



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

第二版
2025-10

信息安全、网络安全与隐私保护——隐私保护管理体系——要求与建议



版权保护文件

© ISO/IEC 2025

版权所有。除非另有说明或实施要求，未经事先书面许可，不得以任何形式或任何手段（包括电子或机械方式）复制或使本出版物的任何部分，包括影印、在互联网或内联网上发布。许可申请可向下述地址的ISO或申请者所在国的ISO成员机构提出。

ISO版权办公室

邮政信箱401 • 布兰东内路8号 CH-

1214维尔尼耶尔，日内瓦 电话：

+41 22 749 01 11

电子邮箱：copyright@iso.org 网站

： www.iso.org

瑞士出版

目录

页码

致两位Fd,	V
引言	vi
1 范围。	1
2 规范性引用	1
3 术语、定义和缩写。	1
4 组织的背景	4
4.1 理解组织及其背景。	4
4.2 理解相关方的需求和期望。	5
4.3 确定 隐私信息管理系统的范围。	5
4.4 隐私信息管理系统。	6
5 领导力与承诺	6
5.1 领导力与承诺	6
5.2 隐私政策	6
5.3 角色、职责与权限	7
6 规划。	7
6.1 应对风险与机遇的行动方案。	7
6.1.1 将军	
6.1.2 隐私风险评估。	7
6.1.3 隐私风险处理。	8
6.2 隐私目标及其实 现 规划	9
6.3 变更规划	10
7 支持	10
7.1 资源	10
7.2 意识	10
7.3 沟通。	10
7.4 文件化信息。	11
7.5.1 一般	11
7.5.2 创建和更新文件化信息	11
7.5.3 文件信息的控制	11
8 运营规划与控制	12
8.1 运营规划与控制	12
8.2 隐私风险评估。	12
8.3 隐私风险处理	12
9 绩效评估	12
9.1 监测、测量、分析和评估。	12
9.2 内部审计	13
9.2.1 一般	13
9.2.2 内部审计计划,	13
9.3 管理评审。	13
9.3.1 通用	13
9.3.2 管理评审输入。	13
9.3.3 管理评审结果。	14
10 改进	14

10.1	持续改进。	14
10.2	不符合项与纠正措施	14
11	附件的进一步信息	14
附件A（规范性） PIMS参考控制目标及PII控制器与PII的控制措施		
	3rOCeSSOFS	15
附件 B（规范性）	PII 控制器和 PII 处理器的实施指南	21
附件 C（参考性）	与 ISO/IEC 29100 的对照表。	51
附件 D（信息性）	与《通用数据保护条例》的对照表。	53
附录E（参考性）	与ISO/IEC 27018及ISO/IEC 29151的对照关系	56
附录 F（信息性）	与 ISO/IEC 27701:2019 的对应关系。	58
参考文献。		64

前言

国际标准化组织（ISO）与国际电工委员会（IEC）共同构成了全球标准化的专业体系。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的领域开展协作。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。

有关标准自愿性质的说明、ISO特定术语及符合性评估相关表述的定义，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。IEC相关信息请参阅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（JTC 1）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，依据国际标准化组织与欧洲标准化委员会技术合作协议（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：

— 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）。随着组织间处理PII的合作场景日益增多，PII的处理量与类型也在持续增长。在PII处理过程中保障隐私既是社会需求，也是全球专项法律法规的核心议题。

本文档涵盖以下内容的映射：

- ISO/IEC 29100定义的隐私框架与原则；
- ISO/IEC 27018；
- ISO/IEC 29151；
- 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衔接。

信息安全、网络安全和隐私保护——隐私信息管理体系——要求和指南

1 适用范围

本文件规定了建立、实施、保持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 and 规模的组织，包括公共和私营公司、政府实体及非营利组织。

2 规范性引用

以下文件在本文中被引用时，其全部或部分內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、定义及缩写

为本文件之目的，采用ISO/IEC 29100标准中给出的术语和定义，并适用下列规定。ISO和IEC在下列地址维护用于标准化工作的术语数据库：

- ISO在线浏览平台：<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* 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者、公司、企业、机构、企业实体、当局、合伙企业、慈善组织或机构，或其部分或组合形式，无论是否注册成立，亦不论公营或私营。

条目注释2：若该组织隶属于更大实体，则“组织”一词仅指该实体中属于 *隐私信息管理体系* 范围的部分（3.23）。

3.2

利益相关方

个人或 *组织*（3.1），其可能影响、受影响或认为自己受某项决定或活动的影响

3.3

高层管理人员

在组织最高层负责指导和控制的人员或群体（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、规划与运作。

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、环境等）。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，隐私目标由组织设定（3.5），以实现特定结果，且符合隐私政策（3.5）。组织（3.1）制定，需符合隐私政策（3.5），以实现特定成果。

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活动的活动，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）；已实现结果的证据（记录）。

3.11

绩效

可测量的结果

注1：绩效可涉及定量或定性结果。

注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)。

组织 (3.1)。

3.12

持续改进

定期开展活动以提升*绩效* (3.11)

3.13

有效性

计划活动实现程度与预期成果达成程度

3.14

要求

明示、默示或强制性的需求或期望

注1：“通常暗示”是指*组织* (3.1) 和相关方 (3.2) 惯例或惯例认为所考虑的需求或期望是暗示的。相关方 (3.2) 认为该需求或期望是默示的。

注2：规定要求是指明确说明的要求，例如在*文件化信息* (3.10) 中。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)，旨在获取证据并客观评估，以确定审核标准的满足程度

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），也可组合审核（融合两个或多个学科领域）。

注2：内部审核由*组织* (3.1) 自身实施，或由外部方代为实施。注3：“审核证据”和“审核准则”的定义见ISO 19011。

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：为确定状态，可能需要进行核查、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) 控制者共同决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**

能够或实际接收特定产品或服务的人员或组织 (3.1)，该产品或服务系为该人员或组织设计或由其要求

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、受益者及购买者。

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，或与PII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) 旨在处理因处理个人身份信息而可能受到影响的隐私保护问题

3.24**信息安全计划**

旨在管理组织资产风险 (3.7) 的一套政策 (3.5)、目标 (3.6) 和流程 (3.8)，以确保信息的保密性、完整性和可用性
(3.1) 资产的风险 (3.7)，以确保信息的保密性、完整性和可用性

注释 1：信息安全计划可以是基于 ISO/IEC 27001 标准的信息安全管理体系。

3.25**适用性声明**

记录所有必要控制措施，并说明纳入或排除这些控制措施的理由

4 组织的背景**4.1 理解组织及其隐私信息管理 () 背景**

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 and 内部事项。

组织应确定气候变化是否为相关事项。

组织应确定自身是否作为个人身份信息 (PII) 控制者 (包括联合控制者) 或处理者开展活动。

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

注1 外部和内部事项可包括但不限于：

适用的隐私立法；适用的法规；

— 适用的司法裁决；

适用的组织环境、治理结构、政策和程序；

— 适用的行政决定；

— 适用合同要求。

当组织同时承担两种角色（即个人信息控制者和个人信息处理者）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 该组织在处理个人信息（PII）的每个具体场景中可能承担不同角色，因为其职能取决于谁决定了处理的目的和方式。

4.2 理解相关方的需求与期望

组织应确定：

— 与隐私信息管理体系相关的利益相关方；

— 这些相关方的具体要求；

— 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。

组织应将与个人信息处理相关的权益方或责任方纳入其利益相关方范畴，包括个人信息主体。

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

根据组织的角色，"客户"可理解为：

a) 与PII控制者签订合同的组织（例如PII控制者的客户）；注3 此情形可能涉及作为共同PII控制者的组织；

b) 与PII处理者签订合同的PII控制者（例如PII处理者的客户）；或

c) 与分包商签订个人信息处理合同的处理者（例如分包个人信息处理者的客户）。

注4 本文件中，在商业关联中（例如消费者、雇员、供应商、访客关系中）其PII被处理的个人称为"PII主体"。

注5 与PII处理相关的要求可由法律法规要求、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 为证明符合组织的义务，某些相关方可期望该组织符合特定标准，例如本文件规定的管理体系或任何相关规范。这些方可要求组织通过独立审核来证明符合这些标准。

4.3 确定隐私信息管理体系的范围

组织应确定隐私信息管理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条款所述的外部和内部问题；
- 4.2节所述的要求。

该范围应作为文件化信息提供。

在确定个人信息管理体系的范围时，组织应包括个人身份信息的处理。

4.4 隐私信息管理 系统

组织应根据本文件的要求，建立、实施、维护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 领导层

5.1 领导层和管理层的承诺

最高管理层应通过以下方式展现对隐私信息管理体系的领导力和承诺：

- 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；
- 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。
- 指导并支持相关人员为 隐私信息管理体系的有效运作作出贡献；
- 推动持续改进；
- 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。

5.2 隐私政策

高层管理人员应制定隐私政策，确保：

- a) 符合组织宗旨；
- b) 提供设定隐私目标的框架；
- c) 包含遵守适用要求的承诺；
- d) 包含对隐私信息管理体系持续改进的承诺。隐私政策应：
 - 以文件化信息形式提供；

- 在组织内部传达；
- 酌情向相关方提供。

5.3 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) 确保隐私信息管理系统符合本文件的要求；
- b) 向高层管理人员汇报隐私信息管理系统的运行情况。

6 规划

6.1 应对风险与 机遇的行动

6.1.1 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：

- 确保隐私信息管理系统能够实现预期效果；
- 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行动；
 - 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。

6.1.2 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能产生一致、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隐私保护及信息安全风险相关的隐私风险；以及

2) 确定风险责任人的风险；

d) 分析隐私风险：

1) 评估c)1)项中识别出的风险若发生时，对组织及个人身份信息主体可能造成的潜在后果；

2) 评估c) 1)中识别出的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：

1) 将风险分析结果与a)项中确立的风险标准进行比较；以及

2) 为风险处理对分析风险进行优先级排序。

组织应保留隐私风险评估过程的文件化信息。注 有关隐私风险评估过程的更多信息，请参阅ISO/IEC 27557。

6.1.3 隐私风险 处理

该组织应制定并实施隐私风险处理流程，以应对与个人信息处理相关的风险，包括对个人身份信息主体的风险以及个人信息的安全风险，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

— 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，可参考 ISO/IEC 27002 以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中的控制措施进行比对，并核实是否遗漏了任何必要的控制措施；

注3 附件A包含可能的隐私控制措施清单。可查阅附件A以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，必要时可增补其他控制措施。

注5 组织在处理PII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：

- 必要的控制措施[参见b)、c)和d)项]；
- 纳入这些控制措施的依据；
- 必要控制措施是否已实施；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主体的法律要求，则可排除该控制措施。

f) 制定隐私风险处理方案；

g) 获取隐私风险责任人的隐私风险处理方案批准及残余隐私风险接受确认；以及

h) 参考附件B中的指导原则实施b)和c)项确定的控制措施。组织应保留隐私风险处理流程的文件化信息。

6.2 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；
- d) 接受监控；
- e) 予以传达；
- f) 应酌情更新；
- 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；

- 所需资源；
- 责任归属；
- 何时完成；
- 如何评估结果。

6.3 变更规划

当组织确定需要变更隐私信息管理系统时，应按计划实施变更。

7 支持

7.1 资源

该组织应确定并提供建立、实施、维护和持续改进隐私信息管理体系所需的资源。

7.2 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；
- 确保这些人员通过适当的教育、培训或经验获得相应能力；
- 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：对现有雇员提供培训、指导或重新分配工作；或招聘或签约合格人员。

7.3 认知

在组织控制下从事工作的人员应知晓：

- 隐私政策（参见5.2）；
- 其对隐私信息管理体系有效性的贡献，包括提升隐私保护绩效带来的益处；
- 未遵守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：

- 沟通内容；
- 沟通时机；
- 沟通对象；
- 沟通方式。

7.5 文件化的信息

7.5.1 总则

本组织的隐私信息管理体系应包含：

- a) 本文件要求记录的信息；
- b) 组织确定为保障隐私信息管理体系有效性所必需的文件化信息。

注 隐私信息管理体系中记录信息的范围可能因组织而异，原因包括：

组织规模及其业务类型、流程、产品与服务；流程复杂度及其交互关系；

人员能力水平。

7.5.2 创建和更新文件化的信息

在创建和更新文件化信息时，组织应确保适当：

- 标识与描述（如标题、日期、作者或参考编号）；
- 格式（如语言、软件版本、图形）和载体（如纸质、电子）；
- 审查并批准其适用性和充分性。

7.5.3 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，包括可读性的保存；
- 变更控制（例如版本控制）；
- 保留与处置。

由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，或同时包含查看与修改文件化信息的权限及授权。

8 操作

8.1 操作规划与控制

组织应通过以下方式规划、实施和控制满足要求所需的流程，并实施第6条款确定的措施：

- 建立过程准则；
- 根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，并审查非预期的变更后果，必要时采取行动减轻任何不利影响。

组织应确保对与隐私信息管理体系相关的外部提供的流程、产品或服务进行控制。

8.2 隐私风险评估

组织应在计划间隔期或当重大变更被提出或发生时，参照6.1.2 a)条款确立的标准，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。

8.3 隐私风险处理

组织应实施隐私风险处理计划。

该组织应保留隐私风险处理结果的文件化信息。

9 评估

9.1 监测、测量、分析和评估

组织应确定：

- 需监测和测量的内容；
- 适用时，为确保结果有效而采用的监测、测量、分析和评估方法；
- 何时进行监测和测量；
- 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。

该组织应评估隐私保护绩效及隐私信息管理体系的有效性。

9.2 内部审核

9.2.1 一般

组织应按计划间隔开展内部审核，以提供隐私信息管理体系是否符合以下要求的依据：

- a) 是否符合：
 - 组织自身对隐私信息管理体系的要求；
 - 本文件的要求；
- b) 是否得到有效实施和维护。

9.2.2 内部审核计划

组织应规划、建立、实施并保持（一项或多项）审核计划，包括审核频率、方法、责任、规划要求及报告。

在制定内部审计计划时，组织应考虑相关流程的重要性及以往审计的结果。

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) 确保将审计结果报告给相关管理人员。

应提供文件化信息作为实施审计计划及审计结果的证据。

9.3 管理层审查

9.3.1 一般

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

9.3.2 管理评审输入项

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 and 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) 隐私信息管理体系运行状况信息，包括以下趋势：
 - 不符合项及纠正措施；
 - 监测与测量结果；
 - 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 的持续改进

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。

10.2 不符合项与纠正措施

当发生不符合项时，组织应：

- a) 对不符合项作出反应，并视情况：
 - 采取行动控制并纠正；
 - 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出现，具体通过：
 - 复核不符合项；
 - 确定不符合项的根源；
 - 确定是否存在类似不符合项或潜在风险；
- c) 实施所需措施；
- d) 复核所采取纠正措施的有效性；
- e) 如有必要，应对隐私信息管理系统进行修改。纠正措施应与所发现的不符合项的影响程度相适应。文件

化信息应作为以下事项的证据：

- 不符合项的性质及后续采取的任何措施；
- 任何纠正措施的结果。

11 附件的补充说明

[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包含本文件中控制措施与欧盟《通用数据保护条例》的对照关系。

[附录E](#)包含本文件条款与ISO/IEC 27018及ISO/IEC 29151条款的对照表。

[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PH控制者与PH处理者的控制措施

本附录适用于作为个人信息（PII）控制者或处理者（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控制者和PII处理者双方的信息安全控制措施。

注 表A.1、A.2和A.3中"控制参考"项下的引用对应于附件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，具有适用司法管辖区的法律依据，且目的明确且正当。		
控制参考	控制措施名称	控制措施
A.1.2.2	确定并记录目的	该组织应确定并记录处理个人信息（PII）的具体目的。
A.1.2.3	确定合法依据	该组织应确定、记录并能够证明其为已确定目的处理PII时符合相关合法依据。
A.1.2.4	确定何时及如何获取同意	组织应确定并记录一个流程，以证明是否、何时以及如何从个人信息主体处获得处理个人信息的同意。
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 的各自角色和职责（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，以支持其处理个人信息（PII）的义务。

表 A.1 (续)

对PII主体的义务		
目标：确保向PII主体提供关于其PII处理的适当信息，并履行与处理其PII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对 PII 主体在处理其 PII 方面的法律、法规和商业义务，并提供履行这些义务的手段。
A.1.3.3	确定个人信息主体的信息	该组织应确定并记录向个人信息主体提供的关于其个人信息处理情况的信息内容及提供时间。
A.1.3.4	向PII主体提供信息	组织应向PII主体提供清晰且易于获取的信息，明确标识PII控制者并说明其PII的处理方式。
A.1.3.5	提供修改或撤回同意的机制	组织应为PII主体提供修改或撤回其同意的机制。
A.1.3.6	提供机制以反对PII处理	该组织应提供机制，使个人信息主体能够反对对其个人信息的处理。
A.1.3.7	访问、更正或删除	该组织应实行政策、程序或机制，以履行其对个人信息主体访问、更正或删除其个人信息的义务。
A.1.3.8	PII 控制者向第三方告知的义务	组织应将共享个人信息的任何修改、撤回或异议告知共享方的第三方，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	当个人信息主体提出要求时，组织应能够提供所处理个人信息的副本。
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信息自动化处理所作出的、与个人信息主体相关的决策而产生的义务（包括法律义务），并能证明其如何履行这些义务。
隐私保护目标：通过设计和默认隐私机制确保流程与系统在使用、披露、收集、存储、保留、传输及处置个人信息时，		A.1.4.2. 确保隐私保护措施（包括隐私保护目标、隐私保护设计和隐私保护默认设置）的设计，使个人信息的收集、处理、处置仅限于实现已确定目的所必需的范围。
A.1.4.2	限制收集	该组织应将个人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	处理结束时的个人信息去标识化与删除	该组织应在原始个人信息不再用于已确定目的时，立即删除该信息或将其转换为无法识别或重新识别信息主体的格式。
A.1.4.7	临时文件	组织应确保根据文件记录的程序，在规定的文件记录期限内处置（例如删除或销毁）因处理 PII 而创建的临时文件。

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	该组织应制定关于处理个人身份信息的书面政策、程序或机制。
A.1.4.10	个人身份信息传输控制	组织应针对通过数据传输网络传输的个人身份信息（例如发送至其他组织）实施适当控制措施，确保数据送达预定目的地。
PII 共享、目的转移和披露确定是否以及根据适用：确定是否进行传输和披露，并根据适用情况进行记录。		A.1.5.2
A.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个人身份信息的依据。
A.1.5.3	可向其转移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PII的情况，包括披露了哪些PII、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	营销和广告用途	该组织不得在未事先获得相关个人身份信息主体同意的情况下，将合同处理的个人身份信息用于营销和广告目的。该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	如果组织认为某项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	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，以证明其履行了（适用合同中规定的）代表客户处理个人身份信息（PII）的义务。
义务目标：针对PII主体及本人	确保向PII主体提供其PII处理相关的适当信息	向PII主体提供与其PII处理相关的适当信息。

表 A.1 (续)

A.2.3.2	遵守对PII主体的义务	该组织应向客户提供履行其与PII主体相关义务的手段。
---------	-------------	----------------------------

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（PII）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	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销毁（例如删除或销毁）
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。
PII共享，目标：转移和披露 根据适用义务确定是否共享、确定是否进行转移或披露个人身份信息，并记录相关情况。披露，并记录情况。根据适用义务记录。		是否共享、向其他司法管辖区或第三方转移个人身份信息。
A.2.5.2	管辖区间个人身份信息转移的依据	该组织应及时告知客户跨司法管辖区转移个人身份信息（PII）的依据及任何拟议变更，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	组织应记录向第三方披露的PII信息，包括披露了哪些PII信息、向谁披露以及何时披露。
A.2.5.5	PII 披露请求的通知	该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。
A.2.5.6	具有法律约束力的PII披露	该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 之前应咨询相应的客户，并接受经相应客户授权的、合同约定的 PII 披露请求。
A.2.5.7	披露处理PII的分包商	在使用之前，组织应向客户披露是否使用任何分包商处理 PII。
A.2.18	聘请分包商处理PII	该组织仅应根据客户合同聘请分包商处理个人身份信息。
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，组织应将任何关于增加或更换处理 PII 的分包商的变更计划告知客户，从而让客户有机会对此类变更提出异议。

表 A.3 — 个人身份信息控制者和处理者的控制目标与控制措施

PII 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	涉及个人身份信息处理的信息安全政策应予以制定，经管理层批准后发布，并传达给相关人员及相关利益相关方以供确认。方确认，并按计划周期及发生重大变更时进行审查。

表 A.2 (续)

A.3.4	信息安全角色与职责	应根据组织需求定义并分配与个人身份信息处理相关的信息安全角色与职责。
-------	-----------	------------------------------------

表 A.3 (续)

A.3.5	信息分类	应根据组织的资讯安全需求对资讯进行分类，同时考虑个人身份信息，并基于保密性、完整性、可用性以及相关利益方的要求。
A.3.6	信息标记	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）。
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	与个人身份信息处理相关的个人身份信息及其他关联资产的访问权限，应依据组织关于访问控制的专题政策及规则进行配置、审查、修改和撤销。
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	与个人身份信息处理相关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	与处理个人身份信息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，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	该组织处理个人身份信息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。
A.3.16	信息安全政策、规则和标准的合规性	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（与 PII 处理相关）的合规性。
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、与其工作职能相关的组织信息安全政策、专题政策和程序。
A.3.18	保密或不披露协议	保密协议或不披露协议应明确体现组织对个人身份信息（PII）的保护需求，需予以识别、记录、定期审查，并由相关人员及其他利益相关方签署。
A.3.19	书桌与清屏	应制定并适当执行针对纸质文件和可移动存储介质的书桌规则，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	含有存储个人身份信息的存储介质的设备，在处置或再利用前应进行验证，确保已清除所有敏感数据及授权软件，或已进行安全覆盖。
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	应根据信息访问限制实施与 PII 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	密码技术的使用	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，包括加解密密钥管理。
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安全信息要求。
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PII相关安全系统的工程原则，以指导任何信息系统开发活动。
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得到适当选择、保护和管理。

附件B (规范性)

个人身份信息控制者与处理者的实施指南

B.1 PII控制者的实施指南

B.1.1 总则

本条款为PII控制器提供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 识别并记录目的 控制

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悉其信息处理目的。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.1.3.3](#)）。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

该组织应确定、记录并能够证明其处理个人身份信息（PII）以实现已识别目的的行为符合相关法律依据。

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充分确立。

处理PII的法律依据可包括：

—— 个人身份信息主体的同意；

- 履行合同；
- 履行法律义务；
- 保护PII主体的重大利益；
- 为公共利益而执行的任务；
- 个人身份信息控制者的合法利益。

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，但需与保护隐私的个人身份信息主体义务保持平衡。

每当根据个人身份信息的性质（例如健康信息）或相关主体（例如涉及儿童的个人身份信息）定义特殊类别的个人身份信息时，组织应将其纳入分类体系。

此类PII的分类标准可能因司法管辖区而异，也可能因适用于不同业务类型的监管制度存在差异，因此组织应明确所处理PII适用的具体分类标准。

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 确定何时及如何获取同意 控制

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）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。

部分司法管辖区对同意的收集与记录方式有特殊要求（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）及特定类别的PII主体（如儿童）可能需满足额外要求。组织应考虑此类要求，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

该组织应根据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（例如同意提供的时间、PII主体的身份识别信息及同意声明）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：

- 自由给予；
- 明确处理目的；且
- 明确且明确。

B.1.2.6 隐私影响评估控制

当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，组织应评估隐私影响评估的必要性，并在适当情况下实施该评估。

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。某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（例如健康相关信息、种族或族裔、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。这些要素可包括处理的个人身份信息（PII）类型清单、PII的存储位置及其可能的传输路径。数据流图和数据映射在此过程中同样具有参考价值。

注：有关可为隐私影响评估或其他风险评估提供依据的PII处理文档化信息详情，请参见[B.1.2.9条款](#)。

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方签订书面合同，并确保合同中明确要求实施[表A.2](#)所列的相应控制措施。

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，但为保持与本文件的一致性，所有控制措施均应纳入考量并载入文件化信息。

B.1.2.8 联合PII控制者控制

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

实施指南

应以透明方式确定处理PII的职责分工。

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信息（PII）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：

- 共享PII的目的/共同PII控制者关系；
- 参与共同控制关系的组织（PII控制者）身份；
- 协议下共享或转移及处理的PII类别；
- 处理操作的概述（例如转移、使用）；
- 相关角色与职责的描述；
- 实施保护个人信息的技术和组织安全措施的责任；
- 个人信息泄露事件中的责任划分（例如：通知主体、通知时限、信息共享机制）；
- PII的保留或处置条款；
- 违反协议的责任承担；
- 如何履行对PII主体的义务；
- 如何向PII主体提供涵盖联合PII控制者之间安排核心内容的信息；
- PII主体如何获取其有权接收的其他信息；以及
- 个人信息主体的联络点。

B.1.2.9 与处理PII相关的记录控制

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

可通过记录组织开展的PII处理活动清单或目录来维护PII处理的书面信息。该清单可包含：

- 处理类型；
- 处理目的；
- 个人信息的类别及其主体（例如儿童）的描述；
- 已披露或将披露PII的接收方类别，包括第三国或国际组织的接收方；
- 技术和组织安全措施的一般性描述；以及
- 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PII主体的义务

B.1.3.1 目标

确保向个人信息主体提供关于其个人信息处理的适当信息，并履行与处理其个人信息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

组织应确定并记录其在处理个人信息过程中对个人信息主体的法律、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 主体的义务及支持这些义务的手段因司法管辖区域而异。

该组织应确保提供适当的途径，以便以可及且及时的方式履行对个人信息主体的义务。应向个人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。

该联络点应采用与收集PII及获取同意时相同的方式提供（例如：若通过电子邮件或网站收集PII，则联络点应通过电子邮件或网站实现，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

该组织应确定并记录向个人信息主体提供的关于其个人信息处理情况的信息内容及提供时间。

实施指南

组织应确定向PII主体提供信息（例如在处理前、自请求起特定时限内）的法律、法规或业务要求，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示例如下：

- 处理目的说明（参见B.1.2.2）；
- 个人数据控制者或其代表的联系方式；
- 处理个人身份信息的合法依据说明（参见B.1.2.3）；
- 若非直接从个人信息主体处获取，则需说明获取来源；
- 提供个人信息是否属于法定或合同要求的信息，以及在适用情况下，未提供个人信息可能产生的后果；
- 关于对PII主体的义务（如B.1.3.2所述）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、要求删除、获取其PII副本以及反对处理的权利；
- 关于PII主体如何撤回同意的信息（参见B.1.3.5）；
- 关于PII转移的信息；
- 关于PII接收方或接收方类别的信息；

- 关于PII保留期限的信息；
- 关于基于个人信息自动化处理的自动化决策使用信息；
- 关于投诉权及投诉方式的信息；
- 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

该组织应向个人信息主体提供清晰且易于获取的信息，明确个人信息控制者的身份，并说明其个人信息的处理方式。

实施指南

该组织应以清晰简洁、完整透明、通俗易懂且便于获取的形式，向PII主体提供[B.1.3.3条款](#)所列信息，使用符合目标受众需求的简明语言。

在适当情况下，应在收集PII时提供上述信息，且该信息应永久可获取。

注 图标和图像可通过提供处理目的的视觉概览，对PII主体有所帮助。

B.1.3.5 提供修改或撤销同意的机制

组织应为PII主体提供修改或撤回同意的机制。

实施指南

该组织应告知个人信息主体其随时撤回同意的权利（具体权利可能因司法管辖区而异），并提供相应的撤回机制。撤回机制的选择取决于系统特性，在可能的情况下应与获取同意时采用的机制保持一致。例如，若通过电子邮件或网站获取同意，撤回机制也应采用相同渠道，而非电话或传真等替代方案。

修改同意书可包含对PII处理的限制条款，包括在特定情况下禁止PII控制者删除相关信息。

某些司法管辖区对个人信息主体修改或撤回同意的时间和方式施加了限制。

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

当撤回对特定个人信息（PII）处理的同意时，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

用于新的处理活动。例如，若PII主体撤回其对画像处理的同意，则不应继续使用或查阅其画像信息。

B.1.3.6 提供反对处理PII的机制控制

组织应为PII主体提供反对处理其PII的机制。

实施指南

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

组织应记录与个人信息主体反对处理行为相关的法律法规要求（例如反对将个人信息用于直接营销目的的处理）。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，使个人信息主体能够在提出请求时及时获取、更正或删除其个人信息，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的时间与方式设有限制。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

该组织应采取适当措施，在考虑现有技术的前提下，向第三方通报任何涉及共享PII的修改、撤销同意或异议事项。

该组织应确定并保持与第三方之间的有效沟通渠道。相关职责可分配给负责其运营和维护的个人。在向第三方通报时，该组织应监控其对信息接收的确认情况。

注：因个人信息主体权利产生的变更可能包括：修改或撤销同意、要求更正、删除或限制处理，或根据个人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

该组织应能在个人信息主体提出请求时，提供所处理的个人身份信息的副本。

实施指南

该组织应以结构化、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了组织应向PII主体或接收方PII控制者提供可移植格式（通常为结构化、常用且机器可读）的已处理PII副本的情形。

该组织应确保向PII主体提供的任何PII副本均与该主体直接相关。

若所请求的个人信息（PII）已根据保留与处置政策（详见B.1.4.8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，或要求提交投诉。

某些司法管辖区允许组织在特定情况下收取费用（例如处理过多或重复请求时）。

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

组织应明确对PII主体承担的义务（包括法律义务），包括：

组织基于个人身份信息（PII）的自动化处理所作出的、与PII主体相关的决策，并能证明其如何履行这些义务。

实施指南

某些司法管辖区规定了当仅基于个人身份信息自动化处理的决策对其产生重大影响时，对个人身份信息主体的具体义务，例如通知自动化决策的存在、允许个人身份信息主体反对此类决策，或获取人工干预。

注 在某些司法管辖区，某些PII处理无法完全自动化。

在这些司法管辖区内运营的组织应能证明其如何考虑遵守这些义务。

B.1.4 隐私设计与隐私默认

B.1.4.1 目标

确保流程和系统设计时，个人身份信息（PII）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.1.4.2 限制收集控制

组织应将PII收集范围限制在与已确定目的相关、相称且必要的最小限度。

实施指南

组织应将个人身份信息的收集限制在与已确定目的相关、必要且充分的范围内。这包括限制组织间接收集的个人身份信息量（例如通过网络日志、系统日志）。

默认隐私原则意味着：在收集和处置PII存在任何可选性时，所有选项应默认禁用，仅在PII主体明确选择后启用。

B.1.4.3 限制处理控制

组织应将PII的处理限制在与已确定目的相关、必要且充分的范围内。

实施指南

应通过信息安全与隐私政策（参见5.2节）及配套的实施与合规性书面程序来管理PII处理的限制。

个人身份信息的处理应默认限制在实现已确定目的所需的最低限度。此类处理包括：

— 披露；

- 个人身份信息存储期限；以及
- 谁可以访问其PII。

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其整个生命周期内，始终保持与处理目的相符的必要准确性、完整性和时效性。

实施指南

该组织应实施政策、程序或机制，以最大限度地减少其处理的个人身份信息中的不准确信息。还应制定政策、程序或机制，以应对个人身份信息不准确的情况。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），并应贯穿个人身份信息的整个生命周期。

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标准第6.2节。

B.1.4.5 个人身份信息最小化目标控制

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

实施指南

组织应说明所收集和处理的特定个人身份信息及其数量如何限定于已确定的目的范围。这可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，在此情况下，组织应能描述此类处理活动。

在其他情况下，既定目的并不要求处理原始个人身份信息，而处理经去标识化的个人身份信息即可满足既定目的。此类情形下，组织应明确并记录个人身份信息与信息主体关联的程度，同时制定处理个人身份信息的机制与技术看案，确保实现去标识化与个人身份信息最小化目标。

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）。

在处理去标识化数据足以满足使用目的的情况下，组织应及时记录任何为实现其设定的去标识化目标而设计的机制（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即可满足组织实现其既定目的的要求。在其他情况下，可采用其他去标识化技术（如概化处理——例如四舍五入，或随机化技术——例如添加噪声）来实现足够的去标识化水平。

注1 有关去标识化技术的更多信息，请参阅ISO/IEC 20889。

注2对于云计算，ISO/IEC 19944-1提供了数据识别限定符的定义，可用于分类数据识别PII主体的程度，或将PII主体与PII中的一组特征关联起来。

B.1.4.6 处理结束时的 PII 去标识化和删除 控制

组织应删除PII或将其转换为无法识别或重新识别主体的形式。
一旦原始个人信息不再用于已确定的目的，应立即识别个人信息主体。

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 临时文件管控

组织应确保因处理PII而产生的临时文件
(例如删除或销毁)，且须遵循记录在案的程序并在规定期限内完成。

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可能生成临时文件。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，但"垃圾回收"程序应能识别相关文件，并判定其上次使用时间。

B.1.4.8 保留控制

组织不应将个人信息保留超过处理该信息之目的所需的期限。
处理目的所需的时间。

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。当相关要求存在冲突时，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

组织应制定书面化的政策、程序或机制来处置个人信息。

实施指南

个人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，通常通过确保仅授权人员可访问传输系统，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，并准确送达至正确接收方。

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信息（PII），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

个人身份信息的转移可能受法律要求约束，具体取决于数据转移的管辖区或国际组织（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。

某些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此类要求。

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信息而涉及的国家名单亦应包含在内。所列国家应参照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。

在正常运营之外，可能存在应法律机构要求进行数据转移的情况，此类转移无法预先指定国家身份，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.1.5.4 个人信息控制转移记录

该组织应记录向第三方或从第三方转移个人信息的行为，并确保与这些第三方合作，以支持未来与个人信息主体义务相关的请求。

实施指南

记录内容可包括：因PII控制者履行管理义务而修改后从第三方接收的PII，或为响应PII主体的合法请求（包括撤销同意后要求删除PII的请求）而向第三方传输的PII。

该组织应制定政策明确此类记录的保留期限。

该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管控

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

个人信息在常规运营中可能被披露，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）也需记录。记录应包含披露来源及授权披露的依据来源。

B.2 个人信息处理者的实施指南

B.2.1 总则

本条款为个人信息处理者提供个人信息管理系统的指导，涉及表A.2所列的控制措施。

B.2.2 收集与处理的条件

B.2.2.1 目标

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

B.2.2.2 客户协议控制措施

组织应确保（在相关情况下）处理PII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（视具体情况而定，并根据客户的角色——即个人身份信息控制者或个人身份信息处理者）：

- 隐私设计与隐私默认（参见B.1.4和B.2.4）；
- 实现处理过程的安全性；
- 向监管机构通报涉及PII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PII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。

为实现客户目标，组织在符合客户总体指示但未获客户明确指示的情况下，可基于技术原因自主确定个人身份信息（PII）的处理方式。例如，为高效利用网络或处理能力，可能需要根据PII主体的特定特征分配专属处理资源。

该组织应允许客户验证其是否符合目的限定原则。这同时确保组织及其分包商不会将个人身份信息用于客户书面指示中未明确的其他目的。

B.2.2.4 营销与广告用途管控

组织不得在未获得相关PII主体事先同意的情况下，将合同处理的PII用于营销和广告目的。组织不应将提供此类同意作为接受服务的条件。

实施指南

个人身份信息处理方应遵守客户的合同要求，并对此进行记录，尤其在计划开展营销或广告活动时。

若未从个人身份信息主体处公平获得明确同意，组织不应坚持将营销或广告用途纳入条款。

注 本控制措施是对B.2.2.3中更普遍控制措施的补充，而非替代或取代。

B.2.2.5 侵权指令控制

如果组织认为某项处理指令违反了适用的法律要求，应告知客户。
法律要求时，应告知客户。

实施指南

该组织能否核实指令是否违反法律要求，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

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：组织是否允许并协助客户或客户指定/认可的其他审计机构进行审计。

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记录以支持证明
遵守其（在适用合同中规定的）代表客户处理个人身份信息（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；
- 向第三国或国际组织转移的情况；以及
- 技术与组织安全措施的描述。

B.2.3 对个人身份信息主体的义务

B.2.3.1 目标

确保向PII主体提供其PII处理相关的适当信息，并履行与PII处理相关的其他适用义务。

B.2.3.2 遵守对个人身份信息主体的义务 控制

该组织应向客户提供履行其与PII原则相关义务的手段。

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为履行相关义务而使用组织服务的情形，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以履行对PII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（PII）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。

B.2.4.2 临时文件管控

组织应确保因处理PII而产生的临时文件（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 个人身份信息控制的归还、转移或处置

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个人身份信息处置政策，并在客户要求时提供该政策。

该政策应涵盖合同终止后个人身份信息（PII）处置前的保留期限，以防止因合同意外失效导致客户的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

组织应针对通过数据传输网络传输的 PII 实施适当的控制措施，以确保数据到达预定目的地。

实施指导

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），以确保个人信息在传输过程中不被泄露，并准确送达至指定接收方。传输管控要求可纳入个人信息处理方与客户之间的合同条款。

若未签订涉及传输的合同条款，传输前可酌情征询客户意见。

B.2.5 个人身份信息的共享、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信息，或根据适用义务披露个人信息，并记录相关时间节点。

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的依据及任何拟议变更，以便客户可对变更提出异议或终止合同。

实施指南

个人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，但不得将个人信息转移至其他国家）。

涉及个人信息跨境转移时，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向其转移个人身份信息国家及国际组织。

实施指南

应向客户披露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。该名单应包含因外包个人信息处理业务而涉及的国家。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数据转移的情况，此类转移无法事先指定国家身份，或适用司法管辖区为保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

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。对象及时间。

实施指南

个人信息可在常规运营过程中披露。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。记录应包含披露来源及披露授权来源。

B.2.5.5 个人信息披露请求通知管控

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

该组织应拒绝任何不具法律约束力的个人信息披露请求，在披露任何个人信息前应咨询相关客户，并接受经相关客户授权且合同约定的个人信息披露请求。

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、法庭及行政机构，且可能涉及任何司法管辖区。

B.2.5.7 披露用于处理个人身份信息的分包商控制

使用前，组织应向客户披露是否使用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。披露信息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）。

当评估认为公开分包商信息会导致安全风险超出可接受范围时，应在保密协议框架下或应客户要求披露。需告知客户该信息可供查阅。

此规定不涉及个人身份信息可转移的国家名单。该名单应在所有情况下向客户披露，以便客户通知相关个人身份信息主体。

B.2.5.8 委托分包商处理个人身份信息管控

该组织仅应根据客户合同要求分包商处理个人身份信息。

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必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。

该组织应与其委托处理个人身份信息的分包商签订书面合同。该组织应确保与分包商签订的合同涵盖**实施表A.2**中规定的相应控制措施。

组织与任何代其处理个人身份信息的分包商签订的合同，应要求分包商实施**表A.2**中规定的适当控制措施，同时需考虑信息安全风险评估流程（参见6.1.2）以及个人身份信息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，所有控制措施均应纳入考量并载入文件化信息。

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，使客户有权对变更提出异议。

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 针对PH控制者与PH处理者的实施指南

B.3.1 目标

确保个人信息处理的安全性。

B.3.2 通用要求

本条款为个人信息（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 信息安全控制政策

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

无论是通过制定独立的隐私政策，还是通过完善信息安全政策，组织都应发布声明，表明其支持并致力于遵守适用于个人信息保护的法律要求，以及遵守组织与其合作伙伴、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保护的法律法规。

B.3.4 信息安全角色与职责管控

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PII处理事宜联系的对接人。当组织作为PII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与隐私计划，以确保遵守所有关于处理个人信息（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信息处理的管理事务；

- 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；
- 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；
- 就组织开展的隐私影响评估提供建议。

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 信息分类与管控

信息应根据组织的资讯安全需求进行分类，在考虑个人身份信息的基础上，依据保密性、完整性、可用性及相关利益相关方要求进行划分。

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）、存储位置及流通过程至关重要。

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个人身份信息的定义以及如何识别属于个人身份信息的信息。

B.3.7 信息传输

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

应管理与个人身份信息处理相关的身份的完整生命周期。

实施指南

处理PII的系统及服务管理员或操作员的注册与注销流程，需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）的损毁或泄露。

对于处理 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。

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特定要求。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

访问个人身份信息（PII）及其相关处理资产的权限应依据组织针对访问控制制定的专题政策与规则进行配置、审查、修改及撤销。

实施指南

组织应为获准访问信息系统及其所含PII的用户，建立准确且持续更新的用户档案记录。每份档案包含用户相关数据集（含用户ID），这些数据是实施已确定技术控制措施以实现授权访问的必要依据。

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，并追踪其进行的增删改操作。此举不仅保护了组织机构，也保障了用户权益——用户可清晰辨识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个人身份信息处理时，客户可负责访问管理的部分或全部环节。在适当情况下，组织应为客户提供执行访问管理的手段，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 供应商协议中的信息安全管控

应根据供应商关系类型，与各供应商建立并确认与PII处理相关的信息安全要求。

实施指南

组织应在与供应商的协议中明确说明是否处理个人身份信息，并规定供应商必须满足的最低技术和组织措施要求，以确保组织履行其信息安全和个人身份信息保护义务（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，明确划分组织与其合作伙伴、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，且该合规性须为客户所接受。

注 此类审核可考虑参照ISO/IEC 27001等相关适用安全标准的合规性。

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：个人身份信息仅可依据其指令进行处理。

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、建立并传达事件管理流程、角色与职责，为处理涉及个人身份信息（PII）的信息安全事件制定管理计划并做好准备。

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PII泄露事件的责任与程序。此外，组织还应制定向相关方通报PII泄露事件（包括通报时限）及向监管机构披露的责任与程序，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

涉及个人身份信息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。

事件未必必然触发此类审查。

注1：信息安全事件未必会导致实际或极可能发生的对 PII 或组织内存储 PII 的任何设备或设施的未经授权访问。这些事件包括但不限于：对防火墙或边缘服务器的 ping 及其他广播攻击、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形，以及应向个人身份信息主体通报的情形。

通知应清晰明确。

注释2 通知可包含以下细节：

- 可获取更多信息的联络点；数据泄露事件的描述及可能后果；
- 违规事件说明（含受影响个人数量及相关记录数量）；
- ；
- 已采取或计划采取的应对措施。

注3 有关安全事件管理的信息可参见ISO/IEC 27035系列标准。

当涉及个人身份信息（PII）的泄露事件发生时，应保留包含充分信息的记录，以便为监管或取证目的提供报告，例如：

- 事件描述；
- 时间段；

- 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）；
- 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，记录还应包含已知受损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具体步骤。

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（即发现后尽快）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；
- 时间段；
- 事件后果；
- 报告人姓名；
- 事件上报对象；
- 为解决事件采取的措施（包括负责人及恢复的数据）；
- 该事件导致个人身份信息不可用、丢失、泄露或被篡改的事实。

若发生涉及个人身份信息的泄露事件，记录还应包含已知泄露个人身份信息的描述；若已采取通知措施，则需说明通知客户或监管机构的具体步骤。

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PII保护机构）通报涉及PII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

组织应识别与个人信息处理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，概述双方在安全、隐私及个人身份信息保护方面的责任。合同条款可在责任违约时提供合同制裁依据。

B.3.14 记录保护控制

与PII处理相关的记录应受到保护，防止丢失、毁损、篡改、未经授权的访问及未经授权的披露。

实施指南

可能需要审查当前及历史政策和程序（例如在客户争议解决及监管机构调查等情形下）。

组织应按照其保留计划（参见B.1.4.8）规定的期限，保留隐私政策及相关程序的副本。这包括在文件更新时保留其历史版本。

B.3.15 信息安全控制的独立审查

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、规则和标准的合规性控制

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合规性。

实施指南

作为安全政策与标准合规性技术审查的一部分，组织应纳入审查处理PII相关工具及组件的方法，包括：

- 持续监控以验证仅进行许可处理；或
- 特定渗透或漏洞测试（例如，去标识化数据集可接受动机入侵者测试，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培训，并定期更新组织信息安全

政策、特定主题政策和程序，这些内容与其工作职能相关，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 需求的保密或不披露协议。

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

应制定并适当执行针对文件和可移动存储介质的清桌规则，以及针对信息处理设备的清屏规则。

实施指南

组织应将包含个人身份信息的纸质材料创建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

应根据组织的分类方案和处理要求，对包含个人身份信息的存储介质在其获取、使用、运输和处置的生命周期内进行管理。

实施指南

组织应记录任何使用可移动介质或设备存储PII的情况。在可行时，组织应使用支持加密功能的物理可移动介质或设备存储PII。未加密介质仅在不可避免时使用，且使用未加密介质或设备时，组织应实施程序及补偿性控制措施（如防篡改包装）以降低PII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，应建立系统记录含个人身份信息的进出物理介质，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，确保数据仅在目的地可被访问，传输过程中不可被获取。

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PII。

注： 确保离开组织场所的物理介质上的PII不被普遍访问的一种可行措施是加密相关PII，并将解密权限限制在授权人员范围内。

可移动存储介质一旦带离组织物理边界，便容易丢失、损坏或遭不当访问。对可移动存储介质进行加密可为个人身份信息（PII）增添一层保护，即使存储介质遭泄露，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

含有存储个人身份信息的存储介质的设备，在处置或再利用前应进行验证，确保所有敏感数据和授权软件已被移除或安全覆盖。

实施指南

组织应确保每次重新分配存储空间时，此前存储于该空间的任何个人身份信息均不可被访问。

关于从信息系统中删除个人身份信息（PII），性能问题可能导致明确清除该PII难以实现。这会产生其他用户可能访问PII的风险。应通过具体技术措施规避此类风险。

为确保安全处置或再利用，凡可能存有PII的存储介质设备，均应按实际存有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上、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

应根据信息访问限制实施与 PII 处理相关的安全认证技术和程序。

实施指南

当客户要求时，组织应为客户控制下的任何用户账户提供安全登录程序的能力。

B.3.24 信息备份控制

应定期维护并测试个人身份信息（PII）的备份副本，以及与PII处理相关的软件和系统。
定期测试。

实施指南

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

在此方面，与个人信息相关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。

若组织明确向客户提供备份与恢复服务，则应向其提供关于个人信息备份与恢复能力的清晰说明。

部分司法管辖区对PII备份频率、备份审查测试周期或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规定。

在某些情况下，可能需要恢复个人信息（PII），例如系统故障、攻击或灾难发生时。当恢复PII（通常从备份介质恢复）时，应建立相应流程，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情况时，立即启动解决流程（可能需要涉及PII主体）。

组织应建立PII恢复操作规程及相关日志记录。PII恢复操作日志至少应包含以下内容：

- 修复负责人姓名；
- 恢复的个人信息（PII）的描述。

部分司法管辖区对个人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的个人信息（PII）的复制件或备份副本，适用本文件中针对分包处理PII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 日志控制

应生成、存储、保护并分析记录与PII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，事件日志应记录对个人信息（PII）的访问行为，包括：访问者身份、访问时间、被访问的PII主体信息，以及事件导致的变更内容（如有），例如新增、修改或删除操作。

当多个服务提供商参与服务提供时，在实施本指南过程中可能存在多样化或共享的角色。这些角色应明确定义并纳入文件化信息中，同时需明确各提供商之间日志访问权限的协议。

用于安全监控和运行诊断等目的的日志信息可能包含个人信息（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。

应建立程序（最好是自动程序），确保日志信息按照保留计划（参见B.1.4.8）的规定进行删除或去标识化处理。

PII处理者的实施指南

该组织应制定相关标准，明确日志信息何时、如何以及是否可供客户获取或使用。这些标准应向客户公开。

当组织允许客户访问其控制的日志记录时，组织应实施适当控制措施，确保客户：

- 仅能访问与其自身活动相关的记录；
- 不得访问涉及其他客户活动的日志记录；以及
- 不得以任何形式修改日志。

B.3.26 密码技术使用控制

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、护照号和驾驶执照号。

该组织应向客户说明其在处理个人身份信息时采用加密技术进行保护的具体情形。同时，该组织还应向客户说明其提供的任何可协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

应建立并实施与PII处理相关的软件及系统安全开发规则。

实施指南

系统开发与设计政策应包含组织处理个人身份信息需求的指导方针，该方针需基于对个人身份信息主体的义务、任何适用的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隐私原则（参见ISO/IEC 29100）的指导；
- b) 设计阶段的隐私与PII保护要求，可基于隐私风险评估或隐私影响评估（参见B.1.2.6）的输出结果；
- c) 项目里程碑中的个人身份信息保护检查点；
- d) 必需的隐私与PII保护知识；
- e) 默认情况下，尽量减少对PII的处理。

B.3.28 应用程序安全要求控制

在开发或获取应用程序时，应识别、明确并批准与PII处理相关的信息安全要求开发或采购应用程序时。

实施指南

组织应确保通过不可信数据传输网络传输的PII进行加密传输。

不可信网络包括公共互联网及其他超出组织运营控制范围的设施。

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部或流量数据以实现有效传输。

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相关的安全系统工程原则，以指导所有信息系统开发活动。

实施指南

涉及个人身份信息处理的系统或组件应遵循隐私设计和隐私默认原则进行设计，并预先规划和促进相关控制措施的实施（如B.1和B.2分别针对个人身份信息控制者和处理者所述），尤其应确保该类系统中个人身份信息的收集与处理仅限于实现已确定处理目的所必需的范围（参见B.1.2）。2）。

例如，处理PII的组织应确保在规定期限后销毁PII。处理该PII的系统设计应便于满足此删除要求。

注 法律要求可能适用。

B.3.30 外包开发管控

该组织应指导、监督并审查与外包的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个人身份信息。当无法避免使用个人身份信息进行测试时，应实施与生产环境中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，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
）

与ISO/IEC 29100的对照关系

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

表 C.1 — 个人身份信息（PII）控制者与 ISO/IEC 29100 隐私原则的对照表

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 确定获取同意的时间与方式 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. 目的合法性与规范性（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/IEC 29100:2024, 6.4）	A.1.2.6 隐私影响评估 A.1.4.2 限制收集
4. 数据最小化（ISO/IEC 29100:2024, 6.5）	A.1.4.3 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、保留与披露限制（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 销毁 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. 个人参与与访问权限 (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 向个人身份信息主体提供信息 A.1.3.7 访问、更正或删除 A.1.3.9 提供已处理个人身份信息的副本 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PII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PII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信息的国家及国际组织 A.1.5.4 PII 转移记录
10. 信息安全 (ISO/IEC 29100:2024, 6.11)	A.1.2.7 与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 隐私原则的对照表

ISO/IEC 29100 的隐私原则	PII处理者的相关控制措施
1. 同意与选择 (ISO/IEC 29100:2024, 6.2)	A. 2.2.6 客户义务
2. 目的合法性与具体说明 (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. 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的记录 A.2.5.5 个人身份信息披露请求通知 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 分包商变更以处理个人身份信息
8. 个人参与与访问权限 (ISO/IEC 29100:2024, 6.9)	A.2.3.2 履行对个人身份信息主体的义务
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 可转移PII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

附件 D
(信息性)

与《通用数据保护条例》的对照表

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（第43条除外）的参考对照关系。[\[61\]](#)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 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)
	(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)

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)(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)(l)、(32)(1)(a)
B.1.4.7	(5)(1)(c)

表 D.1 (续)

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)(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)

附录E（信息性）

与ISO/IEC 27018和ISO/IEC 29151的映射关系

ISO/IEC 27018为作为个人信息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为个人信息控制者处理个人信息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；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

本文件条款 本文件	ISO/IEC 27018 中的子条款	ISO/IEC 29151中的子条款
4	不适用	不适用
5	不适用	不适用
6	不适用	不适用
7	不适用	不适用
8	不适用	不适用
9	不适用	不适用
10	不适用	不适用
B.3.2	不适用	不适用
B.3.3、B.3.4、B.3.5、B.3.6、B.3.7、 B.3.8、B.3.9、B.3.10、B.3.11、 B.3.12、B.3.13、B.3.14、B.3.15、B.3.16	5.1、5.2、5.12、5.13、5.14、5.16、 5.18、5.20、5.24、5.26、5.31、 5.33、5.35、5.36、A.10.1、A.10.2、 A.11.8、A.11.9、A.11.10、A.11.11	5.1、5.2、5.12、5.13、5.14、5.16、 5.18、5.22、5.24、5.26、5.31、 5.33、5.35、5.36
B.3.17、B.3.18	6.3、6.6、A.11.1	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

附录F（信息性）

与ISO/IEC 27701:2019的对应关系

本附录旨在为当前使用该文件并希望过渡到新版文件的组织提供与前版文件（ISO/IEC 27701:2019）的向后兼容性。

表F.1列出了本文件附录A所规定控制措施与ISO/IEC 27701:2019中控制措施的对应关系。第一列中的"N/A"标识本文件未包含的控制措施，第二列中的"新增"标识ISO/IEC 27701:2019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 中的控制措施对应关系

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	与当局的关系
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合理使用
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	遵守信息安全政策、规则 and 标准
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	雇佣条款和条件
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	设备定位与保护
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	新增	信息删除
不适用	新	数据遮蔽
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	日志记录
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	安全系统架构和工程原则
不适用	新增	安全编码
不适用	6.11.2.8, 6.11.2.9	开发与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	审计测试期间的信息系统保护

表F.2列出了ISO/IEC 27701:2019第6条款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"不适用"标识了未包含在本文件中的控制措施。

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	内部安全角色与职责
6.3.1.2	不适用	职责分离
6.3.1.3	不适用	与当局的关系
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	可移动介质管理
6.5.3.2	A.3.20	介质处置
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	用户秘密认证信息管理
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	防范外部及环境威胁
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

表 F.2 (续)

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	恶意软件防护措施
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	信息传输政策和程序
6.10.2.2	A.3.7	信息传输协议
6.10.2.3	A.3.7	电子信息
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	公共网络上应用服务的保护
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

表 F.2 (续)

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, 管理体系审计指南
- [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
- [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
— 第二部分: 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及技术分类
- [5] ISO/IEC 27001, 信息安全、网络安全与隐私保护——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保护指南
- [9] ISO/IEC 27035 (全部部分), 信息技术——信息安全事件管理
- [10] ISO/IEC 150/27557, 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——个人身份信息保护实践准则
- [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) — 欧盟议会和理事会条例(EU) 2016/79



ICS 55.030
基于64页的定价

© ISO/IEC 2025
版权所有

[iso.org](https://www.iso.org)