国际标准

ISO/IEC 27701

信息安全、网络安全与隐私保护——隐私信息管理体系——要求和指南

信息安全、网络安全与隐私保护——隐私保护管理体系——要求和指南

第二版 2025 年 10 月

参考编号
ISO/IEC 27701:2025

目录

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 https://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(VTO)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(SC27)——信息安会,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/IEC27701:2019)。

主要变更如下:

——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;

——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

1 范围

本文件规定了建立、实施、维护和持续改进隐私信息管理体系(PIMS)的要求。

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。

2 规范性引用文件

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》

3 术语、定义和缩略语

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 EC 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、权限和关系以实现其目标的个人或群体(3.6)

注 1：组织的概念包括但不限于个体经营户、公司、企业、商行、机构、合伙企业、慈善组织或机构，或其组成部分或组合形式，无论是否已注册、属于公共或私人性质。

注 2：如果该组织隶属于一个更大的实体，则“组织”一词仅指该更大实体中位于隐私信息管理体系(3.23)范围之内的部分。

3.2

相关方

能够影响、受影响或自认为受某项决定或活动影响的个人或组织（3.1）。

3.3

最高管理者

在最高层级指导和控制组织的人或群体(3.1)

注 1:最高管理者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，则最高管理者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。

注 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

方针

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。

注 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:管理体系(3.4),包括相关过程(3.8);

为组织运作而创建的信息(文件);

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、体系或组织(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

审核

体系化且独立的过程(3.8),用于获取证据并客观评估其有效性，以确定审核标准的达成程度。

注 1:审核可分为内部审核(第一方)或外部审核(第二方或第三方),亦可为组合审核(融

合两个或多个领域)。

注 2：内部审核由组织(3.1)自身或代表其的外部方实施。

注 3：“审核证据”和“审核标准”在 ISO 19011 中定义。

3.19

测量

确定数值的过程(3.8)

3.20

监测

确定体系、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(PID) 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 PII 控制者，或是与 PII 处理分包商签订合同的 PII 处理者。

3.23

隐私信息管理体系 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

一套旨在管理组织(3.1)资产风险(3.7),以确保信息保密性、完整性和可用性的政策(3.5)、目标(3.6)和流程(3.8)。

注 1:信息安全计划可以是，例如，基于 ISO/IEC27001 的信息安全管理体系。

3.25

适用性声明

所有必要控制措施的文档以及对这些控制措施纳入或排除的理由说明。

4 组织环境

4.1 理解组织及其环境

该组织应识别与其宗旨相关并影响其实现隐私信息管理体系预期目标能力的内外部问题。

组织应确定气候变化是否为相关议题。

组织应确定其是否作为PII控制者(包括作为联合PII控制者)或作为PII处理者。

组织应确定与其背景相关且影响其PIMS预期成果实现能力的外部和内部问题。

注1：外部和内部问题可包括但不限于:

——适用的隐私立法;

——适用的法规;

——适用的司法裁决;

——适用的组织背景、治理结构、政策和程序;—适用的行政决定;

——适用的合同要求。

当组织同时扮演两种角色(即PII控制者和PII处理者)时，应确定不同的角色，每个角色都属于一套独立的控制措施。

注2：组织的角色可能因每次处理PII的不同实例而异，因为这取决于谁决定处理的目的和手段。

4.2 理解相关方的需求和期望

组织应确定:

——与隐私信息管理体系相关的利益相关方;

——这些相关方的相关要求;

——这些要求中哪些将通过隐私信息管理体系来解决。

注1：相关利益方可能具有与气候变化相关的诉求。

组织应将其与PII处理相关的利益或责任方(包括PII主体)纳入其利益相关方范围。

注2：其他利益相关方可以包括客户、监管机构、其他PI1控制者、PII处理者及其分包商。

根据组织的角色，“客户”可以理解为以下两种情况:

a)与PII控制者签订合同的组织(例如PII控制者的客户);

注3：这可能适用于作为联合PII控制者的组织。

b)与PII处理者签订合同的PII控制方(例如，PII处理者的客户);或

c)与分包商签订PII处理合同的PII处理器(例如，被分包的PII处理器的客户)。

注4：在商业协会中处理其个人身份信息(PII)的自然人，在本文档中称为"PII主体"。

注5：与处理个人身份信息(PII)相关的要求可通过法律法规要求、合同义务以及自我设定的组织目标来确定。ISO/IEC 29100中阐述的隐私原则为处理PII事宜提供了指导。

注6：为证明符合组织的义务，某些利益相关方可能会期望该组织已符合特定的标准，例如本文件中所述的管理体系或任何相关的规范集。这些方可以要求对这些标准进行独立

审核以确认其符合性。

4.3 确定隐私信息管理体系的范围

组织应确定隐私信息管理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：

——4.1 所述的外部和内部问题:

——4.2 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。

4.4 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。

5 领导力

5.1 领导与承诺

高层管理应通过以下方式展示对隐私信息管理体系的领导力和承诺:

——确保隐私方针(见 5.2)和隐私目标(见 6.2)已建立，并且与其组织的战略方向相一致;

——确保将隐私信息管理体系要求融入到组织的业务流程中;

——确保隐私信息管理体系所需资源可用;

——传达有效隐私信息管理以及遵守隐私信息体系要求的重要性;

——确保隐私信息管理体系实现其预期结果;

——指导和支持人员为隐私信息管理体系的有效性做出贡献;

——促进持续改进;

——支持其他相关角色，以在其职责范围内展示其领导力。

注:本文档中对“业务”的引用可广泛理解为与组织存在目的核心相关的活动。

5.2 隐私方针

最高管理者应建立一项隐私方针，该方针:

a)与组织的目标相适应;

b)提供设定隐私目标的框架;

c)包含承诺满足适用要求;

d)包含对隐私信息管理体系持续改进的承诺。

隐私方针应:

——应以文档形式提供;

——在组织内部进行沟通;

——根据需要向相关方提供。

5.3 角色、职责与权限

最高管理者应确保相关角色的责任和权限在组织内被分配并传达。

最高管理者应分配以下职责和权限:

a)确保隐私信息管理体系符合本文件的要求;

b)向最高管理者报告隐私信息管理体系的运行情况。

6 策划

6.1 应对风险与机遇的措施

6.1.1 总则

在策划隐私信息管理体系时，组织应考虑到 4.1 所提及的因素和 4.2 所提及的要求，并确定需要应对风险与机遇，以:

——确保隐私信息管理体系能够实现其预期结果;

——防止或减少不良影响;

——实现持续改进。

组织应策划:

a)应对这些风险和机遇的措施;

b)如何

——将这些行动整合并实施到其隐私信息管理体系流程中;

——评估这些措施的有效性。

6.1.2 隐私风险评估

组织应定义并实施隐私风险评估流程，该流程应:

a)建立并维护包含以下内容的隐私风险标准:

1)风险接受标准;以及

2)进行隐私风险评估的标准;

b)确保重复的隐私风险评估产生一致、有效且可比的结果;

c)识别隐私风险:

1)与隐私信息管理体系范围内的隐私保护和信息安全风险相关;以及

2)确定风险责任人的风险;

d)分析以下隐私风险:

1)评估如果 c)1)中确定的风险得以实现，将对组织和 PII 主体可能产生的潜在后果;

2)评估在 c)1)中识别的风险发生的现实可能性;以及

3)确定风险等级;

e)评估以下隐私风险:

1)将风险分析结果与 a)中设定的风险标准进行比较;以及

2)对分析出的风险进行优先排序，以进行风险处理。组织应保留有关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，请参见 ISO/IEC 27557。

6.1.3 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(PII)处理相关的风险，包括对 PII 主体的风险以及 PII 的安全性风险，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措施;

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：组织可根据需要设计控制措施，或从任何来源识别这些控制措施。

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

——物理和环境安全。

注 2：ISO/IEC 27002 提供了一份可能的信息安全控制措施的清单。如果信息安全方案是基于 ISO/IEC 27001 制定的，则可查阅 ISO/IEC 27002 以确保不会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录 A 中的内容进行对照，并验证是否遗漏了必要的控制措施;

注 3：附录 A 包含可能的隐私控制列表。可查阅附录 A，以确保不遗漏必要的隐私控制措施。

注 4：附录 A 中列出的隐私控制措施并非详尽无遗，如有需要可增加额外的隐私控制措施。

注 5：在考虑个人身份信息处理的安全性时，组织可以以综合方式处理信息安全和隐私问题，例如将信息安全与隐私风险评估相结合，或者作为拥有重叠领域的独立实体加以处理。

e)编制适用性声明，包括:

——必要的控制措施[参见 b)、c)和 d)];

——其纳入的合理性说明;

——是否已实施必要的控制措施;以及

——排除附件 A 中任何控制措施的理由。

无需包含附件 A 中列出的所有控制措施。例如，如果风险评估认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)制定隐私风险处理计划;

g)获取隐私风险责任人对隐私风险处理计划的批准对残余隐私风险的接受；以及

h)考虑附录 B 中关于在 b)和 c)项所确定的控制措施的指导意见。组织应保留有关隐私风险处理流程的文件化信息。

6.2 隐私目标及其实现规划

组织应在相关职能和层级建立隐私目标。隐私目标应:

a)与隐私方针保持一致(见 5.2);

b)可测量(如可行);

c)考虑适用的要求;

d)接受监控;

e)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:

——要做什么;

——需要什么资源;

——由谁负责;

——何时完成;

——如何评价结果。

6.3 变更的策划

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。

7 支持

7.1 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体系所需资源。

7.2 能力

组织应:

——确定在其控制下从事影响其隐私信息管理绩效工作的人员所需的能力;

——确保这些人员具备相应的教育、培训或经验所形成的能力;

——如适用，采取措施获取必要的能力，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的证明。

注:适用的措施可包括，例如:为现有员工提供培训、指导或重新分配工作;或招聘或签约合格人员。

7.3 意识

在组织控制下工作的人员应知晓:

——隐私方针(见 5.2);

——他们对隐私信息管理体系有效性的贡献，包括改进隐私绩效带来的益处;

——不符合隐私信息管理体系要求的后果。

7.4 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:

——沟通什么;

——何时沟通;

——与谁沟通;

——如何沟通。

7.5 文件化信息

7.5.1 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)组织确定为保障隐私信息管理体系有效性的文件化信息。

注:隐私信息管理体系的文件化信息范围可能因组织而异，原因包括:

——组织的规模及其活动、流程、产品和服务类型;

——流程及其相互作用的复杂程度;

——人员能力水平。

7.5.2 创建和更新

在创建和更新文件化信息时，组织应确保适当的:

——标别和说明(例如标题、日期、作者或参考编号);

——形式(例如语言、软件版本、图形)和介质(例如纸质的、电子的);

——评审和批准，以保持适宜性和充分性。

7.5.3 文件化信息的控制

隐私信息管理体系和本文件要求的文件化信息应受控，以确保:

a)在需要的场合和时机，均可获得并适用;

b)予以妥善保护(例防止机密、不当使用或缺失)。

为控制文件化信息，适用时，组织应进行下列活动:

——分发、访问、检索和使用;

——存储与保存，包括保持可读性;

——变更控制(如版本控制);

——保留和处置。

由组织判定对隐私信息管理体系的规划与运行而言必不可少的、源自外部的已记录信息，应酌情予以识别并加以控制。

注:对成文信息的“访问”可能意味着仅允许查阅,或者意味着允许查阅并授权修改。

8 运行

8.1 运行策划与控制

组织应策划、实施并控制满足要求所需的流程，并执行第 6 章中确定的措施，具体方式如下:

——确定流程的标准;

——根据标准实施对流程的控制。

应提供必要的文件化信息，以确保过程按计划执行。

组织应控制计划变更，并审查意外变更的后果，必要时采取措施减轻任何不利影响。

组织应确保与隐私信息管理体系相关的外部提供的流程、产品或服务受到控制。

8.2 隐私风险评估

组织应在策划的时间间隔或当提出或发生重大变更时,根据 6.1.2a)中规定的标准进行隐私风险评估。

组织应保留隐私风险评估结果的文件化信息。

8.3 隐私风险处理

组织应实施隐私风险处理计划。

组织应保留隐私风险处理结果的文件化信息。

9 绩效评价

9.1 监控、测量、分析和评价

组织应确定:

——需要监控和测量的内容;

——适用的监控、测量、分析和评估方法，以确保结果的有效性;

——监控和测量应在何时执行;

——监测和测量结果何时应进行分析与评估。

应提供可证明结果的文件化信息。

组织应评估隐私绩效以及隐私信息管理体系的有效性。

9.2 内部审核

9.2.1 总则

组织应按照策划的时间间隔进行内部审核，以提供有关隐私信息管理体系是否符合以下信息:

a)符合:

——组织自身对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。

9.2.2 内部审核计划

组织应策划、建立、实施和维护(一项或多项)审核计划，包括频率、方法、责任、规划要求和报告。

在制定内部审核计划时，组织应考虑相关流程的重要性以及以往审核的结果。

组织应:

a)确定每次审核的目标、标准和范围;

b)选择审核员并开展审核，以确保审核过程的客观性和公正性;

c)确保审核结果向相关管理者报告。

应提供文件化信息作为审核计划实施及审核结果的证据。

9.3 管理评审

9.3.1 总则

高层管理应按计划间隔审查组织的隐私信息管理体系，以确保其持续适用性、充分性和有效性。

9.3.2 管理评审输入

管理评审应包括:

a)以往管理评审中所采取措施的状态;

b)与隐私信息管理体系相关的外部和内部问题的变化;

c)与隐私信息管理体系相关的利益相关方需求和期望的变化;

d)关于隐私信息管理体系绩效的信息，包括以下方面的趋势:

——不符合项和纠正措施;

——监控和测量结果;

——审核结果;

e)持续改进的机会。

9.3.3 管理评审结果

管理评审的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。

10 改进

10.1 持续改进

组织应持续改进隐私信息管理体系的适宜性、充分性和有效性。

10.2 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;

——处置后果;

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

——评审和分析不符合;

——确定不符合项的原因;

——确定是否存在或可能发生类似的不符合项;

c)实施任何必要的措施;

d)审查已采取的纠正措施的有效性;

e)必要时，对隐私信息管理系统进行变更。

纠正措施应与不符合项所产生的影响相适应。

应提供文件化信息作为以下内容的证据:

——不符合项的性质以及后续所采取的任何措施;

——任何纠正措施的结果。

11 附件补充信息

附录 C 包含本文件条款与 ISO/IEC 29100 隐私原则之间的映射。

附录 D 包含本文件中控制措施与欧盟通用数据保护条例的映射。

附录 E 包含本文件条款与 ISO/IEC 27018 和 ISO/IEC 29151 条款的对应关系映射。

附录 F 显示了本版 ISO/IEC 27701 中控制措施与前一版本(ISO/IEC 27701:2019)之间的对应关系。

附录 A
（规范性）
PII 控制者与 PII 处理者的 PIMS 参考控制目标与控制措施

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)。6.1.3 e))。

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

收集和处理条件 目的：证明处理是合法的，具有适用司法管辖区的法律依据，并且具有明确定义的合法目的。		
控制参考	控制标题	控制
A.1.2.2	识别和文件目的	组织应明确并记录处理个人身份信息的具体目的。
A.1.2.3	确定法律依据	组织应确定、记录并能够证明其处理个人信息用于已确定目的的相关合法依据。
A.1.2.4	确定何时以及如何获得同意。	该组织应确定并记录一个流程，通过该流程可以证明是否、何时以及如何从 PII 主体处获得了处理 PII 的同意。
A.1.2.5	获取并记录同意书	组织应按照已记录的流程获取并记录 PII 主体的同意。
A.1.2.6	隐私影响评估	每当计划对个人身份信息进行新的处理或对现有的个人身份信息处理进行更改时，组织应评估是否需要进行隐私影响评估，并在适当情况下实施隐私影响评估。
A.1.2.7	与 PII 处理者的合同	该组织应与它使用的任何 PII 处理者签订书面合同，并应确保其与 PII 处理者的合同涵盖附件 A 中适当控制措施的实施（见表 A.2）。
A.1.2.8	联合 PII 控制器	该组织应与任何联合 PII 控制者确定处理 PII 的各自角色和责任（包括 PII 保护和安全要求）。
A.1.2.9	与处理个人身份信息相关的记录	组织应确定并妥善保管必要的记录，以履行其处理个人身份信息（PII）的义务。
对 PII 委托人的义务 目标：确保向个人身份信息主体提供有关其个人身份信息处理的适当信息，并履行与个人身份信息处理相关的任何其他适用义务。		
A.1.3.2	确定并履行对 PII 委托人的义务	该组织应确定并记录其对个人身份信息主体在处理其个人身份信息方面的法律、监管和业务义务，并提供履行这些义务的手段。
A.1.3.3	确定 PII 主体的信息	组织应确定并记录向 PII 主体提供的有关其 PII 处理的信息以及提供此类信息的时间。
A.1.3.4	向 PII 负责人提供信息	该组织应向 PII 主体提供清晰易懂的信息，明确 PII 控制者的身份，并描述其 PII 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，使个人身份信息主体能够修改或撤回其同意。
A.1.3.6	提供反对个人身份信息处理的机制	该组织应提供机制，使个人身份信息主体能够反对对其个人身份信息进行处理。
A.1.3.7	访问、更正或删除	组织应实施政策、程序或机制，以履行其对个人身份信息主体访问、更正或删除其个人身份信息的义务。
A.1.3.8	个人身份信息控制者告知第三方的义务	组织应将与共享的个人身份信息（PII）的任何修改、撤回或异议告知已与之共享 PII 的第三方，并实施适当的政策、程序或机制来实现这一点。
A.1.3.9	提供已处理的个人身份信息副本	当 PII 主体提出要求时，组织应能够提供所处理 PII 的副本。
A.1.3.10	处理请求	组织应制定并记录处理和回应来自 PII 负责人的合法请求的政策和程序。
A.1.3.11	自动化决策	该组织应明确其因自身决策而对个人身份信息主体承担的义务，包括法律义务。 与 PII 主体相关的组织，仅基于 PII 的自动化处理，并能够证明其如何履行这些义务。
隐私设计和默认隐私 目标：确保流程和系统的设计使得个人身份信息（PII）的收集和处理（包括使用、披露、保留、传输和处置）仅限于为实现已确定的目的所必需的范围。		
A.1.4.2	限价征收	组织应将个人身份信息的收集限制在与已确定的目的相关的、适度的和必要的最低限度。
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已确定的目的所必需的、充分的、相关的和必要的范围内。
A.1.4.4	准确性和质量	组织应确保并记录个人身份信息在其整个生命周期内，始终保持其准确性、完整性和时效性，以满足处理目的。
A.1.4.5	个人身份信息最小化目标	组织应明确并记录数据最小化目标，以及为实现这些目标而使用的机制（如去标识化）。
A.1.4.6	在处理结束时对个人身份信息进行去标识化和删除。	一旦原始个人身份信息不再用于已确定的目的，组织应立即删除该个人身份信息，或将其转换为无法识别或重新识别个人身份信息主体的形式。
A.1.4.7	临时文件	组织应确保在规定的、有记录的期限内，按照有记录的程序，对因处理个人身份信息而创建的临时文件进行处置（例如，删除或销毁）。
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	处理	组织应有书面政策、程序或机制来处置个人身份信息。
A.1.4.10	PII 传输控制	组织应通过数据传输网络对传输的个人身份信息（例如，发送到其他组织的个人身份信息）采取适当的控制措施，以确保数据到达其预期目的地。
个人身份信息共享、转移和披露 目的：确定是否以及何时根据适用的义务共享、转移到其他司法管辖区或第三方或披露个人身份信息。		
A.1.5.2	确定跨司法管辖区个人身份信息转移的依据	该组织应确定并记录在不同司法管辖区之间转移个人身份信息的相关依据。
A.1.5.3	可将个人身份信息传输至的国家和国际组织	该组织应明确并记录可能将个人身份信息转移至的国家和国际组织。

A.1.5.4	个人身份信息转移记录	该组织应记录向第三方转移或从第三方转移个人身份信息的情况，并确保与这些第三方合作，以支持未来与履行对个人身份信息主体的义务相关的请求。
A.1.5.5	向第三方披露个人身份信息的记录	组织应记录向第三方披露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。

表 A.2—PII 处理器的控制目标和控制措施

收集和处理条件 目的：证明处理是合法的，具有适用司法管辖区的法律依据，并且具有明确定义的合法目的。		
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能够明确组织在协助客户履行义务方面所扮演的角色（考虑到处理的性质和组织可获得的信息）。
A.2.2.3	组织宗旨	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规定的用途。
A.2.2.4	营销和广告用途	未经事先获得相关个人身份信息主体的同意，该机构不得将根据合同处理的个人身份信息用于营销和广告目的。该机构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	如果组织认为处理指令违反了适用的法律要求，则应通知客户。
A.2.2.6	客户义务	该组织应向客户提供适当的信息，以便客户能够证明其已履行其义务。
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，以证明其已履行其在代表客户处理个人身份信息时所承担的义务（如适用合同中所述）。
对 PII 委托人的义务 目标：确保向 PII 主体提供有关其 PII 处理的适当信息，并履行与处理其 PII 相关的任何其他适用义务。		
A.2.3.2	遵守对个人身份信息的义务	该组织应向客户提供履行其与个人身份信息主体相关的义务的手段。
隐私设计和默认隐私 目标：确保流程和系统的设计使得个人身份信息（PII）的收集和处理（包括使用、披露、保留、传输和处置）仅限于为实现已确定的目的所必需的范围。		
A.2.4.2	临时文件	组织应确保在规定的、有记录的期限内，按照有记录的程序，对因处理 PII 而创建的临时文件进行处置（例如，删除或销毁）。
A.2.4.3	退回、转移或处置个人身份信息	该组织应能够以安全的方式退回、转移或处置个人身份信息（PII）。此外，该组织还应向客户提供其相关政策。
A.2.4.4	PII 传输控制	组织应通过数据传输网络对个人身份信息进行适当的控制，以确保数据到达其预期目的地。
个人身份信息共享、转移和披露 目的：确定是否以及何时根据适用的义务共享、转移到其他司法管辖区或第三方，或披露个人身份信息。		
A.2.5.2	司法管辖区间 PLL 转移的依据	组织应及时告知客户在不同司法管辖区之间进行个人身份信息传输的依据以及任何拟议的变更，以便客户可以反对此类变更或终止合同。

A.2.5.3	可将个人身份信息传输至的国家和国际组织	该组织应明确规定并记录可能将个人身份信息转移至的国家和国际组织。
A.2.5.4	向第三方披露个人身份信息的记录	组织应记录向第三方披露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	个人身份信息披露请求通知	对于任何具有法律约束力的个人身份信息披露请求，组织应通知客户。
A.2.5.6	具有法律约束力的个人身份信息披露	本组织应拒绝任何不具有法律约束力的个人身份信息披露请求，在进行任何个人身份信息披露之前应咨询相应的客户，并接受经相应客户授权的任何合同约定的个人身份信息披露请求。
A.2.5.7	披露用于处理个人身份信息的转包商	在使用前，该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	聘请分包商处理个人身份信息	该组织只能按照客户合同的规定，聘请分包商处理个人身份信息。
A.2.5.9	变更处理 PII 的分包商	如获得一般书面授权，该组织应将有关增加或更换处理 PII 的分包商的任何拟议变更告知客户，从而使客户有机会对这些变更提出异议。

表 A.3—PII 控制器和 PII 处理器的控制目标和控制措施

个人身份信息控制器和处理器的安全考量 目的：确保 PII 处理的安全性。		
控制参考	控制标题	控制
A.3.3	信息安全政策	与个人身份信息处理相关的信息安全政策应予以制定、经管理层批准、公布、传达给相关人员和相关利益方并获得其认可，并按计划间隔进行审查，如发生重大变更，则应进行审查。
A.3.4	信息安全角色和职责	与个人身份信息（PII）相关的信息安全角色和职责 应根据组织需要对资金进行定义和分配。
A.3.5	信息分类	信息应根据组织的信息安全需求进行分类，同时考虑到个人身份信息，并基于保密性、完整性、可用性和相关利益方的要求。
A.3.6	信息标签	应根据本组织采用的信息分类方案，制定并实施一套适当的信息标签程序，该程序应考虑个人身份信息（PII）。
A.3.7	信息传递	组织内部以及组织与其他各方之间所有类型的传输设施，都应制定与处理个人身份信息（PII）相关的信息传输规则、程序或协议。
A.3.8	身份管理	应管理与个人身份信息处理相关的身份的整个生命周期。
A.3.9	访问权限	对个人身份信息（PII）和其他与 PII 处理相关的资产的访问权限，应按照组织的特定主题访问控制政策和规则进行提供、审查、修改和删除。
A.3.10	在供应商协议中解决信息安全问题	与个人身份信息处理相关的相关信息安全要求，应根据与供应商关系的类型，与每个供应商共同制定并达成一致。
A.3.11	信息安全事件管理规划和准备	组织应通过定义、建立和沟通事件管理流程、角色和职责，规划和准备管理与个人身份信息处理相关的信息安全事件。
A.3.12	应对信息安全事件	对于与个人身份信息处理相关的信息安全事件，应按照已记录的程序进行应对。

A.3.13	法律、法规、规章和合同要求	与个人身份信息处理相关的信息安全方面的法律、法规、规章和合同要求，以及 组织为满足这些要求所采取的方法，都应记录在案，并且这些文件应保持最新状态。
A.3.14	记录保护	与个人身份信息处理相关的记录应防止丢失。 破坏、伪造、未经授权的访问和未经授权的发布。
A.3.15	信息安全独立审查	组织在个人身份信息处理及其实施方面的信息安全管理方法（包括人员、流程和技术）应按计划间隔进行独立审查，或在发生重大变化时进行审查。
A.3.16	遵守信息安全政策、规则和标准	应定期审查组织的信息安全政策、特定主题政策、规则和标准与个人身份信息处理相关的遵守情况。
A.3.17	信息安全意识、教育和培训	组织人员和相关利益方应接受适当的信息安全意识教育和培训，并定期更新组织的信息安全政策、特定主题政策和程序，这些政策和程序与其工作职能相关，且与个人身份信息处理有关。
A.3.18	保密协议或不披露协议	应确定、记录、定期审查并由员工和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协议或不披露协议。
A.3.19	桌面和屏幕都要清理干净。	应制定并适当执行桌面文件和可移动存储介质的清理规则以及信息处理设施的屏幕清理规则。
A.3.20	存储介质	存储个人身份信息的介质应按照组织的分类方案和处理要求，在其获取、使用、运输和处置的整个生命周期中进行管理。
A.3.21	安全处置或再利用设备	存放个人身份信息（PII）存储介质的设备在处置或重新使用之前，应进行核实，以确保所有敏感数据和许可软件已被删除或安全覆盖。
A.3.22	用户终端设备	存储在用户终端设备上、由用户终端设备处理或通过用户终端设备访问的个人身份信息应受到保护。
A.3.23	安全认证	应根据信息访问限制实施与个人身份信息处理相关的安全认证技术和程序。
A.3.24	信息备份	个人身份信息（PII）的备份副本以及与 PII 处理相关的软件和系统应予以维护并定期测试。
A.3.25	日志记录	应生成、存储、保护和分析记录与个人身份信息处理相关的活动、异常、故障和其他相关事件的日志。
A.3.26	密码学的应用	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	应制定并实施与个人身份信息处理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	在开发或获取应用程序时，应确定、规定和批准与个人身份信息处理相关的信息安全要求。
A.3.29	安全系统架构和工程原则	应制定、记录、维护和应用与处理个人身份信息相关的安全系统工程原则，并将其应用于任何信息系统开发活动。
A.3.30	外包开发	该组织应指导、监督和审查与外包 PII 处理系统开发相关的活动。
A.3.31	测试信息	与个人身份信息处理相关的测试信息应进行适当的选择、保护和管理。

附件 B
（规范性）
PII 控制者与 PII 处理者实施指南

B.1 个人身份信息控制者的实施指南

B.1.1 总则

本条款为 PII 控制者提供 PIMS 指导，与表 A.1 中列出的控制措施有关。

B.1.2 收集和处理的条件

B.1.2.1 目标

为了证明处理是合法的，具有适用司法管辖区的法律依据，并且具有明确定义的合法目的。

B.1.2.2 确定并记录目的

控制

组织应明确并记录处理个人身份信息的具体目的。

实施指南

组织应确保个人身份信息（PII）主体了解其 PII 被处理的目的。组织有责任清晰地记录并向 PII 主体传达此目的。如果没有明确说明处理目的，就无法充分给予同意和选择。

处理个人身份信息（PII）的目的的文档应足够清晰和详细，以便可以作为提供给 PII 主体的信息的一部分（参见 B.1.3.3）。该文档应包含获得同意所需的信息（参见 B.1.2.4），以及政策和程序的文档信息（参见 B.1.2.9）。

其他信息

在部署云计算服务时，ISO/IEC 19944—1 中的分类和定义可以帮助提供描述处理 PII 的目的的术语。

B.1.2.3 确定合法依据

控制

组织应确定、记录并能够证明其处理个人身份信息（PII）用于已确定目的的相关合法依据。

实施指南

有些司法管辖区要求组织能够证明，在进行数据处理之前，数据的合法性已经得到正式确立。

处理个人身份信息的法律依据可以包括：

—获得 PII 主体的同意；

—履行合同；

—遵守法律义务；

—保护 PII 委托人的重大利益；

—为公共利益而执行的任务；

—个人身份信息控制者的合法权益。

组织应记录每项 PII 处理活动的依据（见 B.1.2.9）。

组织的合法利益可以包括信息安全目标，这应与保护个人身份信息主体隐私方面的义务相平衡。

每当根据个人身份信息（PII）的性质（例如健康信息）或相关 PII 主体（例如与儿童有关的 PII）定义特殊类别的 PII 时，组织应将这些类别的 PII 纳入其分类方案中。

属于这些类别的个人身份信息（PII）的分类可能因司法管辖区而异，也可能因适用于不同类型业务的不同监管制度而异，因此组织应了解适用于正在执行的 PII 处理的分类。

特殊类别的个人身份信息（PII）的使用也可能受到更严格的控制。
变更或扩展个人身份信息处理目的可能需要更新或修订法律依据，也可能需要获得个人身份信息主体的额外同意。

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，通过该流程可以证明是否、何时以及如何从 PII 主体处获得了处理 PII 的同意。

实施指南

处理个人身份信息（PII）可能需要获得同意。机构应明确记录何时需要获得同意以及获得同意的要求。将处理目的与是否以及如何获得同意的信息关联起来可能很有帮助。

注意：可能存在法律要求。
某些司法管辖区对如何收集和记录同意有具体要求（例如，不得与其他协议捆绑）。此外，某些类型的数据收集（例如，用于科学研究）以及某些类型的个人身份信息主体（例如儿童）可能需要遵守额外的要求。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

组织应按照已记录的流程获取并记录 PII 主体的同意。

实施指南

组织应以某种方式获得并记录 PII 主体的同意，以便能够根据要求提供所提供同意的详细信息（例如，提供同意的时间、PII 主体的身份和同意声明）。
在同意程序之前向 PII 主体提供的信息应遵循 B.1.3.4 中的指导。
同意书应包含以下内容：
—自愿给予的；
—明确说明处理目的；以及
明确无误。

B.1.2.6 隐私影响评估

控制

每当计划对个人身份信息进行新的处理或对现有的个人身份信息处理进行更改时，组织应评估是否需要进行隐私影响评估，并在适当情况下实施隐私影响评估。

实施指南

个人身份信息（PII）处理会给 PII 主体带来风险。这些风险应通过隐私影响评估进行评估。一些司法管辖区规定了必须进行隐私影响评估的情况。评估标准可能包括：对 PII 主体产生法律影响的自动化决策；大规模处理特殊类别的 PII （例如，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、基因数据或生物识别数据）；或大规模系统性地监控公共区域。

组织应确定完成隐私影响评估所需的要素。这些要素可以包括处理的个人身份信息（PII）类型列表、PII 的存储位置以及可能的传输位置。数据流图和数据地图在此过程中也很有帮助。

注：有关处理 PIL 的记录信息的详细信息，请参阅 B.1.2.9，这些信息可以为隐私影响或其他风险评估提供依据。

其他信息

有关处理个人身份信息（PII）的隐私影响评估的指南可在 ISO/IEC 29134 中找到。

B.1.2.7 与 PII 处理者的合同

控制

该组织应与它使用的任何 PII 处理者签订书面合同，并应确保其与 PII 处理者的合同涵盖表 A.2 中适当控制措施的实施。

实施指南

组织与代表其处理个人身份信息（PII）的任何 PII 处理者之间的合同应要求 PII 处理者实施表 A.2 中规定的适当控制措施，同时考虑信息安全风险评估流程（参见 6.1.2）以及 PII 处理者执行的 PII 处理范围。默认情况下，应假定表 A.2 中规定的所有控制措施均适用。如果组织决定无需 PII 处理者实施表 A.2 中的某项控制措施，则应说明其排除的理由（参见 6.1.3）。

合同可以对各方的责任做出不同的定义，但为了与本文件保持一致，所有控制措施都应予以考虑并纳入文件化信息中。

B.1.2.8 联合 PII 控制器

控制

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

实施指南

处理个人身份信息的角色和职责应以透明的方式确定。

这些角色和职责应在合同或任何类似的具有约束力的文件中予以明确规定，该文件应包含共同处理个人身份信息的条款和条件。在某些司法管辖区，此类协议被称为数据共享协议。

联合个人身份信息控制协议可以包括：

—个人身份信息共享 / 共同个人身份信息控制者关系的目的；

—参与联合 PII 控制者关系的组织（PII 控制者）的身份；

—根据本协议需要共享、转移和处理的个人身份信息类别；

—处理操作概述（例如传输、使用）；

—对各角色和职责的描述；

—负责实施个人身份信息保护的技术和组织安全措施；

—个人身份信息泄露事件中责任的界定（例如，谁将通知、何时通知、相互信息）；

—个人身份信息的保留或处置条款；

—因未履行协议而承担的责任；

—如何履行对 PII 委托人的义务；

—如何向 PII 委托人提供涵盖联合 PII 控制者之间安排实质内容的信息；

—个人身份信息主体如何获取其有权接收的其他信息；以及

—PII 负责人联络点。

B.1.2.9 与处理个人身份信息相关的记录

控制

组织应确定并妥善保管必要的记录，以履行其处理个人身份信息（PII）的义务。

实施指南

组织可以通过编制一份 PII 处理活动清单来保存 PII 处理的相关记录信息。该清单可以包括：

—加工类型；
—处理的目的；
—对 PII 和 PII 主体（例如儿童）的类别进行描述；
—个人身份信息已披露或将要披露的接收者类别，包括第三国或国际组织的接收者；
—对技术和组织安全措施进行总体描述；以及
—一份隐私影响评估报告。
这样的库存清单应该有负责人，负责确保清单的准确性和完整性。

B.1.3 对 PII 委托人的义务

B.1.3.1 目标

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

B.1.3.2 确定和履行对 PII 委托人的义务

控制

该组织应确定并记录其对个人身份信息主体在处理其个人身份信息方面的法律、监管和业务义务，并提供履行这些义务的手段。

实施指南

对个人身份信息主体的义务以及履行这些义务的手段因司法管辖区而异。

组织应确保以便捷、及时的方式提供适当途径，履行对个人身份信息（PII）主体的义务。应向 PII 主体提供清晰的文件，说明其义务的履行程度和方式，并提供最新的联系方式，以便主体提出请求。

联系点应以与收集个人身份信息和同意的方式类似的方式提供（例如，如果通过电子邮件或网站收集个人身份信息，则联系点也应通过电子邮件或网站提供，而不是电话或传真等其他方式）。

B.1.3.3 确定 PII 主体的信息

控制

组织应确定并记录向 PII 主体提供有关其 PII 处理的信息以及提供此类信息的时间。

实施指南

组织应确定向 PII 主体提供信息的法律、监管或业务要求（例如，在处理之前、在收到请求后的一定时间内），以及要提供的信息类型。

根据具体要求，这些信息可以以通知的形式提供。可提供给个人身份信息主体的信息类型示例包括：

—关于处理目的的信息（见 B.1.2.2）；
—个人身份信息控制者或其代表的联系方式；
—处理的法律依据信息（见 B.1.2.3）；
—如果个人身份信息并非直接从个人身份信息主体处获得，则需提供该信息获取途径的信息；

—提供个人身份信息是否为法定要求或合同要求的信息，以及在适当情况下，不提供个人身份信息的可能后果；
—根据 B.1.3.2 确定的对 PII 主体的义务的信息，以及 PII 主体如何从中受益，特别是关于访问、修改、更正、请求删除、接收其 PII 的副本以及反对处理；
—关于 PII 主体如何撤回同意的信息（见 B.1.3.5)；
—关于个人身份信息转移的信息；
—关于个人身份信息接收者或接收者类别的信息；
—关于个人身份信息保留期限的信息；
—关于基于个人身份信息自动处理的自动决策的使用信息；
—有关投诉权利以及如何提出投诉的信息；
—有关提供信息的频率的信息（例如“及时”通知、组织定义的频率）。

如果处理个人身份信息的目的发生变更或扩展，组织应提供更新信息。

B.1.3.4 向 PII 负责人提供信息

控制

该组织应向 PII 主体提供清晰易懂的信息，明确 PII 控制者的身份，并描述其 PII 的处理方式。

实施指南

该组织应以及时、简洁、B.1.3.3 中详述的信息，并根据完整、透明、易懂和易于获取的形式，使用清晰简洁的语言，向 PII 委托人提供目标受众的需要使用清晰简洁的语言。

在适当情况下，应在收集个人身份信息时提供相关信息，并且这些信息应永久可访问。

注意：图标和图像可以通过提供预期处理的视觉概览来帮助 PII 主体。

B.1.3.5 提供修改或撤回同意的机制

控制

该组织应提供一种机制，使个人身份信息主体能够修改或撤回其同意。

实施指南

组织应告知个人身份信息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），并提供相应的撤回机制。撤回机制取决于系统；应尽可能与获取同意的机制保持一致。例如，如果同意是通过电子邮件或网站收集的，则撤回机制也应相同，而不应采用电话或传真等其他方式。

修改同意可以包括对个人身份信息（PII）的处理施加限制，在某些情况下，这可以包括限制 PII 控制者删除 PII。

某些司法管辖区对个人身份信息主体何时以及如何修改或撤回其同意施加了限制。

组织应以与记录同意本身类似的方式记录任何撤回或更改同意的请求。

任何同意变更都应通过适当的系统传达给授权用户和相关第三方。

组织应制定响应时间，并按照该时间处理请求。

附加信息

当特定 PII 处理的同意被撤回时，撤回前进行的所有 PI 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 提供反对个人身份信息处理的机制

控制

该组织应提供一种机制，使个人身份信息主体能够反对对其个人身份信息进行处理。

实施指南

某些司法管辖区赋予个人身份信息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约束的组织应能够证明其如何确保保留行使该权利的个人身份信息主体的记录。

组织应记录与个人身份信息主体对处理提出异议相关的法律和监管要求（例如，反对将个人身份信息用于直接营销目的）。组织应向主体提供有关在这些情况下提出异议的信息。提出异议的机制可能有所不同，但应与所提供的服务类型保持一致（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

组织应实施政策、程序或机制，以履行其对个人身份信息主体访问、更正或删除其个人身份信息的义务。

实施指南

组织应实施相关政策、程序或机制，使个人身份信息主体能够在提出请求时及时、无故拖延地获取、更正和删除其个人身份信息。

组织应制定响应时间，并按照该时间处理请求。

任何更正或删除都应通过系统或授权用户进行传播，并应传递给已将个人身份信息转移给的第三方（参见 B.1.3.8）。

注：B.1.5.4 中规定的控制所生成的文档信息在这方面会有所帮助。

当个人身份信息主体对数据的准确性或更正提出异议时，组织应制定相应的政策、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已进行的更改，以及无法进行更正的原因（如适用）。

某些司法管辖区对个人身份信息主体何时以及如何请求更正或删除其个人身份信息施加了限制。组织应密切关注此类限制。

B.1.3.8 个人身份信息控制者告知第三方的义务

控制

组织应将与共享的个人身份信息（PII）的任何修改、撤回或异议告知已与之共享 PII 的第三方，并实施适当的政策、程序或机制来做到这一点。

实施指南

组织应根据现有技术采取适当措施，将任何关于共享个人身份信息的修改、撤回或异议告知第三方。

组织应建立并维护与第三方之间的有效沟通渠道。相关职责可分配给负责渠道运营和维护的人员。在向第三方发布信息时，组织应监控其对信息接收情况的确认。

注意：因对 PII 主体的义务而产生的变更可能包括修改或撤回同意、请求更正、删除或限制处理，或 PII 主体要求对 PII 的处理提出异议。

B.1.3.9 提供已处理的个人身份信息副本

控制

当个人身份信息主体提出要求时，该组织应该能够提供所处理的个人身份信息的副本。

实施指南

组织应提供一份以结构化、常用格式处理的 PII 副本，以便 PII 主体可以访问。

有些司法管辖区规定了组织应向 PII 主体或接收方 PII 控制者提供以可移植格式处理的 PII 副本的情况（通常是结构化的、常用的和机器可读的）。

组织应确保提供给个人身份信息主体的任何个人身份信息副本都与该个人身份信息主体密切相关。

如果根据保留和处置政策（如 B.1.4.8 所述）请求的 PII 已被删除，则 PII 控制者应通知 PII 主体请求的 PII 已被删除。

如果组织无法再识别个人身份信息主体（例如，由于去标识化流程），则组织不应仅为实施此控制措施而寻求（重新）识别个人身份信息主体。但是，在某些司法管辖区，合法请求可能需要向个人身份信息主体索取额外信息，以便重新识别并进行后续披露。

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

B.1.3.10 处理请求

控制

组织应制定并记录处理和回应 PII 主体合法请求的政策和程序。

实施指南

合法请求可以包括索取已处理的个人身份信息副本的请求，或者提出投诉的请求。
有些司法管辖区允许组织在特定情况下收取费用（例如，过多的或重复的请求）。

请求应在规定的响应时间内处理。
某些司法管辖区会根据请求的复杂性和数量，以及告知个人身份信息主体任何延迟情况的要求，规定响应时间。适当的响应时间应在隐私政策中明确规定。

B.1.3.11 自动化决策

控制

该组织应明确其对个人身份信息主体承担的义务（包括法律义务），这些义务源于该组织基于对个人身份信息的自动化处理而做出的与个人身份信息主体相关的决定，并且该组织应能够证明其如何履行这些义务。

实施指南

有些司法管辖区规定，当仅基于 PII 的自动化处理做出的决定对 PII 主体产生重大影响时，应向 PII 主体规定具体的义务，例如通知其存在自动化决策、允许 PII 主体反对此类决策，或寻求人工干预。

注意：在某些司法管辖区，某些知识产权的处理无法完全自动化。
在这些司法管辖区运营的组织应该能够证明他们是如何考虑到遵守这些义务的。

B.1.4 隐私设计和默认隐私

B.1.4.1 目标

确保流程和系统的设计使得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）仅限于为实现已确定的目的所必需的范围。

B.1.4.2 限制征收

控制

组织应将个人身份信息的收集限制在与已确定的目的相关的、适度的和必要的最低限度。

实施指南

组织应将个人身份信息（PII）的收集限制在与已确定的目的相关的、充分的、必要的范围内。这包括限制组织间接收集的 PII 的数量（例如，通过网络日志、系统日志）。
默认隐私意味着，在收集和处理个人身份信息（PII）的过程中，如果存在任何可选性，则每个选项都应默认禁用，并且只有在 PII 主体明确选择的情况下才能启用。

B.1.4.3 限制处理

控制

组织应将个人身份信息的处理限制在为已确定的目的所必需、相关和充分的范围内。

实施指南

限制 PII 的处理应通过信息安全和隐私政策（见 5.2）以及记录在案的采用和遵守程序来管理。

个人身份信息（PII）的处理应默认限制在与已确定目的相关的最低必要范围内。此类处理包括：
—信息披露；
—个人身份信息存储期限；以及
—谁可以访问他们的个人身份信息。

B.1.4.4 准确性和质量

控制

组织应确保并记录个人身份信息在其整个生命周期内，对于其处理目的而言，其准确性、完整性和时效性均达到必要水平。

实施指南

组织应实施相关政策、程序或机制，以最大程度地减少其处理的个人身份信息（PII）中的不准确情况。此外，还应制定相应的政策、程序或机制来应对不准确的 PII 情况。这些政策、程序或机制应纳入文档

化信息（例如，通过技术系统配置），并适用于 PII 的整个生命周期。

附加信息

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

B.1.4.5 个人身份信息最小化目标

控制

组织应明确并记录数据最小化目标，以及为实现这些目标而使用的机制（例如去标识化）。

实施指南

组织应明确如何限制所收集和处理的具体个人身份信息（PII）及其数量，使其与既定目的相符。这可以包括使用去标识化或其他数据最小化技术。

已确定的目的（见 B.1.2.2）可能需要处理尚未去标识化的 PII，在这种情况下，组织应该能够描述这种处理。

在其他情况下，已确定的目的并不需要处理原始个人身份信息（PII），处理已去标识化的 PII 即可达到该目的。在这些情况下，组织应明确并记录 PII 与 PII 主体关联的程度，以及为实现去标识化和 PII 最小化目标而设计的处理机制和技术。

用于最大限度减少个人身份信息（PII）的机制因处理类型和处理系统而异。组织应记录用于实施数据最小化的任何机制（例如，技术系统配置）。

如果处理去标识化数据足以达到预期目的，则组织应记录所有旨在及时实施其设定的去标识化目标的机制（例如技术系统配置）。例如，移除与个人身份信息主体相关的属性可能足以使组织实现其既定目标。在其他情况下，可以使用其他去标识化技术，例如概括化（例如四舍五入）或随机化技术（例如添加噪声），以达到足够的去标识化水平。

注 1 有关去标识化技术的更多信息，请参阅 ISO/IEC 20889。
注 2 对于云计算，ISO/IEC 19944—1 提供了数据标识限定符的定义，可用于对数据识别 PII 主体或将 PII 主体与 PII 中的一组特征关联起来的程度进行分类。

B.1.4.6 处理结束时的个人身份信息去标识化和删除

控制

一旦原始PII不再需要用于已确定的目的,组织就应该删除PII或将其转换为不允许识别或重新识别PII主体的形式。

实施指南

组织应建立机制，在预计不再进行进一步处理时删除个人身份信息（PII）。或者，可以使用一些去标识化技术，只要由此产生的去标识化数据不能合理地允许重新识别 PII 主体即可。

B.1.4.7 临时文件

控制

组织应确保在规定的、有记录的期限内，按照有记录的程序，对因处理个人身份信息而创建的临时文件进行处置（例如，删除或销毁）。

实施指南

组织应定期检查未使用的临时文件是否在规定的时间内被删除。

其他信息

信息系统在正常运行过程中会创建临时文件。这些文件特定于某个系统或应用程序，但可能包括文件系统回滚日志以及与数据库更新和其他应用程序软件运行相关的临时文件。相关信息处理任务完成后，这些临时文件不再需要，但在某些情况下，它们无法被删除。这些文件的使用时长并非总是确定的，但“垃圾回收”程序应能识别相关文件并确定它们上次使用至今的时间。

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

组织应制定并维护信息保留期限表，并考虑到个人身份信息（PII）的保留期限不得超过必要期限。此类期限表应兼顾法律、监管和业务要求。如果这些要求相互冲突，则应根据风险评估做出业务决策，并将该决策记录在相应的期限表中。

B.1.4.9 处置

控制

组织应制定书面政策、程序或机制来处置个人身份信息。

实施指南

个人身份信息（PII）处置技术的选择取决于多种因素，因为不同的处置技术在特性和结果上存在差异（例如，最终物理介质的粒度，或从电子介质中恢复已删除信息的能力）。选择合适的处置技术时需要考虑的因素包括但不限于：待处置 PII 的性质和范围、PII 是否包含元数据，以及存储 PII 的介质的物理特性。

B.1.4.10PII 变速器控制

控制

组织应将通过数据传输网络传输（例如，发送到其他组织）的个人身份信息（PII）置于适当的控制之下，以确保数据到达其预期目的地。

实施指南

个人身份信息的传输应受到控制，通常的做法是确保只有授权人员才能访问传输系统，并遵循适当的流程（包括保留审计日志），以确保个人身份信息在不泄露的情况下传输给正确的接收者。

B.1.5 个人身份信息共享、转移和披露

B.1.5.1 目标

确定是否以及何时共享、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。

B.1.5.2 确定跨司法管辖区个人身份信息转移的依据

控制

该组织应确定并记录在不同司法管辖区之间转移个人身份信息的相关依据。

实施指南

个人身份信息（PII）的传输可能受法律法规的约束，具体取决于数据传输至的司法管辖区或国际组织（以及数据来源地）。组织应以符合此类要求为依据进行数据传输，并应提供相关证明文件。

某些司法管辖区可能要求信息传输协议须经指定监管机构审查。在这些司法管辖区开展业务的组织应注意此类要求。

注意：如果转账发生在特定司法管辖区内，则对汇款人和收款人适用的法律要求相同。

B.1.5.3 个人身份信息可转移至的国家和国际组织

控制

该组织应明确规定并记录可能将个人身份信息传输到的国家和国际组织。

实施指南

应向客户提供在正常运营过程中可能将个人身份信息（PII）传输至的国家和国际组织的身份信息。
ISO/IEC 27701:2025(en)

应将外包个人身份信息处理纳入考虑范围。所涵盖的国家 / 地区应参照 B.1.5.2 条款进行考量。

在正常操作之外，可能会出现应法律机关要求进行转移的情况，但事先无法确定涉及国家的身份，或者适用司法管辖区可能禁止此类转移，以维护执法调查的机密性（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

控制

该组织应记录向第三方转移或从第三方转移个人身份信息的情况，并确保与这些第三方合作，以支持未来与履行对个人身份信息主体的义务相关的请求。

实施指南

记录可能包括从第三方传输因 PII 控制者履行其义务而修改的 PII，或者传输给第三方以执行 PII 主体的合法请求，包括删除 PII 的请求（例如，在撤回同意后）。
组织应制定政策，明确这些记录的保存期限。
该组织应在转账记录中应用数据最小化原则，仅保留绝对必要的信息。

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，个人身份信息（PII）可能会被披露。这些披露应当记录在案。任何其他向第三方

披露的信息，例如因法律调查或外部审计而产生的披露，也应当记录在案。记录应包括披露来源以及披露授权来源。

B.2 个人身份信息处理者的实施指南

B.2.1 总则

本条款为PII处理者提供PIMS指导，与表A.2中列出的控制措施有关。

B.2.2 收集和处理的条件

B.2.2.1 目标

为了证明处理是合法的，具有适用司法管辖区的法律依据，并且具有明确定义的合法目的。

B.2.2.2 客户协议

控制

该组织应确保在相关情况下，处理个人身份信息（PII）的合同能够体现该组织在协助客户履行义务方面的作用（考虑到处理的性质和该组织可获得的信息）。

实施指南

组织与客户之间的合同应包含以下方面（如适用），具体取决于客户的角色（即个人身份信息控制者或个人身份信息处理者）：

—设计和隐私保护（参见B.1.4和B.2.4）；
—实现处理安全；
—向监管机构通报涉及个人身份信息的违规行为；
—向客户和PII委托人通知涉及PII的违规行为；
—进行隐私影响评估；以及
—如果需要事先与相关的个人身份信息保护机构进行磋商，个人身份信息处理者保证提供协助。

某些司法管辖区要求合同包含处理的主题和期限、处理的性质和目的、PII的类型以及PII主体的类别。

B.2.2.3 组织的宗旨

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规定的用途。

实施指南

组织与客户之间的合同应包括但不限于服务的目标和时间框架。

为了实现客户的目标，有时出于技术原因，组织可以根据客户的一般指示（即使没有客户的明确指示）来确定处理个人身份信息（PII）的方法。例如，为了有效利用网络或处理能力，可能需要根据PII主体的某些特征分配特定的处理资源。

组织应允许客户验证其是否符合用途规范和限制原则。这也能确保组织及其任何分包商不会将个人身份信息用于客户书面指示之外的其他用途。

B.2.2.4 市场营销和广告用途

控制

未经事先获得相关个人身份信息主体的同意，机构不得将根据合同处理的个人身份信息用于营销和广告

目的。机构不应将提供此类同意作为接受服务的条件。

实施指南

应记录 PII 处理者是否遵守客户的合同要求，尤其是在计划进行营销或广告活动的情况下。

组织不应坚持将个人身份信息用于营销或广告用途，除非已获得个人身份信息主体的明确同意。

注：本控制是对 B.2.2.3 中更一般控制的补充，而不是取代或凌驾于其之上。

B.2.2.5 侵权指令

控制

如果组织认为处理指令违反了适用的法律要求，则应告知客户。

实施指南

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

B.2.2.6 客户义务

控制

该组织应向客户提供适当的信息，以便客户能够证明其已履行义务。

实施指南

客户需要的信息可能包括：该组织是否允许并配合客户或客户授权或同意的其他审计师进行的审计。

B.2.2.7 与处理个人身份信息相关的记录

控制

组织应确定并保存必要的记录，以证明其已履行代表客户处理个人身份信息 (PII) 的义务（如适用合同中所述）。

实施指南

某些司法管辖区可能要求组织记录以下信息：

—代表每位客户进行的处理类别；

—向第三国或国际组织转移资金；以及

—对技术和组织安全措施的总体描述。

B.2.3 对 PII 委托人的义务

B.2.3.1 目标

确保向个人身份信息主体提供有关其个人身份信息处理的适当信息，并履行与个人身份信息处理相关的任何其他适用义务。

B.2.3.2 履行对 PII 委托人的义务

控制

该组织应向客户提供履行其与个人身份信息主体相关的义务的途径。

实施指南

个人身份信息控制者的义务可以由法律要求或合同规定。这些义务可能包括客户使用该组织提供的服务来履行这些义务的情况。例如，这可能包括及时更正或删除个人身份信息。

如果客户依赖组织提供信息或技术措施来履行对 PII 主体的义务，则应在合同中明确规定相关信息或技术措施。

B.2.4 隐私设计和默认隐私

B.2.4.1 目标

确保流程和系统的设计使得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）仅限于为实现已确定的目的所必需的范围。

B.2.4.2 临时文件

控制

组织应确保在规定的、有记录的期限内，按照有记录的程序，对因处理个人身份信息而创建的临时文件进行处置（例如，删除或销毁）。

实施指南

组织应定期核查未使用的临时文件是否在规定的时间内被删除。

其他信息

信息系统在正常运行过程中会创建临时文件。这些文件特定于某个系统或应用程序，但可能包括文件系统回滚日志以及与数据库更新和其他应用程序软件运行相关的临时文件。相关信息处理任务完成后，这些临时文件不再需要，但在某些情况下，它们无法被删除。这些文件的使用时长并非总是确定的，但“垃圾回收”程序应能识别相关文件并确定它们上次使用至今的时间。

B.2.4.3 个人身份信息的返还、转移或处置

控制

组织应能够以安全的方式退回、转移或处置个人身份信息（PII）。此外，组织还应向客户提供其相关政策。

实施指南

在某些特定时刻，以某种方式处理 PII 可能是必要的。这可能包括将 PII 返还给客户、将其转移至另一组织或 PII 控制器(例如因合并所致)、删除或以其他方式销毁它、进行去标识化处理或归档。对 PII 的返还、转移或处理能力应通过安全的方式进行管理。

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)在被认为不再对客户所确定的目的具有必要性的情况下，被从存储的任何位置(包括用于备份和业务连续性之目的)彻底删除(由该组织及其任何分包商负责执行)。

组织应制定并实施关于 PII 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 PII 处置前的保留期限，以防止客户因合同意外终止而失去 PI 信息。

注:本控制与指导原则同样适用于保留原则(参见 B.1.4.8)。

B.2.4.4PII 变速器控制

控制
组织应通过数据传输网络对个人身份信息进行适当的控制，以确保数据到达其预期目的地。

实施指南

个人身份信息（PII）的传输应受到控制，通常的做法是确保只有授权人员才能访问传输系统，并遵循适当的流程（包括保留审计数据），以确保 PII 在传输过程中安全无损地送达正确的接收方。传输控制要求可以纳入 PII 处理者与客户之间的合同中。

如果没有与传输相关的合同要求，则可以在传输前征求客户的意见。

B.2.5 个人身份信息共享、转移和披露

B.2.5.1 目标

确定是否以及何时共享、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。

B.2.5.2 跨司法管辖区个人身份信息转移的依据

控制

组织应及时告知客户在不同司法管辖区之间进行个人身份信息（PII）传输的依据以及任何拟议的变更，以便客户可以反对此类变更或终止合同。

实施指南
在不同司法管辖区之间传输个人身份信息（PII）可能需要遵守法律规定，具体取决于 PII 的接收司法管辖区或组织（以及 PII 的来源地）。组织应记录其符合这些规定的情况，以此作为传输的依据。

组织应告知客户任何个人身份信息（PII）的转移情况，包括转移至：

—供应商；
—其他各方；
—其他国家或国际组织。
如有变更，组织应按照约定的时间提前通知客户，以便客户能够对这些变更提出异议或终止合同。

组织与客户之间的协议可以包含允许组织在不通知客户的情况下进行变更的条款。在这种情况下，应设定此项权限的限制（例如，组织可以在不通知客户的情况下更换供应商，但不能将个人身份信息转移到其他国家）。

如果涉及个人身份信息（PII）的国际传输，则应明确是否存在示范合同条款、具有约束力的公司规则或跨境隐私规则等协议，以及涉及的国家和适用此类协议的情况。

B.2.5.3 个人身份信息可转移至的国家和国际组织

控制
该组织应明确规定并记录可能将个人身份信息传输到的国家和国际组织。

实施指南

在正常运营中可能将个人身份信息（PII）传输至的国家和国际组织的身份信息应提供给客户。因使用外包 PII 处理而产生的国家 / 地区的身份信息也应包括在内。所包含的国家 / 地区应根据 B.2.5.2 进行考虑。

在正常操作之外，可能会出现应法律机关要求进行转移的情况，但事先无法确定涉及国家的身份，或者适用司法管辖区可能禁止此类转移，以维护执法调查的机密性（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

控制

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，个人身份信息（PII）可能会被披露。这些披露应当记录在案。任何其他向第三方披露的信息，例如因法律调查或外部审计而产生的披露，也应当记录在案。记录应包括披露来源以及披露授权来源。

B.2.5.5 个人身份信息披露请求的通知

控制

组织应将任何具有法律约束力的个人身份信息披露请求通知客户。

实施指南

组织可能会收到具有法律约束力的个人身份信息披露请求（例如，来自执法机构的请求）。在这种情况下，组织应在约定的时间内，按照约定的程序（可纳入客户合同）通知客户此类请求。

在某些情况下，具有法律约束力的要求包括禁止组织向任何人透露事件信息。例如，刑法中为维护法律调查的保密性而禁止披露信息的情况就属于此类。

B.2.5.6 具有法律约束力的个人身份信息披露

控制

组织应拒绝任何不具有法律约束力的个人身份信息披露请求，在进行任何个人身份信息披露之前咨询相应的客户，并接受任何经相应客户授权的、合同约定的个人身份信息披露请求。

实施指南

与控制措施实施相关的细节可以包含在客户合同中。

此类请求可能来自多个来源，包括法院、仲裁机构和行政机关。它们可以来自任何司法管辖区。

B.2.5.7 披露用于处理个人身份信息的转包商

控制

在使用前，该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。

实施指南

客户合同中应包含关于使用分包商处理个人身份信息的条款。

披露的信息应包括使用分包的事实以及相关分包商的名称。披露的信息还应包括分包商可以向其传输数据的国家和国际组织（参见 B.2.5.3），以及分包商履行或超越该组织义务的方式（参见 B.2.5.8）。

如果评估认为公开分包商信息会增加超出可接受范围的安全风险，则应在签订保密协议或应客户要求的情况下进行披露。应告知客户该信息已公开。

这并不涉及个人身份信息（PII）可传输的国家 / 地区列表。在任何情况下，都应以客户能够通知相关 PII 主体的方式向客户披露此列表。

B.2.5.8 聘用分包商处理个人身份信息

控制

组织应仅根据客户合同聘用分包商处理个人身份信息。

实施指南

如果机构将部分或全部个人身份信息（PII）处理工作外包给其他机构，则在分包商处理 PII 之前，必须获得客户的书面授权。该授权可以以客户合同中的相应条款形式存在，也可以是单独的“一次性”协议。

该组织应与其委托处理个人身份信息（PII）的任何分包商签订书面合同。该组织应确保其与分包商签订的合同涵盖表 A 中 2. 中适当控制措施的实施。

组织与任何代表其处理个人身份信息（PII）的分包商之间的合同应要求分包商实施表 A.2 中规定的适当控制措施，同时考虑信息安全风险评估流程（参见 6.1.2）以及 PII 处理者执行的 PII 处理范围。默认情况下，应假定表 A.2 中规定的所有控制措施均适用。如果组织决定不要求分包商实施表 A.2 中的某项控制措施，则应说明排除该控制措施的理由。合同可以对各方的责任做出不同的规定，但为了与本文件保持一致，所有控制措施都应予以考虑并纳入文件化信息中。

B.2.5.9 变更处理 PII 的分包商

控制

如果获得一般书面授权，组织应将有关增加或更换处理 PII 的分包商的任何拟议变更告知客户，从而使客户有机会对这些变更提出异议。

实施指南

如果组织变更了部分或全部个人身份信息（PII）处理外包的组织，则在新的外包商处理 PII 之前，必须获得客户的书面授权。该授权可以采用客户合同中的相应条款或单独的“一次性”协议的形式。

B.3 个人身份信息控制器和个人身份信息处理器的实施指南

B.3.1 目标

确保个人身份信息处理的安全性。

B.3.2 总则

本条款为 PII 控制者和 PII 处理者提供 PIMS 指导，涉及表 A.3 中列出的控制措施。除非表 A.3 中的具体规定另有规定，或组织另有决定，否则相同的指导适用于 PII 控制者和 PII 处理者。

B.3.3 信息安全政策

控制

与个人身份信息处理相关的信息安全政策应予以制定、管理层批准、公布、传达给相关人员和相关利益方并获得其认可，并按计划定期审查，如发生重大变更，则应进行审查。

实施指南

无论是通过制定单独的隐私政策，还是通过加强信息安全政策，该组织都应发表声明，表明其支持并致力于遵守适用于个人身份信息保护的法律要求，以及该组织与其合作伙伴、分包商和适用的第三方（客户、供应商等）之间达成的合同条款，这些条款应明确划分各方之间的责任。

任何处理个人身份信息的组织，无论是个人身份信息控制者还是个人身份信息处理者，在制定和维护信息安全策略时，都应考虑适用于个人身份信息保护的法律要求。

B.3.4 信息安全角色和职责

控制

应根据组织需要，明确和分配与个人身份信息处理相关的信息安全角色和职责。

实施指南

该组织应指定一个联系人，供客户就 PII 的处理事宜使用。当该组织是 PII 控制者时，应为 PII 主体指定一个联系人，就其 PII 的处理事宜使用（参见 B.1.3.4）。

组织应指定一名或多名人员负责制定、实施、维护和监督全组织的治理和隐私计划，以确保遵守有关处理个人身份信息的所有适用法律要求。

负责人应在适当情况下：

—保持独立性，直接向组织内适当的管理层汇报，以确保有效管理隐私风险；

—参与处理与个人身份信息处理相关的所有问题的管理；

—精通数据保护法律、法规和实践；

—作为与监管机构的联络点；

—告知组织高层管理人员和员工其在处理个人身份信息方面的义务；

—为组织开展的隐私影响评估提供建议。

注：某些司法管辖区将此人称为数据保护官。各司法管辖区对何时需要设立此职位、其职位和职责均有明确规定。此职位可由内部员工担任，也可外包。

B.3.5 信息分类

控制

信息应根据组织的信息安全需求进行分类，同时考虑到个人身份信息，并基于保密性、完整性、可用性和相关利益方的要求。

实施指南

组织的信息分类方案应明确将个人身份信息（PII）纳入其实施范围。在整体分类方案中考虑 PII，对于理解组织处理哪些 PII（例如，类型、特殊类别）、这些 PII 的存储位置以及它们可能流经的系统至关重要。

B.3.6 信息标注

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签程序，该程序应考虑个人身份信息。

实施指南

该组织应确保其控制下的人员了解 PII 的定义以及如何识别 PII 信息。

B.3.7 信息传递

控制

组织内部以及组织与其他各方之间所有类型的传输设施都应制定与处理个人身份信息（PII）相关的信息传输规则、程序或协议。

实施指南

该组织应考虑采取相应措施，确保与处理个人身份信息相关的规则在系统内外得到执行（如适用）。

B.3.8 身份管理

控制

应管理与个人身份信息处理相关的身份的整个生命周期。

实施指南

对于管理或运营处理个人身份信息（PII）的系统和服务的用户，其注册和注销程序应解决用户访问控制受到损害的情况，例如密码或其他用户注册数据损坏或泄露（例如，由于无意泄露）。

对于处理个人身份信息（PII）的系统和服务，组织不应向用户重新发放任何已停用或过期的用户 ID。

如果机构以服务形式提供个人身份信息（PII）处理，则客户可能负责用户 ID 管理的部分或全部工作。此类情况应记录在案。

某些司法管辖区对处理个人身份信息（PII）的系统未使用的身份验证凭证的检查频率有具体要求。在这些司法管辖区运营的组织应考虑遵守这些要求。

B.3.9 访问权限

控制

对个人身份信息（PII）和其他与 PII 处理相关的资产的访问权限应根据组织的特定主题访问控制政策和规则进行配置、审查、修改和删除。

实施指南

组织应维护一份准确、最新的用户配置文件记录，该记录包含已获授权访问信息系统及其中所含个人身

份信息（PII）的用户配置文件。每个配置文件都包含有关用户的数据集，包括用户 ID，这些数据对于实施已确定的、提供授权访问的技术控制措施至关重要。

实施个人用户访问 ID 可以让配置合适的系统识别出哪些人访问了个人身份信息（PII），以及他们进行了哪些添加、删除或更改。这不仅保护了组织，也保护了用户，因为他们可以识别自己处理过哪些信息，以及未处理过哪些信息。

如果机构以服务形式提供个人身份信息（PII）处理，则客户可能负责部分或全部访问管理工作。在适当情况下，机构应向客户提供执行访问管理的手段，例如授予其管理或终止访问权限的权限。此类情况应记录在案。

B.3.10 供应商协议中的信息安全问题

控制

应根据与供应商的关系类型，与每个供应商建立并商定与个人身份信息处理相关的信息安全要求。

实施指南

该组织应在与供应商的协议中明确规定是否处理个人身份信息，以及供应商为使该组织履行其技术和组织措施（参见信息安全和个人身份信息保护义务而必须满足的最低 B.1.2.7 和 B.2.2.2）。

供应商协议应明确划分组织、其合作伙伴、其供应商及其相关第三方（客户、供应商等）之间的责任，同时考虑到处理的个人身份信息的类型。

组织与其供应商之间的协议应建立一种机制，以确保组织支持并管理所有适用法律要求的合规性。协议应要求进行客户认可的、经独立审计的合规性检查。

注：就此类审核而言，可以考虑是否符合相关适用的安全标准，例如 ISO/IEC 27001。

如果组织的角色是个人身份信息（PII）处理者，则该组织应在与任何供应商的合同中明确规定，PII 只能按照其指示进行处理。

B.3.11 信息安全事件管理规划和准备

控制

组织应通过定义、建立和沟通事件管理流程、角色和职责，来规划和准备管理与个人身份信息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，组织应制定识别和记录个人身份信息（PII）泄露事件的责任和程序。此外，组织还应制定与通知相关方 PII 泄露事件（包括通知时间）以及向有关当局披露信息相关的责任和程序，并应考虑适用的法律要求。

某些司法管辖区对违规应对措施（包括通知）制定了具体规定。在这些司法管辖区运营的组织应确保了解这些规定，并记录其如何遵守这些规定。

B.3.12 信息安全事件应对

控制

对于与个人身份信息处理相关的信息安全事件，应按照已记录的程序进行应对。

个人身份信息控制者的实施指南

涉及个人身份信息的事件应触发组织进行审查，作为其信息安全事件管理流程的一部分，以确定是否发生了需要采取应对措施的涉及个人身份信息的泄露事件。
事件本身并不一定会导致此类审查。

注 1：信息安全事件并不一定会导致实际发生或极有可能发生未经授权访问个人身份信息（PII）或组织内存储 PII 的任何设备或设施的情况。这些事件包括但不限于：对防火墙或边缘服务器的 ping 和其他广播攻击、端口扫描、登录失败尝试、拒绝服务攻击和数据包嗅探。
当发生个人身份信息泄露事件时，应对程序应包括相关通知和记录。
有些司法管辖区规定了在哪些情况下应将违规行为通知相关监管机构，以及在哪些情况下应将违规行为通知个人身份信息主体。

通知内容应清晰明了。

注 2 通知可以包含以下详细信息：
—可获取更多信息的联系点；
—对违规行为及其可能造成的后果进行描述；
—对违规行为的描述，包括涉及的个人人数以及涉及的记录数量；

已采取或计划采取的措施。

注 3 有关安全事件管理的信息可在 ISO/IEC 27035 系列中找到。
如果发生涉及个人身份信息泄露事件，应保存包含足够信息的记录，以便为监管或取证目的提供报告，例如：
—对事件的描述；
—时间段；
—事件的后果；
—记者的姓名；
—向谁报告了这起事件；
—为解决该事件所采取的措施（包括负责人和已恢复的数据）；
—该事件导致个人身份信息不可用、丢失、泄露或更改。

如果发生涉及个人身份信息（PII）的泄露事件，记录中还应包含被泄露 PII 的描述（如果已知）。如果使用了通知机制，还应记录通知 PII 主体、监管机构或客户的具体步骤。

个人身份信息处理者的实施指南

关于涉及个人身份信息（PII）泄露事件的通知条款应纳入机构与客户之间的合同。合同应明确规定机构将如何向客户提供履行其通知相关机构义务所需的信息。此通知义务不适用于由客户或 PII 主体自身或其负责的系统组件造成的泄露事件。合同还应明确规定通知响应时间的预期时限和外部强制规定的时限。

在某些司法管辖区，PII 处理者应在发现违规行为后立即通知 PII 控制者，以便 PII 控制者采取适当的措施。

如果发生涉及个人身份信息泄露事件，应保存包含足够信息的记录，以便为监管或取证目的提供报告，例如：

—对事件的描述；
—时间段；
—事件的后果；
—记者的姓名；
—向谁报告了这起事件；
—为解决该事件所采取的措施（包括负责人和已恢复的数据）；
—该事件导致个人身份信息不可用、丢失、泄露或更改。

如果发生涉及个人身份信息泄露事件，记录还应包括被泄露的个人身份信息的描述（如果已知）；以及如果使用了通知，则应包括通知客户或监管机构所采取的步骤。
在某些司法管辖区，适用的法律要求可能要求组织直接通知适当的监管机构（例如，PII 保护机构）有关 PII 泄露事件。

B.3.13 法律、法规、规章和合同要求

控制

与个人身份信息处理相关的信息安全方面的法律、法规、规章和合同要求，以及组织为满足这些要求而采取的方法，都应该记录在案，并且这些文件应该保持最新状态。

实施指南

该组织应确定与处理个人身份信息相关的任何潜在法律制裁（可能是由于未履行某些义务而导致的），包括当地监管机构直接处以的巨额罚款。

在某些司法管辖区，诸如此类的国际标准可作为组织与客户之间合同的基础，明确双方各自的安全、隐私和个人身份信息（PII）保护责任。合同条款可为违反这些责任的情况提供合同制裁依据。

B.3.14 记录保护

控制

与个人身份信息处理相关的记录应防止丢失、销毁、篡改、未经授权的访问和未经授权的泄露。

实施指南

可能需要对当前和历史政策和程序进行审查（例如，在客户纠纷解决和监管机构调查的情况下）。

该组织应按照其保留计划中规定的期限保留其隐私政策及相关程序的副本（参见 B.1.4.8）。这包括保留这些文件的先前版本。

B.3.15 信息安全独立审查

控制

组织在管理与个人身份信息处理相关的信息安全方面的方法及其实施（包括人员、流程和技术）应按计划定期进行独立审查，或在发生重大变化时进行审查。

实施指南

如果机构作为个人身份信息（PII）处理者，且对每个客户进行单独审计不切实际或可能增加安全风险，则该机构应在签订合同之前以及合同有效期内，向客户提供独立证据，证明其信息安全措施已按照机构的政策和程序实施和运行。如果机构选择的相关独立审计能够满足预期用户的需求，并且审计结果以足够透明的方式提供，则通常应视为满足客户审查机构处理操作需求的可接受方法。

B.3.16 遵守信息安全政策、规则和标准

控制

应定期审查组织的信息安全政策、特定主题的政策、规则和标准（与个人身份信息处理相关）的遵守情况。

实施指南

作为安全策略和标准合规性技术审查的一部分，组织应纳入对处理个人身份信息（PII）相关的工具和组件的审查方法。这可以包括：

—持续监控，以核实是否仅进行允许的处理；或
—特定的渗透或漏洞测试（例如，可以对去标识化的数据集进行有动机的入侵者测试，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、教育和培训

控制

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，并定期了解组织的信息安全动态。

政策、特定主题的政策和程序，以及与个人身份信息处理相关的政策和程序，只要与他们的岗位职能相关即可。

实施指南

应采取措施，包括提高事件报告意识，以确保相关员工了解违反隐私或安全规则和程序（尤其是有关个人身份信息处理的规则和程序）可能造成的后果。这些后果包括对组织（例如法律后果、业务损失和品牌或声誉损害）、对员工（例如纪律处分）以及对个人身份信息主体（例如身体、物质和精神后果）的后果。
注：此类措施可以包括对能够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、定期审查并由员工和其他相关利益方签署反映组织对保护个人身份信息（PII）需求的保密协议或不披露协议。

实施指南

组织应确保在其控制下能够接触个人身份信息（PII）的人员负有保密义务。保密协议（无论是作为合同的一部分还是单独签订）都应明确规定保密义务的履行期限。

当组织是个人身份信息处理者时，组织、其员工和代理人之间应签订任何形式的保密协议，以确保员工和代理人遵守有关数据处理和保护的政策和程序。

B.3.19 清理桌面和屏幕

控制

应制定并适当执行桌面文件和可移动存储介质的清理规则以及信息处理设备的屏幕清理规则。

实施指南

组织应将包括个人身份信息在内的纸质材料的创建限制在满足已确定的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介质应按照组织的分类方案和处理要求，在其获取、使用、运输和处置的整个生命周期中进行管理。

实施指南

组织应记录所有使用可移动介质或设备存储个人身份信息（PII）的情况。在可行的情况下，组织应使用支持加密的可移动物理介质或设备来存储 PII。只有在不可避免的情况下才应使用未加密的介质；如果必须使用未加密的介质或设备，组织应实施相应的程序和补偿控制措施（例如防篡改包装），以降低 PII 面临的风险。

对于存储了个人身份信息的可移动介质，在处置过程中，应在记录的信息中包含安全处置程序，并予以实施，以确保先前存储的个人身份信息无法被访问。

如果使用物理介质进行信息传输，则应建立一套系统来记录包含个人身份信息（PII）的传入和传出物理介质，包括物理介质类型、授权发送方、授权接收方、日期和时间以及物理介质数量。在条件允许的情况下，应采取加密等额外措施，以确保数据只能在目的地访问，而不能在传输过程中访问。

组织应在将包含个人身份信息的物理介质带离其场所之前对其进行授权程序，并确保除授权人员外，任何人都无法访问个人身份信息。

注意：为确保离开组织场所的物理介质上的 PII 不被普遍访问，一种可能的措施是对相关的 PII 进行加密，并将解密功能限制为授权人员。

被带出组织机构物理边界的移动存储介质容易丢失、损坏和遭到不当访问。对移动存储介质进行加密可以为个人身份信息（PII）提供额外的保护，从而降低移动存储介质遭到入侵时的安全和隐私风险。

B.3.21 安全处置或再利用设备

控制

应核实含有个人身份信息（PII）存储介质的设备，以确保在处置或重新使用之前，所有敏感数据和许可软件均已被删除或安全覆盖。

实施指南

组织应确保，每当重新分配存储空间时，之前驻留在该存储空间上的任何个人身份信息都无法访问。

就信息系统中存储的个人身份信息（PII）的删除而言，性能问题可能导致显式删除 PII 变得不切实际。这会造成其他用户可能访问该 PII 的风险。应通过特定的技术措施来避免此类风险。

为了安全处置或再利用，含有可能包含个人身份信息的存储介质的设备应视为含有个人身份信息。

B.3.22 用户终端设备

控制

存储在用户终端设备上、由用户终端设备处理或通过用户终端设备访问的个人身份信息应受到保护。

实施指南

该组织应确保移动设备的使用不会导致个人身份信息泄露。

B.3.23 安全认证

控制

应根据信息访问限制实施与个人身份信息处理相关的安全认证技术和程序。

实施指南

根据客户要求，组织应为客户控制下的任何用户帐户提供安全登录程序的功能。

B.3.24 信息备份

控制

应维护个人身份信息（PII）的备份副本，以及与 PII 处理相关的软件和系统，并定期进行测试。

实施指南

组织应制定政策，以解决个人身份信息（PII）的备份、恢复和还原要求（这可以作为整体信息备份政策的一部分），以及任何其他要求（例如合同或法律要求），以删除为备份要求而保存的信息中所包含的 PII。

在这方面，针对个人身份信息（PII）的具体责任可能取决于客户。组织应确保客户已了解备份服务的限制。

如果组织明确向客户提供备份和恢复服务，则组织应向客户提供有关其在个人身份信息备份和恢复方面的能力的明确信息。

某些司法管辖区对个人身份信息（PII）的备份频率、备份审查和测试频率，或 PII 的恢复程序有具体要求。在这些司法管辖区运营的组织应证明其符合这些要求。

在某些情况下，例如由于系统故障、攻击或灾难，可能需要恢复个人身份信息（PII）。当恢复 PII 时（通常从备份介质恢复），应制定相应的流程，以确保 PII 恢复到完整性可保证的状态；或者，如果发现 PII 存在不准确或不完整之处，则应制定相应的流程来解决这些问题（这可能需要 PII 主体参与）。

组织应制定个人身份信息（PII）恢复流程并建立日志记录。PII 恢复日志至少应包含以下内容：

—负责修复工作的人员姓名；
—对已恢复的 PII 的描述。

某些司法管辖区对个人身份信息（PII）恢复日志的内容有具体规定。组织应能够提供文件，证明其符合任何此类恢复日志内容要求。相关讨论的结论应包含在已记录的信息中。

使用分包商存储已处理的 PII 的复制或备份副本受本文件中适用于分包 PII 处理的控制措施的约束（参见 B.3.10、B.3.20）。如果发生与备份和恢复相关的物理介质传输，也受本文件中的控制措施的约束（参见 B.3.7）。

B.3.25 日志记录

控制

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

实施指南

应建立一套流程，利用持续的自动化监控和警报流程来审查事件日志，或者在需要时进行手动审查，并按照规定的、有记录的周期进行审查，以识别异常情况并提出补救措施。

事件日志应尽可能记录对 PII 的访问，包括访问者、访问时间、访问了哪个 PII 主体的 PII，以及由于该事件而进行了哪些（如果有）更改（例如添加、修改或删除）。

当多个服务提供商参与提供服务时，在实施本指南的过程中，各服务提供商可能承担不同的角色或共同承担部分角色。这些角色应明确界定并纳入书面文件，同时还应就服务提供商之间的日志访问权限达成一致。

例如，用于安全监控和运行诊断的日志信息可能包含个人身份信息（PII）。应采取控制访问等措施，以确保记录的信息仅用于预期用途。
应制定程序（最好是自动程序），以确保按照保留计划（见 B.1.4.8）的规定删除或匿名化记录的信息。

个人身份信息处理者的实施指南

组织应制定相关标准，明确何时、如何以及是否向客户提供或供其使用日志信息。这些标准应向客户公开。

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

—只能访问与该客户活动相关的记录；
—无法访问任何与其它客户活动相关的日志记录；
—无法以任何方式修改日志。

B.3.26 密码学的应用

控制

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。

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个人身份信息，例如健康数据、居民登记号码、

护照号码和驾驶执照号码。

组织应向客户提供信息，说明其在何种情况下使用加密技术保护所处理的个人身份信息（PII）。组织还应向客户提供信息，说明其提供的任何可帮助客户实施自身加密保护的功能。

B.3.27 安全开发生命周期

控制

应制定并实施与个人身份信息处理相关的软件和系统安全开发规则。

实施指南

系统开发和设计政策应包括组织处理个人身份信息（PII）需求的指导，该指导应基于对 PII 主体的义务或任何适用的法律要求以及组织执行的处理类型。

旨在通过设计和默认设置来保护隐私的政策应考虑以下几个方面：

a）关于个人身份信息保护和在软件开发生命周期中实施隐私原则（参见 ISO/IEC 29100）的指导；

b）设计阶段的隐私和个人身份信息保护要求，可以基于隐私风险评估或隐私影响评估的输出（参见 B.1.2.6)；

c）项目里程碑内的 PII 保护检查点；

d）具备必要的隐私和个人身份信息保护知识；

e）默认情况下，尽量减少对个人身份信息的处理。

B.3.28 应用安全要求

控制

在开发或获取应用程序时，应识别、规定和批准与个人身份信息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（PII）进行加密传输。

不受信任的网络可能包括公共互联网和组织运营控制范围之外的其他设施。

注意：在某些情况下（例如电子邮件的交换），不受信任的数据传输网络系统的固有特性可能需要暴露一些标头或流量数据才能有效传输。

B.3.29 安全系统架构和工程原则

控制

与处理个人身份信息（PII）相关的安全系统工程原则应予以建立、记录、维护，并应用于任何信息系统开发活动。

实施指南

与处理个人身份信息（PII）相关的系统或组件的设计应遵循隐私设计原则和隐私默认原则，并预见和促进相关控制措施的实施（如 B.1 和 B.2 分别针对 PII 控制者和 PII 处理者所述），特别是确保这些系统中 PII 的收集和处理仅限于为实现已确定的 PII 处理目的所必需的内容（参见 B.1.2.2）。

例如，处理个人身份信息（PII）的组织应确保在特定期限后销毁 PII。处理 PII 的系统应设计成能够满足这一删除要求。

注：可能适用法律规定。

B.3.30 外包开发

控制

该组织应指导、监督和审查与外包 PII 处理系统开发相关的活动。

实施指南

如果适用，也应将隐私设计和隐私默认原则（见 B.3.29）应用于外包信息系统。

B.3.31 测试信息

控制

与个人身份信息处理相关的测试信息应进行适当的选择、保护和管理。

实施指南

个人身份信息（PII）不应用于测试目的；应使用虚假或合成的 PII。如果无法避免将 PII 用于测试目的，则应实施与生产环境同等的技术和组织措施，以最大程度地降低风险。如果无法采取此类同等措施，则应进行风险评估，并据此选择适当的缓解控制措施。

附件 C
（资料性）
与 ISO/IEC 29100 的映射

表 C.1 和 C.2 给出了本文件条款与 ISO/IEC 29100 表 C.1 中的隐私原则之间的指示性映射。和 C.2 以纯粹指示性的方式显示了符合本文件要求和控制措施与 ISO/IEC 29100 中规定的通用隐私原则之间的关系。表 C.1 和 C.2 中的交叉引用对应于表 A.1 至 A.3 中引用控制措施的位置。

表 C.1—PII 控制器和 ISO/IEC 29100 的控制映射

隐私原则 ISO/IEC 29100	PII 控制器的相关控制
1.同意和选择（ISO/IEC 29100:2024,6.2）	A.1.2.2 确定并记录目的 A.1.2.3 确定合法依据 A.1.2.4 确定何时以及如何获得同意 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 提供反对个人身份信息处理的机制 A.1.3.8 个人身份信息控制者告知第三方的义务
2.目的合法性和规范（ISO/IEC 29100:2024，6.3)	A.1.2.2 确定并记录目的 A.1.2.3 确定合法依据 A.1.2.6 隐私影响评估 A.1.3.3 确定 PII 主体的信息 A.1.3.4 向 PII 负责人提供信息 A.1.3.11 自动化决策
3.收集限制（ISO/IEC 29100:2024,6.4）	A.1.2.6 隐私影响评估 A.1.4.2 限制收款
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和删除
5.使用、保留和披露限制（ISO/IEC 29100:2024，6.6)	A.1.4.5 个人身份信息最小化目标 A.1.4.6 处理结束时的个人身份信息去标识化和删除 A.1.4.7 临时文件 A.1.4.8 保留 A.1.4.9 处置 A.1.5.2 确定跨司法管辖区个人身份信息转移的依据 A.1.5.5 向第三方披露个人身份信息的记录
6.准确度和质量（ISO/IEC 29100:2024, 6.7）	A.1.4.4 准确性和质量
7.公开性、透明度和公示性（ISO/IEC 29100:2024，6.8)	A.1.3.3 确定 PII 主体的信息 A.1.3.4 向 PII 负责人提供信息
8.个人参与和访问（ISO/IEC 29100:2024,6.9）	A.1.3.2 确定和履行对 PII 委托人的义务 A.1.3.4 向 PII 负责人提供信息 A.1.3.7 访问、更正或删除 A.1.3.9 提供已处理的个人身份信息副本 A.1.3.10 处理请求

9.问责制（ISO/IEC 29100:2024,6.10）	A.1.2.7 与 PII 处理者的合同 A.1.2.8 联合 PII 控制器 A.1.2.9 与处理个人身份信息相关的记录 A.1.3.10 处理请求 A.1.5.2 确定跨司法管辖区个人身份信息转移的依据 A.1.5.3 知识产权可转让的国家和国际组织 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 PII 处理者的合同 A.1.4.10PII 变速器控制
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—PII 处理器和 ISO/IEC 29100 的控制映射

ISO/IEC 29100 的隐私原则	PII 处理器的相关控制
1.同意和选择（ISO/IEC 29100:2024,6.2）	A.2.2.6 客户义务
2.目的合法性和规范〔ISO/IEC 29100:2024,6.3）	A.2.2.2 客户协议 A.2.2.3 组织宗旨 A.2.2.4 市场营销和广告用途 A.2.2.5 侵权指示 A.2.3.2 履行对 PII 委托人的义务
3.收集限制（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、保存和披露限制（ISO/IEC 29100:2024,6.6）	A.2.5.4 向第三方披露个人身份信息的记录 A.2.5.5 个人身份信息披露请求的通知 A.2.5.6 具有法律约束力的个人身份信息披露
6.准确度和质量（ISO/IEC 29100:2024, 6.7）	不适用
7.公开性、透明度和公示性（ISO/IEC 29100:2024,6.8）	A.2.5.7 披露用于处理个人身份信息的转包商 A.2.5.8 聘用分包商处理个人身份信息 A.2.5.9 变更处理 PII 的分包商
8.个人参与和访问（ISO/IEC 29100:2024,6.9）	A.2.3.2 履行对 PII 委托人的义务
9.问责制（ISO/IEC 29100:2024,6.10）	A.2.2.7 与处理个人身份信息相关的记录 A.2.4.3 个人身份信息的返还、转移或处置 A.2.5.2 跨司法管辖区个人身份信息转移的依据 A.2.5.3 个人身份信息可转移至的国家和国际组织
10.信息安全（ISO/IEC 29100:2024,6.11）	A.2.4.4PII 变速器控制
11.隐私合规性（ISO/IEC 29100:2024,6.12）	A.2.2.6 客户义务

附件 D
（资料性）
与《通用数据保护条例》（GDPR）的映射

表 D.1 给出了本文件条款与欧盟通用数据保护条例第 5 至 49 条（43 条除外）之间的指示性映射。[16]

表 D.1 显示了遵守本文件的要求和控制措施如何与履行 GDPR 的义务相关。

注：此表仅供参考。组织有责任评估其法律义务并决定如何履行这些义务。

表 D.1—本文档与 GDPR 条款的对应关系

本文档子条款	相关 GDPR 文章
4.1	(24) (3), (25) (3), (28) (5), (28) (6), (28) (10), (322) (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)

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)
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)

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

ISO/IEC 27018 为作为个人身份信息（PII）处理者和提供公共云服务的组织提供了更多信息。ISO/IEC 29151 为 PII 控制者处理 PII 提供了额外的控制措施和指导。

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

表 E.1 中所示的映射关系仅供参考；这些条款之间的特定联系并不意味着它们是等效的。

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

本文档子条款	ISO/IEC 27018 中的子条款	ISO/IEC 29151 中的子条款
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
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

附件 F
（资料性）
与 ISO/IEC 27701:2019 的对应关系

本附件的目的是为目前正在使用本文件先前版本（ISO/IEC 27701:2019）并希望过渡到本新版本的组织提供与该先前版本的向后兼容性。

表 F.1 提供了附件 A 中规定的控制措施与 ISO/IEC 27701:2019 中规定的控制措施的对应关系。第一列中的“"N/A"”表示本文件中未包含的控制措施。第二列中的“新的”表示 ISO/IEC 27701:2019 中未包含的控制措施。

表 F.1—本文件中的控制措施与 ISO/IEC 27701:2019 中控制措施的对应关系

ISO/IEC 27701 控制标识符	ISO/IEC 27701:2019 控制标识符	控件名称
A.3.3	6.2.1.1,6.2.1.2	信息安全政策
A.3.4	6.3.1.1	信息安全角色和职责
N/A	6.3.1.2	职责分离
N/A	6.4.2.1	管理职责
N/A	6.3.1.3	与当局联系
N/A	6.3.1.4	与特殊利益集团的联系
N/A	新的	威胁情报
N/A	6.3.1.5,6.11.1.1	项目管理中的信息安全
N/A	6.5.1.1,6.5.1.2	信息及其他相关资产清单
N/A	6.5.1.3,6.5.2.3	信息及其他相关资产的合理使用
N/A	6.5.1.4	资产返还
A.3.5	6.5.2.1	信息分类
A.3.6	6.5.2.2	信息标签
A.3.7	6.10.2.1,6.10.2.2, 6.10.2.3	信息传递
N/A	6.6.1.1,6.6.1.2	访问控制
A.3.8	6.6.2.1	身份管理
N/A	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	在供应商协议中解决信息安全问题
N/A	6.12.1.3	信息通信技术供应链中的信息安全管理
N/A	6.12.2.1,6.12.2.2	供应商服务的监控、审查和变更管理
N/A	新的	云服务使用的信息安全
N/A	6.13.1.1	信息安全事件管理规划和准备
A.3.11	6.13.1.4	信息安全事件的评估和决策
A.3.12	6.13.1.5	应对信息安全事件
N/A	6.13.1.6	从信息安全事件中吸取教训
N/A	6.13.1.7	证据收集

N/A	6.14.1.1,6.14.1.2, 6.14.1.3	中断期间的信息安全
N/A	新的	信息通信技术对业务连续性的准备情况
A.3.13	6.15.1.1,6.15.1.5	法律、法规、规章和合同要求
N/A	6.15.1.2	知识产权
A.3.14	6.15.1.3	记录保护
N/A	6.15.1.4	隐私和个人身份信息保护
A.3.15	6.15.2.1	信息安全独立审查
A.3.16	6.15.2.2,6.15.2.3	遵守信息安全政策、规则和标准
N/A	6.9.1.1	已记录的操作规程
N/A	6.4.1.1	筛查
N/A	6.4.1.2	雇佣条款和条件
A.3.17	6.4.2.2	信息安全意识、教育和培训
N/A	6.4.2.3	纪律处分程序
N/A	6.4.3.1	终止雇佣关系或变更雇佣关系后的职责
A.3.18	6.10.2.4	保密协议或不披露协议
N/A	6.3.2.2	远程办公
N/A	6.13.1.2,6.13.1.3	信息安全事件报告
N/A	6.8.1.1	物理安全周界
N/A	6.8.1.2,6.8.1.6	实体入口
N/A	6.8.1.3	确保办公室、房间和设施的安全
N/A	新的	物理安全监控
N/A	6.8.1.4	防范物理和环境威胁
N/A	6.8.1.5	在安全区域工作
A.3.19	6.8.2.9	桌面和屏幕都要清理干净。
N/A	6.8.2.1	设备选址和保护
N/A	6.8.2.6	非营业场所资产安全
A.3.20	6.5.3.1,6.5.3.2, 6.5.3.3,6.8.2.5	存储介质
N/A	6.8.2.2	支持公用事业
N/A	6.8.2.3	布线安全
N/A	6.8.2.4	设备维护
A.3.21	6.8.2.7	安全处置或再利用设备
A.3.22	6.3.2.1,6.8.2.8	用户终端设备
N/A	6.6.2.3	特权访问权限
N/A	6.6.4.1	信息访问限制
N/A	6.6.4.5	访问源代码
A.3.23	6.6.4.2	安全认证
N/A	6.9.1.3	容量管理
N/A	6.9.2.1	防范恶意软件
N/A	6.9.6.1	技术漏洞管理
N/A	新的	配置管理
N/A	新的	信息删除
N/A	新的	数据脱敏

N/A	新的	防止数据泄露
A.3.24	6.9.3.1	信息备份
N/A	6.14.2.1	信息处理设施的冗余
A.3.25	6.9.4.1、6.9.4.26.9.4.3	日志记录
N/A	新的	监测活动
N/A	6.9.4.4	时钟同步
N/A	6.6.4.4	使用特权实用程序
N/A	6.9.5.1,6.9.6.2	在操作系统上安装软件
N/A	6.10.1.1	网络安全
N/A	6.10.1.2	网络服务安全
N/A	6.10.1.3	网络隔离
N/A	新的	网络过滤
A.3.26	6.7.1.1,6.7.1.2	密码学的应用
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	应用安全要求
A.3.29	6.11.2.5	安全系统架构和工程原则
N/A	新的	安全编码
N/A	6.11.2.8,6.11.2.9	开发和验收过程中的安全测试
A.3.30	6.11.2.7	外包开发
N/A	6.9.1.4,6.11.2.6	开发、测试和生产环境的分离
N/A	6.9.1.2,6.11.2.2,6.11.2.3,6.11.2.4	变革管理
A.3.31	6.11.3.1	测试信息
N/A	6.9.7.1	审计测试期间信息系统的保护

表 F.2 列出了 ISO/IEC 27701:2019 第 6 章中规定的控制措施与本文件中规定的控制措施的对应关系。第二列中的“N/A”表示本文件中未包含的控制措施。

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

ISO/IEC 27701:2019 控制标识符	ISO/IEC 27701 控制标识符	根据 ISO/IEC 27701:2019 标准的控制名称
6.2.1.1	A.3.3	信息安全政策
6.2.1.2	A.3.3	信息安全政策审查
6.3.1.1	A.3.4	内部安全角色和职责
6.3.1.2	N/A	职责分离
6.3.1.3	N/A	与当局联系
6.3.1.4	N/A	与特殊利益集团的联系
6.3.1.5	N/A	项目管理中的信息安全
6.3.2.1	A.3.22	移动设备策略
6.3.2.2	N/A	远程办公
6.4.1.1	N/A	筛查
6.4.1.2	N/A	雇佣条款和条件
6.4.2.1	N/A	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	N/A	纪律处分程序
6.4.3.1	N/A	终止或变更雇佣职责
6.5.1.1	N/A	资产清单
6.5.1.2	N/A	资产所有权
6.5.1.3	N/A	资产的合理使用
6.5.1.4	N/A	资产返还
6.5.2.1	A.3.5	信息分类
6.5.2.2	A.3.6	信息标签
6.5.2.3	N/A	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	媒体处置
6.5.3.3	A.3.20	物理介质传输
6.6.1.1	N/A	访问控制策略
6.6.1.2	N/A	网络和网络服务的访问
6.6.2.1	A.3.8	用户注册和注销
6.6.2.2	A.3.9	用户访问权限配置
6.6.2.3	N/A	特权访问权限的管理
6.6.2.4	N/A	用户秘密认证信息的管理
6.6.2.5	A.3.9	用户访问权限审查
6.6.2.6	A.3.9	移除或调整访问权限
6.6.3.1	N/A	使用秘密认证信息
6.6.4.1	N/A	信息访问限制
6.6.4.2	A.3.23	安全登录程序
6.6.4.3	N/A	密码管理系统
6.6.4.4	N/A	使用特权实用程序
6.6.4.5	N/A	对程序源代码的访问控制
6.7.1.1	A.3.26	关于使用加密控制的政策
6.7.1.2	A.3.26	关键管理
6.8.1.1	N/A	物理安全周界
6.8.1.2	N/A	物理入口控制
6.8.1.3	N/A	确保办公室、房间和设施的安全
6.8.1.4	N/A	抵御外部和环境威胁
6.8.1.5	N/A	在安全区域工作
6.8.1.6	N/A	交货和装货区
6.8.2.1	N/A	设备选址和保护
6.8.2.2	N/A	支持公用事业
6.8.2.3	N/A	布线安全
6.8.2.4	N/A	设备维护
6.8.2.5	N/A	资产移除
6.8.2.6	N/A	异地设备和资产的安全保障
6.8.2.7	A.3.21	安全处置或再利用设备
6.8.2.8	A.3.22	无人值守用户设备
6.8.2.9	A.3.19	桌面和屏幕清理政策
6.9.1.1	N/A	记录操作规程

6.9.1.2	N/A	变革管理
6.9.1.3	N/A	容量管理
6.9.1.4	N/A	开发、测试和运行环境的分离
6.9.2.1	N/A	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	事件日志记录
6.9.4.2	A.3.25	日志信息保护
6.9.4.3	A.3.25	管理员和操作员日志
6.9.4.4	N/A	时钟同步
6.9.5.1	N/A	在操作系统上安装软件
6.9.6.1	N/A	技术漏洞管理
6.9.6.2	N/A	软件安装限制
6.9.7.1	N/A	信息系统审计控制
6.10.1.1	N/A	网络控制
6.10.1.2	N/A	网络服务安全
6.10.1.3	N/A	网络中的隔离
6.10.2.1	A.3.7	信息传输政策和程序
6.10.2.2	A.3.7	信息转移协议
6.10.2.3	A.3.7	电子信息
6.10.2.4	A.3.18	保密协议或不披露协议
6.11.1.1	N/A	信息安全需求分析与规范
6.11.1.2	A.3.28	保护公共网络上的应用服务
6.11.1.3	A.3.28	保护应用程序服务交易
6.11.2.1	A.3.27	安全开发政策
6.11.2.2	N/A	系统变更控制程序
6.11.2.3	N/A	操作系统平台变更后的应用程序技术审查
6.11.2.4	N/A	对软件包变更的限制
6.11.2.5	A.3.29	安全系统工程原则
6.11.2.6	N/A	安全的开发环境
6.11.2.7	A.3.30	外包开发
6.11.2.8	N/A	系统安全测试
6.11.2.9	N/A	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	供应商关系信息安全政策
6.12.1.2	A.3.10	在供应商协议中解决安全问题
6.12.1.3	N/A	信息通信技术供应链
6.12.2.1	N/A	供应商服务的监控和审查
6.12.2.2	N/A	管理供应商服务的变更
6.13.1.1	N/A	职责和程序
6.13.1.2	N/A	报告信息安全事件
6.13.1.3	N/A	报告信息安全漏洞
6.13.1.4	A.3.11	信息安全事件的评估和决策
6.13.1.5	A.3.12	应对信息安全事件
6.13.1.6	N/A	从信息安全事件中吸取教训

6.13.1.7	N/A	证据收集
6.14.1.1	N/A	规划信息安全连续性
6.14.1.2	N/A	实施信息安全连续性
6.14.1.3	N/A	验证、更新和评估信息安全连续性
6.14.2.1	N/A	信息处理设施的可用性
6.15.1.1	A.3.13	确定适用的法律法规和合同要求
6.15.1.2	N/A	知识产权
6.15.1.3	A.3.14	记录保护
6.15.1.4	N/A	隐私和个人身份信息保护
6.15.1.5	A.3.13	密码控制条例 1
6.15.2.1	A.3.15	信息安全独立审查
6.15.2.2	A.3.16	遵守安全策略和标准
6.15.2.3	A.3.16	技术合规性审查

参考文献

［1］ISO19011，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，云计算和分布式平台—数据流、数据类别和数据使用—第 2 部分：应用和可扩展性指南

［4］ISO/IEC 20889，隐私增强数据去标识化术语和技术分类

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

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

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

［8］ISO/IEC 27018，信息安全、网络安全和隐私保护—作为 PII 处理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—ISO 31000:2018 在组织隐私风险管理中的应用

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

［12］ISO/IEC 29134，信息技术—安全技术—隐私影响评估指南

［13］ISO/IEC 29151，信息技术—安全技术—个人身份信息保护实践守则

［14］ISO/IEC 29184，信息技术—在线隐私声明和同意

［15］ISO 31000，风险管理指南

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