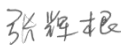


个人数据隐私保护管理体系认证技术规范

受控状态：（  ）

文件编号：CTS TBGL136-2026

编制：技术部

审核：张辉根 

批准：周春阳 

首次发布日期：20221220

首次生效日期：20221220

修订日期：20260210

江西腾标认证有限公司

目 录

1. 范围 3

2. 规范性引用文件 3

3. 术语和定义 3

4. 组织环境 3

5. 领导作用 4

6. 策划 5

7. 支持 5

8. 运行 8

9. 绩效评价 8

10. 改进 9

1. 范围

本标准给出了个人隐私保护管理体系的要求。本标准适用于所有类型及规模的组织。

2. 规范性引用文件

无规范性引用文件。

3. 术语和定义

下列术语和定义适用于本文件。

3.1 最高管理者

在最高层指挥和控制组织的一个人或者一组人。

注1：最高管理者在组织内有授权和通过资源的权力。

注2：如果个人隐私保护管理体系的范围仅覆盖组织的一部分，在这种情况下，最高管理者是指管理

和控制组织的这部分的一个人或者一组人。

3.2 相关方

可影响决策或活动、受决策或活动所影响、或自认为受决策或活动所影响的个人或组织。

3.3 组织

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨和战略方向相关并影响其实现个人隐私保护管理体系预期结果的能力的各种外部和内部因素。

组织应对这些外部和内部因素的相关信息监视和评审。注 1:这

些因素可能包括需要考虑的正面和负面要素或条件。

注 2:考虑来自于国际、国内、地区或当地的各种法律法规、技术、竞争、市场、文化、社会和经济环境的因素，有助于理解外部环境。

注 3:考虑与组织的价值观、文化、知识和绩效等有关的因素，有助于理解内部环境。

4.2 理解相关方的需求和期望

由于相关方对组织稳定提供符合顾客要求及适用法律法规要求的产品和服务的能力具有影响或潜在影响，因此，组织应确定：

- a) 与个人隐私保护管理体系有关的相关方；
- b) 与个人隐私保护管理体系有关的相关方的要求。

组织应监视和评审这些相关方的信息及其相关要求。

4.3 确定个人隐私保护管理体系的范围

组织应确定个人隐私保护管理体系的边界和适用性，以确定其范围。

在确定范围时，组织应考虑：

- a) 4.1 中提及的各种外部和内部因素；
- b) 4.2 中提及的相关方的要求；

若组织使用了其他管理体系，考虑其与这些管理体系的相互作用。

该范围应以文件化信息的形式获取。

4.4 个人隐私保护管理体系

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进个人数据隐私保护管理体系，包括所需过程及其相互作用。

4.4.2 在必要的范围和程度上，组织应：

- a) 保持成文信息以支持过程运行；
- b) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1 领导作用和承诺

5.1.1 总则

最高管理者应通过以下方面，证实其对个人数据隐私保护管理体系的领导作用和承诺：

- a) 对个人数据隐私保护管理体系的有效性负责；
- b) 确保制定个人数据隐私保护管理体系的方针和目标，并与组织环境相适应，与战略方向相一致；
- c) 确保个人数据隐私保护管理体系要求融入组织的业务过程；
- d) 促进使用过程方法和基于风险的思维；
- e) 确保个人数据隐私保护管理体系所需的资源是可获得的；
- f) 沟通有效的管理和符合个人数据隐私保护管理体系要求的重要性；
- g) 确保个人数据隐私保护管理体系实现其预期结果；
- h) 促使人员积极参与，指导和支持他们为个人数据隐私保护管理体系的有效性做出贡献；
- i) 推动改进；
- j) 支持其他相关管理者在其职责范围内发挥领导作用。

注：本标准使用的“业务”一词可广义地理解为涉及组织存在目的的核心活动，无论是公有、私有、营利或非营利组织。

5.2 方针

5.2.1 制定方针

最高管理者应制定、实施和保持方针：

- a) 与组织的宗旨和环境并支持其战略方向；
- b) 为建立目标提供框架；
- c) 包括满足适用要求的承诺；
- d) 包括持续改进个人数据隐私保护管理体系的承诺。

5.2.2 沟通方针应：

- a) 可获取并保持成文信息；
- b) 在组织内得到沟通、理解和应用；
- c) 适宜时，可为有关相关方所获取。

5.3 组织的岗位、职责和权限

最高管理者应确保组织相关岗位的职责、权限得到分配、沟通和理解。最高管理者应分配职责和权限，以：

- a) 确保个人数据隐私保护管理体系符合本标准的要求；
- b) 确保各过程获得其预期输出；
- c) 报告个人数据隐私保护管理体系的绩效以及改进机会,特别是向最高管理者报告；
- d) 确保个人数据隐私保护管理体系的适宜性、充分性和有效性；
- e) 确保在策划和实施个人数据隐私保护管理体系变更时保持其完整性。

6. 策划

6.1 应对风险和机遇的措施

6.1.1 在策划个人隐私保护管理体系时，组织应考虑到 4.1 所提及的因素和 4.2 所提及的要求，并确定需要应对的风险和机遇，以：

- a) 确保个人隐私保护管理体系能够实现其预期结果；
- b) 增强有利影响；
- c) 预防或减少不利影响；
- d) 实现改进。

6.1.2 组织应策划：

- a) 应对这些风险和机遇的措施；
- b) 如何：
 - 1) 在个人隐私保护管理体系过程中整合并实施这些措施；
 - 2) 评价这些措施的有效性。

应对措施应与风险和机遇对产品和服务符合性的潜在影响相适应。

注 1:应对风险可选择规避风险，为寻求机遇承担风险，消除风险源，改变风险的可能性或后果，分担风险，或通过信息充分的决策而保留风险。

注 2:机遇可能导致采用新实践、推出新产品、开辟新市场、赢得新顾客，建立合作伙伴关系、利用新技术和其他可行之处，以应对组织或其顾客的需求。

6.2 目标及其实现的策划

6.2.1 组织应针对相关职能、层次和个人隐私保护管理体系所需的过程建立目标。目标应：

- a) 与方针保持一致；
- b) 可测量
- c) 考虑适用的要求；
- d) 与增强顾客满意相关；
- e) 予以监视；
- f) 予以沟通；
- g) 适时更新。

组织应保持有关目标的成文信息。

6.2.2 策划如何实现目标时，组织应确定：

- a) 要做什么；
- b) 需要什么资源；
- c) 由谁负责；
- d) 何时完成；
- e) 如何评价结果。

6.3 变更的策划

当组织确定需要对个人隐私保护管理体系进行变更时，变更应按所策划的方式实施。组织应考虑：

- a) 变更目的及其潜在后果；
- b) 个人隐私保护管理体系的完整性；
- c) 资源的可获得性；
- d) 职责和权限的分配或再分配。

7. 支持

7.1 资源

7.1.1 总则

组织应确定并提供所需的资源，以建立、实施、保持和持续改进个人数据隐私保护管理体系。

组织应考虑：

- a) 现有内部资源的能力和局限；
- b) 需要从外部供方获得的资源。

7.1.2 人员

组织应确定并配备所需的人员，以有效实施个人数据隐私保护管理体系，并运行和控制其过程。

7.1.3 基础设施

组织应确定、提供并维护所需的基础设施，以运行过程，并获得合格产品和服务。注：基础设施可包括：

- a) 建筑物和相关设施；
- b) 设备，包括硬件和软件；
- c) 运输资源；
- d) 信息和通讯技术。

7.1.4 过程运行环境

组织应确定、提供并维护所需的环境，以运行过程，并获得合格产品和服务。注：适宜的过程运行环境可能是人为因素与物理因素的结合，例如：

- a) 社会因素(如非歧视、安定、非对抗)；
- b) 心理因素(如减压、预防过度疲劳、稳定情绪)；
- c) 物理因素(如温度、热量、湿度、照明、空气流通、卫生、噪声)。由于所提供的产品和服务不同，这些因素可能存在显著差异。

7.1.5 监视和测量资源

7.1.5.1 总则

当利用监视或测量来验证产品和服务符合要求时，组织应确定并提供所需的资源，以确保结果有效和可靠。

组织应确保所提供的资源：

- a) 适合所开展的监视和测量活动的特定类型；
- b) 得到维护，以确保持续适合其用途。

组织应保留适当的成文信息，作为监视和测量资源适合其用途的证据。

7.1.5.2 测量溯源

当要求测量溯源时，或组织认为测量溯源是信任测量结果有效的基础时，测量设备应：

- a) 对照能溯源到国际或国家标准的测量标准，按照规定的时间间隔或使用前进行校准和(或) 检定，当不存在上述标准时，应保留作为校准或验证依据的成文信息；
- b) 予以识别，以确定其状态；
- c) 予以保护，防止由于调整、损坏或衰减所导致的校准状态和随后的测量结果的失效。当发现测量设备不符合预期用途时，组织应确定以往测量结果的有效性是否受到不利影响，

必要时 应采取适当的措施。

7.1.6 组织的知识

组织应确定必要的知识，以运行过程，并获得合格产品和服务。这些知识应予以保持，并能在所需的范围内得到。

为应对不断变化的需求和发展趋势，组织应审视现有的知识，确定如何获取或接触更多必要的知识 和知识更新。

注 1:组织的知识是组织特有的知识，通常从其经验中获得，是为实现组织目标所使用和共享的信息。

注 2:组织的知识可基于：

- a) 内部来源(如知识产权、从经验获得的知识、从失败和成功项目汲取的经验和教训、获取和分享未成文的知识和经验，以及过程、产品和服务的改进结果)；
- b) 外部来源(如标准、学术交流、专业会议、从顾客或外部供方收集的知识)。

7.2 能力

组织应：

- a) 确定在其控制下工作的人员所需具备的能力，这些人员从事的工作影响个人隐私保护管理体系绩效和有效性；
- b) 基于适当的教育、培训或经验，确保这些人员是胜任的；
- c) 适用时，采取措施以获得所需的能力，并评价措施的有效性；
- d) 保留适当的成文信息，作为人员能力的证据。

注：适用措施可包括对在职人员进行培训、辅导或重新分配工作，或者聘用、外包胜任的人员。

7.3 意识

组织应确保在其控制下工作的人员知晓：

- a) 方针；
- b) 相关的目标；
- c) 他们对个人隐私保护管理体系有效性的贡献，包括改进绩效的益处；
- d) 不符合个人隐私保护管理体系要求的后果。

7.4 沟通

组织应确定与个人隐私保护管理体系相关的内部和外部沟通，包括：

- a) 沟通什么；
- b) 何时沟通；
- c) 与谁沟通；
- d) 如何沟通；
- e) 谁来沟通。

7.5 成文信息

7.5.1 总则

组织的个人隐私保护管理体系应包括：

- a) 本标准要求的成文信息；
- b) 组织所确定的、为确保个人隐私保护管理体系有效性所需的成文信息。

注：对于不同组织，个人隐私保护管理体系成文信息的多少与详略程度可以不同，取决于：

- 组织的规模，以及活动、过程、产品和服务的类型；
- 过程及其相互作用的复杂程度；
- 人员的能力。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：

- a) 标识和说明(如标题、日期、作者、索引编号)；
- b) 形式(如语言、软件版本、图表)和载体(如纸质的、电子的)；
- c) 评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

7.5.3.1 应控制个人隐私保护管理体系和本标准所要求的成文信息，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(如防止泄密、不当使用或缺失)。

7.5.3.2 为控制成文信息，适用时，组织应进行下列活动：

- a) 分发、访问、检索和使用；
- b) 存储和防护，包括保持可读性；
- c) 更改控制(如版本控制)；
- d) 保留和处置。

对于组织确定的策划和运行个人隐私保护管理体系所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

对所保留的、作为符合性证据的成文信息应予以保护，防止非预期的更改。

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 运行策划和控制

为满足产品和服务提供的要求，并实施第 6 章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

- a) 确定产品和服务的要求；
- b) 建立下列内容的准则：
 - ① 过程；
 - ② 产品和服务的接收。
- c) 确定所需的资源以使产品和服务符合要求；
- d) 按照准则实施过程控制；
- e) 在必要的范围和程度上，确定并保持、保留成文信息，以：
 - ① 确信过程已经按策划进行；
 - ② 证实产品和服务符合要求。

策划的输出应适合于组织的运行。

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

组织应确保外包过程得到控制。

9. 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

- a) 需要监视和测量什么；
- b) 需要什么方法进行监视、测量、分析和评价，以确保结果有效；
- c) 何时实施监视和测量；
- d) 何时对监视和测量的结果进行分析和评价。
- e) 组织应评价个人隐私保护管理体系的绩效和有效性。

组织应保留适当的成文信息，以作为结果的证据。

9.2 内部审核

9.2.1 组织应按照策划的时间间隔进行内部审核，以提供有关个人隐私保护管理体系的下列信息：

a) 是否符合：

- ① 组织自身的个人隐私保护管理体系要求；
- ② 本标准的要求；

b) 是否得到有效的实施和保持。

9.2.2 组织应：

- a) 依据有关过程的重要性、对组织产生影响的变化和以往的审核结果，策划、制定、实施和保持审核方案，审核方案包括频次、方法、职责、策划要求和报告；
- b) 规定每次审核的审核准则和范围；
- c) 选择审核员并实施审核，以确保审核过程客观公正；
- d) 确保将审核结果报告给相关管理者；
- e) 及时采取适当的纠正和纠正措施；
- f) 保留成文信息，作为实施审核方案以及审核结果的证据。注：相关指南参见 GB/T 19011。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔对组织的个人隐私保护管理体系进行评审，以确保其持续的适宜性、充分性和有效性，并与组织的战略方向保持一致。

9.3.2 管理评审输入

策划和实施管理评审时应考虑下列内容：

- a) 以往管理评审所采取措施的情况；
- b) 与个人隐私保护管理体系相关的内外部因素的变化；
- c) 下列有关个人隐私保护管理体系绩效和有效性的信息，包括其趋势：
- ① 目标的实现程度；
 - ② 过程绩效；
 - ③ 不合格及纠正措施；
 - ④ 监视和测量结果；
 - ⑤ 审核结果；
- d) 资源的充分性；
- e) 应对风险和机遇所采取措施的有效性；
- f) 改进的机会。

9.3.3 管理评审输出

管理评审的输出应包括与下列事项相关的决定和措施：

- a) 改进的机会；
- b) 个人隐私保护管理体系所需的变更；
- c) 资源需求。

组织应保留成文信息，作为管理评审结果的证据。

10. 改进

10.1 总则

组织应确定和选择改进机会，并采取必要措施，以实现其个人隐私保护管理体系的预期结果。

10.2 不符合和纠正措施

10.2.1 当出现不符合时，组织应：

a) 对不符合做出应对，适用时：

- ① 采取措施控制并纠正不符合；
- ② 处置后果。

b) 通过下列活动，评价消除不符合原因的措施需求，以防止不符合再次发生或者在其他地方发生：

- ① 评审不符合；
- ② 确定不符合的原因；
- ③ 确定是否存在或是否可能发生类似的不符合。

c) 实施任何所需的措施；

d) 评审所采取的任何纠正措施的有效性；

e) 需要时，更新在策划期间确定的风险和机遇；

f) 需要时，变更个人数据隐私保护管理体系。

纠正措施应与不符合所产生的影响相适应。

10.2.2 组织应保留成文信息，作为下列事项的证据：

- a) 不符合的性质以及随后所采取的措施；
- b) 纠正措施的结果。

10.3 持续改进

组织应持续改进个人数据隐私保护管理体系的适宜性、充分性和有效性。

—————