含的。

注2:规定要求是指明确表述的要求，例如在文件化信息(3.10)中表述的要求。

3.15
符合性
满足要求(3.14)

3.16
不符合
未满足要求(3.14)

3.17
纠正措施
消除不符合项(3.16)原因并防止再发的措施

3.18
审计
系统化且独立的过程(3.8),用于获取证据并客观评估其有效性，以确定审计标准的达成程度

注1:审计可分为内部审计(第一方)或外部审计(第二方或第三方),亦可为组合审计(融合两个或多个领域)

条目注释2:内部审计由组织(3.1)自身或代表其的外部方实施。条目注释3:“审计证据”和“审计标准”在ISO 19011中定义。

3.19
测量
确定数值的过程(3.8)

3.20
监测
确定系统、过程(3.8)或活动的状态

注1:确定状态时，可能需要进行检查、监督或批判性观察。

3.21
共同个人身份信息(PII)控制者
与一个或多个其他个人身份信息(PII)控制者共同确定个人身份信息处理目的和方式的个人身份信息控制者

3.22
客户
个人或组织(3.1)，能够或实际接收某项产品或服务，该产品或服务是为该个人或组织准备的或其所需的

示例 消费者、客户、最终用户、零售商、内部流程(3.8)的产品或服务接收方、受益方及购买方。

注1:客户可属于组织内部或外部。

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PI控制者，或是与PI处理分包商签订合同的PII处理者。

3.23
隐私信息管理系统PIMS
管理制度(3.4)，该制度旨在应对个人身份信息处理过程中可能影响隐私保护的问题

3.24
信息安全计划
旨在管理组织风险(3.7)的一套政策(3.5)、目标(3.6)和流程(3.8)
(3.1)资产，以确保信息的机密性、完整性和可用性

注1:信息安全计划可采用信息安全管理体系形式，例如基于ISO/IEC 27001标准的体系。

3.25
适用性声明
所有必要控制措施的文件记录，以及纳入或排除此类控制措施的理由

3 组织背景

3.1 理解组织及其环境

该组织应确定与其宗旨相关且影响其实现隐私信息管理体系预期结果能力的外部和内部事项。

组织应确定气候变化是否为相关事项。

组织应确定其是否作为个人身份信息(PII)的控制者(包括作为共同控制者)或处理者。

该组织应确定与其环境相关且影响其实现计划信息管理系统的预期成果能力的外部和内部事项。

注1 外部和内部事项可包括但不限于：

一 适用的隐私立法；

一 适用法规；

— 适用的司法裁决；

— 适用的组织环境、治理结构、政策和程序；

— 适用的行政决定：

— 适用的合同要求。

当组织同时承担两种角色(即个人身份信息控制者和个人身份信息处理者)时，应分别确定各自角色，并针对每个角色实施独立的控制措施。

注2 由于组织的角色取决于谁决定处理的目的和手段，因此该角色在每次处理PII时可能不同。

3.2 理解相关方的需求和期望

组织应确定：

一 与隐私信息管理体系相关的利益相关方；

一 这些相关方的相关要求；

一 哪些要求将通过隐私信息管理体系予以满足。

注1 相关利益相关方可能存在与气候变化相关的要求。

组织应将那些与个人身份信息处理相关联的利益相关方纳入其中，包括个人身份信息主体。

注2其他相关方可包括客户、监管机构、其他个人身份信息控制者、个人身份信息处理者及其分包商。

根据组织的职能定位，“客户”可理解为：

a) 与个人身份信息(PII) 控制者签订合同的组织(例如PII控制者的客户)；
注3 此情形可能涉及作为共同PII控制者的组织：

b) 与PI 处理者签订合同的PI 控制者(例如PII处理者的客户)；或

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

注4 在商业关联中(例如消费者、雇员、供应商、访客关系中)其个人身份信息被处理的个人，在本文件中称为“个人身份信息主体”。

注5 与PII处理相关的义务可由法律法规要求、合同义务及组织自主设定的目标确定。ISO/IEC 29100系列标准中规定的隐私原则为PII处理提供了指导。

注6 为证明符合组织义务，某些相关方可要求组织符合特定标准(如本文件规定的管理体系或任何相关规范体系)，并可要求组织提供经独立审核的符合性证明。

3.3 确定隐私信息管理体系的范围

组织应确定隐私信息管理体系的边界和适用性，以建立其范围。

确定范围时，组织应考虑：

一 第4.1条所述的外部和内部问题；

一 4.2节所述的要求。

该范围应作为文件化信息提供。

在确定PIMS范围时，组织应包含个人身份信息 (PII) 的处理。

3.4 隐私信息管理体系

组织应根据本文件的要求建立、实施、保持并持续改进隐私信息管理体系，包括所需流程及其相互作用。

4 领导层

4.1 领导层与承诺

最高管理层应通过以下方式展现对隐私信息管理系统的领导力与承诺：

— 确保隐私政策（参见5.2）和隐私目标（参见6.2）已建立且符合组织的战略方向；

— 确保隐私信息管理体系要求融入组织业务流程；

— 确保隐私信息管理体系所需资源的可用性；

一 传达有效隐私信息管理及符合隐私信息管理系统要求的重要性；

— 确保隐私信息管理体系实现预期结果；

一 指导并支持相关人员为隐私信息管理体系的有效性作出贡献；

一 推动持续改进；

一 支持其他相关角色在其职责范围内展现领导力。

注： 本文件中提及的"业务"可广义理解为组织存在目的的核心活动。

4.2 隐私政策

最高管理层应制定隐私政策，确保：

a) 符合组织宗旨；

b) 为设定隐私目标提供框架；

c) 包含满足适用要求的承诺；

d) 包括对隐私信息管理体系持续改进的承诺。隐私政策应：

— 以文件化形式提供；

一 在组织内部传达；

一 酌情向相关方提供。

4.3 角色、职责与权限

最高管理层应确保相关职责与权限在组织内部明确分配并传达。

最高管理层应分配以下职责与权限：

a) 确保隐私信息管理体系符合本文件要求；

b) 向最高管理层报告隐私信息管理体系的运行情况。

5 规 划

5.1 应对风险与机遇的行动方案

5.1.1 总则

在规划隐私信息管理体系时，组织应考虑4.1节所述问题及4.2节所述要求，确定需应对的风险与机遇，以：

—确保隐私信息管理体系能够实现预期结果；

— 防止或减少不良影响：

— 实现持续改进。组织应规划：

a) 应对这些风险和机遇的措施；

b) 如何

—将行动方案整合并实施于隐私信息管理体系流程中；

— 评估这些措施的有效性。

5.1.2 隐私风险评估

组织应制定并实施隐私风险评估流程，该流程需：

a) 建立并维护隐私风险标准，包括：

1）风险接受标准；以及

2）执行隐私风险评估的标准；

b) 确保重复进行的隐私风险评估产生一致、有效且可比的结果；

c) 识别隐私风险：

1) 隐私信息管理体系范围内与隐私保护相关的风险及信息安全风险；以及

2) 确定风险责任人的风险；

d) 分析隐私风险：

1）评估若c)1)中识别出的风险实际发生时，可能对组织及PII主体造成的潜在后果；

2）评估c)1)中识别风险发生的实际可能性；以及

3）确定风险等级：

e) 评估隐私风险时需：

1)将风险分析结果与a)项确立的风险标准进行比对；

2)对分析出的风险进行优先级排序以实施风险应对措施。

组织应保留隐私风险评估过程的文件化信息。

注 有关隐私风险评估流程的更多信息，请参阅ISO/IEC 27557标准。

5.1.3 隐私风险处理

组织应定义并实施隐私风险处理流程，以应对与个人身份信息处理相关的风险(包括对个人身份信息主体的风险及个人身份信息安全风险)，具体措施包括：

a) 根据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方案所需的所有控制措施；

注1 组织可按需设计控制措施，或从任何来源识别控制措施。

c) 识别并记录组织实施的信息安全计划，包括相应的安全控制措施；

信息安全计划至少应涵盖以下内容：

— 信息安全风险管理；

— 信息安全政策；

— 信息安全组织架构；

— 人力资源安全；

— 资产管理；

— 访问控制；

— 运行安全；

— 网络安全管理；

— 开发安全；

— 供应商管理；

— 事件管理；

— 信息安全连续性；

— 信息安全审查；

— 密码学；以及

一 物理与环境安全。

注2 ISO/IEC 27002提供了可能的信息安全控制措施清单。若信息安全计划基于ISO/IEC 27001制定，可参照ISO/IEC 27002确保未遗漏任何必要的信息安全控制措施。

d) 将上述b) 和c)项确定的控制措施与附件A中 的对照，并验证是否遗漏必要控制措施；

注3 附录A 包含可能的隐私控制措施清单。可参考附录A确保未遗漏任何必要的隐私控制措施。

注4 附件A所列隐私控制措施并非穷尽性清单，必要时可增补其他隐私控制措施。

注5 组织在处理PI 安全时，可将信息安全与隐私保护整合处理(例如合并风险评估)，也可作为存在交叉领域的独立实体分别处理。

e) 编制适用性声明，其中应包含：

—必要控制措施(参见b)、c)和d]项]；

—纳入这些控制措施的依据；

一 是否实施了必要的控制措施；以及

— 排 除附件A中任何控制措施的依据。

无需包含附件A中列出的所有控制措施。例如，若风险评估认定某项控制措施非必要，或其未被适用法律要求涵盖(或受例外条款约束)，包括适用于PII主体的相关要求，则可予以排除。

f) 制定隐私风险处理方案；

g) 获取隐私风险责任人对隐私风险处理方案的批准及对残余隐私风险的接受；以及

h) 考虑到附件B中关于实施b)和c)项所确定控制措施的指导意见。组织应保留有关隐私风险处理流程的文件化信息。

5.2 隐私目标及实现规划

组织应在相关职能和层级建立隐私目标。隐私目标应：

a) 与隐私政策保持一致(参见5.2)；

b) 可衡量(如可行)；

c) 考虑适用要求；
接受监控；

予以传达；

f) 适时更新；

g) 作为文件化信息予以提供。

在规划如何实现其隐私目标时，组织应确定：

— 采取哪些措施；

一 需要哪些资源；

— 由谁负责；

— 何时完成；

一 如何评估结果。

5.3 变更规划

当组织确定需要变更隐私信息管理体系时，应按计划实施变更。

6 支持

6.1 资源

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。

6.2 能力

组织应：

— 确定在其控制下从事影响隐私信息管理绩效工作的人员所需的必要能力；

— 确保这些人员具备相应的教育、培训或经验所形成的能力；

— 在适用情况下，采取措施获取必要能力，并评估所采取措施的有效性。

应提供适当的文件化信息作为能力证明。

注 适用措施可包括：为现有雇员提供培训、指导或重新分配工作；或招聘或签约合格人员。

6.3 认知

在组织控制下开展工作的人员应知晓：

一 隐私政策（参见5.2）；

一 其对隐私信息管理体系有效性的贡献，包括隐私保护成效提升带来的益处；

一 不符隐私信息管理体系要求所产生的影响。

6.4 沟通

组织应确定与隐私信息管理体系相关的内部和外部沟通，包括：

— 沟通内容；

一沟通时机；

一 沟通对象；

— 沟通方式。

6.5 文件化信息

6.5.1 总则

组织的隐私信息管理体系应包括：

a) 本文件要求的文件化信息；

b) 组织确定为隐私信息管理体系有效运行所必需的文件化信息。

注 隐私信息管理体系的文件化信息范围可能因以下因素而存在差异：

一 组织规模及其活动类型、流程、产品和服务；

一 流程及其交互作用的复杂程度；

— 人员能力水平。

6.5.2 文件化信息的创建与更新

在创建和更新文件化信息时，组织应确保适当：

一 识别与描述(例如标题、日期、作者或参考编号)；

— 格式(例如语言、软件版本、图形)和介质(例如纸质、电子)；

一 审查与批准以确保适用性与充分性。

6.5.3 文件化信息的控制

隐私信息管理体系及本文件要求的文件化信息应受控以确保：

a) 在需要时能够获取且适用；

b) 得到充分保护(例如防止机密性丧失、不当使用或完整性丧失)。

组织应针对文件化信息的控制开展以下适用活动：

—分发、访问、检索和使用：

— 存储与保存(包括可读性保存)；

一 变更控制(例如版本控制)；

— 保 留 与 处 置 。

组织确定为隐私信息管理体系规划和运行所必需的外部来源的文件化信息，应进行适当识别和控制。

注 访问权限可仅指查看文件化信息的许可，或指查看和更改文件化信息的许可和权限。

7 操作

7.1 运行规划与控制

组织应通过以下方式规划、实施和控制满足要求及执行第6条款所确定行动所需的流程：

一 建立流程标准；

— 依据标准实施过程控制。

应提供必要的文件化信息，以确保流程按计划执行。

组织应控制计划变更，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。

组织应确保与隐私信息管理体系相关的外部提供过程、产品或服务得到控制。

7.2 隐私风险评估

组织应在计划的时间间隔内或当重大变更被提出或发生时，参照6.1.2 a)中确立的标准，执行隐私风险评估。

组织应保留隐私风险评估结果的文件化信息。

7.3 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文件化信息。

8 绩 效 评 估

8.1 监测、测量、分析和评估

组织应确定：

一 需要监测和测量的内容；

一 适用时，采用何种监控、测量、分析和评估方法以确保结果有效；

一 何时进行监测和测量：

一 何时分析和评估监测与测量结果。应提供文件化信息作为结果的证据。

组织应评估隐私保护绩效及隐私信息管理体系的有效性。

8.2 内部审核

8.2.1 总则

组织应按计划周期开展内部审核，以获取隐私信息管理体系是否符合以下要求的依据：

a) 符合：

一 该组织对自身隐私信息管理体系的要求；

— 本 文 件 的 要 求 ；

b) 有效实施并持续维护。

8.2.2 内部审核计划

组织应规划、建立、实施和维持(一项或多项)审计计划，包括频率、方法、责任、规划要求和报告。

制定内部审核计划时，组织应考虑相关过程的重要性及以往审核的结果。

组织应：

a) 为每次审计定义审计目标、标准和范围；

b) 选定审计人员并实施审计，以确保审计过程的客观性与公正性；

c) 确保审计结果已向相关管理人员报告。

应提供文件化信息作为实施审核计划及审核结果的证据。

8.3 管 理 评 审

8.3.1 一 般

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

8.3.2 管理评审输入

管理评审应包括：

a) 先前管理评审行动的执行状态；

b) 与隐私信息管理体系相关的外部和内部事项的变化；

c) 相关方需求与期望中与隐私信息管理体系相关的变化；

d) 隐私信息管理体系绩效信息，包括以下方面的趋势：

—不符合项与纠正措施；

一 监测与测量结果；

一 审核结果；

e) 持续改进机会。

8.3.3 管理评审结果

管理评审结果应包括与持续改进机会相关的决策，以及对隐私信息管理体系进行任何变更的必要性。

文件化信息应作为管理评审结果的证据予以保留。

9 改进

9.1 持续改进

组织应持续改进隐私信息管理体系的适用性、充分性和有效性。

9.2 不符合项与纠正措施

当发生不符合项时，组织应：

a) 应对不符合项，并视情况：

— 采取控制和纠正措施；

— 处理后果；

b) 评估消除不符合项根源的必要性，以防止其再次发生或在其他地方发生，具体通过：

— 复核不符合项；

— 确定不符合项的原因；

—确定是否存在类似的不符合项，或可能发生此类情况；

c) 实施任何必要的行动；

d) 审查已采取的纠正措施的有效性；

e) 必要时对隐私信息管理体系进行变更。纠正措施应与所遇不符合项的影响程度相适应。文件化信息应作为以下内容的证据：

— 不符合项的性质及后续采取的任何行动；

— 任何纠正措施的结果。

10 附件的进一步说明

附件C包含本文件条款与ISO/IEC 29100隐私原则的对照表。

附件D 包含本文件控制措施与欧盟《通用数据保护条例》的对照关系。

附录E 包含了本文件条款与ISO/IEC 27018及ISO/IEC 29151条款的对照关系。

附录F展示了本版ISO/IEC 27701与上一版(ISO/IEC 27701:2019) 控制措施的对应关系。

附录A

（规范性）

PIMS 参考控制目标及针对PII 控制者和PII 处理者的控制措施

本附录适用于作为PII控制者或PII处理者（或兼具两者身份）的组织。

在实施PIMS时，无需包含本附件所列的所有控制目标和控制措施。若排除任何控制目标，须在适用性声明中说明理由[参见6.1.3 e)]。排除理由可包括：风险评估认定该控制措施非必要，或适用法律要求未作强制规定（或存在豁免条款）。

表A.1适用于PII控制者，表A.2适用于PII处理者，表A.3涉及PII控制者与处理者共同适用的信息安全控制措施。

注 表A.1、A.2和A.3中”控制参考”项下的引用对应附件B中的等效条款编号（例如控制A.1.2.2的指导原则见B.1.2.2）。

表A.1— 个人身份信息控制者的控制目标与控制措施

收集与处理条件 目标：证明处理合法，依据适用司法管辖区的法律依据，具有明确界定且正当的目的。		
控制措施参考	控制措施名称	控制措施
A.1.2.2	确定并记录处理目的	组织应确定并记录处理个人身份信息（PII）的具体目的。
A.1.2.3	确定合法依据	组织应确定、记录并能够证明其在为已确定目的处理PI时符合相关合法依据。
A.1.2.4	确定何时及如何获取同意	组织应确定并记录可证明是否、何时及如何从PII主体处获得处理PII同意的流程。
A.1.2.5	获取并记录同意	组织应根据记录在案的流程获取并记录来自PII主体的同意。
A.1.2.6	隐私影响评估	组织应评估隐私影响评估的必要性，并在计划对个人身份信息进行新的处理或变更现有处理时，酌情实施该评估。
A.1.2.7	与PII处理方的合同	组织应与所使用的任何PII处理者签订书面合同，并确保其与PII处理者的合同涉及附件A（参见表A.2）中适当控制措施的实施。
A.1.2.8	共同PII控制者	组织应与任何共同PII控制者确定处理PII的各自角色和责任（包括PII保护和安全要求）。
A.1.2.9	与处理PII相关的记录	该组织应确定并安全维护必要的记录，以支持其处理PII的义务。

表 A.1（续）

对PII主体的义务 目标：确保向个人身份信息主体提供关于其个人身份信息处理的适当信息，并履行与处理其个人身份信息相关的其他适用义务。		
A.1.3.2	确定并履行对PII主体的义务	组织应确定并记录其在处理个人身份信息过程中对个人身份信息主体承担的法律、法规及业务义务，并提供履行这些义务的手段。
A.1.3.3	确定向PII主体提供的信息	组织应确定并记录向PII主体提供的关于其PII处理的信息内容及提供时间。
A.1.3.4	向PI主体提供信息	该组织应向个人身份信息主体提供清晰且易于获取的信息，明确个人身份信息控制者的身份，并说明其个人身份信息的处理方式。
A.1,3.5	提供修改或撤回同意的机制	该组织应提供机制，使PII主体能够修改或撤回其同意。
A.1.3.6	提供反对处理PII的机制 处理	该组织应为个人身份信息主体提供反对处理其个人身份信息的机制。
A.1.3.7	访问、更正或删除	组织应实施政策、程序或机制，以履行其对PII主体访问、更正或删除其PII的义务。
A.1.3.8	PII控制者向第三方告知的义务	该组织应将共享个人身份信息(PII)的任何修改、撤回或异议通知相关第三方，并为此实施适当的政策、程序或机制。
A.1.3.9	提供已处理PII的副本	当个人身份信息主体提出要求时，组织应能够提供所处理的个人身份信息的副本。
A.1.3.10	处理请求	组织应制定并记录处理和响应个人身份信息主体合法请求的政策和程序。
A.1.3.11	自动化决策	该组织应识别因其基于个人身份信息(PII)的自动化处理而作出的、与PII主体相关的决策所产生的义务(包括法律义务),并能证明其如何履行这些义务。
隐私设计与隐私默认 目标：确保流程和系统设计使个人身份信息的收集与处理(包括使用、披露、保留、传输及处置)仅限于实现已识别目的所必需的范围。		
A.1.4.2	限制收集	组织应将个人身份信息的收集限制在与已确定目的相关、相称且必要的最低限度。
A.1.4.3	限制处理	组织应将个人身份信息的处理限制在为实现已确定目的所必需、相关且适当的范围内。
A.1.4.4	准确性与质量	组织应确保并记录个人身份信息在其整个生命周期内，始终保持为处理目的所必需的准确性、完整性和及时性。
A.1.4.5	PII最小化目标	组织应定义并记录数据最小化目标，以及为实现这些目标所采用的机制(如去标识化）。
A.1.4.6	处理结束时的PII去标识化与删除	当原始个人身份信息不再用于已确定的目的时，组织应立即删除该信息或将其转换为无法识别或重新识别主体身份的形式。
A.1.4.7	临时文件	组织应确保根据处理个人身份信息(PII)产生的临时文件，在规定且有记录的期限内，遵循记录在案的程序予以处置(例如删除或销毁)。

表 A.1（续）

A.1,4.8	保留	组织不得将个人身份信息保留超过处理该信息所需的时间。
A.1.4.9	销毁	组织应制定书面政策、程序或机制来处置个人身份信息。
A.1.4.10	PII传输控制	组织应针对通过数据传输网络传输(例如发送至其他组织)的PI实施适当的控制措施，以确保数据到达预定目的地。
个人身份信息的共享、转移和披露 目标：确定是否共享、向其他管辖区或第三方转移或披露PII,并记录相关情况，以符合适用的义务。		
A.1.5.2	确定跨司法管辖区转移个人身份信息(PII)的依据	组织应确定并记录跨司法管辖区转移个人身份信息的相关依据。
A.1.5.3	可接收个人身份信息的国家及国际组织	该组织应明确并记录可能接收个人身份信息的国家及国际组织。
A.1.5.4	PII转移记录	组织应记录向第三方或从第三方转移PII的情况，并确保与这些第三方合作，以支持未来与PII主体义务相关的请求。
A.1.5.5	向第三方披露PII的记录	组织应记录向第三方披露的PI信息，包括披露了哪些PII信息、向谁披露以及何时披露。

表 A.2— 个人身份信息处理者的控制目标和控制措施

收集与处理的条件 目标：证明处理行为合法，依据适用司法管辖区的法律依据，且具有明确界定且正当的目的。		
控制参考	控制标题	控制
A.2.2.2	客户协议	组织应确保，在相关情况下，处理个人身份信息的合同明确规定组织在协助客户履行义务中的角色(同时考虑处理的性质及组织可获取的信息)。
A.2.2.3	组织目的	组织应确保代表客户处理的个人身份信息仅用于客户书面指示中明确的目的。
A.2.2.4	营销与广告用途	除非已获得相关个人身份信息主体的事先同意，否则组织不得将合同处理的个人身份信息用于营销和广告目的。组织不得将提供此类同意作为接受服务的条件。
A.2.2.5	侵权指令	若组织认为处理指令违反适用法律要求，应告知客户。
A.2.2.6	客户义务	组织应向客户提供适当信息，以便客户能够证明其履行了义务。
A.2.2.7	与处理个人身份信息相关的记录	该组织应确定并保存必要的记录，以支持证明其履行了(适用合同中规定的)代表客户处理PII的义务。
对PII主体的义务 目标：确保向PII主体提供其PI处理相关的适当信息，并履行与处理其PII相关的其他适用义务。		
A.2.3.2	遵守对PII主体的义务	该组织应向客户提供符合其个人身份信息原则相关义务的手段。

表A.2（续）

隐私设计与隐私默认 目标：确保流程和系统设计使个人身份信息的收集与处理(包括使用、披露、保留、传输及处置)仅限于实现已识别目的所必需的范围。		
A.2.4.2	临时文件	该组织应确保在处理个人身份信息过程中产生的临时文件，须在规定且有记录的期限内，遵循记录在案的程序予以处置(例如删除或销毁)。 销毁)的记录程序，并在规定的记录期限内完成。
A.2.4.3	个人身份信息的返还、转移或处置	组织应能够以安全方式退回、转移或处置PII,并向客户公开相关政策。
A.2.4.4	PII传输控制	组织应针对通过数据传输网络传输的PII实施适当控制措施，确保数据准确送达指定接收方。
个人身份信息的共享、转移与披露 目标：确定是否存在个人身份信息(PII)共享、向其他司法管辖区或第三方转移，或根据适用义务进行披露的情况，并记录具体时间点。		
A.2.5.2	跨司法管辖区转移PII的依据	组织应及时告知客户跨司法管辖区转移个人身份信息的依据及任何相关变更计划，以便客户可对变更提出异议或终止合同。
A.2.5.3	可转移PII的国家及国际组织	该组织应明确并记录可能接收个人身份信息的国家及国际组织。
A.2.5.4	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个人身份信息的情况，包括披露了哪些个人身份信息、向谁披露以及何时披露。
A.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。
A.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，在披露任何PII前应咨询相关客户，并接受经相关客户授权的、合同约定的PII披露请求。
A.2.5.7	披露用于处理PII的分包商信息	使用前，组织应向客户披露是否使用任何分包商处理个人身份信息。
A.2.5.8	委托分包商处理PII	组织仅可根据客户合同约定委托分包商处理PII。
A.2.5.9	处理PII的分包商变更	在获得一般书面授权的情况下，组织应将任何涉及增加或更换处理PII分包商的变更计划告知客户，从而使客户有机会对这些变更提出异议。

表A.3 一个人身份信息控制者和处理者的控制目标与控制措施

个人身份信息控制者和处理者的安全考虑 目标；确保个人身份信息处理的安全性。		
控制参考	控制标题	控制措施
A.3.3	信息安全政策	应制定与个人身份信息处理相关的信息安全政策，经管理层批准后发布，并传达给相关人员和相关利益相关方，由其确认知悉。 方确认，并按计划周期及发生重大变更时进行审查。
A.3.4	信息安全角色与职责	与个人身份信息处理相关的信息安全角色与职责应根据组织需求进行定义和分配。

表A.3（续）

A.3.5	信息分类	信息应根据组织的保密需求进行分类，同时考虑个人身份信息(PII),并基于保密性、完整性、可用性以及相关利益相关方的要求。
A.3.6	信息标识	应根据组织采用的信息分类方案，制定并实施一套适当的信息标识程序，该程序应考虑个人身份信息。
A.3.7	信息传输	组织内部所有类型的传输设施以及组织与其他方之间的传输设施，均应制定与处理PII相关的信息传输规则、程序或协议。
A.3.8	身份管理	应管理与PII处理相关的身份的完整生命周期。
A.3.9	访问权限	应根据组织关于访问控制的特定主题政策和规则，对PII及其他与PII处理相关的资产的访问权限进行配置、审查、修改和删除。
A.3.10	供应商协议中的信息安全条款	应根据供应商关系的类型，与每个供应商建立并商定与PII处理相关的信息安全要求。
A.3.11	信息安全事件管理规划与准备	组织应通过定义、建立和传达事件管理流程、角色和职责，规划并准备处理与个人身份信息处理相关的信息安全事件。
A.3.12	信息安全事件响应	涉及个人身份信息处理的信息安全事件响应应遵循文件化程序。
A.3.13	法律、法规、监管及合同要求	与个人信息处理相关的信息安全相关的法律、法规、监管和合同要求，以及组织满足这些要求的方法应记录在案，并保持文件的最新状态。
A.3.14	记录保护	与个人身份信息处理相关的记录应受到保护，防止丢失、毁坏、篡改、未经授权的访问和未经授权的披露。
A.3.15	信息安全的独立审查	组织对与PII处理相关信息安全的管理方法及其实施(包括人员、流程和技术)应在计划的时间间隔内或发生重大变化时进行独立审查。
A.3.16	遵守信息安全政策、规则和标准	应定期审查对组织信息安全政策、特定主题政策、规则和标准(涉及个人身份信息处理)的遵守情况。
A.3.17	信息安全意识、教育和培训	组织人员及相关利益方应接受适当的信息安全意识教育和培训，并定期更新与个人身份信息处理相关的组织信息安全政策、专题政策和程序，这些内容应与其工作职能相关。
A.3.18	保密或不披露协议	应确定、记录、定期审查并由人员及其他相关利益方签署反映组织保护个人身份信息需求的保密或非披露协议。
A.3.19	清桌与清屏	应制定并适当执行针对纸质文件和可移动存储介质的清桌规则，以及针对信息处理设施的清屏规则。
A.3.20	存储介质	包含个人身份信息的存储介质应根据组织的分类方案和处理要求，在其获取、使用、运输和处置的生命周期内进行管理。

表A.3（续）

A.3.21	设备的安全处置或再利用	在处置或再利用前，应验证含有个人身份信息的存储介质的设备，确保已清除或安全覆盖所有敏感数据和授权软件。
A.3.22	用户终端设备	存储于用户终端设备上、由其处理或可通过其访问的个人身份信息应受到保护。
A.3.23	安全认证	应基于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。
A.3.24	信息备份	应维护并定期测试与PII处理相关的PII、软件和系统的备份副本。
A.3.25	日志记录	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。
A.3.26	加密技术的使用	应制定并实施与个人身份信息处理相关的加密技术有效使用规则，包括加密密钥管理。
A.3.27	安全开发生命周期	应制定并应用与处理个人身份信息相关的软件和系统安全开发规则。
A.3.28	应用程序安全要求	在开发或采购应用程序时，应确定、规定并批准与个人身份信息处理相关的信息安全要求。
A.3.29	安全系统架构与工程原则	应建立、记录、维护并应用处理个人身份信息(PII)相关安全系统的工程原则，以指导所有信息系统开发活动。
A.3.30	外包开发	组织应指导、监督和审查与外包的PI处理系统开发相关的活动。
A.3.31	测试信息	与个人身份信息处理相关的测试信息应得到适当选择、保护和管理。

附件B
（规范性）

PII 控制者和PII 处理者的实施指南

B.1 PII控制者的实施指南

B.1.1 通 用

本条款为PII控制者提供PIMS指导，涉及表A.1所列控制措施。

B.1.2 收集与处理条件

B.1.2.1 目标

证明处理行为合法，依据适用司法管辖区的法律依据，并具有明确界定且正当的目的。

B.1.2.2 识别并记录处理目的的控制措施

该组织应确定并记录处理个人身份信息 (PII) 的具体目的。

实施指南

组织应确保个人身份信息主体知晓其信息处理目的。组织有责任将此目的明确记录并传达给信息主体。若未清晰说明处理目的，则无法获得充分的同意与选择权。

处理个人身份信息的目的应有充分清晰且详细的记录，以便作为向个人身份信息主体提供信息的一部分（参见B.13.3 ）。 该记录应包含获取同意所需的信息（参见B.1.2.4）， 以及政策和程序的书面信息（参见B.1.2.9 ）。

其他信息

在部署云计算服务时，ISO/IEC 19944-1中的分类法和定义可为描述PII处理目的提供术语支持。

B.1.2.3 确定合法依据控制

组织应确定、记录并能够证明其为已确定目的处理PII 符合相关合法依据。

实施指南

某些司法管辖区要求组织能够证明处理行为的合法性已在处理前得到正式确立。

处理个人身份信息的法律依据可包括：

一 个人身份信息主体的同意：

一　履行合同：

一　履行法律义务；

—　保　护PII主体的重大利益；

一　履行公共利益任务；

—PII　　控制者的合法利益。

该组织应为每项个人身份信息处理活动记录此依据(参见B.1.2.9)。

组织的合法利益可包括信息安全目标等，但应与保护隐私的个人身份信息主体义务相平衡。

无论根据个人身份信息的性质(例如健康信息)还是相关主体(例如涉及儿童的个人身份信息)来定义特殊类别的个人身份信息，组织都应将其纳入分类体系。

属于这些类别的个人身份信息的分类可能因司法管辖区的不同而有所差异，也可能因适用于不同类型业务的监管制度不同而有所差异，因此组织应了解适用于其个人身份信息处理的分类。

特殊类别的个人身份信息使用也可能受到更严格的管控。

变更或扩展个人身份信息处理目的时，可能需要更新或修订法律依据，并可能要求从信息主体处获取额外同意。

B.1.2.4　　确 定何时以及如何获得同意控制

该组织应确定并记录一个流程，通过该流程可证明是否、何时以及如何从个人身份信息主体处获得了处理个人身份信息的同意。

实施指南

处理PI 时可能需要征得同意。组织应明确记录何时需要获取同意以及获取同意的要求。将处理目的与是否及如何获取同意的信息相关联可能有所帮助。

注　　法律要求可能适用。

某些司法管辖区对同意的获取和记录方式有具体要求(例如不得与其他协议捆绑)。此外，特定类型的数据收集(如科学研究)以及特定类别的个人身份信息主体(如儿童)可能需遵守额外要求。组织应考虑这些要求，并记录同意机制如何满足这些要求。

B. 1. 2. 5　　获取并记录同意控制

该组织应按照记录在案的流程获取并记录个人身份信息主体的同意。

实施指南

组织应以能够应要求提供所获同意的详细信息(例如同意时间、PII 主体身份及同意声明)的方式，获取并记录PII主体的同意。

在同意流程前向PII主体提供的信息应遵循B. 1. 3. 4节的指导原则。

同意应满足以下条件：

— 自由给予；

— 明确处理目的；且

— 明确且无歧义。

B.1.2.6 隐私影响评估管控

组织应评估隐私影响评估的必要性，并在计划对个人身份信息进行新的处理或变更现有处理方式时，酌情实施该评估。

实施指南

个人身份信息处理会为信息主体产生风险。这些风险应通过隐私影响评估进行评估。部分司法管辖区规定了必须进行隐私影响评估的情形。相关标准可包括：对PII主体产生法律效力的自动化决策；大规模处理特殊类别的PII(如健康相关信息、种族或民族血统、政治观点、宗教或哲学信仰、工会会员身份、基因数据或生物特征数据);或对公共区域进行大规模系统性监控。

组织应确定完成隐私影响评估所需要素，包括处理的PII 类型清单、存储位置及可能的转移路径。数据流图和数据映射在此过程中亦具参考价值。

注： 有关可为隐私影响或其他风险评估提供依据的PII处理文档化信息详情，参见B.1.2.9。

其他信息

有关处理个人身份信息 (PII) 的隐私影响评估指南，可参阅ISO/IEC 29134标准。

B.1.2.7 与PII处理方的合同管控

组织应与所使用的任何个人身份信息处理者签订书面合同，并确保其与个人身份信息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

组织与任何代表其处理个人身份信息的处理者签订的合同，应要求该处理者实施 表A.2中规定的适 当控制措施，同时需考虑信息安全风险评估流程 （ 参 见6.1.2 ）以及该处理者所执行个人身份信息处理的范围。默认情况下，表A.2中规定的所有控制措施均应视为适用。若组织决定免除PII 处理者实施表A.2中某项控制措施，应说明豁免理由(参见6.1.3)。

合同可对各方责任作出不同规定，但为符合本文件要求，所有控制措施均应纳入书面信息中予以考虑。

B.1.2.8 联 合PII控制者控制

该组织应与任何共同控制个人身份信息的实体确定各自在处理个人身份信息(包括个人身份信息保护和安全要求)方面的角色与责任。

实施指南

个人身份信息处理的职责分工应以透明方式确定。

这些角色和职责应通过合同或任何类似的具有法律约束力的文件予以明确，该文件应包含共同处理个人身份信息 (PI) 的条款和条件。在某些司法管辖区，此类协议被称为数据共享协议。

共同PII控制者协议可包含：

一 共 享PII的目的/共同PII控制者关系的目的；

— 参与共同控制关系各组织(PII控制者)的身份信息；

— 根据协议将共享或转移并处理的个人身份信息类别；

— 处理操作概述(例如：转移、使用)；

一 各方角色与职责的描述；

— 实施保护PII的技术和组织安全措施的责任；

— 发生PII泄露时的责任划分(例如：由谁通知、何时通知、信息共享机制)；

—PII 的保留或处置条款；

一 因未遵守协议而产生的责任：

一 如何履行对PII主体的义务；

一 如 何 向PII主体提供涵盖联合PII控制者间协议核心内容的信息；

一 PII主体如何获取其有权接收的其他信息；以及

一 个人身份信息主体的联络点。

B.1.2.9 与个人身份信息处理相关的记录管控

组织应确定并安全保存支持其处理PII义务所需的必要记录。

实施指南

组织可通过建立个人身份信息处理活动清单或目录，来维护个人身份信息处理的记录信息。该清单可包含：

— 处理类型；

一 处理目的；

—个人身份信息类别及主体描述(如儿童)；

一 已披露或将披露PII的接收方类别(含第三国接收方及国际组织接收方)；

—技术和组织安全措施的一般性描述：以及

一 隐私影响评估报告。

该清单应指定负责人，确保其准确性和完整性。

B.1.3 对个人身份信息主体的义务

B.1.3.1 目标

确保向PII 主体提供有关其PII 处理情况的适当信息，并履行与PII 处理相关的其他适用义务。

B.1.3.2 确定并履行对PII 主体的义务控制

该组织应确定并记录其在处理个人身份信息 (PII) 时对相关主体所承担的法律、法规及商业义务，并提供履行这些义务的手段。

实施指南

对PII主体的义务及履行方式因司法管辖区而异。

该组织应确保提供适当的途径，以便以可获取且及时的方式履行对个人身份信息主体的义务。应向个人身份信息主体提供清晰的文件，说明履行义务的范围及方式，并提供最新的联络点以便其提出请求。

联系方式的提供方式应与收集个人身份信息及获取同意的方式保持一致(例如：若通过电子邮件或网站收集个人身份信息，则联系方式也应通过电子邮件或网站提供，而非电话或传真等替代方式)。

B.1.3.3 确定PII主体的信息控制

组织应确定并记录向PII主体提供的关于其PII处理的信息内容及提供时间节点。

实施指南

该组织应确定向个人身份信息主体提供信息的法律、监管或业务要求(例如：在处理前、自请求起一定时间内),以及应提供的信息类型。

根据具体要求，此类信息可采用通知形式呈现。可向PII主体提供的信息类型包括：

一 处理目的说明(参见B.1.2.2)；

—PII 控制者或其代表的联系方式；

一 处理的合法依据信息(参见B.1.2.3)；

一 若非直接从个人身份信息主体处获取，则需说明该信息获取来源；

一 说明提供PII是否属于法定或合同要求，并在适用情况下说明未提供PII的可能后果；

一 根据B.1.3.2 条款确定的对PII主体的义务说明，以及PII主体如何从中受益(特别是关于访问、修改、更正、要求删除、获取PII副本及反对处理的权利)；

一 个人身份信息主体撤回同意的方式说明(参见B.1.3.5)；

一 关于PII转移的信息；

—PII 接收方或接收方类别的信息；

一　关 于PII保留期限的信息；

一　关于基于个人身份信息自动化处理的自动化决策使用信息；

一　关于投诉权及投诉方式的信息；

一　信息提供的频率说明(例如“即时通知”、组织规定的频率)。

若个人身份信息处理目的发生变更或扩展，组织应提供更新信息。

B.1.3.4　向PII主体提供信息控制

组织应向PI主体提供清晰且易获取的信息，明确标识PII控制者并说明其PII的处理方式。

实施指南

组织应以清晰简洁的语言，向个人身份信息主体及时、完整、透明、易懂且便于获取的形式提供B.1.3.3条款所列信息，并根据目标受众特点调整表达方式。

在适当情况下，应在收集个人身份信息时提供该信息。该信息还应永久可获取。

注　图标和图像可通过提供处理目的的视觉概览，对个人身份信息主体有所帮助。

B.1.3.5　提供修改或撤回同意的机制控制

该组织应为个人身份信息主体提供修改或撤回其同意的机制。

实施指南

组织应告知PII主体其随时撤回同意的权利(该权利可能因司法管辖区而异),并提供相应机制。撤回机制应与获取同意时采用的机制保持一致(在可行情况下)。例如，若通过电子邮件或网站获取同意，撤回机制应采用相同渠道，而非电话或传真等替代方案。

修改同意书可能包括对个人身份信息处理设置限制，例如在某些情况下禁止个人身份信息控制者删除该信息。

某些司法管辖区对个人身份信息主体修改或撤回同意的时间和方式设有限制。

组织应以与记录同意本身类似的方式记录任何撤销或更改同意的请求。

任何同意变更均应通过适当系统传达给授权用户及相关第三方。

组织应设定响应时限，并据此处理相关请求。

补充信息

当特定PII处理的同意被撤回时，撤回前进行的所有PII处理通常应视为适当，但此类处理的结果不应

用于新的处理。例如，若个人身份信息主体撤销其对建立个人档案的同意，则不应继续使用或查阅其档案。

B.1.3.6 提供反对处理个人身份信息(PII)的机制控制

组织应为个人身份信息主体提供反对处理其个人身份信息的机制。

实施指南

部分司法管辖区赋予PII主体反对处理其个人身份信息的权利。受此类司法管辖区法律要求约束的组织，应能证明其 如何确保保留PII主体行使该权利的记录。

组织应记录与PII主体反对处理相关的法律法规要求(例如反对将PII 用于直接营销目的)。组织应向主体说明在这些情形下行使反对权的能力。反对机制形式可多样化，但应与所提供服务类型相匹配(例如在线服务应在线提供此功能)。

B.1.3.7 访问、更正或删除控制

组织应制定政策、程序或机制，以履行其对PII主体访问、更正或删除其PII的义务。

实施指南

该组织应制定政策、程序或机制，使个人身份信息主体能够在提出请求时及时获取、更正或删除其个人身份信息，且不得无故拖延。

该组织应规定响应时间，并据此处理请求。

任何更正或删除操作应通过系统或向授权用户传达，并应传递给已接收该PII的第三方(参见B.1.3.8)。

注 B.1.5.4规定的控制措施所产生的记录信息可为此提供帮助。

当个人身份信息主体对数据准确性或更正提出争议时，组织应实施相应的政策、程序或机制。这些政策、程序或机制应包括告知个人身份信息主体所作的变更内容，以及无法进行更正的原因(如存在此类情况)。

部分司法管辖区对PII主体请求更正或删除其PII的时机与方式设有限制。组织应及时掌握此类限制规定。

B.1.3.8 PII控制者向第三方告知的义务控制

该组织应将共享个人身份信息的任何修改、撤回或异议通知相关第三方，并为此实施适当的政策、程序或机制。

实施指南

组织应采取适当措施(同时考虑现有技术条件)，向第三方通报共享PII的任何修改、撤销同意或相关异议。

组织应建立并保持与第三方的主动沟通渠道。相关职责可分配给负责运营和维护的个人。在通知第三方时，组织应监控其对信息接收的确认情况。

注： 因个人身份信息主体权利产生的变更可能包括：修改或撤回同意、要求更正、删除或限制处理，或根据个人身份信息主体要求对处理行为提出异议。

B.1.3.9 提供已处理PII的副本控制

当PII主体提出请求时，组织应能提供所处理PII的副本。

实施指南

组织应以结构化、常用且可供PII主体访问的格式提供所处理PII的副本。

某些司法管辖区规定，在特定情况下，组织应以便于个人身份信息主体或接收方个人身份信息控制者进行数据迁移的格式(通常为结构化、常用且机器可读的格式)提供所处理个人身份信息的副本。

组织应确保向PII主体提供的任何PII副本均与该主体直接相关。

若所请求的个人身份信息 (PII) 已根据保留与处置政策(详见B...8节)被删除，PII 控制者应告知PII主体相关信息已被删除。

若组织已无法识别PII主体(例如因去标识化处理)，则不应仅为实施本控制措施而试图(重新)识别PII主体。但在某些司法管辖区，合法请求可能要求向PII主体索取额外信息以实现重新识别及后续披露。

在技术可行的情况下，应允许根据个人身份信息主体的要求，将该信息的副本直接从一个组织转移至另一个组织。

B.1.3.10 请求处理控制

该组织应制定并记录处理和响应PII主体合法请求的政策和程序。

实施指南

合法请求可包括要求提供已处理的PII 副本或提出投诉。

某些司法管辖区允许组织在特定情况下(例如过量或重复请求)收取费用。

请求应在规定的响应时限内处理。

部分司法管辖区根据请求的复杂程度和数量规定响应时限，并要求在延迟时通知个人身份信息主体。隐私政策中应明确规定相应的响应时限。

B.1.3.11 自动化决策控制

组织应确定其基于个人身份信息的自动化处理所作出的、与个人身份信息主体相关的决策所产生的义务(包括法律义务),并能够证明其如何履行这些义务。

实施指南

某些司法管辖区规定，当仅基于个人身份信息自动化处理作出的决策对其产生重大影响时，需履行特定义务，例如告知自动化决策的存在、允许个人身份信息主体对该决策提出异议，或获取人工干预。

注 在某些司法管辖区，部分PII处理无法完全自动化。

在这些司法管辖区内运营的组织应能够证明其如何考虑遵守这些义务。

B.1.4 设计隐私和默认隐私

B.1.4.1 目标

确保流程和系统设计时，将个人身份信息的收集和处理(包括使用、披露、保留、传输和处置)限制在实现既定目的所必需的范围内。

B.1.4.2 限制收集控制

组织应将个人身份信息的收集限制在与已确定目的相关、相称且必要的最小范围内。

实施指南

组织应将PII收集范围限定在与既定目的相关、相称且必要的合理限度内。这包括限制组织间接收集的PII 数量(例如通过网站日志、系统日志等途径)。

默认隐私意味着，在收集和处理个人身份信息 (PII) 存在任何可选性时，每个选项都应默认禁用，仅在PII主体明确选择时启用。

B.1.4.3 限制处理控制

组织应将PII的处理限制在为已确定目的所必需、相关且充分的范围内。

实施指南

应通过信息安全和隐私政策(参见5.2)以及其实施和合规的书面程序来管理PII 处理的限制。

默认情况下， PII 处理应限定在实现已识别目的所需的最小范围内。此类处理包括：

— 披露;

一 PII存储期限：以及

— 可访问其PII的对象。

B.1.4.4 准确性与质量控制

该组织应确保并记录个人身份信息在整个生命周期内，其准确性、完整性及及时性均符合处理目的所需。

实施指南

组织应实施政策、程序或机制，以最大限度地减少其处理的PII中的不准确性。还应制定政策、程序或机制，以应对不准确PII的情况。这些政策、程序或机制应纳入文件化信息(例如通过技术系统配置)，并应适用于PII的整个生命周期。

补充信息

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

B.1.4.5 个人身份信息最小化目标控制

该组织应定义并记录数据最小化目标，以及为实现这些目标所采用的机制(例如去标识化)。

实施指南

组织应说明如何在已确定用途范围内限制特定个人身份信息 (PII) 的收集与处理规模，包括采用去标识化或其他数据最小化技术。

已确定的目的(参见B.1.2.2）可能要求处理未经去标识化的PII，此时组织应能描述此类处理方式。

在其他情况下，既定目的无需处理原始PII，经去标识化的PII 即可满足实现既定目的。此时组织应界定并记录PII与主体关联的程度，同时明确处理PII的机制与技术方案，确保实现去标识化及PII最小化目标。

用于最小化个人身份信息 (PII) 的机制因处理类型和所用处理系统而异。组织应记录为实施数据最小化所采用的任何机制(例如技术系统配置）。

当处理去标识化数据足以满足目的时，组织应及时记录为实现其设定的去标识化目标而设计的任何机制(例如技术系统配置)。例如，移除 与PII主体相关的属性即可使组织达成既定目的。在其他情况下，可采用其他去识别化技术(如概化处理(例如四舍五入)或随机化技术（例如添加噪声))以达到充分的去识别化水平。

注I 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，可用于分类数据识别PII 主体或将PII 主体与 PII中的一组特征相关联的程度。

B.1.4.6 处理结束时的PII去标识化和删除控制

该组织应在原始个人身份信息不再用于特定目的时，立即删除该信息或将其转换为无法识别或重新识别主体身份的形式。

实施指南

当预计不再需要进一步处理时，组织应建立机制清除PII。或可采用去标识化技术，前提是处理后的去标识化数据在合理范围内无法重新识别PII主体。

B.1.4.7 临时文件控制

该组织应确保在处理个人身份信息过程中产生的临时文件，须在规定且有记录的期限内，遵循记录在案的程序予以处置(例如删除或销毁）。

实施指南

该组织应定期检查，确保未使用的临时文件在规定时间内被删除。

其他信息

信息系统在正常运行过程中会生成临时文件。此类文件虽具有系统或应用程序专属性，但可能包含文件系统回滚日志、数据库更新相关的临时文件以及其他应用软件运行时产生的临时文件。相关信息处理任务完成后，临时文件即失去存在必要性，但某些情况下无法直接删除。这些文件的存留时长并非始终可确定，需通过”垃圾回收”程序识别相关文件，并判定其上次使用时间。

B.1.4.8 保留控制

组织不应将个人身份信息保留超过处理该信息所需的时间。

实施指南

组织应制定并维护所保留信息的保留计划，同时考虑个人身份信息保留期限不得超过必要时长的要求。此类计划应兼顾法律、监管及业务需求。当上述要求存在冲突时，应基于风险评估作出业务决策，并在相应计划中予以记录。

B.1.4.9 处置控制

组织应制定并记录处理PII的处置政策、程序或机制。

实施指南

个人身份信息处置技术的选择取决于多种因素，因不同处置技术在特性与结果上存在差异(例如：物理介质的碎片化程度，或电子介质上已删除信息的可恢复性)。选择适当处置技术时需考虑的因素包括但不限于：待处置PII 的性质与范围、是否存在关联元数据，以及存储PII的介质物理特性。

B.1.4.10 PII传输控制控制

该组织应针对通过数据传输网络传输(例如发送至其他组织)的个人身份信息实施适当控制措施，以确保数据送达预定目的地。

实施指南

应控制PII的传输，通常通过确保只有授权人员才能访问传输系统，并遵循适当流程(包括保留审计日志)来确保PII 在传输过程中不被泄露，并准确送达正确接收方。

B.1.5 个人身份信息的共享、转移与披露

B.1.5.1 目标

确定是否共享、转移至其他司法管辖区或第三方，或根据适用义务披露个人身份信息，并记录相关时间节点。

B.1.5.2 确定跨司法管辖区转移个人身份信息的依据

该组织应确定并记录跨司法管辖区转移PII的相关依据。

实施指南

个人身份信息 (PII) 的转移可能受法律要求约束，具体取决于数据转移的目的地司法管辖区或国际组织(以及数据的来源地)。组织应记录对这些要求的合规性，作为转移的依据。

部分司法管辖区可能要求信息转移协议须经指定监管机构审核。在该类司法管辖区运营的组织应知悉相关要求。

注: 当转移发生在特定司法管辖区内时，发送方和接收方均须遵守相同的适用法律要求。

B.1.5.3 可接收个人身份信息的国家与国际组织管控

组织应明确并记录可能接收个人身份信息的国家及国际组织。

实施指南

在正常运营中可能接收个人身份信息的国家及国际组织名单应向客户公开。因使用分包商处理个人身份信息而涉及的国家名单亦应包含在内。所列国家应结合B.1.5.2条款进行考量。

应包含因使用分包处理PII而涉及的国家。所列国家应参照B.1.5.2条款进行考量。

在常规运营之外，可能存在应法律机构要求进行转移的情况，此类转移的国家身份无法预先确定，或为维护执法调查的保密性而被适用司法管辖区禁止(参见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管控

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

实施指南

记录可包括：因个人身份信息控制者履行其义务而修改的、来自第三方的个人身份信息转移；或为执行个人身份信息主体的合法请求(包括删除个人身份信息的请求，例如在撤回同意后)而向第三方转移的信息。

组织应制定政策明确此类记录的保存期限。

组织应将数据最小化原则应用于转移记录，仅保留严格必要的信息。

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，包括披露了哪些PII、向谁披露以及何时披露。

实施指南

个人身份信息(PII) 在正常运营过程中可能被披露。此类披露应予以记录。任何向第三方进行的额外披露(例如因法律调查或外部审计产生的披露)也应记录在案。记录内容应包含披露来源及披露授权的依据。

B.2 PII处理者的实施指南

B.2.1 总 则

本条款为PII处理者提供PIMS指导，涉及表A.2所列控制措施。

B.2.2 收集与处理条件

B.2.2.1 目 标

为证明处理行为合法，需依据适用司法管辖区的法律依据，并具有明确界定且正当的目的。

B.2.2.2 客户协议控制

组织应确保(在相关情况下)处理个人身份信息的合同明确规定组织在协助客户履行义务中的角色(需考虑处理性质及组织掌握的信息)。

实施指南

组织与客户之间的合同应包含以下方面(视客户角色而定，即个人身份信息控制者或处理者)：

一 隐私设计与隐私默认(参见B.1.4和B.2.4)；

一 实现处理过程的安全性；

一 向监管机构通报涉及个人身份信息的违规事件；

— 向客户及PII主体通报涉及PII的泄露事件；

—开展隐私影响评估；以及

— 确保在需要事先咨询相关PII保护机构时，获得PIII处理方的协助。

某些司法管辖区要求合同须包含以下内容：处理的主题事项及期限、处理的性质与目的、个人身份信息的类型及个人身份信息主体的类别。

B.2.2.3 组织目的控制

组织应确保代表客户处理的个人身份信息仅用于客户书面指示中明确的目的。

实施指南

组织与客户之间的合同应包含但不限于服务需达成的目标及时间框架。

为实现客户目的，组织在符合客户总体指示但未获客户明确指示的情况下，可基于技术原因自行确定处理个人身份信息的方法。例如，为高效利用网络或处理能力，可能需要根据个人身份信息主体的特定特征分配处理资源。
组织应允许客户验证其对目的限定原则的合规性。此举同时确保组织及其分包商不会将PII 用于客户书面指令中未明确的其他目的。

B.2.2.4 营销与广告用途管控

未经相关主体事先同意，组织不得将合同处理的PII用于营销及广告目的。组织不得将此类同意作为获取服务的先决条件。

实施指南

PII处理者对客户合同要求的合规性应予以记录，尤其在涉及营销或广告用途时。

若未从PII主体处公平获得明确同意，组织不得坚持将营销或广告用途纳入合同条款。

注 本控制措施是对B.2.2.3中更普遍控制措施的补充，并非替代或取代该措施。

B.2.2.5 侵权指令控制

若组织认为某项处理指令违反适用法律要求，应告知客户。

实施指南

组织验证指令是否违反法律要求的能力，取决于技术环境、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信息，使客户能够证明其履行了相关义务。

实施指南

客户所需的信息可包括：该组织是否允许并配合客户或客户指定/认可的其他审计机构开展的审计工作。

B.2.2.7 与处理个人身份信息相关的记录控制

该组织应确定并保存必要的记录，以支持证明其履行了(适用合同中规定的)代表客户处理PII的义务。

实施指南

某些司法管辖区可能要求组织记录以下信息：

—代表每位客户执行的处理类别；

一 向第三国或国际组织转移的情况；以及

一 技术与组织安全措施的概括性描述。

B.2.3 对个人身份信息主体的义务

B.2.3.1 目标

确保向个人身份信息主体提供关于其个人身份信息处理的适当信息，并履行与处理其个人身份信息相关的其他适用义务。

B.2.3.2 遵守对PII主体的义务管控

该组织应向客户提供履行其与PII主体相关义务的手段。

实施指南

PII控制者的义务可由法律要求或合同规定。这些义务可能涉及客户使用组织服务来履行相关义务的情形，例如及时更正或删除PII。

当客户依赖组织提供的信息或技术措施来履行对个人身份信息主体的义务时，相关信息或技术措施应在合同中明确规定。

B.2.4 隐私设计与隐私默认

B.2.4.1 目标

确保流程和系统设计时，个人身份信息的收集与处理(包括使用、披露、保留、传输及处置)仅限于实现既定目的所需范围。

B.2.4.2 临时文件管控

该组织应确保在处理个人身份信息过程中产生的临时文件，须在规定且有记录的期限内，遵循记录在案的程序予以处置(例如删除或销毁）。

实施指南

该组织应定期核查未使用的临时文件是否在规定时间内被删除。

其他信息

信息系统在正常运行过程中会生成临时文件。此类文件虽具有系统或应用程序专属性，但可能包含文件系统回滚日志、数据库更新相关的临时文件以及其他应用软件运行时产生的临时文件。相关信息处理任务完成后，临时文件即失去存在必要性，但某些情况下无法直接删除。这些文件的存留时长并非始终可确定，需通过”垃圾回收”程序识别相关文件，并判定其上次使用时间。

B.2.4.3 个人身份信息（PII）的归还、转移或处置控制

组织应能够以安全的方式退回、转移或处置PII。同时应向客户公开其相关政策。

实施指南

在特定情况下，可能需要以某种方式处置PII 。这可能包括将PII 返还客户、转移至其他组织或PII 控制方(例如因合并而转移)、删除或销毁、去标识化或归档。PII的返还、转移或处置能力应以安全方式进行管理。

该组织应提供必要的保证，使客户能够确保根据合同处理的个人身份信息(PII) 在不再需要用于客户指定目的时，立即从所有存储位置(包括备份和业务连续性目的)中被删除(由该组织及其任何分包商执行)。

该组织应制定并实施关于个人身份信息处置的政策，并在客户要求时提供该政策。

该政策应涵盖合同终止后处置PII前的保留期限，以防止因合同意外失效导致客户PII丢失。

注 本控制措施与指导原则同样适用于保留原则(参见B.1.4.8)。

B.2.4.4 PII传输控制控制

该组织应针对通过数据传输网络传输的个人身份信息实施适当控制措施，以确保数据送达预定目的地。

实施指南

个人身份信息的传输应受到管控，通常需确保仅授权人员可访问传输系统，并遵循相应流程(包括保留审计数据),以确保信息在传输过程中不被篡改且准确送达指定接收方。传输控制要求可纳入个人身份信息处理方与客户之间的合同条款。
在未签订涉及传输的合同要求时，传输前征询客户意见是适当的做法。

B.2.5 个人身份信息共享、转移与披露

B.2.5.1 目标

确定是否共享、向其他司法管辖区或第三方转移个人身份信息，或根据适用义务披露个人身份信息，并记录相关时间。

B.2.5.2 跨司法管辖区转移PII的依据控制

组织应及时告知客户跨司法管辖区转移PII的依据及任何相关变更计划，以便客户可对变更提出异议或终止合同。

实施指南

个人身份信息在不同司法管辖区之间的转移，可能受限于接收方(或信息来源地)司法管辖区或组织的法律要求。组织应记录其符合此类要求的依据作为转移的依据。
组织应告知客户任何PII转移行为，包括向以下对象的转移：

— 供应商；

— 其他方；

— 其他国家或国际组织。

若发生变更，组织应按约定时间框架提前告知客户，以便客户有权对变更提出异议或终止合同。

组织与客户之间的协议可包含条款，允许组织在不通知客户的情况下实施变更。此类情况下应设定权限边界(例如：组织可在不通知客户的情况下更换供应商，但不得将个人身份信息转移至其他国家)。

涉及个人身份信息的跨境转移时，应明确适用相关协议(如示范合同条款、具有约束力的公司规则或跨境隐私规则),并指明涉及的国家及协议适用的具体情形。

B.2.5.3 可转移PII的国家与国际组织管控

该组织应明确并记录可能接收个人身份信息的国家及国际组织。

实施指南

在正常运营中，应向客户披露可能接收个人身份信息的国家和国际组织的身份信息。若涉及分包处理个人身份信息的情形，应包含由此产生的相关国家身份信息。所列国家应参照B.2.5.2 条款进行评估。

在正常运营之外，可能存在应法律机构要求进行转移的情况，此类转移无法预先确定国家身份，或适用司法管辖区为维护执法调查的保密性而禁止此类转移(参见B.1.5.2 、B.2.5.5和B.2.5.6)。

B.2.5.4 向第三方披露个人身份信息的记录管控

该组织应记录向第三方披露个人身份信息的情况，包括披露了哪些个人身份信息、向谁披露以及何时披露。

实施指南

在正常运营过程中可能发生PII披露，此类披露应予以记录。任何额外向第三方披露的情形(如因法律调查或外部审计引发的披露)也应记录在案。记录内容须包含披露来源及授权披露的依据。

B.2.5.5 PII披露请求通知控制

组织应就任何具有法律约束力的PII披露请求通知客户。

实施指南

该组织可能收到具有法律约束力的个人身份信息披露请求(例如来自司法机关)。在此类情况下，组织应在约定时限内并遵循约定程序(可纳入客户合同)向客户通报此类请求。

某些情况下，具有法律约束力的请求包含禁止组织向任何人披露事件的要求。例如，为维护刑事调查的保密性而实施的刑事法律禁止披露即属于此类情形。

B.2.5.6 具有法律约束力的PII披露管控

对于不具法律约束力的PII披露请求，组织应予以拒绝；在披露PII 前须征询相关客户意见；对于经客户授权且合同约定明确的披露请求，组织应予以接受。

实施指南

与控制措施实施相关的细节可纳入客户合同。

此类请求可能来自多个来源，包括法院、法庭及行政机关，且可能涉及任何司法管辖区。

B.2.5.7 处理个人身份信息（PII） 所用分包商的披露控制

使用前，组织应向客户披露是否使用分包商处理PII。

实施指南

客户合同中应包含关于使用分包商处理PII的条款。

披露的信息应涵盖使用分包的事实及相关分包商的名称。披露内容还应包括分包商可向其转移数据的国家及国际组织（参见B.2.5.3），以及分包商必须通过何种方式满足或超越本组织的义务（参见B.2.5.8 ）。

若评估认为公开披露分包商信息将导致安全风险超出可接受范围，则应在保密协议框架下或应客户要求进行披露。客户应知悉该信息可供获取。

这不涉及可转移PII的国家名单。该名单应在所有情况下向客户披露，以便客户能够通知相应的PII 主体。

B.2.5.8 委托分包商处理PII的管控

组织仅应根据客户合同约定委托分包商处理PII。

实施指南

当组织将部分或全部个人身份信息处理工作分包给其他组织时，分包商处理该信息前须获得客户的书面授权。该授权可通过客户合同中的相应条款体现，也可采用特定的"一次性"协议形式。

组织应与任何代其处理PII的分包商签订书面合同。组织应确保其与分包商的合同涵盖实施表A.2中规定的相应控制措施。

组织与代为处理PII的分包商签订的合同，应要求分包商实施表A.2 中规定的相应控制措施，同时需考虑信息安全风险评估流程（参见6.1.2 ） 及PII 处理者所执行PII 处理的范围。默认情况下，表A.2 中所有控制措施均应视为适用。若组织决定不要求分包商实施表A.2 中的某项控制措 施 ，应说明排除该措施的合理依据。

合同可对各方的责任作出不同规定，但为保持与本文件的一致性，所有控制措施均应予以考虑并纳入文件化信息中。

B.2.5.9 处理个人身份信息（PII） 的分包商变更控制

若组织持有书面授权，在计划增补或更换处理个人身份信息的分包商时，应及时通知客户，使客户有机会对变更提出异议。

实施指南

当组织变更其分包处理部分或全部个人身份信息 (PII) 的分包商时，必须在新的分包商开始处理PII 之前获得客户的书面授权。该授权可通过客户合同中的相应条款或单独签订的"一次性"协议形式实现。

B.3 个人身份信息控制者与处理者的实施指南

B.3.1 目 标

确保个人身份信息处理的安全性。

B.3.2 通用要求

本条款为个人身份信息 (PII) 控制者和处理者提供PIMS 指导，涉及表A.3所列控制措施。除非表A.3 的具体条款另有规定，或由组织另行决定，否则相同指导原则适用于PII控制者和处理者。

B.3.3 信息安全政策

控制措施

应制定与PII处理相关的信息安全政策，经管理层批准后发布，向相关人员及相关利益方传达并获得确认，同时按计划周期及发生重大变更时进行审查。

实施指南

组织应通过制定独立的隐私政策或补充信息安全政策，发布声明表明支持并承诺遵守适用于PII保护的法律要求，以及组织与其合作伙伴、分包商及相关第三方(客户、供应商等)之间约定的合同条款，该声明应明确划分各方责任。

任何处理个人身份信息 (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政策时，都应考虑适用于PII 保护的法律要求。

B.3.4 信息安全职责分工

控制

应根据组织需求定义并分配与PII处理相关的信息安全角色与职责。

实施指南

组织应指定客户就PI 处理事宜联系的对接人。当组织作为PI 控制者时，应为PII主体指定处理其PII事宜的对接人(参见B.1.3.4)。

该组织应任命一名或多名负责人，负责制定、实施、维护和监督全组织范围的治理和隐私计划，以确保遵守所有关于处理个人身份信息 (PII) 的适用法律要求。

该负责人应在适当情况下：

— 保持独立性并直接向组织相应管理层汇报，以确保隐私风险得到有效管理；

— 参与处理所有涉及个人身份信息处理的管理事务；

一 精通数据保护法律法规及实践操作；

— 作为监管机构的联络点；

一 向组织高层管理人员及员工告知其在处理个人身份信息方面的义务；

一 就组织开展的隐私影响评估提供专业建议。

注 :部分司法管辖区将此职位称为数据保护官。各司法管辖区会规定设立该职位的具体情形及其职责范围。该职位可由内部员工担任，也可通过外包方式实现。

B.3.5 信息分类

控制

信息应根据组织的资讯安全需求进行分类，同时考虑个人身份信息(PII), 基于保密性、完整性、可用性及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纳入实施框架。在整体分类体系中考量PII, 对于理解组织处理的PII类型(如数据类别、特殊类别)、存储位置及流通路径至关重要。

B.3.6 信息标识

控制

应根据组织采用的信息分类方案，制定并实施一套适当的信息标识程序，该程序需考虑个人身份信息 (PII)。

实施指南

组织应确保其控制范围内的人员了解PII的定义以及如何识别属于PII的信息。

B.3.7 信息转移

控制

应制定与处理PII 相关的信息传输规则、程序或协议，适用于组织内部所有类型的传输设施以及组织与其他方之间的传输。

实施指南

该组织应考虑制定相关程序，确保与处理PII 相关的规则在整个系统内外得到执行(如适用)。

B.3.8 身 份 管 理

控制

应管理与PII处理相关的身份的完整生命周期。

实施指南

处理个人身份信息 (PII) 的系统及服务的管理员或操作员的注册与注销流程，应涵盖用户访问控制遭破坏的情形，例如密码或其他用户注册数据(如因无意泄露导致)的损坏或泄露。

对于处理个人身份信息的系统及服务，组织不得向用户重新发放已被停用或过期的用户ID。

当组织以服务形式提供个人身份信息处理时，客户可负责用户身份管理的部分或全部环节。此类情况应纳入文件化信息范围。

部分司法管辖区对涉及PII处理系统的闲置认证凭证检查频率有具体要求。在这些辖区运营的组织应考虑遵守相关规定。

B.3.9 访问权限

控制

应根据组织关于访问控制的专题政策和规则，对与PII 处理相关的PI 及其他关联资产的访问权限进行配置、审查、修改和删除。

实施指南

组织应准确维护并及时更新用户档案记录，涵盖所有获准访问信息系统及其中PII 的用户。每个档案包含用户数据集(含用户ID), 这些数据是实施授权访问技术控制措施的必要依据。

实施个人用户访问ID可使配置得当的系统识别访问个人身份信息 (PII) 的用户身份，以及其进行的增删改操作。这不仅保护了组织，也保障了用户权益——用户可清晰追溯自身处理过的数据与未处理的数据。

当组织以服务形式提供PI 处理时，客户可负责部分或全部访问管理职责。在适用情况下，组织应为客户提供访问管理手段，例如授予管理或终止访问权限的行政权限。此类情形应纳入文件化信息中。

B.3.10 在供应商协议中处理信息安全问题

控制

应根据供应商关系类型，与每位供应商建立并达成关于处理个人身份信息的相关信息安全要求。

实施指南

组织应在与供应商的协议中明确是否处理PII, 并规定供应商必须满足的最低技术和组织措施，以确保组织履行其信息安全和PII 保护义务(参见B.1.2.7和B.2.2.2)。

供应商协议应根据所处理PII的类型，明确划分组织、其合作伙伴、供应商及相关第三方(客户、供应商等)之间的责任。

该组织与其供应商之间的协议应建立机制，确保该组织支持并管理对所有适用法律要求的合规性。协议应要求通过独立审计的合规性，且该合规性需被客户接受。

注 :此类审核可考虑采用ISO/IEC 27001等相关适用安全标准作为合规依据。

当组织担任个人身份信息处理者时，应在与供应商的合同中明确规定个人身份信息仅可根据其指令进行处理。

B.3.11 信息安全事件管理规划与准备

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，规划并准备处理与PII处理相关的信息安全事件。

实施指南

作为整体信息安全事件管理流程的一部分，组织应建立识别和记录个人身份信息泄露事件的责任与程序。此外，组织还应建立向相关方通报个人身份信息泄露事件(包括通报时限)以及向监管机构披露信息的责任与程序，同时需考虑适用的法律要求。
部分司法管辖区对违规响应(包括通知程序)制定了具体法规。在这些区域运营的组织应确保知悉相关法规，并记录其合规措施。

B.3.12 信 息安全事件响应

控制措施

涉及PII处理的信息安全事件响应应遵循已记录的程序。

PII控制者的实施指南

涉及PII的事件应触发组织在信息安全事件管理流程中的审查，以确定是否发生了需要响应的涉及PII的泄露事件。

事件本身未必必然触发此类审查。

注1:信息安全事件未必导致实际发生或存在重大可能性的未经授权访问个人身份信息(PII), 亦未必涉及存储PII 的组织设备或设施。此类事件包括但不限于：针对防火墙或边缘服务器的ping测试及其他广播攻击、端口扫描、登录失败尝试、拒绝服务攻击及数据包嗅探。
当发生PII泄露事件时，响应程序应包含相关通知与记录。

某些司法管辖区规定了应向相关监管机构通报违规事件的情况，以及应向PII 主体通报的情况。

通知应清晰明确。

注2 通知可包含以下细节：

— 可获取更多信息的联络点;

— 违规行为的描述及其可能后果;

— 违规事件的描述，包括涉及的个人数量及相关记录数量;

— 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参阅ISO/IEC 27035系列标准。

若发生涉及个人身份信息的泄露事件，应保留包含充分信息的记录以供监管或取证报告使用，例如：

— 事件描述：

— 时间段;

— 事件的后果；

一 报告人的姓名；

一 事件上报对象；

一 为解决事件采取的措施(包括负责人及恢复的数据)；

一 该事件导致个人身份信息(PII)不可用、丢失、泄露或被篡改的事实。

若涉及PI 的泄露事件发生，记录还应包含已知泄露PII的描述。若已启动通知程序，则需记录通知PII主体、监管机构或客户所采取的步骤。

PII处理者的实施指南

涉及个人身份信息泄露的通知条款应纳入组织与客户之间的合同。合同应明确规定组织将如何提供必要信息，以协助客户履行向相关监管机构通报的义务。此项通报义务不适用于由客户或个人身份信息主体造成的泄露事件，也不适用于其负责的系统组件内部发生的泄露事件。合同还应界定通知响应时间的预期时限及外部强制要求时限。

在某些司法管辖区，PII处理者应在发现泄露后立即(即发现时)通知PII控制者，以便后者采取相应措施。

当发生涉及PII的泄露事件时，应保留包含充分信息的记录以供监管或取证报告之用，例如：

— 事件描述；

一 事件发生时间段；

一 事件后果；

— 报告人姓名；

— 事件上报对象；

—为解决该事件所采取的措施(包括负责人及恢复的数据)；

一 该事件导致个人身份信息(PII)不可用、丢失、泄露或被篡改的事实。

若发生涉及PII的泄露事件，记录还应包含已知泄露PII的描述；若采取了通知措施，则需说明向客户或监管机构通报的具体步骤。

在某些司法管辖区，适用法律要求组织必须直接向相关监管机构(例如个人身份信息保护机构)通报涉及个人身份信息的泄露事件。

B.3.13 法律、法规、监管及合同要求

控制

应记录与PII 处理相关的信息安全相关的法律、法规、监管和合同要求，以及组织为满足这些要求所采取的方法，并保持文件的及时更新。

实施指南

组织应识别与处理个人身份信息相关的任何潜在法律制裁(可能因未履行某些义务而产生),包括当地监管机构直接施加的巨额罚款。

在某些司法管辖区，本文件等国际标准可作为组织与客户之间合同的基础，明确双方在安全、隐私及PII保护方面的责任。合同条款可在责任违约时为合同制裁提供依据。

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、伪造、未经授权的访问和未经授权的披露。

实施指南

可能需要审查当前和历史政策及程序(例如在客户争议解决和监管机构调查的情况下)。

组织应按照其保留计划(参见B.1.4.8) 规定的期限保留其隐私政策及相关程序的副本。这包括在更新这些文件时保留其旧版本。

B.3.15 信息安全的独立审查

控制

该组织处理个人身份信息 (PII) 相关信息安全的管理方法及其实施(包括人员、流程和技术),应在计划周期内或发生重大变更时进行独立审查 。

实施指南

当组织作为个人身份信息处理者时，若实施单独客户审计不可行或可能增加安全风险，该组织应在签订合同前及合同有效期内，向客户提供独立证据，证明其信息安全措施的实施与运行符合组织政策和程序。由组织选定的相关独立审计，通常可作为满足客户审查组织处理操作需求的可行方式——前提是该审计能覆盖预期用户的需求，且结果以充分透明的方式呈现。

B.3.16 遵守信息安全政策、规则和标准

控制

应定期审查对组织信息安全政策、特定主题政策、规则及与个人身份信息处理相关标准的遵守情况。

实施指南

在对安全政策和标准合规性的技术审查中，组织应纳入审查与处理PII相关的工具和组件的方法。这可包括：

— 持续监控以验证仅进行许可处理；或

— 特定渗透测试或漏洞测试(例如：可对去标识化数据集实施动机入侵者测试，以验证去标识化方法是否符合组织要求)。

B.3.17 信息安全意识、教育与培训

控制措施

组织人员及相关利益方应接受适当的信息安全意识教育培训，并定期更新组织的信息安全政策、与工作职能相关的特定主题政策及程序，这些内容均涉及个人身份信息处理。

政策、特定主题政策及程序，这些内容应与其工作职能相关，且涉及个人身份信息处理。

实施指南

应采取相应措施，包括提高事件报告意识，确保相关员工了解违反隐私或安全规则及程序可能带来的后果，特别是涉及个人身份信息处理的相关规定。这些后果包括：对组织(例如法律后果、业务损失、品牌或声誉损害)、对员工(例如纪律处分)以及对个人身份信息主体(例如身体、物质和情感后果)造成的损害。

注　　此类措施可包括对接触个人身份信息的人员进行适当的定期培训。

B.3.18　保密或不披露协议

控制

应确定、记录、定期审查并由人员及其他相关利益方签署反映组织保护PII 需求的保密或非披露协议。

实施指南

该组织应确保在其控制下接触个人身份信息 (PII)　的个人承担保密义务。保密协议(无论作为合同组成部分或单独文件)应明确规定义务的履行期限。

当组织作为个人身份信息处理方时，其与员工及代理人签订的保密协议(无论何种形式)均应确保员工和代理人遵守数据处理与保护的相关政策及程序。

B.3.19　清桌面与清屏幕

控制

应制定并严格执行针对纸质文件和可移动存储介质的清桌规则，以及针对信息处理设施的清屏规则。

实施指南

组织应将包含个人身份信息的纸质材料制作限制在满足已确定处理目的所需的最低限度。

B.3.20　存 储 介 质

控制

存储个人身份信息的存储介质应遵循组织分类方案及处理要求，在其获取、使用、运输及处置的生命周期内进行管理。

实施指南

组织应记录所有用于存储PII的可移动介质或设备的使用情况。在可行情况下，存储PII 时应优先选用支持加密功能的物理介质或设备。未加密介质仅限于不可避免的情形使用，若使用未加密介质或设备，组织应实施相应程序及补偿性控制措施(如防篡改包装)，以降低PII 面临的风险。

当处置存储过PII的可移动介质时，应将安全处置程序纳入文件化信息并予以实施，确保先前存储的PII 无法被访问。

若使用物理介质传输信息，应建立系统记录进出含个人身份信息的物理介质，包括介质类型、授权发送方、授权接收方、日期时间及介质数量。在可行情况下，应实施加密等额外措施，确保数据仅能在目的地而非传输过程中被访问。

组织应在含PII的物理介质离开场所前执行授权程序，确保除授权人员外任何人无法访问该PII。

注 确保离场物理介质上的PII不被普遍访问的可行措施包括：对相关PII进行加密，并将解密权限限制在授权人员范围内。

带离组织物理边界的可移动介质易遭丢失、损坏及不当访问。对可移动介质进行加密可为PI 增添保护层，即使介质遭泄露也能降低安全与隐私风险。

B.3.21 设备的安全处置或再利用

控制

含有存储P 介质的设备在处置或再利用前，应进行验证以确保所有敏感数据及授权软件已被移除或安全覆盖。

实施指南

组织应确保在重新分配存储空间时，确保该存储空间中先前存储的任何个人身份信息均不可访问。

关于信息系统中PII的删除操作，性能限制可能导致明确清除该PII不可行，从而产生其他用户访问PII 的风险。此类风险应通过特定技术措施加以规避。

为实现安全处置或再利用，凡可能含有PII的存储介质设备，均应按实际含有PII的标准进行处理。

B.3.22 用户终端设备

控制

存储于用户终端设备、由其处理或可通过其访问的PII均应受到保护。

实施指南

组织应确保移动设备的使用不会导致个人身份信息的泄露，

B.3.23 安 全 认 证

控制

应基于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。

实施指南

若客户提出要求，组织应为客户控制下的任何用户账户提供安全登录程序功能。

B.3.24 信息备份

控制

应维护并定期测试与PII 处理相关的PII、软件和系统的备份副本。

实施指南

该组织应制定政策，明确个人身份信息 (PII) 备份、恢复及还原的要求(可纳入整体信息备份政策)，并规定备份需求所涉信息中PII销毁的其他要求(如合同或法律要求)。

此类PI 的具体责任可能因客户而异。组织应确保客户已知悉服务在备份方面的限制。

当组织明确向客户提供备份和恢复服务时，应向其提供关于个人身份信息 (PII) 备份与恢复能力的清晰说明。

某些司法管辖区对PI 备份频率、备份审查测试频率或PII恢复流程设定了具体要求。在这些辖区运营的组织应证明其符合相关要求。

可能存在因系统故障、攻击或灾难等情况需要恢复PII的情形。当进行PII 恢复(通常从备份介质恢复)时，应建立流程确保恢复后的PII处于完整性可保障的状态，或在发现PII存在不准确或不完整时启动处理流程予以解决(该流程可能涉及PII主体)。

组织应建立PII恢复操作规程及记录机制。PII恢复记录至少应包含：

— 负责恢复操作的人员姓名；

— 已恢复PII的描述。

某些司法管辖区对个人身份信息恢复工作的日志内容有具体规定。组织应能证明其恢复日志内容符合此类要求。相关讨论结论应纳入文件化信息中。

使用分包商存储已处理PII的复制件或备份副本，适用本文件中关于分包PII 处理的控制措施(参见B.3.10、B.3.20)。涉及备份与恢复的物理介质传输，同样受本文件控制措施约束(参见B.3.7)。

B.3.25 日志记录

控制

应生成、存储、保护并分析记录与个人身份信息处理相关的活动、异常、故障及其他相关事件的日志。

实施指南

应建立流程，通过持续的自动化监控和警报机制审查事件日志，或在无法实现自动化时，按规定周期进行手动审查，以识别异常情况并提出补救措施。

在可行情况下，事件日志应记录对PII的访问行为，包括访问者身份、访问时间、涉及的PII 主体信息，以及事件导致的变更内容(如有，如增补、修改或删除)。

当多个服务提供商参与服务时，实施本指南可能涉及不同或共享的角色。这些角色应明确定义并纳入文件化信息，同时需明确各提供商间日志访问的协作机制。

用于安全监控和运行诊断等目的的日志信息可能包含PII。应采取访问控制等措施，确保日志信息仅按预期用途使用。

应建立一套程序(最好是自动程序),确保记录的信息按照保留计划(参见B.1.4.8) 的规定予以删除或去标识化。

个人身份信息处理者的实施指南

组织应制定关于日志信息何时、如何向客户开放或供客户使用的准则，并向客户披露这些准则。

当组织允许客户访问其控制的日志记录时，应实施适当控制措施确保客户：

一 仅能访问与该客户活动相关的记录；

一 不得访问任何与其他客户活动相关的日志记录；且

— 不得以任何方式修改日志。

B.3.26 加密技术的使用

控制

应制定并实施与处理个人身份信息相关的加密技术有效使用规则，包括加密密钥管理。

实施指南

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

组织应向客户说明其使用加密技术保护所处理个人身份信息的具体情形。组织还应向客户说明其提供的任何可协助客户应用自身加密保护功能的能力。

B.3.27 安全开发生命周期

控制

应制定并实施与处理个人身份信息相关的软件和系统安全开发规则。

实施指南

系统开发与设计政策应包含组织处理PI 需求的指导原则，该原则需基于对PII主体的义务、适用法律要求以及组织实施的处理类型。

促进隐私设计和隐私默认的政策应考虑以下方面：

a) 在软件开发生命周期中实施PII保护及隐私原则(参见ISO/IEC 29100)的指导方针；

b) 在设计阶段纳入隐私和个人身份信息保护要求，该要求可基于隐私风险评估或隐私影响评估的输出结果(参见B.1.2.6)；

c) 项目里程碑中的PII保护检查点；

d) 必需的隐私与PII保护知识；

e) 默认情况下，最大限度减少对PII的处理。

B.3.28 应用程序安全要求

控制

在开发或采购应用程序时，应识别、明确并批准与PII处理相关的信息安全要求。

实施指南

组织应确保通过不可信数据传输网络传输的个人身份信息进行加密传输。

不可信网络包括公共互联网以及组织运营控制范围之外的其他设施。

注： 在某些情况下(例如电子邮件交换)，不可信数据传输网络系统的固有特性可能要求暴露某些头信息或流量数据才能实现有效传输。

B.3.29 安全系统架构与工程原则

控制

应建立、记录、维护并应用处理个人身份信息 (PII) 相关的安全系统工程原则，以指导任何信息系统开发活动。

实施指南

与处理 PII 相关的系统或组件应遵循“隐私设计”和“隐私默认”原则进行设计，并预测和促进相关控制措施的实施(分别在B.1和B2 中针对PII 控制者和 PII 处理者进行了描述)，特别是确保这些系统中的 PII收集和处理仅限于为已确定的PII 处理目的所必需的范围(参见B.1.2)。2)。

例如，处理个人身份信息的组织应确保在规定期限后销毁该信息。处理个人身份信息的系统应在设计上便于满足此删除要求。

注 法律要求可能适用。

B.3.30 外包开发

控制

该组织应指导、监督和审查与外包的PII处理系统开发相关的活动。

实施指南

在适用情况下，应将隐私设计和隐私默认原则(参见B,3.29) 同样应用于外包信息系统。

B.3.31 测试信息

控制

应适当选择、保护和管理与个人身份信息处理相关的测试信息。

实施指南

不应使用个人身份信息 (PII) 进行测试：应使用虚假或合成的PII。 当测试目的必须使用PII 时，应实施与生产环境同等的技术和组织措施以降低风险。若此类同等措施不可行，则应进行风险评估并据此确定适当的缓解控制措施。

附件C
（参考性）

映射至ISO/IEC 29100

表C.1和C.2提供了本文件条款与以及ISO/IEC 29100隐私原则之间指示性对照关系。表C.1和C.2以纯示例性方式展示了本文件要求与控制措施的符合性如何关联ISO/IEC29100 规定的一般隐私原则。表C.1和C.2中的交叉引用对应于表A.1至A.3中控制措施的引用位置。

表C.1— 个人身份信息(PII) 控制者与ISO/IEC 29100控制措施的映射关系

ISO/IEC 29100隐私原则	PII控制者相关控制措施
1. 同意与选择(ISO/IEC 29100:2024,6.2)	A.1.2.2确定并记录处理目的 A.1.2.3确定合法依据 A.1.2.4确定何时以及如何获取同意 A.1.2.5获取并记录同意 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提供反对处理个人身份信息的机制 A.1.3.8个人信息控制者向第三方告知的义务
2. 目的合法性与具体化(ISO/EC 29100:2024,6.3)	A.1.2.2确定并记录处理目的 A.1.2.3确定合法依据 A.1.2.6隐私影响评估 A.1.3.3确定个人身份信息主体的信息 A.1,3.4向PII主体提供信息 A.1.3.11自动化决策
3. 收集限制(ISO/IEC29100:2024,6.4)	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限制处理 A.1.4.5个人身份信息最小化目标 A.1.4.6处理结束时的个人身份信息去标识化与删除
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去标识化与删除 A.1.4.7临时文件 A.1.4.8保留 A.1.4.9处置 A.1.5.2确定跨司法管辖区转移个人身份信息的依据 A.1.5.5向第三方披露个人身份信息的记录
6. 准确性与质量(ISO/IEC 29100:2024,6.7)	A.1.4.4准确性与质量
7. 公开性、透明度与通知(ISO/IEC 29100:2024,6.8)	A.1.3.3确定个人身份信息主体的信息 A.1.3.4向PII主体提供信息
8. 个人参与与访问(ISO/IEC 29100:2024,6.9)	A.1.3.2确定并履行对PII主体的义务 A.1.3.4向PII主体提供信息 A.1.3.7访问、更正或删除 A.1.3.9提供已处理PII的副本 A.1.3.10处理请求

表C.1 (续)

ISO/IEC 29100隐私原则	与PII控制者相关的控制措施
9.问责制(ISO/IEC 29100:2024,6.10)	A.1.2.7与PI处理者签订的合同 A.1.2.8联合PII控制者 A.1.2.9与处理P相关的记录 A.1.3.10请求处理 A.1.5.2确定跨司法管辖区转移PII的依据 A.1.5.3可接收个人身份信息的国家及国际组织 A.1.5.4个人身份信息转移记录
10.信息安全(ISO/IEC 29100:2024,6.11)	A.1.2.7与个人身份信息处理方的合同 A.1.4.10个人身份信息传输控制
11.隐私合规性(ISO/IEC 29100:2024,6.12)	A.1.2.6隐私影响评估

表C.2— 个人身份信息处理者控制措施与ISO/IEC 29100映射

ISO/IEC 29100的隐私原则	PI处理器的相关控制措施
1.同意与选择(ISO/IEC 29100:2024, 6.2)	A.2.2.6客户义务
2. 目的合法性与明确性(ISO/IEC 29100:2024,6.3)	A.2.2.2客户协议 A.2.2.3组织的宗旨 A.2.2.4营销与广告用途 A.2.2.5侵权指令 A.2.3.2遵守对个人身份信息主体的义务
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/IEC 29100:2024,6.6)	A.2.5.4向第三方披露个人身份信息(PII)的记录 A.2.5.5 PII披露请求通知 A.2.5.6具有法律约束力的PI披露
6.准确性与质量(ISO/IEC 29100:2024, 6.7)	不适用
7.公开性、透明度与通知(ISO/IEC 29100:2024,6.8)	A.2.5.7披露处理PII的分包商 A.2.5.8委托分包商处理PII A.2.5.9更换处理PI的分包商
8.个人参与与访问权限(ISO/IEC 29100:2024,6.9)	A.2.3.2履行对PII主体的义务
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、转移或处置 A.2.5.2跨司法管辖区转移PII的依据 A.2.5.3可接收个人身份信息的国家及国际组织
10.信息安全(ISO/IEC 29100:2024,6.11)	A.2.4.4个人身份信息传输控制
11.隐私合规性(ISO/IEC 29100:2024,6.12)	A.2.2.6客户义务

附录D
（参考性）

与《通用数据保护条例》的对照关系

表D.1提供了本文件条款与欧盟《通用数据保护条例》第5至49条（不含第43条）的参考对照关系。[1]该表展示了遵守本文件要求与控制措施如何有助于履行GDPR义务。

注释　本对照表仅供参考。组织有责任评估其法律义务并决定如何履行。

表D.1— 本文件条款与GDPR条款对照表

本文件子条款	相关GDPR条款
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)(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)
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)()、(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)()、(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)(b)
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条款
B.3.21	(5)(1)f)
B.3.22	(5)(1)f)
B.3.23	(5)(1)①)
B.3.24	(5)(1)(f)、(32)(1)(c)
B.3.25	(5)(1)f)
B.3.26	(32)(1)(a)
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)①)、(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.1.29	(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)(1)(e)、(13)(1)()、(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)(1)、(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)(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)(1)(c)、(17)(1)(d)、(17)(1)(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)(1)、(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)(d)
B.1.4.5	(5)(1)(e)、(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条款
B.1.4.9	(5)(1)f)
B.1.4.10	(5)(1)f)
B.1.5.2	(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)(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.1.54	(30)(1)(e)
B.1.5.5	(30)(1)(d)
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)(h)
B.2.2.6	(28)(3)(h)
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)(c)
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)()、(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.2.54	(30)(1)(d)
B.2.5.5	(28)(3)(a)
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
（参考性）

映射至ISO/IEC 27018和ISO/IEC29151

ISO/IEC 27018为作为PII 处理者并提供公共云服务的组织提供了进一步信息。 ISO/IEC 29151为 PII 控制者处理PII 提供了额外的控制措施和指导。

表E 1提供了本文件条款与ISO/IEC 27018及ISO/IEC 29151条款之间的参考对照关系。该表展示了本文件的要求和控制措施如何与ISO/IEC 27018或ISO/IEC 29151的条款相对应。

表E.1所示映射仅为参考性说明；条款间的对应关系并不意味着它们具有等效性。

表E.1—ISO/IEC 27701与ISO/IEC 27018及ISO/IEC 29151的映射关系

本文件中的分条款	ISO/EC 27018中的子条款	ISO/IEC 29151中的分条款
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、B3.13、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、B.3.29、B.3.30、B.3.31	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.1.2.2	不适用	A.4
B.1.2.3	不适用	A.4.1
B.1.2.4	不适用	A.3.1
B.1.2.5	不适用	A.3.1
B.1.2.6	不适用	A.11.2
B.1.2.7	不适用	A.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	A.10
B.1.3.3	不适用	A.9.2
B.1.3.4	不适用	A.9

表E.1（续）

B.1.3.5	不适用	A.3.2
B.1.3.6	不适用	A.3.2
B.1.3.7	不适用	A.10.1、A.10.2
B.1.3.8	不适用	A.10.2
B.1.3.9	不适用	A.10.1
B.1.3.10	不适用	A.10.1
B.1.3.11	不适用	不适用
B.1.4.2	不适用	A.5
B.1.4.3	不适用	A.7.1
B.1.4.4	不适用	A.8
B.1.4.5	不适用	A.6
B.1.4.6	不适用	A.7.1
B.1.4.7	不适用	A.7.2
B.1.4.8	不适用	A.7.1
B.1.4.9	不适用	A.7.14
B.1.4.10	不适用	不适用
B.1.5.2	不适用	A.13.2
B.1.5.3	不适用	A.13.2
B.1.5.4	不适用	A.13.2
B.1.5.5	不适用	A.7.4
B.2.2.2	不适用	不适用
B.2.2.3	A.3.1	不适用
B.2.2.4	A.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	A.7.4
B.2.3.2	A.2.1	不适用
B.2.4.2	A.5.1	A.7.2
B.2.4.3	A.10.3	A.11.3
B.2.4.4	A.12.2	不适用
B.2.5.2	不适用	A.4.1、A.13.2
B.2.5.3	A.12.1	A.13.2
B.2.5.4	A.6.2	A.7.4
B.2.5.5	A.6.1	A.7.3
B.2.5.6	A.6.1	A.7.3
B.2.5.7	A.8.1	A.7.5
B.2.5.8	A.8.1	不适用
B.2.5.9	A.8.1	不适用

附件F
（信息性）

与ISO/IEC 27701:2019的对应关系

本附录旨在为当前使用此文件（ISO/IEC 27701:2019）并希望过渡到新版的组织提供向后兼容性。

表E.1提供了附 件A中规定的控制措施与ISO/IEC 27701:2019标准中控制措施的对应关系。第一列中的"N/A" 标识未包含在本文件中的控制措施。第二列中的"新增"标识未包含在ISO/IEC 27701:2019标准中的控制措施。

表F.1— 本文件控制措施与ISO/IEC 27701:2019控制措施对照表

ISO/IEC 27701 控制措施标识符	ISO/ IEC 27701:2019 控制标识符	控制名称
A.3.3	6.2.1.1,6.2.1.2	信息安全政策
A.3.4	6.3.1.1	信息安全角色与职责
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	与当局的联系
不适用	6.3.1.4	与特殊利益团体的联系
不适用	新	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	信息及其他相关资产的清单
不适用	6.5.1.3,6.5.2.3	信息及其他相关资产的可接受使用
不适用	6.5.1.4	资产归还
A.3.5	6.5.2.1	信息分类
A.3.6	6.5.2.2	信息标识
A.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	访问控制
A.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
A.3.9	6.6.2.2,6.6.2.5, 6.6.2.6	访问权限
A.3.10	6.12.1.1 6.12.1.2	供应商协议中的信息安全条款
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	云服务使用中的信息安全
不适用	6.13.1.1	信息安全事件管理规划与准备
A.3.11	6.13.1.4	信息安全事件的评估与决策
A.3.12	6.13.1.5	信息安全事件的响应
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	ISO/ 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	业务连续性的信息通信技术准备情况
A.3.13	6.15.1.1、6.15.1.5	法律、法规、监管和合同要求
不适用	6.15.1.2	知识产权
A.3.14	6.15.1.3	记录保护
不适用	6.15.1.4	隐私与个人身份信息保护
A.3.15	6.15.2.1	信息安全的独立审查
A.3.16	6.15.2.2、6.15.2.3	信息安全政策、规则和标准的合规性
不适用	6.9.1.1	文件化的操作程序
不适用	6.4.1.1	筛选
不适用	6.4.1.2	雇佣条款与条件
A.3.17	6.4.2.2	信息安全意识、教育和培训
不适用	6.4.2.3	纪律程序
不适用	6.4.3.1	离职或变更工作后的责任
A.3.18	6.10.2.4	保密或不披露协议
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	物理出入
不适用	6.8.1.3	办公室、房间和设施的安全保障
不适用	新	实体安全监控
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
A.3.19	6.8.2.9	桌面和屏幕清理
不适用	6.8.2.1	设备选址与防护
不适用	6.8.2.6	场外资产安全
A.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	辅助工具
不适用	6.8.2.3	布线安全
不适用	6.8.2.4	设备维护
A.3.21	6.8.2.7	设备的安全处置或再利用
A.3.22	6.3.2.1、6.8.2.8	用户终端设备
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
A.3.23	6.6.4.2	安全认证
不适用	6.9.1.3	容量管理
不适用	6.9.2.1	恶意软件防护
不适用	6.9.6.1	技术漏洞管理
不适用	新	配置管理

表F.1 (续)

ISO/IEC 27701 控制标识符	ISO/ IEC 27701:2019 控制标识符	控制名称
不适用	新	信息删除
不适用	新	数据屏蔽
不适用	新	数据泄露防护
A.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性
A.3.25	6.9.4.1,6.9.4.2, 6.9.4.3	记录
不适用	新	监测活动
不适用	6.9.4.4	时钟同步
不适用	6.6.4.4	特权实用程序的使用
不适用	6.9.5.1、6.9.6.2	在操作系统上安装软件
不适用	6.10.1.1	网络安全
不适用	6.10.1.2	网络服务的安全性
不适用	6.10.1.3	网络隔离
不适用	新	网络隔离
A.3.26	6.7.1.1、6.7.1.2	加密技术的使用
A.3.27	6.11.2.1	安全开发生命周期
A.3.28	6.11.1.2、6.11.1.3	应用程序安全要求
A.3.29	6.11.2.5	安全系统架构与工程原则
不适用	新	安全编码
不适用	6.11.2.8、6.11.2.9	开发和验收阶段的安全性测试
A.3.30	6.11.2.7	外包开发
不适用	6.9.1.4、6.11.2.6	开发、测试和生产环境的分离
不适用	6.9.1.2,6.11.2.2, 6.11.2.3,6.11.2.4	变更管理
A.3.31	6.11.3.1	测试信息
不适用	6.9.7.1	审计测试期间信息系统的保护

表F 2提供了ISO/EC27701:2019 第6条款中规定的控制措施与本文件中控制措施的对应关系。第二列中的“N/A” 标识了未包含在本文件中的控制措施。

表 F.2—ISO/IEC 27701:2019控制措施与本文件控制措施的对应关系

ISO/ IEC 27701:2019 控制措施标识符	ISO/IEC 27701 控制措施标识符	根据ISO/IEC 27701:2019的控制名称
6.2.1.1	A.3.3	信息安全政策
6.2.1.2	A.3.3	信息安全政策的审查
6.3.1.1	A.3.4	内部安全职责分工
6.3.1.2	不适用	职责分离
6.3.1.3	不适用	与当局的联系
6.3.1.4	不适用	与特殊利益团体联系
6.3.1.5	不适用	项目管理中的信息安全
6.3.2.1	A.3.22	移动设备政策
6.3.2.2	不适用	远程办公

表F.2（续）

ISO/ IEC 27701:2019 控制标识符	ISO/IEC 27701 控制标识符	根据ISO/IEC 27701:2019的控制名称
6.4.1.1	不适用	筛选
6.4.1.2	不适用	雇佣条款与条件
6.4.2.1	不适用	管理职责
6.4.2.2	A.3.17	信息安全意识、教育和培训
6.4.2.3	不适用	纪律处分程序
6.4.3.1	不适用	终止或变更雇佣职责
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	资产的可接受使用
6.5.1.4	不适用	资产归还
6.5.2.1	A.3.5	信息分类
6.5.2.2	A.3.6	信息标识
6.5.2.3	不适用	资产处理
6.5.3.1	A.3.20	可移动介质的管理
6.5.3.2	A.3.20	介质的处置
6.5.3.3	A.3.20	物理介质转移
6.6.1.1	不适用	访问控制策略
6.6.1.2	不适用	网络及网络服务的访问
6.6.2.1	A.3.8	用户注册与注销
6.6.2.2	A.3.9	用户访问权限配置
6.6.2.3	不适用	特权访问权限管理
6.6.2.4	不适用	用户机密认证信息的管理
6.6.2.5	A.3.9	用户访问权限审查
6.6.2.6	A.3.9	访问权限的删除或调整
6.6.3.1	不适用	使用秘密认证信息
6.6.4.1	不适用	信息访问限制
6.6.4.2	A.3.23	安全登录程序
6.6.4.3	不适用	密码管理系统
6.6.4.4	不适用	特权实用程序的使用
6.6.4.5	不适用	程序源代码访问控制
6.7.1.1	A.3.26	加密控制的使用政策
6.7.1.2	A.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	物理出入控制
6.8.1.3	不适用	办公室、房间和设施的安全保障
6.8.1.4	不适用	防范外部与环境威胁
6.8.1.5	不适用	在安全区域工作
6.8.1.6	不适用	交付和装载区域
6.8.2.1	不适用	设备定位与防护
6.8.2.2	不适用	辅助设施
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）

ISO/ IEC 27701:2019 控制标识符	ISO/IEC 27701 控制标识符	根据ISO/IEC 27701:2019的控制名称
6.8.2.6	不适用	场外设备和资产的安全性
6.8.2.7	A.3.21	设备的安全处置或再利用
6.8.2.8	A.3.22	无人看管的用户设备
6.8.2.9	A.3.19	清桌清屏政策
6.9.1.1	不适用	记录操作程序
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、测试和运行环境的分离
6.9.2.1	不适用	针对恶意软件的控制措施
6.9.3.1	A.3.24	信息备份
6.9.4.1	A.3.25	事件记录
6.9.4.2	A.3.25	日志信息的保护
6.9.4.3	A.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	操作系统软件安装
6.9.6.1	不适用	技术漏洞管理
6.9.6.2	不适用	限制软件安装
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	网络隔离
6.10.2.1	A.3.7	信息传输政策与程序
6.10.2.2	A.3.7	信息传输协议
6.10.2.3	A.3.7	电子信息传递
6.10.2.4	A.3.18	保密或不披露协议
6.11.1.1	不适用	信息安全要求分析与规范
6.11.1.2	A.3.28	在公共网络上保障应用服务的安全
6.11.1.3	A.3.28	保护应用服务交易
6.11.2.1	A.3.27	安全开发政策
6.11.2.2	不适用	系统变更控制程序
6.11.2.3	不适用	操作平台变更后应用程序的技术审查
6.11.2.4	不适用	软件包变更限制
6.11.2.5	A.3.29	安全系统工程原则
6.11.2.6	不适用	安全开发环境
6.11.2.7	A.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	A.3.30	测试数据保护
6.12.1.1	A.3.10	供应商关系的信息安全政策
6.12.1.2	A.3.10	供应商协议中的安全条款
6.12.1.3	不适用	信息和通信技术供应链
6.12.2.1	不适用	供应商服务的监测与审查
6.12.2.2	不适用	供应商服务变更管理

表F.2（续）

ISO/ IEC 27701:2019 控制标识符	ISO/IEC 27701 控制标识符	根据ISO/IEC 27701:2019的控制名称
6.13.1.1	不适用	责任与程序
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	A.3.11	信息安全事件的评估与决策
6.13.1.5	A.3.12	信息安全事件的响应
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	A.3.13	适用法律和合同要求的确定
6.15.1.2	不适用	知识产权
6.15.1.3	A.3.14	记录保护
6.15.1.4	不适用	隐私与个人身份信息的保护
6.15.1.5	A.3.13	加密控制的监管
6.15.2.1	A.3.15	信息安全的独立审查
6.15.2.2	A.3.16	遵守安全政策和标准
6.15.2.3	A.3.16	技术合规性审查

参考文献

[1] ISO 19011, 管理体系审核指南

[2] ISO/IEC 19944-1, 云计算和分布式平台—数据流、数据类别和数据使用—第1部分：基础知识

[3] ISO/IEC 19944-2, 云计算与分布式平台——数据流、数据类别与数据使用—第2部分：应用与可扩展性指南

[4] ISO/IEC 20889, 增强隐私的数据去标识化术语与技术分类

[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—作为个人身份信息处理者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——组织隐私风险管理中ISO 31000:2018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—个人可识别信息保护实践准则

[14] ISO/IEC 29184,信息技术—在线隐私声明与同意

[15] ISO 31000,风险管理 —指南

[16] 《通用数据保护条例》(欧盟)——欧洲议会和理事会第2016/79号条例

ICS 35.030
基于64页的定价

iso.org

International Standard

ISO/IEC 27701

Second edition
2025-10

Information security,cybersecurity and privacy protection—Privacy information management systems —Requirements and guidance

Sécurité de I'information,cybersécurité et protection de la vie privée—Systèmes de management de la protection de la vie privee—Exigences et recommandations

Reference number
ISO/IEC 27701:2025(en)

ISO copyright office
CP 401·Ch.de Blandonnet8
CH-1214 Vernier,Geneva
Phone:+41227490111
Email:copyright@iso.org
Website: www.iso.org
Published in Switzerland

Contents

Page

Foreword

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

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

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a)patent(s).ISO and IEC take no position concerning the evidence,validity or applicability of any claimed patent rights in respect thereof.As of the date of publication of this document,ISO and IEC had not received notice of (a)patent(s)which may be required to implement this document.However,implementers are cautioned that this may not represent the latest information,which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch . ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1,Information technology, *Subcommittee SC 27,Information security,cybersecurity and privacy protection,in collaboration with the* European Committee for Standardization (CEN)Technical Committee CEN/CLC/JTC 13,Cybersecurity and data protection,in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition(ISO/IEC 27701:2019),which has been technically revised.

The main changes are as follows:

—the document has been redrafted as a stand-alone management system standard.

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

Introduction

0.1 General

Almost every organization processes personally identifiable information (PII).Further,the quantity and types of PIIl processed are increasing,as are the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII.Protection of privacy in the context of the processing of PII is a societal need,as well as the topic of dedicated legal requirements worldwide.

This document includes mapping to:

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

— ISO/IEC 27018;

— ISO/IEC 29151;

— the EU General Data Protection Regulation.

NOTE These mappings can be interpreted to take into account locallegal requirements.

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

By complying with the requirements in this document,an organization can generate evidence of how it handles the processing of PII.Such evidence can be used to facilitate agreements with business partners where the processing of PIIis mutually relevant.This can also assist in relationships with other interested parties.The use of this document can provide independent verification of this evidence.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its management system standards.

This document enables an organization to align or integrate its privacy information management system (PIMS)with the requirements of other management system standards,and in particular with thee information security management system specified in ISO/IEC 27001.

Information security,cybersecurity and privacy protection—Privacy information management systems—Requirements and guidance

1 Scope

This document specifies requirements for establishing,implementing,maintaining and continually improving a privacy information management system(PIMS).

Guidance is also provided to assist in the implementation of the requirements in this document.

This document is intended for personally identifiable information (PII)controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations,including public and private companies, government entities and not-for-profit organizations.

2 Normative references

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

ISO/IEC 29100,Information technology—Security techniques—Privacyframework

3 Terms,definitions and abbreviations

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

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

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

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

3.1
organization
person or group of people that has its own functions with responsibilities,authorities and relationships to achieve its objectives(3.6)

Note 1 to entry:The concept of organization includes,but is not limited to,sole-trader,company,corporation,firm, enterprise,authority,partnership,charity or institution,or part or combination thereof,whether incorporated or not, public or private.

Note 2 to entry:If the organization is part of a larger entity,the term“organization”refers only to the part of the larger entity that is within the scope of the privacy informationmanagement system(3.23).

3.2
interested party
person or organization (3.1)that can affect,be affected by,or perceive itself to be affected by a decision or activity

3.3
top management
person or group of people who directs and controls an organization (3.1)at the highest level

Note 1 to entry:Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry:If the scope of the management system (3.4)covers only part of an organization,then top management refers to those who direct and control that part of the organization.

3.4
management system
set of interrelated or interacting elements of an organization (3.1)to establish policies(3.5) and objectives (3.6),as wellas processes (3.8)to achieve those objectives

Note 1 to entry:A management system can address a single discipline or several disciplines.

Note 2 to entry:The management system elements include the organization's structure,roles and responsibilities, planning and operation.

3.5
policy
intentions and direction of an organization (3.1)as formally expressed by its top management(3.3)

3.6
objective
result to be achieved

Note 1 to entry:An objective can be strategic,tactical,or operational.

Note 2 to entry:Objectives can relate to different disciplines (such as finance,health and safety,and environment). They can be,for example,organization-wide or specific to a project,product or process (3.8).

Note 3 to entry:An objective can be expressed in other ways,e.g.as an intended result,as a purpose,as an operational criterion,as a privacy objective or by the use of other words with similar meaning(e.g.aim,goal,or target).

Note 4 to entry:In the context of privacy information management systems(3.23),privacy objectives are set by the organization (3.1),consistent with the privacy policy (3.5),to achieve specific results.

3.7
risk
effect of uncertainty

Note 1 to entry:An effect is a deviation from the expected—positive or negative.

Note 2 to entry:Uncertainty is the state,even partial,of deficiency of information related to,understanding or knowledge of,an event,its consequence,or likelihood.

Note 3 to entry:Riskis often characterized by reference to potential events and consequences,or a combination ofthese.

Note 4 to entry:Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances)and the associated likelihood of occurrence.

3.8
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry:Whether the result of a process is called an output,a product or a service depends on the context of the reference.

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
documented information
information required to be controlled and maintained by an organization (3.1) and the medium on which it is contained

Note 1 to entry:Documented information can be in any format and media and from any source.

Note 2 to entry:Documented information can refer to:

— the management system(3.4),including related processes (3.8);

— information created in order for the organization to operate(documentation);

— evidence of results achieved (records).

3.11
performance
measurable result

Note 1 to entry:Performance can relate either to quantitative or qualitative findings.

Note 2 to entry:Performance can relate to managing activities,processes (3.8),products,services,systems or *organizations (3.1)*.

3.12
continual improvement
recurring activity to enhance performance(3.11)

3.13
effectiveness
extent to which planned activities are realized and planned results are achieved

3.14
requirement
need or expectation that is stated,generally implied or obligatory

Note 1 to entry:“Generally implied”means that it is custom or common practice for the organization (3.1)and interested parties(3.2)that the need or expectation under consideration is implied.

Note 2 to entry:A specified requirement is one that is stated,e.g.in documented information (3.10).

3.15
conformity
fulfilment of a requirement(3.14)

3.16
nonconformity
non-fulfilment of a requirement (3.14)

3.17
corrective action
action to eliminate the cause(s)of a nonconformity(3.16)and to prevent recurrence

3.18
audit
systematic and independent process (3.8)for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry:An audit can be an internal audit (first party)or an external audit(second party or third party),and it can be a combined audit(combining two or more disciplines).

Note 2 to entry:An internal audit is conducted by the organization (3.1) itself,or by an external party on its behalf.

Note 3 to entry:"Audit evidence"and “audit criteria”are defined in ISO 19011.

3.19

measurement
process (3.8)to determine a value

3.20
monitoring
determining the status of a system,a process(3.8)or an activity

Note 1 to entry:To determine the status,there can be a need to check,supervise or critically observe.

3.21
joint PII controller
personally identifiable information (PII)controller that determines the purposes and means of the processing of PII jointly with one or more other PII controllers

3.22
customer
person or organization (3.1)that can or does receive a product or a service that is intended for or required by this person or organization

EXAMPLE Consumer,client,end-user,retailer,receiver of product or service from an internal process (3.8), beneficiary and purchaser.

Note 1 to entry:A customer can be internal or external to the organization.

Note 2 to entry:A customer can be an organization that has a contract with a PI controller,a PII ontroller who has a contract with a PIl processor or a PIl processor that has a contract with a subcontractor for PIIprocessing.

3.23
privacy information management system
PIMS
management system(3.4)which addresses the protection of privacy as potentially affected by the processing of personally identifiable information

3.24
information security programme

set of policies (3.5),objectives (3.6)and processes (3.8) designed to manage risks (3.7)to an organization's (3.1)assets,to ensure confidentiality,integrity and availability of information

Note 1 to entry:An information security programme can be,for example,an information security management system such as one based on ISO/IEC 27001.

3.25
statement of applicability
documentation of all necessary controls and justification for the inclusion or exclusion of such controls

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s)of its privacy information management system.

The organization shall determine whether climate change is a relevant issue.

The organization shall determine if it is acting as a PII controller(including as a joint PII controller)or as a PII processor.

The organization shall determine external and internal issues that are relevant to its context and that affect its ability to achieve the intended outcome(s)ofits PIMS.

NOTE 1 External and internal issues can include but are notlimited to:

— applicable privacy legislation;

— applicable regulations;

— applicable judicial decisions;

— applicable organizational context,governance,policies and procedures;

— applicable administrative decisions;

— applicable contractual requirements.

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

NOTE 2 The role of the organization can be different for each instance of the processing of PII,since it depends on who determines the purposes and means of the processing.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

— the interested parties that are relevant to the privacy information management system;

—the relevant requirements of these interested parties;

— which of these requirements will be addressed through the privacy information management system.

NOTE1 Relevant interested parties can have requirements related to climate change.

The organization shall include among its interested parties those parties having interests or responsibilities associated with the processing of PII,including the PII principals.

NOTE 2 Other interested parties can include customers,supervisory authorities,other PII controllers,PII processors and their subcontractors.

Depending on the role of the organization,"customer"can be understood as either:

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

NOTE 3 This can be the case of an organization which is a joint PII controller.

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

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

NOTE4 An individual person whose PIlis processedin a business association(for example in a consumer,employee, vendor,visitor relationship]is referred to as a“PII principal”in this document.

NOTE 5 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements,by contractual obligations and by self-imposed organizational objectives.The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 6 To demonstrate conformity with the organization's obligations,some interested parties can expect that the organization is in conformity with specific standards,such as the management system specified in this document or any relevant set of specifications.These parties can call for independently audited conformity to these standards.

4.3 Determining the scope of the privacy information management system

The organization shall determine the boundaries and applicability of the privacy information management system to establish its scope.

When determining this scope,the organization shall consider:

—the external and internal issues referred to in 4.1;

—the requirements referred to in 4.2.

The scope shallbe available as documented information.

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

4.4 Privacy information management system

The organization shall establish,implement,maintain and continually improve a privacy information management system,including the processes needed and their interactions,in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the privacy information management system by:

— ensuring that the privacy policy (see 5.2) and privacy objectives (see 6.2) are established and are compatible with the strategic direction of the organization;

— ensuring the integration of the privacy information management system requirements into the organization's business processes;

—ensuring that the resources needed for the privacy information management system are available;

— communicating the importance of effective privacy information management and of conforming to the privacy information management system requirements;

—ensuring that the privacy information management system achieves its intended result(s);

— directing and supporting persons to contribute to the effectiveness of the privacy information management system;

— promoting continual improvement;

— supportingotherrelevantrolesto demonstrate theirleadershipasitappliestotheirareas ofresponsibility.

NOTE Reference to "business"in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Privacy policy

Top management shall establish a privacy policy that:

a) is appropriate to the purpose of the organization;

b)provides a framework for setting privacy objectives;

c) includes a commitment to meet applicable requirements;

d)includes a commitment to continual improvement of the privacy information management system.

The privacy policy shall:

— be available as documented information;

—be communicated within the organization;

—be available to interested parties,as appropriate.

5.3 Roles,responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the privacy information management system conforms to the requirements of this document;

b) reporting on the performance of the privacy information management system to top management.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the privacy information management system,the organization shallconsider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

—give assurance that the privacy information management system can achieve its intended result(s);

—prevent,or reduce,undesired effects;

-achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to

—integrate and implement the actions into its privacy information management system processes;

—evaluate the effectiveness of these actions.

6.1.2 Privacy risk assessment

The organization shall define and apply a privacy risk assessment process that:

a) establishes and maintains privacy risk criteria that include:

1)the risk acceptance criteria;and

2)criteria for performing privacy risk assessments;

b) ensures that repeated privacy risk assessments produce consistent,valid and comparable results;

c) identifies the privacy risks:

1)associated with the protection of privacy and information security risks within the scope of the privacy information management system;and

2)that identify the risk owners;

d)analyses the privacy risks that:

1)assess the potential consequences for both the organization and PII principals that would result if the risks identified in c)1)were to materialize;

2)assess the realistic likelihood of the occurrence of the risks identified in c)1);and

3)determine the levels of risk;

e)evaluates the privacy risks that:

1)compare the results of risk analysis with the risk criteria established in a);and

2)prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the privacy risk assessment process.

NOTE For further information on the privacy risk assessment process,see ISO/IEC 27557.

6.1.3 Privacy risk treatment

The organization shall define and apply a privacy risk treatment process to treat risks related to thee processing of PII,including risks to PII principals,and including the security of PII,by:

a) selecting appropriate privacy risk treatment options, taking account of the risk assessment results;

b) determining all controls that are necessary to implement the privacy risk treatment option(s)chosen;
NOTE1 Organizations can design controls as required or identify them from any source.

c) identifying and documenting the information security programme implemented by the organization, including the appropriate security controls;

The information security programme at a minimum should address the following:

— information security risk management;

— policies for information security;

— organization of information security;

—human resources security;

— asset management;

— access control;

— operations security;

—network security management;

— development security;

— supplier management;

—incident management;

—information security continuity;

—information security reviews;

— cryptography;and

—physical and environmental security.

NOTE 2 ISO/IEC 27002 provides a list of possible information security controls.If the information security programme is based on ISO/IEC 27001,ISO/IEC 27002 can be consulted to ensure that no necessary information security controls are overlooked.

d)comparing the controls determined in b)and c)above with those in Annex A and verifying that no necessary controls have been omitted;

NOTE 3 Annex A contains a list of possible privacy controls. Annex A can be consulted to ensure that no necessary privacy controls are overlooked.

NOTE4 The privacy controls listed in Annex A are not exhaustive and additional privacy controls can be included if needed.

NOTE 5 Organizations can addressinformation security and privacy in an integrated manner when considering the security of PIl processing,combining information security and privacy risk assessments for example,or as separate entities with overlapping areas.

e) producing a statement of applicability that includes:

—the necessary controls (see b),c]and d)];

—justification for their inclusion;

— whether the necessary controls are implemented or not;and

—the justification for excluding any of the controls from **Annex A.**

It is not necessary to include all controls listed in AnnexA. For example,controls can be excluded if they are not deemed necessary by the risk assessment or are not covered by(or are subject to exceptions under)the applicable legal requirements,including those applicable to the PII principal.

f) formulating a privacy risk treatment plan;

g)obtaining the privacy risk owners'approval of the privacy risk treatment plan and acceptance of the residual privacy risks;and

h)considering the guidance in Annex B for the implementation of controls determined in b)and c).

The organization shall retain documented information about the privacy risk treatment process.

6.2 Privacy objectives and planning to achieve them

The organization shall establish privacy objectives at relevant functions and levels.

The privacy objectives shall:

a)be consistent with the privacy policy (see 5.2);

b)be measurable (if practicable);

c) take into account applicable requirements;

d)be monitored;

e) be communicated;

f) be updated as appropriate;

g)be available as documented information.

When planning how to achieve its privacy objectives,the organization shall determine:

—what will be done;

— what resources will be required;

— who will be responsible;

— when it willbe completed;

— how the results will be evaluated.

6.3 Planning of changes

When the organization determines the need for changes to the privacy information management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment,implementation, maintenance and continual improvement of the privacy information management system.

7.2 Competence

The organization shall:

—determine the necessary competence of person(s)doing work under its control that affects its privacy information management performance;

— ensure that these persons are competent on the basis of appropriate education,training,or experience;

— where applicable,take actions to acquire the necessary competence,and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include,for example:the provision of training to,the mentoring of,or the re-assignment of currently employed persons;or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

—the privacy policy (see 5.2);

—their contribution to the effectiveness of the privacy information management system,including the benefits of improved privacy performance;

—the implications of not conforming with the privacy information management system requirements.

7.4 Communication

The organization shall determine the internal and external communications relevant to the privacy information management system including:

—on what it will communicate;

— when to communicate;

— with whom to communicate;

— how to communicate.

7.5 Documented information

7.5.1 General

The organization's privacy information management system shall include:

a) documented information required by this document;

b)documented information determined by the organization as being necessary for the effectiveness of the privacy information management system.

NOTE The extent of documented information for a privacy information management system can differ from one organization to another due to:

— the size of organization and its type of activities,processes,products and services;

— the complexity of processes and their interactions;

— the competence of persons.

7.5.2 Creating and updating documented information

When creating and updating documented information,the organization shall ensure appropriate:

— identification and description (e.g.a title,date,author,or reference number);

—format (e.g.language,software version,graphics)and media(e.g.paper,electronic);
—review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the privacy information management system and by this document shall be controlled to ensure:

a) it is available and suitable for use,where and when it is needed;

b)it is adequately protected (e.g.from loss of confidentiality,improper use,or loss of integrity).

For the control of documented information,the organization shall address the following activities,as applicable:

— distribution,access,retrieval and use;

— storage and preservation,including preservation of legibility;

— control of changes (e.g.version control);
—retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the privacy information management system shall be identified as appropriate,and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only,or the permission and authority to view and change the documented information.

8 Operation

8.1 Operational planning and control

The organization shall plan,implement and control the processes needed to meet requirements,and to implement the actions determined in Clause 6,by:

-establishing criteria for the processes;

—implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes,taking action to mitigate any adverse effects,as necessary.

The organization shall ensure that externally provided processes,products or services that are relevant to the privacy information management system are controlled.

8.2 Privacy risk assessment

The organization shall perform privacy risk assessments at planned intervals or when significant changes are proposed or occur,taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the privacy risk assessments.

8.3 Privacy risk treatment

The organization shall implement the privacy risk treatment plan.

The organization shall retain documented information of the results of the privacy risk treatment.

9 Performance evaluation

9.1 Monitoring,measurement,analysis and evaluation

The organization shall determine:

—what needs to be monitored and measured;

—the methods for monitoring,measurement,analysis and evaluation,as applicable,to ensure valid results;

— when the monitoring and measuring shall be performed;

— when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

The organization shall evaluate the privacy performance and the effectiveness of the privacy information management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the privacy information management system:

a) conforms to:

—the organization's own requirements for its privacy information management system;

—the requirements of this document;

b)is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan,establish,implement and maintain (an)audit programmes),including the frequency,methods,responsibilities,planning requirements and reporting.

When establishing the internal audit programme(s),the organization shallconsider the importance of thee processes concerned and the results of previous audits.

The organization shall:

a) define the audit objectives,criteria and scope for each audit;

b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

c) ensure that the results of audits are reported to relevant managers.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's privacy information management system,at planned intervals,to ensure its continuing suitability,adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include:

a)the status of actions from previous management reviews;

b)changes in external and internalissues that are relevantto the privacy information management system;

c) changes in needs and expectations of interested parties that are relevant to the privacy information management system;

d) information on the privacy information management system performance,including trends in:

—nonconformities and corrective actions;

—monitoring and measurement results;

—audit results;

e) opportunities for continual improvement.

9.3.3 Management review results

The results ofthe management review shallinclude decisions related to continualimprovement opportunities and any need for changes to the privacy information management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability,adequacy and effectiveness of the privacy information management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs,the organization shall:

a) react to the nonconformity,and as applicable:

—take action to control and correct it;

—deal with the consequences;

b)evaluate the need for action to eliminate the cause(s)of the nonconformity,in order that it does not recur or occur elsewhere,by:

—reviewing the nonconformity;

—determining the causes of the nonconformity;

—determining if similar nonconformities exist,or can potentially occur;

c) implement any action needed;

d)review the effectiveness of any corrective action taken;

e) make changes to the privacy information management system,if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

—the nature of the nonconformities and any subsequent actions taken;

—the results of any corrective action.

11 Further information on annexes

Annex C contains a mapping between the provisions of this document and the privacy principles from ISO/IEC 29100.

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

Annex E contains a mapping of the provisions of this document and the provisions from ISO/IEC 27018 and ISO/IEC 29151.

Annex F shows the correspondence between the controls in this edition of ISO/IEC 27701 and the previous edition(ISO/IEC 27701:2019).

Annex A
(normative)

PIMS reference control objectives and controls for PII controllers and PII processors

This annex is intended to be used by organizations acting as PII controllers or PIl processors,or both.

Itis not necessarytoinclude allcontrolobjectives and controls listedinthisannexin the PIMSimplementation. A justification for excluding any control objectives shall be included in the statement of applicability [see 6.1.3 e)].Justification for exclusion can include where the controls are not deemed necessary by the risk assessment,and where they are not required by (or are subject to exceptions under)the applicable legal requirements.

Table A.1 applies to PII controllers, Table A.2 applies to PII processors and Table A.3 relates to information security controls for both PII controllers and PII processors.

NOTE The references under“Control reference”in Tables A.1,A.2 andA.3 refer to the equivalent clause numbers in Annex B(e.g.guidance for control A.1.2.2 can be found in B.1.2.2).

Table A.1—Control objectives and controls for PII controllers

Conditions for collection and processing Objective:To demonstrate that processing is lawful,with legal basis as per applicable jurisdictions,with clearly defined and legitimate purposes.		
Control reference	Control title	Control
A.1.2.2	Identify and document purpose	The organization shall identify and document the specific purposes for which the PII will be processed.
A.1.2.3	Identify lawful basis	The organization shall determine,document and be able to demonstrate compliance with the relevant lawful basis for the processing of PII for the identified purposes.
A.1.2.4	Determine when and how consent is to be obtained	The organization shalldetermine and document a process by which it can demonstrate if,when and how consent for the processing of PII was obtained from PII principals.
A.1.2.5	Obtain and record consent	The organization shall obtain and record consent from PII principals according to the documented processes.
A.1.2.6	Privacy impact assessment	The organization shall assess the need for,and implement where appropriate,a privacy impact assessment whenever new processing of PII or changes to existing processing of PIl is planned.
A.1.2.7	Contracts with PII processors	The organization shall have a written contract with any PIl processor that it uses,and shallensure that their contracts with PII processors address the implementation of the appropriate controls in AnnexA (see Table A.2).
A.1.2.8	Joint PIIcontroller	The organization shall determine respective roles and responsibilities for the processing of PII(including PII protection and security requirements)with any joint PII controller.
A.1.2.9	Records related to processing PII	The organization shall determine and securely maintain the necessary recordsin support of its obligations for the processing of PI.

Table A.1 (continued)

Obligations to PII principals objective:To ensure that PIl principals are provided with appropriate information about the processing of their PII, and to meet any other applicable obligations to PIl principals related to the processing of their PII.		
A.1.3.2	Determining and fulfilling obligations to PII principals	The organization shall determine and document its legal,regulatory and business obligations to PII principals related to the processing of their PIl and provide the means to meet these obligations.
A.1.3.3	Determining information for PII principals	The organization shall determine and document the information to be provided to PIl principals regarding the processing of their PIl and the timing of such a provision.
A.1.3.4	Providing information to PII principals	The organization shallprovide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.
A.1.3.5	Providing mechanism to modify or withdraw consent	The organization shall provide a mechanism for PII principals to modify or withdraw their consent.
A.1.3.6	Providing mechanism to object to PII processing	The organization shall provide a mechanism for PII principals to objectto the processing of their PII.
A.1.3.7	Access,correction or erasure	The organization shall implement policies,procedures or mechanisms to meet its obligations to PII principals to access,correct or erase their PII.
A.1.3.8	PIIcontrollers'obligations to inform third parties	The organization shall inform third parties with whom PIl has been shared of any modification,withdrawal or objections pertaining to the shared PII,and implement appropriate policies,procedures or mechanisms to do so.
A.1.3.9	Providing copy of PIIprocessed	The organization shall be able to provide a copy of the PII that is processed,when requested by the PII principal.
A.1.3.10	Handling requests	The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.
A.1.3.11	Automated decision making	The organization shall identify obligations,including legal obligations,to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII,and be able to demonstrate how it addresses these obligations.
Privacy by design and privacy by default objective:To ensure that processes and systems are designed such that the collection and processing of PII (including use,disclosure,retention,transmission and disposal)are limited to what is necessary for the identified purpose.		
A.1.4.2	Limit collection	The organization shall limit the collection of PIIto the minimum that is relevant,proportional and necessary for the identified purposes.
A.1.4.3	Limit processing	The organization shall limit the processing of PIl to that which is adequate,relevant and necessary for the identified purposes.
A.1.4.4	Accuracy and quality	The organization shall ensure and document that PII is as accurate, complete and up to date as necessary for the purposes for which it is processed,throughout the life cycle of the PII.
A.1.4.5	PII minimization objectives	The organization shall define and document data minimization objectives and what mechanisms(such as de-identification)are used to meet those objectives.
A.1.4.6	PII de-identification and deletion at the end of processing	The organization shall either delete PII or render it in a form which does not permit identification or re-identification of PIlprincipals, as soon as the original PII is no longer necessary for the identified purposes).
A.1.4.7	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PIl are disposed of (e.g.erased or destroyed) following documented procedures within a specified,documented period.

Table A.1 (continued)

A.1.4.8	Retention	The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed.
A.1.4.9	Disposal	The organization shall have documented policies, procedures or mechanisms for the disposal of PII.
A.1.4.10	PII transmission controls	The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
PII sharing, transfer and disclosure objective: To determine whether, and document when, PII is shared, transferred to other jurisdictions or third parties or disclosed in accordance with applicable obligations.		
A.1.5.2	Identify basis for PII transfer between jurisdictions	The organization shallidentify and document the relevant basis for transfers of PII between jurisdictions.
A.1.5.3	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.
A.1.5.4	Records of transfer of PII	The organization shall record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.
A.1.5.5	Records of PII disclosures to third parties	The organization shall record disclosures of PII to third parties, including which PII has been disclosed, to whom and at what time.

Table A.2—Control objectives and controls for PII processors

Conditions for collection and processing objective: To demonstrate that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.		
Control reference	Control title	Control
A.2.2.2	Customer agreement	The organization shallensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization).
A.2.2.3	Organization's purposes	The organization shallensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
A.2.2.4	Marketing and advertising use	The organization shall not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.
A.2.2.5	Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legal requirements.
A.2.2.6	Customer obligations	The organization shallprovide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.
A.2.2.7	Records related to processing PII	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.
Obligations to PII principals objective: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.		
A.2.3.2	Comply with obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations related to PII principals.

Table A.2(continued)

Privacy by design and privacy by default objective:To ensure that processes and systems are designed such that the collection and processing of PII(including use, disclosure, retention, transmission and disposal)are limited to what is necessary for the identified purpose.		
A.2.4.2	Temporary files	The organization shallensure that temporary files created as a result of the processing of PIIare disposed of (e.g.erased or destroyed)following documented procedures within a specified, documented period.
A.2.4.3	Return, transfer or disposal of PII	The organization shall be able to return, transfer or dispose of PII in a secure manner.It shall also make its policy available to the customer.
A.2.4.4	PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls, which are designed to ensure that the data reaches its intended destination.
PII sharing, transfer and disclosure objective:To determine whether, and document when, PIIis shared, transferred to other jurisdictions or third parties, or disclosed according to applicable obligations.		
A.2.5.2	Basis for PII transfer between jurisdictions	The organization shall inform the customer in atimely manner of the basis for PIl transfers between jurisdictions and of any intended changes in this regard, so that the customer can object to such changes or terminate the contract.
A.2.5.3	Countries and international organizations to which PIl can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.
A.2.5.4	Records of PII disclosures to third parties	The organization shall record disclosures of PII to third parties, including which PII has been disclosed, to whom and when.
A.2.5.5	Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.
A.2.5.6	Legally binding PIIdisclosures	The organization shall reject any requests for PIIdisclosures that are notlegally binding, consult the corresponding customer before making any PII disclosures and accept any contractually agreed requests for PIIdisclosures that are authorized by the corresponding customer.
A.2.5.7	Disclosure of subcontractors used to process PII	Before use, the organization shall disclose whether any subcontractors are used to process PII to the customer.
A.2.5.8	Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.
A.2.5.9	Change of subcontractor to process PII	The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to objectto such changes.

Table A.3—Control objectives and controls for PII controllers and PII processors

Security considerations for PII controllers and processors Objective:To ensure the security of PIl processing.		
Control reference	Control title	Control
A.3.3	Policies for information security	Information security policies related to Pl processing shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
A.3.4	Information security roles and responsibilities	Information security roles and responsibilities related to PII processing shall be defined and allocated according to the organizational needs.

Table A.3(continued)

A.3.5	Classification of information	Information shall be classified according to the information security needs of the organization, taking into consideration PII, based on confidentiality, integrity, availability and relevant interested party requirements.
A.3.6	Labelling of information	An appropriate set of procedures for information labelling that considers PII shallbe developed and implemented in accordance with the information classification scheme adopted by the organization.
A.3.7	Information transfer	Information transfer rules, procedures, or agreements related to processing PII shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
A.3.8	Identity management	The full life cycle of identities related to PIl processing shall be managed.
A.3.9	Access rights	Access rights to PIl and other associated assets related to PII processing shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.
A.3.10	Addressing information security within supplier agreements	Relevant information security requirements related to PII processing shall be established and agreed with each supplier based on the type of supplier relationship.
A.3.11	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents related to PIl processing by defining, establishing and communicating incident management processes, roles and responsibilities.
A.3.12	Response to information security incidents	Responses to information security incidents related to PII processing shall be according to the documented procedures.
A.3.13	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security related to PIl processing and the organization's approach to meet these requirements shall be documented and this documentation kept up to date.
A.3.14	Protection of records	Records related to PII processing shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
A.3.15	Independent review of information security	The organization's approach to managing information security related to PIl processing and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.
A.3.16	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards related to PIlprocessing shall be regularly reviewed.
A.3.17	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness education and training, and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function, as they relate to PII processing.
A.3.18	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of PII shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
A.3.19	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
A.3.20	Storage media	Storage media with PII shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Table A.3(continued)

A.3.21	Secure disposal or re-use of equipment	Items of equipment containing storage media with PII shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.3.22	User endpoint devices	PII stored on, processed by or accessible via user endpoint devices shall be protected.
A.3.23	Secure authentication	Secure authentication technologies and procedures related to PII processing shallbe implemented based on information access restrictions.
A.3.24	Information backup	Backup copies of PII, and software and systems related to PIl processing shall be maintained and regularly tested.
A.3.25	Logging	Logs that record activities, exceptions, faults and other relevant events related to PII processing shall be produced, stored, protected and analysed.
A.3.26	Use of cryptography	Rules for the effective use of cryptography related to PII processing, including cryptographic key management, shall be defined and implemented.
A.3.27	Secure development life cycle	Rules for the secure development of software and systems related to PIl processing shall be established and applied.
A.3.28	Application security requirements	Information security requirements related to PII processing shall be identified, specified and approved when developing or acquiring applications.
A.3.29	Secure system architecture and engineering principles	Principles for engineering secure systems related to processing PII shall be established, documented, maintained and applied to any information system development activities.
A.3.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced PIl processing system development.
A.3.31	Test information	Test information related to PIl processing shall be appropriately selected, protected and managed.

Annex B
(normative)

Implementation guidance for PII controllers and PII processors

B.1 Implementation guidance for PII controllers

B.1.1 General

This clause provides PIMS guidance for PII controllers,which relates to the controls listed in Table A.1.

B.1.2 Conditions for collection and processing

B.1.2.1 Objective

To demonstrate that processing is lawful,with legal basis as per applicable jurisdictions,and with clearly defined and legitimate purposes.

B.1.2.2 Identify and document purpose

Control

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

Implementation guidance

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

Documentation of the purpose(s)for processing PII should be sufficiently clear and detailed so that it can be used as part of the information to be provided to PII principals (see B.1.3.3).This documentation should include information necessary to obtain consent(see B.1.2.4),as well as documented information of policies and procedures (see B.1.2.9).

Other information

In the deployment of cloud computing services,the taxonomy and definitions in ISO/IEC 19944-1 can be helpful in providing terms for describing the purpose of the processing of PII.

B.1.2.3 Identify lawful basis

Control

The organization should determine,document and be able to demonstrate compliance with the relevant lawful basis for the processing of PII for the identified purposes.

Implementation guidance

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

The legal basis for the processing of PII can include:

— consent from PII principals;

—performance of a contract;

—compliance with a legal obligation;

—protection of the vital interests of PII principals;

—performance of a task carried out in the public interest;

—legitimate interests of the PII controller.

The organization should document this basis for each PII processing activity (see B.1.2.9).

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

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

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

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

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

B.1.2.4 Determine when and how consent is to be obtained

Control

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

Implementation guidance

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

NOTE Legal requirements can apply.

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

B.1.2.5 Obtain and record consent

Control

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

Implementation guidance

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

The information delivered to the PII principal before the consent process should follow the guidance in B.1.3.4.

The consent should be:

—freely given;

— specific regarding the purpose for processing;and

— unambiguous and explicit.

B.1.2.6 Privacy impact assessment

Control

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

Implementation guidance

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

The organization should determine the elements that are necessary for the completion of a privacy impact assessment.These can include a list of the types of PIlprocessed,where the PII is stored and where it can be transferred.Data flow diagrams and data maps can also be helpful in this context.

NOTE See B.1.2.9 for details of documented information of the processing of PII that can inform a privacy impact or other risk assessment.

Other information

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

B.1.2.7 Contracts with PII processors

Control

The organization should have a written contract with any PIl processor that it uses and should ensure that its contracts with PII processors address the implementation of the appropriate controls in Table A.2.

Implementation guidance

The contract between the organization and any PIl processor processing PIl on its behalf should require the PII processor to implement the appropriate controls specified in Table A.2,taking account of the information security risk assessment process (see 6.1.2) and the scope of the processing of PII performed by the PII processor.By default,all controls specified in Table A.2 should be assumed as relevant.If the organization decides that the PII processor is not required to implement a control from Table A.2, it should justify its exclusion (see 6.1.3).

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

B.1.2.8 Joint PII controller

Control

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

Implementation guidance

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

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

A joint PII controller agreement can include:

—the purpose of PII sharing/joint PII controller relationship;

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

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

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

—a description of the respective roles and responsibilities;

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

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

—terms of retention or disposal of PII;

—liabilities for failure to comply with the agreement;

—how obligations to PII principals are met;

—how to provide PIIprincipals with information covering the essence of the arrangement between thee joint PII controllers;

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

— a contact point for PII principals.

B.1.2.9 Records related to processing PII

Control

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

Implementation guidance

Documented information of the processing of PII can be maintained through an inventory or list of the PII processing activities that the organization performs.Such an inventory can include:

—the type of processing;

—the purposes for the processing;

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

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

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

— a privacy impact assessment report.

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

B.1.3 Obligations to PII principals

B.1.3.1 Objective

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

B.1.3.2 Determining and fulfilling obligations to PII principals

Control

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

Implementation guidance

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

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

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

B.1.3.3 Determining information for PII principals

Control

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

Implementation guidance

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

Depending on the requirements,this information can take the form of a notice.Examples of types of information that can be provided to PII principals are:

—information about the purpose of the processing (see B.1.2.2);

—contact details for the PII controller or its representative;

—information about the lawful basis for the processing (see B.1.2.3);

—information on where the PII was obtained,if not obtained directly from the PII principal;

—information about whether the provision of PII is a statutory or contractual requirement,and where appropriate,the possible consequences of failure to provide PII;

—information on obligations to PII principals,as determined in B.1.3.2, and how PII principals can benefit from them,especially regarding accessing,amending,correcting,requesting erasure,receiving a copy of their PII and objecting to the processing;

—information on how the PIl principal can withdraw consent (see B.1.3.5);

— information about transfers of PII;

—information about recipients or categories of recipients of PII;

—information about the period for which the PII will be retained;

—information about the use of automated decision making based on the automated processing of PII;

—information about the right to lodge a complaint and how to lodge such a complaint;

—information regarding the frequency with which information is provided(e.g."just in time"notification, organization defined frequency).

The organization should provide updated information if the purposes for the processing of PII are changed or extended.

B.1.3.4 Providing information to PII principals

Control

The organization should provide PIl principals with clear and easily accessible information identifying thee PII controller and describing the processing of their PII.

Implementation guidance

The organization should provide the information detailed in B.1.3.3 to PII principals in a timely,concise, complete,transparent,intelligible and easily accessible form,using clear and plain language,as appropriate to the target audience.

Where appropriate,the information should be given at the time of PII collection.It should also be permanently accessible.

NOTE Icons and images can be helpful to the PIl principal by giving a visual overview of the intended processing.

B.1.3.5 Providing mechanism to modify or withdraw consent

Control

The organization should provide a mechanism for PII principals to modify or withdraw their consent.

Implementation guidance

The organization should inform PIl principals of their rights related to withdrawing consent (which can vary by jurisdiction)at any time and provide the mechanism to do so.The mechanism used for withdrawal depends on the system;it should be consistent with the mechanisms used for obtaining consent when possible.For example,if the consent is collected by email or a website,the mechanism for withdrawing it should be the same,not an alternative solution such as phone or fax.

Modifying consent can include placing restrictions on the processing of PII,which can include restricting the PII controller from deleting the PIl in some cases.

Some jurisdictions impose restrictions on when and how a PII principal can modify or withdraw their consent.

The organization should record any requestto withdraw or change consent in a similar way to the recording of the consent itself

Any change of consent should be disseminated,through appropriate systems,to authorized users and to relevant third parties.

The organization should define a response time and requests should be handled according to it.

Additional information

When consent for processing of specific PII is withdrawn,all the processing of PII performed before withdrawal should normally be considered as appropriate,but the results of such processing should not be

used for new processing.For example,if a PIl principal withdraws their consent for profiling,their profile should not be further used or consulted.

B.1.3.6 Providing mechanism to object to PII processing

Control

The organization should provide a mechanism for PII principals to object to the processing of their PII

Implementation guidance

Some jurisdictions provide PII principals with a right to object to the processing of their PII.Organizations subject to the legal requirements of such jurisdictions should be able to demonstrate how they ensure that they retain records of PII principals exercising this right.

The organization should document the legal and regulatory requirements related to objections by the PII principals to processing(e.g.objection relating to the processing of PII for direct marketing purposes).Thee organization should provide information to principals regarding the ability to object in these situations. Mechanisms to object can vary but should be consistent with the type of service provided (e.g.online services should provide this capability online).

B.1.3.7 Access,correction or erasure

Control

The organization should implement policies,procedures or mechanisms to meet its obligations to PII principals to access,correct or erase their PII.

Implementation guidance

The organization should implement policies,procedures or mechanisms for enabling PII principals to obtain access to,correct and erase their PII,if requested and without undue delay.

The organization should define a response time and requests should be handled according to it.

Any corrections or erasures should be disseminated through the system or to authorized users,and should be passed to third parties (see B.1.3.8)to whom the PIl has been transferred.

NOTE Documented information generated by the control specified in B.1.5.4 can help in this regard.

The organization should implement policies,procedures or mechanisms for use when there can be a dispute about the accuracy or correction of the data by the PIl principal.These policies,procedures or mechanisms should include informing the PIl principal of what changes were made,and of reasons why corrections cannot be made (where this is the case).

Some jurisdictions impose restrictions on when and how a PII principal can request correction or erasure of their PII.The organization should keep abreast of such restrictions.

B.1.3.8 PII controllers'obligations to inform third parties

Control

The organization should inform third parties with whom PIIhas been shared of any modification,withdrawal or objections pertaining to the shared PII,and implement appropriate policies,procedures or mechanisms to do so.

Implementation guidance

The organization should take appropriate steps,bearing in mind the available technology,to inform third parties of any modification or withdrawal of consent,or objections pertaining to the shared PII.

The organization should determine and maintain active communication channels with third parties. Related responsibilities can be assigned to individuals in charge of their operations and maintenance.When informing third parties,the organization should monitor its acknowledgement of receipt of the information.

NOTE Changes resulting from the obligations to PIl principals can include modification or withdrawal of consent, requests for correction,erasure,or restrictions on processing,or objections to the processing of PIl as requested by the PII principal.

B.1.3.9 Providing copy of PII processed

Control

The organization should be able to provide a copy of the PII that is processed when requested by the PII principal.

Implementation guidance

The organization should provide a copy of the PII that is processed in a structured,commonly used,format accessible by the PII principal.

Some jurisdictions define cases where the organization should provide a copy of the PII processedin a format allowing portability to the PII principals or to recipient PII controllers (typically structured,commonly used and machine readable).

The organization should ensure that any copies of PII provided to a PIl principal relate specifically to that PII principal.

Where the requested PIlhas already been deleted subject to the retention and disposal policy(as described in **B.1.4.8**),the PII controller should inform the PII principal that the requested PII has been deleted.

In cases where the organization is no longer able to identify the PII principal (e.g.as a result of a de-identification process),the organization should not seek to (re-)identify the PIl principals for the sole reason of implementing this control.However,in some jurisdictions,legitimate requests can require that additional information is requested from the PII principal to enable re-identification and subsequent disclosure.

Where technically feasible,it should be possible to transfer a copy of the PII from one organization directly to another organization,at the request of the PII principal.

B.1.3.10 Handling requests

Control

The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals.

Implementation guidance

Legitimate requests can include requests for a copy of PII processed,or requests to lodge a complaint.

Some jurisdictions allow the organization to charge a fee in certain cases (e.g.excessive or repetitive requests).

Requests should be handled within the appropriate defined response times.

Some jurisdictions define response times,depending on the complexity and number of the requests,as well as requirements to inform PIl principals of any delay.The appropriate response times should be defined in the privacy policy.

B.1.3.11 Automated decision making

Control

The organization should identify obligations,including legal obligations,to the PIl principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII,and be able to demonstrate how it addresses these obligations.

Implementation guidance

Some jurisdictions define specific obligations to PII principals when a decision based solely on automated processing of PIIsignificantly affects them,such as notifying the existence of automated decision making, allowing for the PII principals to object to such decision making,or obtaining human intervention.

NOTE In some jurisdictions,some processing of PIIcannot be fully automated.

Organizations operating in these jurisdictions should be able to demonstrate how they take compliance with these obligations into account.

B.1.4 Privacy by design and privacy by default

B.1.4.1 Objective

To ensure that processes and systems are designed such that the collection and processing of PII (including use,disclosure,retention,transmission and disposal)are limited to what is necessary for the identified purpose.

B.1.4.2 Limit collection

Control

The organization should limit the collection of PII to the minimum that is relevant,proportional and necessary for the identified purposes.

Implementation guidance

The organization should limit the collection of PII to what is adequate,relevant and necessary in relation to the identified purposes.This includes limiting the amount of PII that the organization collects indirectly (e.g. through web logs,system logs).

Privacy by default implies that,where any optionality in the collection and processing of PII exists,each option should be disabled by default and only enabled by explicit choice of the PII principal.

B.1.4.3 Limit processing

Control

The organization should limit the processing of PII to that which is adequate,relevant and necessary for the identified purposes.

Implementation guidance

Limiting the processing of PII should be managed through information security and privacy policies (see 5.2) along with documented procedures for their adoption and compliance.

Processing of PII should be limited by default to the minimum necessary,relative to the identified purposes. This processing includes:

— the disclosure;

—the period of PII storage;and

— who can access their PII.

B.1.4.4 Accuracy and quality

Control

The organization should ensure and document that PIl is as accurate,complete and up to date as necessary for the purposes for which it is processed,throughout the life cycle of the PII.

Implementation guidance

The organization should implement policies,procedures or mechanisms to minimize inaccuracies in the PII it processes.There should also be policies,procedures or mechanisms to respond to instances of inaccurate PII.These policies,procedures or mechanisms should be included in the documented information (e.g. through technical system configurations)and should apply throughout the PII life cycle.

Additional information

For further information on the PII processing life cycle,see ISO/IEC 29101:2018,6.2.

B.1.4.5 PII minimization objectives

Control

The organization should define and document data minimization objectives and what mechanisms (such as de-identification)are used to meet those objectives.

Implementation guidance

Organizations should identify how the specific PII and amount of PII collected and processed is limited relative to the identified purposes.This can include the use of de-identification or other data minimization techniques.

The identified purpose (see B.1.2.2)can require the processing of PII that has not been de-identified,in which case the organization should be able to describe such processing.

In other cases,the identified purpose does not require the processing of the original PII,and the processing of PII which has been de-identified can suffice to achieve the identified purpose.In these cases,the organization should define and document the extent to which the PII should be associated with the PII principal,as well as the mechanisms and techniques designed to process PIl,such that the de-identification and PII minimization objectives are achieved.

Mechanisms used to minimize PIl vary depending on the type of processing and the systems used for the processing.The organization should document any mechanisms (e.g.technical system configurations)used to implement data minimization.

In cases where processing of de-identified data is sufficient for the purposes,the organization should document any mechanisms (e.g.technical system configurations)designed to implement de-identification objectives set by the organization in atimely manner.For instance,the removal of attributes associated with PII principals can be sufficient to allow the organization to achieve its identified purpose.In other cases, other de-identification techniques,such as generalization (e.g.rounding)or randomization techniques (e.g. noise addition)can be used to achieve an adequate level of de-identification.

NOTE1 For further information on de-identification techniques,refer to ISO/IEC 20889.

NOTE 2 For cloud computing,ISO/IEC 19944-1 provides a definition of data identification qualifiers that can be used to classify the degree to which the data can identify a PII principal or associate a PIl principal with a set of characteristics in the PII.

B.1.4.6 PII de-identification and deletion at the end of processing

Control

The organization should either delete PII or render it in a form which does not permit identification or re-identification of PII principals,as soon as the original PII is no longer necessary for the identified purpose(s).

Implementation guidance

The organization should have mechanisms to erase the PII when no further processing is anticipated. Alternatively,some de-identification techniques can be used,as long as the resulting de-identified data cannot reasonably permit re-identification of PII principals.

B.1.4.7 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PIl are disposed of (e.g.erased or destroyed)following documented procedures within a specified,documented period.

Implementation guidance

The organization should perform periodic checks that unused temporary files are deleted within thee identified time period.

Other information

Information systems can create temporary files in the normal course of their operation.Such files are specific to the system orapplication but can include file system roll-backjournals and temporary files associated with the updating of databases and the operation of other application software.Temporary files are not needed after the related information processing task has been completed but there are circumstances in which they cannot be deleted.The length of time for which these files remain in use is not always deterministic but a “garbage collection”procedure should identify the relevant files and determine how long it has been since they were last used.

B.1.4.8 Retention

Control

The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed.

Implementation guidance

The organization should develop and maintain retention schedules for information it retains,taking into account the requirement to retain PII for no longer than is necessary.Such schedules should take into account legal,regulatory and business requirements.Where such requirements conflict,a business decision should be taken(based on a risk assessment)and documented in the appropriate schedule.

B.1.4.9 Disposal

Control

The organization should have documented policies,procedures or mechanisms for the disposal of PII.

Implementation guidance

The choice of PII disposal techniques depends on a number of factors,as disposal techniques differ in their properties and outcomes (e.g.in the granularity of the resultant physical media,or the ability to recover deleted information on electronic media).Factors to consider when choosing an appropriate disposal technique include,but are not limited to,the nature and extent of the PIIto be disposed of,whether or not there is metadata associated with the PIl,and the physical characteristics of the media on which the PIl is stored.

B.1.4.10 PII transmission controls

Control

The organization should subject PII that has been transmitted(e.g.sent to another organization)over a data-transmission network to the appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII should be controlled,typically by ensuring that only authorized individuals have access to transmission systems,and by following the appropriate processes (including the retention of audit logs) to ensure that PII is transmitted without compromise to the correct recipients.

B.1.5 PII sharing,transfer and disclosure

B.1.5.1 Objective

To determine whether,and document when,PIl is shared,transferred to other jurisdictions or third parties, or disclosed according to applicable obligations.

B.1.5.2 Identify basis for PII transfer between jurisdictions

Control

The organization should identify and document the relevant basis for transfers of PII between jurisdictions.

Implementation guidance

PII transfer can be subject to legal requirements,depending on the jurisdiction or international organization to which data are to be transferred (and from where the data originate).The organization should document compliance to such requirements as the basis for transfer.

Some jurisdictions can require that information transfer agreements be reviewed by a designated supervisory authority.Organizations operating in such jurisdictions should be aware of any such requirements.

NOTE Where transfers take place within a specific jurisdiction,the applicable legal requirements are the same for the sender and recipient.

B.1.5.3 Countries and international organizations to which PII can be transferred

Control

The organization should specify and document the countries and international organizations to which PII can possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers.The identities of the countries arising from thee

use of subcontracted PII processing should be included.The countries included should be considered in relation to **B.1.5.2**.

Outside of normal operations,there can be cases of transfer made at the request of a legal authority,forr which the identity of the countries cannot be specified in advance,or such transfer can be prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see B.1.5.2, B.2.5.5 and B.2.5.6).

B.1.5.4 Records of transfer of PII

Control

The organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.

Implementation guidance

Recording can include transfers from third parties of PII which has been modified as a result of PII controllers'managing its obligations,or transfers to third parties to implementlegitimate requests from PII principals,including requests to erase PII (e.g.after consent withdrawal).

The organization should have a policy defining the retention period of these records.

The organization should apply the data minimization principle to the records of transfers by retaining only the strictly needed information.

B.1.5.5 Records of PII disclosure to third parties

Control

The organization should record disclosures of PII to third parties,including which PII has been disclosed,to whom and at what time.

Implementation guidance

PII can be disclosed during normal operations.These disclosures should be recorded.Any additional disclosures to third parties,such as those arising from legal investigations or external audits,should also be recorded.The records should include the source of the disclosure and the source of the authority to make the disclosure.

B.2 Implementation guidance for PII processors

B.2.1 General

This clause provides PIMS guidance for PII processors,which relates to the controls listed in Table A.2.

B.2.2 Conditions for collection and processing

B.2.2.1 Objective

To demonstrate that processing is lawful,with legal basis as per applicable jurisdictions,and with clearly defined and legitimate purposes.

B.2.2.2 Customer agreement

Control

The organization should ensure,where relevant,that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization).

Implementation guidance

The contract between the organization and the customer should include the following aspects,where relevant and depending on the customer's role (i.e.PII controller or PII processor):

— privacy by design and privacy by default (see B.1.4 and B.2.4);

—achieving security of processing;

— notification of breaches involving PII to a supervisory authority;

—notification of breaches involving PII to customers and PII principals;

—conducting privacy impact assessments;and

—the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed.

Some jurisdictions require that the contract includes the subject matter and duration of the processing,thee nature and purpose of the processing,the type of PII and categories of PII principals.

B.2.2.3 Organization's purposes

Control

The organization should ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.

Implementation guidance

The contract between the organization and the customer should include,but not be limited to,the objective and time frame to be achieved by the service.

In order to achieve the customer's purpose,there can be technical reasons why it is appropriate for the organization to determine the method for processing PII,consistent with the general instructions of the customer but without the customer's express instruction.For example,in order to efficiently utilize network or processing capacity,it can be necessary to allocate specific processing resources depending on certain characteristics of the PII principal.

The organization should allow the customer to verify its compliance with the purpose specification and limitation principles.This also ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the documented instructions of the customer.

B.2.2.4 Marketing and advertising use

Control

The organization should notuse PIl processed undera contractfor the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal.The organization should not make providing such consent a condition for receiving the service.

Implementation guidance

Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing or advertising is planned.

Organizations should not insist on the inclusion of marketing or advertising uses where express consent has not been fairly obtained from PII principals.

NOTE This control complements the more general controlin B.2.2.3 and does not replace or otherwise supersede it.

B.2.2.5 Infringing instruction

Control

The organization should inform the customer if,in its opinion,a processing instruction infringes applicable legal requirements.

Implementation guidance

The organization's ability to verify if the instruction infringes legal requirements can depend on thee technological context,on the instruction itself,and on the contract between the organization and thee customer.

B.2.2.6 Customer obligations

Control

The organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.

Implementation guidance

The information needed by the customer can include whether the organization allows for and contributes to audits conducted by the customer or another auditor mandated or otherwise agreed by the customer.

B.2.2.7 Records related to processing PII

Control

The organization should determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract)for the processing of PII carried out on behalf of a customer.

Implementation guidance

Some jurisdictions can require the organization to record information such as:

— categories of processing carried out on behalf of each customer;

—transfers to third countries or international organizations;and

— a general description of the technical and organizational security measures.

B.2.3 Obligations to PII principals

B.2.3.1 Objective

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

B.2.3.2 Comply with obligations to PII principals

Control

The organization should provide the customer with the means to comply with its obligations related to PII principals.

Implementation guidance

A PII controller's obligations can be defined by legal requirements or by contract.These obligations can include matters where the customer uses the services of the organization for implementation of these obligations.For example,this can include the correction or deletion of PII in atimely fashion.

Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals,the relevant information or technical measures should be specified in a contract.

B.2.4 Privacy by design and privacy by default

B.2.4.1 Objective

To ensure that processes and systems are designed such that the collection and processing of PII (including use,disclosure,retention,transmission and disposal)are limited to what is necessary for the identified purpose.

B.2.4.2 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g.erased or destroyed)following documented procedures within a specified,documented period.

Implementation guidance

The organization should conduct periodic verification that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation.Such files are specific to the system or application but can include file system roll-backjournals and temporary files associated with the updating of databases and the operation of other application software.Temporary files are not needed after the related information processing task has been completed but there are circumstances in which they cannot be deleted.The length of time for which these files remain in use is not always deterministic but a “garbage collection”procedure should identify the relevant files and determine how long it has been since they were last used.

B.2.4.3 Return,transfer or disposal of PII

Control

The organization should be able to return,transfer or dispose of PII in a secure manner.It should also make its policy available to the customer.

Implementation guidance

At some point in time,it can be necessary to dispose of PII in some manner.This can involve returning the PII to the customer,transferring it to another organization or to a PII controller(e.g.as a result of a merger), deleting or otherwise destroying it,de-identifying it or archiving it.The capability for the return,transfer or disposal of PII should be managed in a secure manner.

The organization should provide the assurance necessary to allow the customer to ensure that PIl processed under a contract is erased(by the organization and any of its subcontractors)from wherever they are stored, including for the purposes of backup and business continuity,as soon as they are no longer necessary for the purposes identified by the customer.

The organization should develop and implement a policy in respect to the disposal of PII and should make this policy available to customers when requested.

The policy should cover the retention period for PII before its disposal after termination of a contract,to protect the customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention principle (see B.1.4.8).

B.2.4.4 PII transmission controls

Control

The organization should subject PII transmitted over a data-transmission network to appropriate controls, which are designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII should be controlled,typically by ensuring that only authorized individuals have access to transmission systems,and by following the appropriate processes (including the retention of audit data)to ensure that PII is transmitted without compromise to the correct recipients.Requirements for transmission controls can be included in the contract between the PII processor and the customer.

Where no contractual requirements related to transmission are in place,it can be appropriate to take advice from the customer prior to transmission.

B.2.5 PII sharing,transfer and disclosure

B.2.5.1 Objective

To determine whether,and document when,PIl is shared,transferred to other jurisdictions or third parties, or disclosed according to applicable obligations.

B.2.5.2 Basis for PII transfer between jurisdictions

Control

The organization should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard,so that the customer can object to such changes or terminate the contract.

Implementation guidance

PII transfer between jurisdictions can be subject to legal requirements depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates).The organization should document compliance with such requirements as the basis for transfer.

The organization should inform the customer of any transfer of PII,including transfers to:

—suppliers;

—other parties;

—other countries or international organizations.

In case of changes,the organization should inform the customer in advance,according to an agreed time frame,so that the customer has the ability to object to such changes or to terminate the contract.

The agreement between the organization and the customer can include clauses where the organization can implement changes without informing the customer.In these cases,the limits of this allowance should be set (e.g.the organization can change suppliers without informing the customer but cannot transfer PII to other countries).

In case of international transfer of PII,agreements such as model contract clauses,binding corporate rules or cross border privacy rules,the countries involved and the circumstances in which such agreements apply, should be identified.

B.2.5.3 Countries and international organizations to which PII can be transferred

Control

The organization should specify and document the countries and international organizations to which PII can possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers.The identities of the countries arising from the use of subcontracted PII processing should be included.The countries included should be considered in relation to B.2.5.2.

Outside of normal operations,there can be cases of transfer made at the request of a legal authority,for which the identity of the countries cannot be specified in advance,or such transfer can be prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see B.1.5.2, B.2.5.5 an d B.2.5.6).

B.2.5.4 Records of PII disclosures to third parties

Control

The organization should record disclosures of PII to third parties,including which PII has been disclosed,to whom and when.

Implementation guidance

PII can be disclosed during normal operations.These disclosures should be recorded.Any additional disclosures to third parties,such as those arising from legal investigations or external audits,should also be recorded.The records should include the source of the disclosure and the source of the authority to make the disclosure.

B.2.5.5 Notification of PII disclosure requests

Control

The organization should notify the customer of any legally binding requests for the disclosure of PII.

Implementation guidance

The organization can receive legally binding requests for the disclosure of PII (e.g.from legal authorities).In these cases,the organization should notify the customer of any such request within agreed time frames and according to an agreed procedure which can be included in the customer contract.

In some cases,the legally binding requests include the requirement for the organization not to notify anyone about the event.An example of a possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a legal investigation.

B.2.5.6 Legally binding PII disclosures

Control

The organization should reject any requests for PII disclosures that are not legally binding,consult thee corresponding customer before making any PII disclosures and accept any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.

Implementation guidance

Details relevant to the implementation of the control can be included in the customer contract.

Such requests can originate from several sources,including courts,tribunals and administrative authorities. They can arise from any jurisdiction.

B.2.5.7 Disclosure of subcontractors used to process PII

Control

Before use,the organization should disclose whether any subcontractors are used to process PII to the customer.

Implementation guidance

Provisions for the use of subcontractors to process PII should be included in the customer contract.

Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors.The information disclosed should also include the countries and international organizations to which subcontractors can transfer data (see B.2.5.3)and the means by which subcontractors are obliged to meet or exceed the obligations of the organization (see B.2.5.8).

Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits,disclosure should be made under a non-disclosure agreement or on the request of the customer.Thee customer should be made aware that the information is available.

This does not concern the list of countries where the PII can be transferred.This list should be disclosed to the customer in allcases in a way that allows them to inform the appropriate PII principals.

B.2.5.8 Engagement of a subcontractor to process PII

Control

The organization should only engage a subcontractor to process PIlaccording to the customer contract.

Implementation guidance

Where the organization subcontracts some or all of the processing of that PII to another organization,a written authorization from the customer is required prior to the PIl processed by the subcontractor.This can be in the form of appropriate clauses in the customer contract or can be a specific"one-off"agreement.

The organization should have a written contract with any subcontractors that it uses for PII processing on its behalf.The organization should ensure that its contracts with subcontractors address the implementation of the appropriate controls in Table A.2.

The contract between the organization and any subcontractor processing PII on its behalf should require the subcontractor to implement the appropriate controls specified in Table A.2, taking account of the information security risk assessment process (see 6.1.2) and the scope of the processing of PII performed by the PII processor.By default,all controls specified in Table A.2 should be assumed as relevant.If the organization decides to not require the subcontractor to implement a controlfrom Table A.2,it should justify its exclusion.

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

B.2.5.9 Change of subcontractor to process PII

Control

The organization should,in the case of having general written authorization,inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PIl,thereby giving the customer the opportunity to object to such changes.

Implementation guidance

Where the organization changes the organization with which it subcontracts some or all of the processing of PII,then written authorization from the customer is required for the change,prior to the PII processed by the new subcontractor.This can be in the form of appropriate clauses in the customer contract or a specific "one-off"agreement.

B.3 Implementation guidance for PII controllers and PII processors

B.3.1 Objective

To ensure the security of PII processing.

B.3.2 General

This clause provides PIMS guidance for PII controllers and PII processors,which relates to the controls listed in Table A.3. Unless otherwise stated by the specific provisions in Table A.3, or determined by the organization,the same guidance applies for PII controllers and PII processors.

B.3.3 Policies for information security

Control

Information security policies related to PII processing should be defined,approved by management, published,communicated to and acknowledged by relevant personnel and relevant interested parties,and reviewed at planned intervals and if significant changes occur.

Implementation guidance

Either by the development of separate privacy policies,or by the augmentation of information security policies,the organization should produce a statement concerning support for and commitment to achieving compliance with legal requirements applicable to PII protection and with the contractual terms agreed between the organization and its partners,its subcontractors and its applicable third parties (customers, suppliers etc.),which should clearly allocate responsibilities between them.

Any organization that processes PII,whether a PII controller or a PIl processor,should consider legal requirements applicable to PIIprotection during the development and maintenance of information security policies.

B.3.4 Information security roles and responsibilities

Control

Information security roles and responsibilities related to PII processing should be defined and allocated according to the organizational needs.

Implementation guidance

The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller,a point of contact should be designated for PII principals regarding the processing of their PII (see B.1.3.4).

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

The responsible person should,where appropriate:

- be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;
- be involved in the management of all issues which relate to the processing of PII;

—be an expert in data protection legislation,regulation and practice;

— act as a contact point for supervisory authorities;

—inform top-level management and employees of the organization of their obligations with respect to the processing of PII;

— provide advice in respect of privacy impact assessments conducted by the organization.

NOTE Some jurisdictions refer to this person as a data protection officer.Jurisdictions define when such a position is required,along with their position and role.This position can be fulfilled by a staff member or outsourced.

B.3.5 Classification of information

Control

Information should be classified according to the information security needs of the organization,taking into consideration PII,based on confidentiality,integrity,availability and relevant interested party requirements.

Implementation guidance

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

B.3.6 Labelling of information

Control

An appropriate set of procedures for information labelling that considers PII should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation guidance

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

B.3.7 Information transfer

Control

Information transfer rules,procedures,or agreements related to processing PII should be in place for all types of transfer facilities within the organization and between the organization and other parties.

Implementation guidance

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

B.3.8 Identity management

Control

The full life cycle of identities related to PII processing should be managed.

Implementation guidance

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

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

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

Some jurisdictionsimpose specific requirements regardingthe frequency of checks forunused authentication credentials related to systems that process PII.Organizations operating in these jurisdictions should take compliance with these requirements into account.

B.3.9 Access rights

Control

Access rights to PIl and other associated assets related to PIl processing should be provisioned,reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Implementation guidance

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

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

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

B.3.10 Addressing information security within supplier agreements

Control

Relevant information security requirements related to PII processing should be established and agreed with each supplier based on the type of supplier relationship.

Implementation guidance

The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier is required to meet for the organization to meet its information security and PII protection obligations (see B.1.2.7 and B.2.2.2).

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

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

NOTE For such audit purposes,compliance with relevantand applicable security standards such as ISO/IEC 27001 can be considered.

Where the role of the organization is a PII processor,the organization should specify in contracts with any suppliers that PII is only processed according to its instructions.

B.3.11Information security incident management planning and preparation

Control

The organization should plan and prepare for managing information security incidents related to PII processing by defining,establishing and communicating incident management processes,roles and responsibilities.

Implementation guidance

As part of the overall information security incident management process,the organization should establish responsibilities and procedures for identifying and recording breaches of PII.Additionally,the organization should establish responsibilities and procedures related to notifying relevant parties of PII breaches (including the timing of such notifications)and the disclosure to authorities,taking into account the applicable legal requirements.

Some jurisdictions impose specific regulations regarding breach responses,including notification. Organizations operating in these jurisdictions should ensure that they are aware of,and document how they comply with,these regulations.

B.3.12 Response to information security incidents

Control

Responses to information security incidents related to PII processing should be according to the documented procedures.

Implementation guidance for PII controllers

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

An event does not necessarily trigger such a review.

NOTE1 An information security event does not necessarily result in actual,or the significant probability of, unauthorized access to PIl or to any of the organization's equipment or facilities storing PI.These can include,but are not limited to,pings and other broadcast attacks on firewalls or edge servers,port scans,unsuccessful log-on attempts,denial of service attacks and packet sniffing.

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

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

Notifications should be clear.

NOTE 2 A notification can contain details such as:

— a contact point where more information can be obtained;

—a description of and the likely consequences of the breach;

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

— measures taken or planned to be taken.

NOTE3 Information on the management of security incidents can be found in the ISO/IEC 27035 series.

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

—a description of the incident;

—the time period;

—the consequences of the incident;

—the name of the reporter;

—to whom the incident was reported;

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

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

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

Implementation guidance for PII processors

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

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

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

—a description of the incident;

—the time period;

—the consequences of the incident;

—the name of the reporter;

—to whom the incident was reported;

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

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

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

In some jurisdictions,applicable legal requirements can require the organization to directly notify appropriate regulatory authorities (e.g.a PII protection authority)of a breach involving PII.

B.3.13 Legal,statutory,regulatory and contractual requirements

Control

Legal,statutory,regulatory and contractual requirements relevant to information security related to PII processing and the organization's approach to meet these requirements should be documented and this documentation kept up to date.

Implementation guidance

The organization should identify any potential legal sanctions (which can result from some obligations being missed)related to the processing of PII,including substantial fines directly from the local supervisory authority.

In some jurisdictions,International Standards such as this document can be used to form the basis for a contract between the organization and the customer,outlining their respective security,privacy and PII protection responsibilities.The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

B.3.14 Protection of records

Control

Records related to PII processing should be protected from loss,destruction,falsification,unauthorized access and unauthorized release.

Implementation guidance

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

The organization should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule (see B.1.4.8).This includes retention of previous versions of these documents when they are updated.

B.3.15 Independent review of information security

Control

The organization's approach to managing information security related to PII processing and its implementation including people,processes and technologies,should be reviewed independently at planned intervals,or when significant changes occur.

Implementation guidance

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

B.3.16 Compliance with policies,rules and standards for information security

Control

Compliance with the organization's information security policy,topic-specific policies,rules and standards related to PII processing should be regularly reviewed.

Implementation guidance

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

—ongoing monitoring to verify that only permitted processing is taking place;or

-specific penetration or vulnerability tests (e.g.de-identified data sets can be subject to a motivated intruder testto validate that de-identification methods are compliant with organizational requirements).

B.3.17 Information security awareness,education and training

Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness education and training and regular updates of the organization's information security

policy,topic-specific policies and procedures,as relevant for their job function,as they relate to PII processing.

Implementation guidance

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

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

B.3.18 Confidentiality or non-disclosure agreements

Control

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of PII should be identified,documented,regularly reviewed and signed by personnel and other relevant interested parties.

Implementation guidance

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

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

B.3.19 Clear desk and clear screen

Control

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Implementation guidance

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

B.3.20 Storage media

Control

Storage media with PII should be managed through its life cycle of acquisition,use,transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Implementation guidance

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

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

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

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

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

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

B.3.21 Secure disposal or re-use of equipment

Control

Items of equipment containing storage media with PII should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation guidance

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

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

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

B.3.22 User endpoint devices

Control

PII stored on,processed by or accessible via user endpoint devices should be protected.

Implementation guidance

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

B.3.23 Secure authentication

Control

Secure authentication technologies and procedures related to PII processing should be implemented based on information access restrictions.

Implementation guidance

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

B.3.24 Information backup

Control

Backup copies of PII,and software and systems related to PII processing should be maintained and regularly tested.

Implementation guidance

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

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

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

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

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

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

-the name of the person responsible for the restoration;

—a description of the restored PII.

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

The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing(see B.3.10,B.3.20).Where physical media transfers take place related to backups and restoration,this is also covered by controls in this document(see B.3.7).

B.3.25 Logging

Control

Logs that record activities,exceptions,faults and other relevant events related to PII processing should bee produced,stored,protected and analysed.

Implementation guidance

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

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

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

Log information recorded for,for example,security monitoring and operational diagnostics,can contain PII. Measures such as controlling access should be put in place to ensure that logged information is only used as intended.

A procedure,preferably automatic,should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (see B.1.4.8).

Implementation guidance for PII processors

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

Where the organization permits its customers to access log records controlled by the organization,the organization should implement appropriate controls to ensure that the customer:

— can only access records that relate to that customer's activities;

—cannot access any log records which relate to the activities of other customers;and

—cannot amend the logs in any way.

B.3.26 Use of cryptography

Control

Rules for the effective use of cryptography related to PII processing,including cryptographic key management,should be defined and implemented.

Implementation guidance

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

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

B.3.27 Secure development life cycle

Control

Rules for the secure development of software and systems related to PIl processing should be established and applied.

Implementation guidance

Policies for system development and design should include guidance for the organization's processing of PII needs,based on obligations to PII principals or any applicable legal requirements and the types of processing performed by the organization.

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

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

b) privacy and PII protection requirements in the design phase,which can be based on the output from a privacy risk assessment or a privacy impact assessment(see B.1.2.6);

c) PII protection checkpoints within project milestones;

d)required privacy and PII protection knowledge;

e) by default,minimize processing of PII.

B.3.28 Application security requirements

Control

Information security requirements related to PII processing should be identified,specified and approved when developing or acquiring applications.

Implementation guidance

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

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

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

B.3.29 Secure system architecture and engineering principles

Control

Principles for engineering secure systems related to processing PIl should be established,documented, maintained and applied to any information system development activities.

Implementation guidance

Systems or components related to the processing of PII should be designed following the principles of privacy by design and privacy by default,and to anticipate and facilitate the implementation of relevant controls (as described in B.1a nd B.2 for PII controllers and PII processors,respectively),in particular such that the collection and processing of PII in those systems is limited to what is necessary for the identified purposes of the processing of PII (see B.1.2.2).

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

NOTE Legal requirements can apply.

B.3.30 Outsourced development

Control

The organization should direct,monitor and review the activities related to outsourced PII processing system development.

Implementation guidance

The same principles (see B.3.29)of privacy by design and privacy by default should be applied,if applicable, to outsourced information systems.

B.3.31 Test information

Control

Test information related to PII processing should be appropriately selected,protected and managed.

Implementation guidance

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

Annex C
(informative)

Mapping to ISO/IEC 29100

Table C.1 and C.2 give an indicative mapping between the provisions of this document and the privacy principles from ISO/IEC 29100. Tables C.1 and C.2 show in a purely indicative manner how conformity to the requirements and controls of this document relates to the general privacy principles specified in ISO/IEC 29100.The cross-references in Tables C.1 and C.2 correspond to where the controls are cited in Tables A.1 to A.3.

Table C.1—Mapping of controls for PII controllers and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
1. Consent and choice (ISO/IEC 29100:2024, 6.2)	A.1.2.2 Identify and document purpose A.1.2.3 Identify lawful basis A.1.2.4 Determine when and how consent is to be obtained A.1.2.5 Obtain and record consent A.1.2.6 Privacy impact assessment A.1.3.5 Providing mechanism to modify or withdraw consent A.1.3.6 Providing mechanism to object to PIl processing A.1.3.8 PIl controllers' obligations to inform third parties
2. Purpose legitimacy and specification (ISO/IEC 29100:2024, 6.3)	A.1.2.2 Identify and document purpose A.1.2.3 Identify lawful basis A.1.2.6 Privacy impact assessment A.1.3.3 Determining information for PII principals A.1.3.4 Providing information to PIl principals A.1.3.11 Automated decision making
3. Collection limitation(ISO/IEC 29100:2024, 6.4)	A.1.2.6 Privacy impact assessment A.1.4.2 Limit collection
4. Data minimization (ISO/IEC 29100:2024, 6.5)	A.1.4.3 Limit processing A.1.4.5 PII minimization objectives A.1.4.6 PII de-identification and deletion at the end of processing
5. Use, retention and disclosure limitation (ISO/IEC 29100:2024, 6.6)	A.1.4.5 PII minimization objectives A.1.4.6 PII de-identification and deletion at the end of processing A.1.4.7 Temporary files A.1.4.8 Retention A.1.4.9 Disposal A.1.5.2 Identify basis for PII transfer between jurisdictions A.1.5.5 Records of PII disclosures to third parties
6. Accuracy and quality(ISO/IEC 29100:2024, 6.7)	A.1.4.4 Accuracy and quality
7. Openness, transparency and notice (ISO/IEC 29100:2024, 6.8)	A.1.3.3 Determining information for PII principals A.1.3.4 Providing information to PIl principals
8. Individual participation and access (ISO/IEC 29100:2024, 6.9)	A.1.3.2 Determining and fulfilling obligations to PII principals A.1.3.4 Providing information to PII principals A.1.3.7 Access, correction or erasure A.1.3.9 Providing copy of PII processed A.1.3.10 Handling requests

Table C.1(continued)

Privacy principles of ISO/IEC29100	Related controls for PII controllers
9.Accountability (ISO/IEC 29100:2024,6.10)	A.1.2.7 Contracts with PII processors A.1.2.8 Joint PII controller A.1.2.9 Records related to processing PII A.1.3.10 Handling requests A.1.5.2 Identify basis for PII transfer between jurisdictions A.1.5.3 Countries and international organizations to which PII can be transferred A.1.5.4 Records of transfer of PII
10.Information security(ISO/IEC 29100:2024,6.11)	A.1.2.7 Contracts with PII processors A.1.4.10 PII transmission controls
11.Privacy compliance(ISO/IEC 29100:2024,6.12)	A.1.2.6 Privacy impact assessment

Table C.2—Mapping of controls for PII processors and ISO/IEC 29100

Privacy principles of ISO/IEC29100	Related controls for PII processors
1.Consent and choice(ISO/IEC29100:2024,6.2)	A.2.2.6 Customer obligations
2.Purpose legitimacy and specification (ISO/IEC 29100:2024,6.3)	A.2.2.2 Customer agreement A.2.2.3 Organization's purposes A.2.2.4 Marketing and advertising use A.2.2.5 Infringing instruction A.2.3.2 Comply with obligations to PIl principals
3.Collection limitation (ISO/IEC 29100:2024,6.4)	N/A
4.Data minimization(ISO/IEC 29100:2024,6.5)	A.2.4.2 Temporary files
5.Use,retention and disclosure limitation (ISO/IEC 29100:2024,6.6)	A.2.5.4 Records of PII disclosure to third parties A.2.5.5 Notification of PII disclosure requests A.2.5.6 Legally binding PI disclosures
6.Accuracy and quality (ISO/IEC 29100:2024,6.7)	N/A
7.Openness,transparency and notice (ISO/IEC 29100:2024,6.8)	A.2.5.7 Disclosure of subcontractors used to process PII A.2.5.8 Engagement of a subcontractor to process PII A.2.5.9 Change of subcontractor to process PII
8.Individual participation and access (ISO/IEC 29100:2024,6.9)	A.2.3.2 Comply with obligations to PII principals
9.Accountability (ISO/IEC 29100:2024,6.10)	A.2.2.7 Records related to processing PII A.2.4.3 Return,transfer or disposal of PII A.2.5.2 Basis for PII transfer between jurisdictions A.2.5.3 Countries and international organizations to which PII can be transferred
10.Information security(ISO/IEC 29100:2024,6.11)	A.2.4.4 PII transmission controls
11.Privacy compliance(ISO/IEC 29100:2024,6.12)	A.2.2.6 Customer obligations

Annex D
(informative)

Mapping to the General Data Protection Regulation

Table D.1 gives an indicative mapping between the provisions of this document and Articles 5 to 49 except 43 of the General Data Protection Regulation of the European Union.[16ITable D.1 shows how compliance to requirements and controls of this document can be relevant to fulfil obligations of GDPR.

NOTE This table is purely indicative.It is the organization's responsibility to assess its legal obligations and decide how to comply with them.

Table D.1—Mapping of this document to GDPR articles

Subclause of this document	Relevant GDPR article
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) (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)
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) (b)
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)

Table D.1(continued)

Subclause of this document	Relevant GDPR article
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) (a)
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) (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)
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) (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) (1) (c), (17) (1) (d), (17) (1) (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) (d)
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)

Table D.1(continued)

Subclause of this document	Relevant GDPR article
B.1.4.9	(5) (1) f)
B.1.4.10	(5) (1) f)
B.1.5.2	(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)
B.1.5.3	(15) (2), (30) (1) (e)
B.1.5.4	(30) (1) (e)
B.1.5.5	(30) (1) (d)
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) (h)
B.2.2.6	(28) (3) (h)
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) C)
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) (d)
B.2.5.5	(28) (3) (a)
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)

Annex E
(informative)

Mapping to ISO/IEC27018 and ISO/IEC 29151

ISO/IEC 27018 gives further information for organizations acting as PII processors and providing public cloud services.ISO/IEC 29151 gives additional controls and guidance for the processing of PII by PII controllers.

Table E.1 gives an indicative mapping between the provisions of this document and the provisions from ISO/IEC27018and ISO/IEC 29151.It shows how requirements and controls of this document can correspond to the provisions from ISO/IEC 27018 or ISO/IEC 29151.

The mapping shown in Table E.1 is purely indicative;a given link between these provisions does not mean they are equivalent.

Table E.1—Mapping of ISO/IEC 27701 to ISO/IEC 27018 and ISO/IEC 29151

Subclause in this document	Subclause in ISO/IEC27018	Subclause in ISO/IEC29151
4	N/A	N/A
5	N/A	N/A
6	N/A	N/A
7	N/A	N/A
8	N/A	N/A
9	N/A	N/A
10	N/A	N/A
B. 3. 2	N/A	N/A
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, B. 3. 29, B. 3. 30, B. 3. 31	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. 1. 2. 2	N/A	A. 4
B. 1. 2. 3	N/A	A. 4. 1
B. 1. 2. 4	N/A	A. 3. 1
B. 1. 2. 5	N/A	A. 3. 1
B. 1. 2. 6	N/A	A. 11. 2
B. 1. 2. 7	N/A	A. 11. 3
B. 1. 2. 8	N/A	N/A
B. 1. 2. 9	N/A	8. 15
B. 1. 3. 2	N/A	A. 10
B. 1. 3. 3	N/A	A. 9. 2
B. 1. 3. 4	N/A	A. 9

Table .1(continued)

B.1.3.5	N/A	A.3.2
B.1.3.6	N/A	A.3.2
B.1.3.7	N/A	A.10.1, A.10.2
B.1.3.8	N/A	A.10.2
B.1.3.9	N/A	A.10.1
B.1.3.10	N/A	A.10.1
B.1.3.11	N/A	N/A
B.1.4.2	N/A	A.5
B.1.4.3	N/A	A.7.1
B.1.4.4	N/A	A.8
B.1.4.5	N/A	A.6
B.1.4.6	N/A	A.7.1
B.1.4.7	N/A	A.7.2
B.1.4.8	N/A	A.7.1
B.1.4.9	N/A	A.7.14
B.1.4.10	N/A	N/A
B.1.5.2	N/A	A.13.2
B.1.5.3	N/A	A.13.2
B.1.5.4	N/A	A.13.2
B.1.5.5	N/A	A.7.4
B.2.2.2	N/A	N/A
B.2.2.3	A.3.1	N/A
B.2.2.4	A.3.2	N/A
B.2.2.5	N/A	N/A
B.2.2.6	N/A	N/A
B.2.2.7	N/A	A.7.4
B.2.3.2	A.2.1	N/A
B.2.4.2	A.5.1	A.7.2
B.2.4.3	A.10.3	A.11.3
B.2.4.4	A.12.2	N/A
B.2.5.2	N/A	A.4.1, A.13.2
B.2.5.3	A.12.1	A.13.2
B.2.5.4	A.6.2	A.7.4
B.2.5.5	A.6.1	A.7.3
B.2.5.6	A.6.1	A.7.3
B.2.5.7	A.8.1	A.7.5
B.2.5.8	A.8.1	N/A
B.2.5.9	A.8.1	N/A

Annex F
(informative)

Correspondence with ISO/IEC 27701:2019

The purpose of this annex is to provide backwards compatibility with the previous edition of this document (ISO/IEC 27701:2019)for organizations that are currently using that document and wish to transition to this new edition.

Table F.1 provides the correspondence of the controls specified in AnnexA with those in ISO/IEC 27701:2019. “N/A”in the first column identifies those controls not included in this document."New"in the second column identifies controls not included in ISO/IEC 27701:2019.

Table F.1—Correspondence between controls in this document and controls in ISO/IEC 27701:2019

ISO/IEC 27701 control identifier	ISO/ IEC27701:2019 control identifier	Control name
A.3.3	6.2.1.1,6.2.1.2	Policies for information security
A.3.4	6.3.1.1	Information security roles and responsibilities
N/A	6.3.1.2	Segregation of duties
N/A	6.4.2.1	Management responsibilities
N/A	6.3.1.3	Contact with authorities
N/A	6.3.1.4	Contact with special interestgroups
N/A	New	Threat intelligence
N/A	6.3.1.5,6.11.1.1	Information security in project management
N/A	6.5.1.1,6.5.1.2	Inventory of information and other associated assets
N/A	6.5.1.3,6.5.2.3	Acceptable use of information and other associated assets
N/A	6.5.1.4	Return of assets
A.3.5	6.5.2.1	Classification of information
A.3.6	6.5.2.2	Labelling of information
A.3.7	6.10.2.1,6.10.2.2, 6.10.2.3	Information transfer
N/A	6.6.1.1,6.6.1.2	Access control
A.3.8	6.6.2.1	Identity management
N/A	6.6.2.4,6.6.3.1, 6.6.4.3	Authentication information
A.3.9	6.6.2.2,6.6.2.5, 6.6.2.6	Access rights
A.3.10	6.12.1.1 6.12.1.2	Addressing information security within supplier agreements
N/A	6.12.1.3	Managing information security in the ICT supply chain
N/A	6.12.2.1,6.12.2.2	Monitoring,review and change management of supplier services
N/A	New	Information security for use of cloud services
N/A	6.13.1.1	Information security incident management planning and preparation
A.3.11	6.13.1.4	Assessment and decision on information security events
A.3.12	6.13.1.5	Response to information security incidents
N/A	6.13.1.6	Learning from information security incidents

Table F.1(continued)

ISO/IEC 27701 control identifier	ISO/ IEC 27701:2019 control identifier	Control name
N/A	6.13.1.7	Collection of evidence
N/A	6.14.1.1,6.14.1.2, 6.14.1.3	Information security during disruption
N/A	New	ICT readiness for business continuity
A.3.13	6.15.1.1,6.15.1.5	Legal,statutory,regulatory and contractual requirements
N/A	6.15.1.2	Intellectual property rights
A.3.14	6.15.1.3	Protection of records
N/A	6.15.1.4	Privacy and protection of PII
A.3.15	6.15.2.1	Independent review of information security
A.3.16	6.15.2.2,6.15.2.3	Compliance with policies,rules and standards for information security
N/A	6.9.1.1	Documented operating procedures
N/A	6.4.1.1	Screening
N/A	6.4.1.2	Terms and conditions of employment
A.3.17	6.4.2.2	Information security awareness,education and training
N/A	6.4.2.3	Disciplinary procedures
N/A	6.4.3.1	Responsibilities after termination or change of employment
A.3.18	6.10.2.4	Confidentiality or non-disclosure agreements
N/A	6.3.2.2	Remote working
N/A	6.13.1.2,6.13.1.3	Information security event reporting
N/A	6.8.1.1	Physical security perimeter
N/A	6.8.1.2,6.8.1.6	Physical entry
N/A	6.8.1.3	Securing offices,rooms and facilities
N/A	New	Physical security monitoring
N/A	6.8.1.4	Protecting against physical and environmental threats
N/A	6.8.1.5	Working in secure areas
A.3.19	6.8.2.9	Clear desk and clear screen
N/A	6.8.2.1	Equipment siting and protection
N/A	6.8.2.6	Security of assets off-premises
A.3.20	6.5.3.1,6.5.3.2, 6.5.3.3,6.8.2.5	Storage media
N/A	6.8.2.2	Supporting utilities
N/A	6.8.2.3	Cabling security
N/A	6.8.2.4	Equipment maintenance
A.3.21	6.8.2.7	Secure disposal or re-use of equipment
A.3.22	6.3.2.1,6.8.2.8	User endpoint devices
N/A	6.6.2.3	Privileged access rights
N/A	6.6.4.1	Information access restriction
N/A	6.6.4.5	Access to source code
A.3.23	6.6.4.2	Secure authentication
N/A	6.9.1.3	Capacity management
N/A	6.9.2.1	Protection against malware
N/A	6.9.6.1	Management of technical vulnerabilities
N/A	New	Configuration management

Table F.1*(continued)*

ISO/IEC 27701 control identifier	ISO/ IEC27701:2019 control identifier	Control name
N/A	New	Information deletion
N/A	New	Data masking
N/A	New	Data leakage prevention
A.3.24	6.9.3.1	Information backup
N/A	6.14.2.1	Redundancy of information processing facilities
A.3.25	6.9.4.1,6.9.4.2, 6.9.4.3	Logging
N/A	New	Monitoring activities
N/A	6.9.4.4	Clock synchronization
N/A	6.6.4.4	Use of privileged utility programme(s)
N/A	6.9.5.1,6.9.6.2	Installation of software on operational systems
N/A	6.10.1.1	Network security
N/A	6.10.1.2	Security of network services
N/A	6.10.1.3	Segregation of networks
N/A	New	Web filtering
A.3.26	6.7.1.1,6.7.1.2	Use of cryptography
A.3.27	6.11.2.1	Secure development life cycle
A.3.28	6.11.1.2,6.11.1.3	Application security requirements
A.3.29	6.11.2.5	Secure system architecture and engineering principles
N/A	New	Secure coding
N/A	6.11.2.8,6.11.2.9	Security testing in development and acceptance
A.3.30	6.11.2.7	Outsourced development
N/A	6.9.1.4,6.11.2.6	Separation of development,testing and production environments
N/A	6.9.1.2,6.11.2.2, 6.11.2.3,6.11.2.4	Change management
A.3.31	6.11.3.1	Test information
N/A	6.9.7.1	Protection of information systems during audit testing

Table E.2 provides the correspondence of the controls specified in ISO/IEC 27701:2019,Clause 6 with those in this document."N/A"in the second column identifies the controls that are not included in this document.

Table F.2—Correspondence between controls in ISO/IEC 27701:2019 and controls in this document

ISO/ IEC27701:2019 control identifier	ISO/IEC27701 control identifier	Control name accordingto ISO/IEC 27701:2019
6.2.1.1	A.3.3	Policies for information security
6.2.1.2	A.3.3	Review of policies for information security
6.3.1.1	A.3.4	Internal security roles and responsibilities
6.3.1.2	N/A	Segregation of duties
6.3.1.3	N/A	Contact with authorities
6.3.1.4	N/A	Contact with special interest groups
6.3.1.5	N/A	Information security in project management
6.3.2.1	A.3.22	Mobile device policy
6.3.2.2	N/A	Teleworking

Table F.2(continued)

ISO/ IEC 27701:2019 control identifier	ISO/IEC27701 control identifier	Control name according to ISO/IEC 27701:2019
6.4.1.1	N/A	Screening
6.4.1.2	N/A	Terms and conditions ofemployment
6.4.2.1	N/A	Management responsibilities
6.4.2.2	A.3.17	Information security awareness,education and training
6.4.2.3	N/A	Disciplinary procedures
6.4.3.1	N/A	Termination or change of employment responsibilities
6.5.1.1	N/A	Inventory of assets
6.5.1.2	N/A	Ownership of assets
6.5.1.3	N/A	Acceptable use of assets
6.5.1.4	N/A	Return of assets
6.5.2.1	A.3.5	Classification of information
6.5.2.2	A.3.6	Labelling of information
6.5.2.3	N/A	Handling of assets
6.5.3.1	A.3.20	Management of removable media
6.5.3.2	A.3.20	Disposal of media
6.5.3.3	A.3.20	Physical media transfer
6.6.1.1	N/A	Access control policy
6.6.1.2	N/A	Access to networks and network services
6.6.2.1	A.3.8	User registration and de-registration
6.6.2.2	A.3.9	User access provisioning
6.6.2.3	N/A	Management of privileged access rights
6.6.2.4	N/A	Management of secret authentication information of users
6.6.2.5	A.3.9	Review of user access rights
6.6.2.6	A.3.9	Removal or adjustment of access rights
6.6.3.1	N/A	Use of secret authentication information
6.6.4.1	N/A	Information access restriction
6.6.4.2	A.3.23	Secure log-on procedures
6.6.4.3	N/A	Password management system
6.6.4.4	N/A	Use of privileged utility programme(s)
6.6.4.5	N/A	Access control to program source code
6.7.1.1	A.3.26	Policy on the use of cryptographic controls
6.7.1.2	A.3.26	Key management
6.8.1.1	N/A	Physical security perimeter
6.8.1.2	N/A	Physical entry controls
6.8.1.3	N/A	Securing offices,rooms and facilities
6.8.1.4	N/A	Protecting against external and environmental threats
6.8.1.5	N/A	Working in secure areas
6.8.1.6	N/A	Delivery and loading areas
6.8.2.1	N/A	Equipment siting and protection
6.8.2.2	N/A	Supporting utilities
6.8.2.3	N/A	Cabling security
6.8.2.4	N/A	Equipment maintenance
6.8.2.5	N/A	Removal of assets

Table F.2(continued)

ISO/IEC27701:2019 control identifier	ISO/IEC27701 control identifier	Control name according to ISO/IEC 27701:2019
6.8.2.6	N/A	Security of equipment and assets off-premises
6.8.2.7	A.3.21	Secure disposal or re-use of equipment
6.8.2.8	A.3.22	Unattended user equipment
6.8.2.9	A.3.19	Clear desk and clear screen policy
6.9.1.1	N/A	Documenting operating procedures
6.9.1.2	N/A	Change management
6.9.1.3	N/A	Capacity management
6.9.1.4	N/A	Separation of development,testing and operational environments
6.9.2.1	N/A	Controls against malware
6.9.3.1	A.3.24	Information backup
6.9.4.1	A.3.25	Event logging
6.9.4.2	A.3.25	Protection of log information
6.9.4.3	A.3.25	Administrator and operator logs
6.9.4.4	N/A	Clock synchronization
6.9.5.1	N/A	Installation of software on operational systems
6.9.6.1	N/A	Management of technical vulnerabilities
6.9.6.2	N/A	Restriction on software installation
6.9.7.1	N/A	Information systems audit controls
6.10.1.1	N/A	Network controls
6.10.1.2	N/A	Security in network services
6.10.1.3	N/A	Segregation in networks
6.10.2.1	A.3.7	Information transfer policies and procedures
6.10.2.2	A.3.7	Agreements for information transfer
6.10.2.3	A.3.7	Electronic messaging
6.10.2.4	A.3.18	Confidentiality or non-disclosure agreements
6.11.1.1	N/A	Information security requirements analysis and specification
6.11.1.2	A.3.28	Securing application services on public networks
6.11.1.3	A.3.28	Protecting application services transactions
6.11.2.1	A.3.27	Secure development policy
6.11.2.2	N/A	System change control procedures
6.11.2.3	N/A	Technical review of applications after operating platform changes
6.11.2.4	N/A	Restrictions of changes to software packages
6.11.2.5	A.3.29	Secure systems engineering principles
6.11.2.6	N/A	Secure development environment
6.11.2.7	A.3.30	Outsourced development
6.11.2.8	N/A	System security testing
6.11.2.9	N/A	System acceptance testing
6.11.3.1	A.3.30	Protection of test data
6.12.1.1	A.3.10	Information security policy for supplier relationships
6.12.1.2	A.3.10	Addressing security within supplier agreements
6.12.1.3	N/A	Information and communication technology supply chain
6.12.2.1	N/A	Monitoring and review of supplier services
6.12.2.2	N/A	Managing changes to supplier services

Table F.2(continued)

ISO/ IEC27701:2019 control identifier	ISO/IEC 27701 control identifier	Control name according to ISO/IEC 27701:2019
6.13.1.1	N/A	Responsibilities and procedures
6.13.1.2	N/A	Reporting information security events
6.13.1.3	N/A	Reporting information security weaknesses
6.13.1.4	A.3.11	Assessment and decisions on information security events
6.13.1.5	A.3.12	Response to information security incidents
6.13.1.6	N/A	Learning from information security incidents
6.13.1.7	N/A	Collection of evidence
6.14.1.1	N/A	Planning information security continuity
6.14.1.2	N/A	Implementing information security continuity
6.14.1.3	N/A	Verify,renew and evaluate information security continuity
6.14.2.1	N/A	Availability of information processing facilities
6.15.1.1	A.3.13	Identification of applicable legislation and contractual requirements
6.15.1.2	N/A	Intellectual property rights
6.15.1.3	A.3.14	Protection of records
6.15.1.4	N/A	Privacy and protection of personally identifiable information
6.15.1.5	A.3.13	Regulation of cryptographic controls
6.15.2.1	A.3.15	Independent review of information security
6.15.2.2	A.3.16	Compliance with security policies and standards
6.15.2.3	A.3.16	Technical compliance review

Bibliography

[1] *ISO 19011,Guidelinesfor auditing management systems*

[2] *ISO/IEC19944-1,Cloud computing and distributed platforms—Data flow,data categories and data use —Part 1:Fundamentals*

[3] *ISO/IEC19944-2,Cloud computing and distributed platforms—Data flow,data categories and data use —Part 2:Guidance on application and extensibility*

[4] *ISO/IEC 20889,Privacy enhancing data de-identification terminology and classification oftechniques*

[5] *ISO/IEC 27001,Information security,cybersecurity and privacy protection —Information security management systems—Requirements*

[6] *ISO/IEC 27002,Information security,cybersecurity and privacy protection —Information security controls*

[7] ISO/IEC 27005,Information security,cybersecurity and privacy protection —Guidance on managing *information security risks*

[8] *ISO/IEC 27018,Information security,cybersecurity and privacy protection —Guidelines for protection ofpersonally identifiable information(PII)in public clouds acting as PIIprocessors*

[9] ISO/IEC 27035(all parts),Information technology—Information security incident management

[10] *ISO/IEC 27557,Information security,cybersecurity and privacy protection —Application of ISO 31000:2018for organizational privacy risk management*

[11] *ISO/IEC 29101:2018,Information technology—Security techniques—Privacy architecture framework*

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

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

[14] *ISO/IEC 29184,Information technology—Online privacy notices and consent*

[15] *ISO 31000,Risk management—Guidelines*

[16] General Data Protection Regulation(EU)-Regulation(EU)2016/79 of the European Parliament and of the Council

ICS 35.030
Price based on 64 pages

iso.org