T/CLAST

团 体 标 准

T/CLAST 002—2021

个人信息处理法律合规性评估指引

Guideline For Legal Compliance Assessment of Personal Information Processing

2021－12－06 发布　　2022－01－01 实施

中 国 科 学 技 术 法 学 会 发 布

T/CLAST

团　体　标　准

T/CLAST 002.1—2021

个人信息处理法律合规性评估指引
第 1 部分：概述和术语

Guideline For Legal Compliance Assessment of Personal Information Processing—

Prat 1：Overview and Vocabulary

2021－12－06 发布　　2022－01－01 实施

中 国 科 学 技 术 法 学 会 发 布

目次

前言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国科学技术法学会提出并归口管理。

本文件主要起草单位：中国科学技术法学会、深圳市北鹏前沿科技法律研究院、中国法学交流基金会、中国法律咨询中心、北京大学法学院/知识产权学院、北京大学粤港澳大湾区知识产权发展研究院、平安科技（深圳）有限公司、上海携程商务有限公司、北京小桔科技有限公司、阿里巴巴(北京)软件服务有限公司、每日互动股份有限公司、深圳市和讯华谷信息技术有限公司、广东北源律师事务所、上海市锦天城律师事务所、北京市浩天信和律师事务所、北京市金杜律师事务所、中国信息通信研究院云计算与大数据研究所、北京北大英华科技有限公司、网易(杭州)网络有限公司、腾讯科技（深圳）有限公司、荣耀终端有限公司、华米科技、OPPO 广东移动通信有限公司、比亚迪股份有限公司、广州小鹏汽车科技有限公司、深圳市大疆创新科技有限公司、深圳市地铁集团有限公司、上海游昆信息技术有限公司、贝壳找房（北京）科技有限公司、深圳市迷你玩科技有限公司、百行征信有限公司、深圳依时货拉拉科技有限公司、广东小天才科技有限公司、安信证券股份有限公司、深圳市安证企业合规管理（集团）有限公司、杭州安信检测技术有限公司、杭州安恒信息技术股份有限公司、深圳市网安计算机安全检测技术有限公司。

本文件主要起草人：张平、毕马宁、南红玉、黄亚英、肖声高、徐美玲、时建中、李玉香、周辉、涂俊峰、谈建、周涛、任晓明、李伟民、崔亚冰、王心阳、赵怡冰、辜凌云、徐子淼、姬祥、牟晋军、周林、秦齐祺、张娜、徐彩曦、张铮、陈津来、陈光炎、植吕梅、梁艳芬、吴卫明、丁峰、田劼、冯红、吴涵、何为、李青、赵紫钰、包一明、石霖、何远琼、李川东、蒋仁熙、梁淳栋、孙海鸣、武杨、张辉、吴迪、王辉、彭星、高凤、杨小娟、林森才、许艳冰、林莹、彭伟、叶娟、白宝龙、张朝、谢晓勇、罗经华、覃江林、白雷、周俊华、陈天伟、李维春、李旻瑞、李良、龙军、黄伟杰、江鑫、洪跃腾、王水兵、何冠辉、杜文琦、倪荣、刘志乐、吴俊雄。

本文件由中国科学技术法学会、深圳市北鹏前沿科技法律研究院负责解释。

引言

01. 背景

大数据时代，组织的个人信息处理合规被赋予了多重意义：

个人信息与自然人的隐私、自由等权益密切相关，个人信息的泄露、过度收集、超范围使用等安全事件与违规行为，极有可能威胁到自然人的合法权益，并因此给组织带来民事和经济索赔以及行政和刑事责任。这对组织实现其合规承诺与目标、满足潜在顾客和消费者隐私期待的能力提出了更高的要求。同时，通过设计和默认设置实现保护的概念，提示了在合规体系中充分考虑信息安全技术规范和实践的要求。

组织所处理的个人信息（尤其是其数据形式）与其他各类信息一同被视为组织的信息资产，是能够为组织带来竞争优势和创造经济价值的新型生产要素。过去组织在信息安全领域的投入主要致力于保护信息资产。这些措施在被用来满足有关个人信息保护的合规目标时，有必要予以调整以适应新的需求，并且需要引入法律领域的视角，帮助组织确认其现有的信息安全能力与《个人信息保护法》等可适用的法施加的合规义务、组织的合规承诺和顾客隐私期待之间的符合性。

从网络空间主权到信息主权的发展，也将个人信息保护引入到了网络安全的语境之下。除了将组织的网络安全（cybersecurity）视为整体网络系统中的一个单元考虑之外，个人信息出境或跨境转移还可能涉及国家对在其管辖之下的个人信息、重要数据的国家安全和信息主权利益的考量。

因此，组织的个人信息处理合规，意味着履行和满足来自多领域多方面的合规要求和期待。

02. 个人信息处理法律合规性评估

合规是组织持续健康发展的基石，要求组织在其活动中遵守适用于组织的全部合规要求，包括组织的合规义务与合规承诺，以及组织的运行环境和相关方所要求或期待的标准、最佳实践或道德准则，以避免因不合规所带来的法律责任、财产和声誉损失等潜在风险。

组织个人信息处理活动的合规要求具有综合性的内容。通常，个人信息处理的合规要求是由作为或不作为的履行要求构成的，但有时，合规要求也可能包括对履行结果符合性的要求。例如，《个人信息保护法》规定的采取技术、管理和其他必要措施的合规义务，包含了“确保个人信息处理活动符合法律法规的规定，并防止未经授权的信息泄露、篡改、丢失”的结果或状态符合性要求。又如，加密传输、匿名化、去标识化等技术处理，包含了对加密、匿名化、去标识化结果的符合性要求。因此，个人信息保护合规，往往意味着组织通过履行合规要求使其个人信息处理的过程和结果均符合规定要求。有时个人信息处理的合规要求也可能包含采取管理措施的要求，例如，将合规的意识与制度融入组织及其工作人员的文化、行为和态度当中，从而确保组织具备持续地满足合规要求和目标的管理体系。

对组织个人信息处理活动的法律合规性评估同样也是一系列具有综合性的确定活动。简言之，法律合规性评估是通过获取证据确定组织与个人信息处理有关的合规要求得到履行或满足的过程。但具体而言，组织的个人信息处理活动所处的环境要素，例如产品、服务、过程、程序、管理体系、信息处理设施、个人信息相关方及其他环境要素，往往决定了法律合规性评估所需确定的内容和程度。

组织个人信息处理的合规要求的综合性以及由此导致评估任务的综合性，都使得组织在向个人信息相关方沟通和证明其个人信息处理是否合规以及具备何种程度的合规能力时面临现实的难题。通过标准化建立个人信息处理合规及其法律合规性评估的语境和基准将有助于解决这一难题。

03. 个人信息处理法律合规性评估指引

个人信息处理法律合规性评估指引的目的在于：支持组织证明和声明其个人信息处理的合规状态和合规能力，也包括支持顾客、监管者等对组织个人信息处理的合规性进行检查和监督，支持个人信息相关方之间建立理解和信任，以及支持独立的评估机构为具有上述需求的个人信息相关方提供法律合规性评估、咨询和认证服务。

个人信息处理法律合规性评估指引由以下三个部分组成：

——第 1 部分：概述和术语。本部分的目的在于为个人信息处理活动及其法律合规性评估活动建立一个共同认可的、易于沟通的语境和概念体系，提供个人信息处理法律合规性评估的概述，为个人信息处理法律合规性评估指引的其他部分和其他标准的开发奠定基础。

——第 2 部分：合规框架。本部分的目的在于为个人信息处理法律合规性评估准则的识别和确定建立一个体系化的框架，以便对富有综合性的合规要求进行清晰的分类和归纳，以支持个人信息处理法律合规性评估活动的启动、规划、实施、报告、评审、监控和再评估。

——第 3 部分：实施指南。本部分的目的在于为个人信息处理法律合规性评估活动的启动、规划、实施、报告、评审、监控和再评估建立一个统一但仍保留灵活性的流程和方法，以支持各类组织能够高效地、可比较地、可问责地和可持续地进行法律合规性评估活动。

个人信息处理法律合规性评估指引的任何一个部分或其整体，可以单独使用，也能与现行的网络安全与信息安全相关标准（如GB/T 22239—2019、GB/T 35273—2020），信息安全、隐私管理体系相关标准（如GB/T 22080—2016、GB/T 22081—2016、ISO/IEC 27701:2019）与合规管理体系相关标准（如GB/T 35770—2017）结合使用。

04. 第1部分：概述和术语

作为个人信息处理法律合规性评估指引的第1部分，本文件界定和汇集了个人信息处理及其法律合规性评估可能涉及的术语和概念体系。尤其是个人信息处理相关术语，编制这些术语和定义的目的不仅仅是在法律合规性评估语境下的标准化，也旨在为政策制定者提供参考。

本文件对个人信息处理法律合规性评估给出了概述，包括评估目的、评估主体、评估对象、评估准则以及评估方法论的整体描述。本文件作为概述和术语类标准不提出具体要求。

个人信息处理法律合规性评估指引　第1部分：概述和术语

1范围

本文件给出了个人信息处理及其法律合规性评估的概述和术语，描述了个人信息处理法律合规性评估的评估目的、评估主体、评估对象、评估准则和评估方法论。

本文件适用于各种类型的组织对其个人信息处理的合规状态或合规能力进行第一方评估和管理，个人信息相关方为采购、监管等特定目的（诸如采购、监管）进行的第二方评估，以及独立的评估机构进行的第三方法律合规性评估和咨询。

2规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010　信息安全技术　术语

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 29246—2017　信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 19000—2016　质量管理体系　基础和术语

GB/T 27000—2006　合格评定　词汇和通用原则

3术语

GB/T 25069—2010、GB/T 35273—2020、GB/T 29246—2017、GB/T 19000—2016、GB/T 27000—2006中界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069—2010、GB/T 35273—2020、GB/T 29246—2017、GB/T 19000—2016、GB/T 27000—2006中的一些术语和定义。

注1：关于信息安全、隐私和信息技术、网络安全主题的现有国家标准和国际标准中已经给出了与个人信息处理有关的大多数术语。为了给个人信息处理法律合规性评估建立一个统一的语境，本文件汇总和抄录了其中的部分术语。为便于将本文件与现有的标准相结合使用，附录 A 给出了本文件中采用的概念与相关标准中对应概念的关系图示。

注2：本文件中的一些术语是现有标准中未涵盖从而必须予以定义的概念，另一些则是标准化和相关活动的通用词汇在适用于个人信息处理法律合规性评估语境时有必要予以调整或解释，本文件通过注释的改写和添加示例解释了这些通用词汇并指明了定义的来源。

3.1法律合规性评估相关术语[1)]

3.1.1

法律合规性评估　legal compliance assessment

1)　GB/T 19000—2016 和 GB/T 27000—2006 均给出了标准化和相关活动的通用术语，尤其是与评估活动相关的术语。如果本文件中使用了在本文件中未改写或抄录的标准化和相关活动通用术语，尤其是与评估活动相关，并且上述两个规范性引用文件中对同一术语给出了不同的定义时，GB/T 27000—2006 的定义优先于 GB/T 19000—2016。

获取客观证据并客观评价以确定评估准则得到遵守或满足的过程。

注1：根据评估主体与评估对象的关系，法律合规性评估可以分为第一方评估、第二方评估或第三方评估。

注2：评估对象中的要素为组织时是确定评估准则得到遵守，其他要素则确定评估准则得到满足。

注3：法律合规性评估可能包括为获取客观证据所需的测量、试验、检验、记录、事实陈述、文件评审等活动，基于客观证据评价合规要求得到满足所需的验证、确认等活动，以及基于客观证据评价合规要求得到满足的程度的专家评审等活动。GB/T 19000—2016给出了上述各项活动的定义。

注4：取决于法律合规性评估的目的、范围和评估结论的用途，法律合规性评估可能得出符合或不符合的评定结论，也可能得出符合程度的评定结论。

3.1.2

评估主体 subject of assessment

实施法律合规性评估的组织。

3.1.3

评估对象 object of assessment

被识别以与评估准则进行比较的组织的个人信息处理，也包括个人信息处理的对象和环境要素，如产品、服务、过程、程序、管理体系、信息处理设施、个人信息相关方及其他环境要素的集合。

注：GB/T 19000—2016给出了产品（3.7.6）、服务（3.7.7）、过程（3.4.1）、程序（3.5.3）、管理体系（3.5.3）的定义。

3.1.4

被评估方 assessee

作为评估对象的组成部分受到评估的组织。

3.1.5

评估委托方 assessment client

向评估机构委托实施法律合规性评估的组织。

3.1.6

第一方评估 first-party assessment

由作为评估对象的组织所实施的法律合规性评估。

注：第一方评估包括由评估对象的组织自行实施的，也包括其委托外部组织代表其利益实施的法律合规性评估。

3.1.7

第二方评估 second-party assessment

由在评估对象中享有利益或利益冲突的组织实施的法律合规性评估。

注：第二方评估的例子包括但不限于顾客、潜在顾客、消费者组织、监管者、投资者或潜在投资者等，也包括这些组织委托外部组织代表其利益实施的法律合规性评估。

3.1.8

第三方评估 third-party assessment

由独立于评估对象并且在评估对象中不具有利益和利益冲突的评估机构实施的法律合规性评估。

3.1.9

评估机构 assessment body

从事第三方评估服务的机构。

3.1.10

评估组 assessment team

为实施法律合规性评估指派的一名或多名评估员，同时评估过程应委托技术专家提供支持。

注：评估组可包括实习评估员。

3.1.11

评估员 assessor

被指派实施法律合规性评估的人员。

3.1.12

评估组长 team leader

在评估组中被指定对整个法律合规性评估的过程和结果负责任的评估员。

3.1.13

技术专家 technical expert

向评估员提供特定专业知识、技能和意见支持的具备相应资质证书人员。

注1：特定专业知识或技术是指与被评估的组织、过程、活动、语言或文化有关的知识或技术。

注2：在评估组中，技术专家不作为评估员。

注3：技术专家应当具备相应的资格证书，比如CISP/CISSP等。

3.1.14

观察员 observer

被指派监督法律合规性评估过程和结果的人员。

3.1.15

协调员 coordinator

第二方评估和第三方评估中被评估方指派的为评估组提供协助的人员。

3.1.16

信息技术产品 IT product

具有采集、存储、传输、处理、交换、加工、显示等信息或数据处理功能的产品。

注1：信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

注2：GB/T 19000—2016，3.7.6给出了产品的定义，产品是在组织和顾客之间未发生任何交易的情况下，组织能够产生的输出。通常，产品的主要要素是有形的，可以分为：有形的、其量具有计数特性的硬件；有形的、其量具有连续特性的流程性材料；以及由信息组成、无论采用何种介质传递的软件。

注3：当产品交付给顾客时，通常包含服务因素。例如，计算机产品交付时可能附带操作培训服务，也可能附带有偿或无偿的售后维修服务。此时产品或服务的区分取决于其主导成分。

3.1.17

基于信息技术的服务 IT-based service

信息技术服务以及提供方以信息技术为手段提供的任何服务。

注1：GB/T 29264—2012，2.1给出了信息技术服务的定义和分类。

注2：GB/T 19000—2016，3.7.7给出了服务的定义，服务是至少有一项活动必需在组织和顾客之间进行的组织的输出。通常，服务的主要要素是无形的，包含与顾客在接触面的活动，由顾客体验。服务中可能包含产品的交付或使用。此时产品或服务的区分取决于其主导成分。基于信息技术的服务的特殊类别是云服务，例如基础设施作为服务（IaaS）、平台作为服务（PaaS）或软件作为服务（SaaS）。

注3：组织和顾客的接触面和服务的交付均可以是在线上或线下，如线上接触和交付的在线服务、线上接触线下交付的服务、线下接触线上交付的服务、线下接触线下交付的服务。

注4：服务可以是有偿的，也可以是无偿的。

3.1.18

评估准则 assessment criteria

以合规框架作为基准，与适用于评估对象的其他合规要求进行比较分析后确定的，用于与证据进行比较并据以得出法律合规性评估结论的一组合规要求。

3.1.19

要求 requirement

明示的、通常隐含的或必须履行的需求或期望。

注1：“通常隐含”是指组织和相关方的惯例或一般做法，所考虑的需求或期望是不言而喻的。

注2：规定要求是经明示的要求，如在成文信息中阐明。

注3：特定要求可使用限定词表示，如产品要求、信息安全要求、系统要求、顾客要求。

注4：要求可由不同的相关方或组织自己提出。

注5：为实现较高的顾客满意，可能有必要满足那些顾客既没有明示、也不是通常隐含或必须履行的期望。

注6：这是GB/T 19000—2016中给出的管理体系标准的通用术语及核心定义之一，修改了注3。

3.1.20

合规框架 compliance framework

T/CLAST 002.2—2021给出的规定要求。

3.1.21

合规要求 compliance requirement

适用于评估对象的合规义务和作为评估对象的组织选择遵守的其他规定要求。

注：当组织选择遵守合规框架时，合规框架构成合规要求。

3.1.22

合规义务 compliance obligation

对作为评估对象的组织有法律意义上的约束力的规定要求。

注：合规义务的来源可以区分为法定要求、监管要求、司法要求和合规承诺。

3.1.23

可适用的法 applicable law

产生可适用于评估对象的法定要求、监管要求、司法要求的规范性文件。

注：法定要求和监管要求包括中国法律、行政法规、部门规章及其他规范性文件，也可以包括适用于特定相关方、特定个人信息或特定个人信息处理活动（如跨境转移）的外国立法和监管要求。

3.1.24

法定要求 statutory requirement

立法机关制定并发布的具有强制力的规定要求。

示例：如全国人民代表大会及其常委会制定并发布的法律、法律解释和决定，地方人民代表大会及其常委会的地方性法规、自治条例和单行条例等。

注：改写自GB/T 19000—2016，定义3.6.6。

3.1.25

监管要求 regulatory requirement

法律或立法机关授权的机关制定并发布的具有强制力的规定要求。

示例：监管要求的例子，如《中华人民共和国立法法》授权的国家机关制定并发布的行政法规、国务院部门规章、地方政府规章等。

注：改写自GB/T 19000—2016，定义3.6.7。

3.1.26

司法要求 Judicial requirement

司法机关制定并发布的具有普遍约束力的要求和适用于评估对象的已生效的决定。

示例：司法要求的例子，如司法机关制定的司法解释，或者评估对象作为一方并受其约束的判决等。

3.1.27

合规承诺 compliance commitment

组织承诺遵守从而对其具有约束力的、适用于评估对象的规定要求。

示例：合规承诺的例子，如组织与个人信息相关方之间的合同，公开发布的个人信息保护政策，产品或服务说明书，向监管部门做出的合规或整改承诺等。

3.1.28

差距 gap

评估对象未遵守或未满足评估准则中的某项合规要求。

注：差距可以是一个单一事件或多项事件，在法律合规性评估中差距并不必然表明不符合，需由评估员确定。

3.1.29

符合 conformity

评估对象遵守或满足评估准则得到确定。

3.1.30

不符合 nonconformity

评估对象遵守或满足评估准则未得到确定。

3.1.31

客观证据 objective evidence

支持事物存在或其真实性的数据。

注1：客观证据可通过观察、测量、试验、检验或其他方法获得。

注2：就法律合规性评估的目的而言，客观证据的形式可以是与评估准则相关的记录、事实陈述、文件、成文信息或其他信息并可用于验证。

注3：GB/T 19000—2016 给出了测量（3.11.4）、试验（3.11.8）、检验（3.11.7）等获取客观证据的方法的定义。这些术语在法律合规性评估语境中的概念关系图示，见附录 A。

注4：GB/T 19000—2016 给出了记录（3.8.10）、信息（3.8.2）、文件（3.8.5）、成文信息（3.8.6）等术语的定义。这些术语在法律合规性评估语境中的概念关系图示，见附录 A。

注5：通过注 2 改写 GB/T 19000—2016，定义 3.8.3，以适应法律合规性评估。

3.1.32

规范 specification

阐明要求的文件。

示例：质量手册、质量计划、技术图纸、程序文件、作业指导书。

注1：规范可能与活动有关（如：程序文件、过程规范和试验规范）或与产品有关（如：产品规范、性能规范和图样）。

注2：规范可以陈述要求，也可以附带设计和开发实现的结果。因此，在某些情况下，规范也可以作为记录使用。

[来源：GB/T 19000—2016，定义3.8.7]

3.1.33

评审 review

对客体实现所规定目标的适宜性、充分性或有效性的确定。

示例：管理评审、设计和开发评审、顾客要求评审、纠正措施评审和同行评审。

注：评审也可包括确定效率。

[来源：GB/T 19000—2016，定义3.11.2]

3.1.34

验证 verification

通过提供客观证据对规定要求已得到满足的认定。

注1：验证所需的客观证据可以是检验结果或其他形式的确定结果，如：变换方法进行计算或文件评审。

注2：为验证所进行的活动有时被称为鉴定过程。

注3：“已验证”一词用于表明相应的状态。

[来源：GB/T 19000—2016，定义3.8.12]

3.1.35

确认 validation

通过提供客观证据对特定的预期用途或应用要求已得到满足的认定。

注1：确认所需的客观证据可以是试验结果或其他形式的确定结果，如：变换方法进行计算或文件评审。

注2：“已确认”一词用于表明相应的状态。

注3：确认所使用的条件可以是实际的或是模拟的。

[来源：GB/T 19000—2016，定义3.8.13]

3.1.36

组织 organization

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。

注：组织的概念包括，但不限于个体经营者、公司、集团、商行、企事业单位、权力机构、合伙企业、慈善机构或研究机构，或上述组织的部分或其组合，无论是否为法人组织，公有的或私有的。

[来源：GB/T 35770—2017，定义2.1]

3.1.37

供方 provider; supplier

提供产品或服务的组织。

示例：产品或服务的制造商、批发商、零售商或商贩。

注：供方可以是组织内部的或外部的。

[来源：GB/T 19000—2016，定义3.2.5]

3.2个人信息处理的主体相关术语

3.2.1

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

[来源：GB/T 35273—2020，定义3.3]

3.2.2

个人信息处理者 personal information processor

自主决定个人信息处理目的、方式等的组织或个人。

3.2.3

个人信息共同处理者 joint personal information processor

与个人信息处理者共同决定个人信息处理目的、方式的个人信息相关方。

3.2.4

个人信息处理受托人 commissioned party for personal information processing

接受委托进行个人信息处理的组织或个人。

3.2.5

个人信息相关方 personal information interested party

可能影响个人信息处理有关的决策或活动、受个人信息处理有关的决策或活动所影响、或自认为受个人信息有关的决策或活动影响的个人或组织。

示例：顾客、投资者、组织内人员、供方、债权人、监管者、工会、合作伙伴以及可包括竞争对手或相对立的社会群体。对于特定个人信息处理者而言，个人信息相关方尤其包括个人信息主体、共同个人信息处理者、个人信息处理受托人及其分包商。

注：改写自ISO/IEC 29100:2012，2.22。

3.2.6

第三方 third party

个人信息主体、个人信息处理者和个人信息处理受托人以外的个人信息相关方。

3.3个人信息处理的对象相关术语

3.3.1

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：关于个人信息的判定方法、相关术语、子分类，参见GB/T 35273—2020附录A。

注3：个人信息处理者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映自然人活动情况的，属于个人信息。

注4：个人信息是信息（属）的种概念，GB/T 5271.1—2000，01.01.01给出了信息（在信息处理中）的定义，是指关于客体（如事实、事件、事物、过程或思想，包括概念）的知识，在一定的场合中具有特定的意义。

注5：个人数据是个人信息（属）的种概念，是个人信息的可再解释的形式化表示，以适用于人或计算机进行通信、解释或处理。因此，当本文件提及个人信息时应理解为包含个人数据，本文件提及个人数据时是特指种概念。

注6：这是《个人信息保护法》第4条第1款给出的定义，注1参考了GB/T 35273—2020，3.1，修改和添加了注2-4。

3.3.2

敏感个人信息 sensitive personal information

一旦泄露、非法使用或滥用，容易危害人身和财产安全，容易导致个人人格尊严、身心健康受到损害或容易使个人受到歧视性待遇等的个人信息。

注1：敏感个人信息包括身份证件号码、个人生物识别信息、宗教信仰、金融账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、不满14周岁未成年人的个人信息等。

注2：个人信息处理者通过个人信息或者其他信息加工处理后形成的信息，如一旦泄露、非法使用或者滥用，可能危害人身和财产安全，容易导致个人人格尊严、身心健康受到损害或容易使个人受到歧视性待遇等的，属于敏感个人信息。

注3：敏感个人信息是个人信息的种概念。个人信息与个人数据的属种关系也适用于敏感个人信息与敏感个人数据。

注4：这是GB/T 35273—2020，3.2给出的术语和定义，添加了注3。

3.4个人信息处理相关术语

3.4.1

个人信息处理 personal information processing

借助信息系统执行的、以个人信息为输入和/或输出的过程。

注1：个人信息处理的示例包括但不限于采集、存储、修改、检索、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁。

注2：通常个人信息处理的输入和输出均为个人信息。个人信息仅为输入的例子如匿名化；个人信息仅为输出的例子如将非个人信息汇聚融合为个人信息。

注3：个人信息处理是过程（属）的种概念。GB/T 19000—2016，3.4.1 给出了过程的定义，是指利用输入实现预期结果的相互关联或相互作用的一组活动。过程的预期结果是称为输出还是称为产品或服务，随相关语境而定。

注4：个人信息处理是至少有一个活动是借助信息系统执行的过程，完全由人工进行的分类、归并、存档、查询、计算、推论、分析，不属于本文件所称个人信息处理。

注5：个人信息处理是信息处理（属）的种概念。GB/T 5721.1—2000，01.01.05 给出了信息处理的定义，是指对信息操作的系统执行。

注6：两个或两个以上相互关联和相互作用的连续过程也可作为一个过程。一个或两个以上的个人信息处理的预期结果可能是导致个人信息控制权变动，如个人信息控制权的获得、保持、转移、丧失，或者使其他个人或组织获得个人信息控制权，表达此类个人信息处理的概念包括收集、持有、转让、共享等。本文件用个人信息处理行为表示预期结果是导致个人信息控制权变动的事实行为或法律行为的整体概念。个人信息处理行为可能由一个或两个以上的个人信息处理操作组成，如个人信息控制权的放弃可能通过删除实现，个人信息的收集可能由采集、传输和存储中的两个以上操作组成。

3.4.2

收集 collect

获得个人信息的控制权的行为。

注1：收集方式包括：

——个人信息主体主动提供，如填写、提交、上传、推送或点击共享等；

——个人信息处理者（包括通过其个人信息处理受托人）的采集，如通过与个人信息主体的交互或者记录个人信息主体的特征或行为等；

——间接获取，如通过第三方的共享、转移披露，搜集公开信息，或者通过其他个人信息主体主动提供或对其他个人信息主体的自动采集获得个人信息；

——通过汇聚融合等加工处理获得个人信息。

注2：控制权不宜理解为法律意义上的权利，而是指能够自主决定个人信息处理目的、方式的权限或能力。

注3：供方提供产品或服务供个人信息主体自行进行个人信息处理，但供方不对个人信息进行访问或虽然访问但不决定个人信息处理的目的和方式的，不属于收集。例如，移动智能终端的供方不访问移动智能终端所处理的个人信息，云服务的供方代表个人信息主体或在个人信息主体的指令下进行个人信息的存储等，应用程序的采集个人信息主体位置信息后不传输至供方，则不属于收集。

注4：这是 GB/T 35273—2020，3.5 给出的核心术语和定义，修改和添加了注 1-3。

3.4.3

使用 use

在不改变对个人信息的控制权的前提下，以个人信息作为输入实现业务功能的行为。

注1：使用中可能包含为适应使用目的而进行的加工处理。

注2：特定业务功能是使用目的。

3.4.4

业务功能 business function

产品或服务为满足顾客特定使用需求，所规划或已实现的目的或任务。

注1：如地图导航、网络约车、即时通信、网络社区、网络支付、新闻资讯、网上购物、快递配送、交通票务等。

注2：这是 GB/T 35273—2020，3.17 给出的术语，最初的定义已被改写。

3.4.5

个性化展示 personalized display

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

[来源：GB/T 35273—2020，定义3.16]

3.4.6**提供 provision**

通过共享、转移、披露、公开等方式，预期结果是使第三方获得个人信息的行为。

3.4.7

共享 sharing

个人信息处理者向其他个人信息处理者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

注：这是GB/T 35273—2020，3.13给出的术语，最初的定义已被改写。

3.4.8

转移 transfer

将个人信息控制权由一个个人信息处理者向另一个个人信息处理者转移的过程。

注：转转的过程中可能包含个人信息的传输或个人信息存储介质的传递，也可能不包含，如因合并、分立等导致的个人信息处理者变更，但转移后个人信息对新的个人信息处理者的披露是必然结果。

注2：这是 GB/T 35273—2020，3.12 给出的定义，最初的术语和定义均已被改写并添加了注。

3.4.9

公开 disclosure

通过传输、发布、展示、提供检索或访问等方式，预期结果是使不特定的人或组织能够感知个人信息内容的过程。

注：这是GB/T 35273—2020，3.11给出的术语，最初的定义已被改写。

3.4.10

传输 transmission

靠信号将信息由一个点传送到另一点或另外多个点的过程。

注1：传输可以直接或间接地带有临时存储或不带有临时存储。

注2：在无线电通信中表达“发射 emission”的含义时拒用英文单词“传输 transmission”。

[来源：GB/T 14733.11-2008，定义704-01-06]

3.4.11

保存；记录 store; record

在非临时存储或临时存储上记录数据的过程。

3.4.12

加工处理 handling

对个人信息或个人数据执行的修改、合并、对齐、计算、分析、可视化等操作。

3.4.13

用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、 教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

[来源：GB/T 35273—2020，定义3.8]

3.4.14

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别特定个人信息主体的过程。

注1：去除标识符与个人信息主体之间关联性。

注2：常用的去标识化技术，如统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术等。见GB/T 37964—2020，附录A。

注3：根据《个人信息保护法》第73条第3项改写，注1参考了GB/T 37964—2019，3.3，添加了注2。

3.4.15

重标识 re-identification

把去标识化的数据集重新关联到原始个人信息主体或一组个人信息主体使其能够识别特定个人信息主体的过程。

3.4.16

匿名化 anonymization

通过对个人信息的技术处理，使其无法识别特定个人信息主体，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

3.4.17

假名化 pseudonymization

对个人信息的技术处理，用假名替换标识符。

注1：假名化可以由个人信息主体或个人信息处理者进行。个人信息主体可以使用假名化来一致地使用资源或服务而不向该资源或服务（或服务之间）披露其身份，同时对其使用仍然可问责。

注2：假名化并不排除对经假名化的个人信息可能有个人信息处理者以外的（一组受限的）个人信息相关方能够基于假名确定个人信息主体的身份和与其相关联的个人信息。

[来源：ISO/IEC 29100—2011，定义2.24]

3.4.18

删除 delete; erase

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[来源：GB/T 35273—2020，定义3.10]

3.4.19

告知 inform

将与个人信息处理有关的信息提供给个人信息主体，使其了解个人信息处理的有关规则。

3.4.20

同意 consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

3.4.21

明示同意 explicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源：GB/T 35273—2020，定义3.6]

3.4.22

个人信息保护影响评估 personal information protection impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

注：定义来源于GB/T 39335—2020，3.4，将术语个人信息安全影响评估改为个人信息保护影响评估。

3.4.23

自动化决策 Automated decision-making

通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

[来源：《个人信息保护法》第73条第2项]

3.5个人信息处理设施相关术语[2)]

3.5.1

信息处理设施 information processing facilities

信息处理系统、服务或基础设施，或者物理放置场所。

[来源：GB/T 25069—2010，定义2.1.55]

3.5.2

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件。

[来源：GB/T 29246—2017，定义2.39]

2) GB/T 25069—2010 给出了信息安全技术术语，GB/T 29246—2017 给出了与信息安全管理体系有关的部分信息安全技术术语。如果本文件中使用了在本文件中未改写或抄录的信息安全技术术语，并且上述两个规范性引用文件中对同一术语给出了不同的定义时，GB/T 29246—2017 的定义优先于 GB/T 25069—2010。

3.5.3

存储 storage

支持数据录入和检索的设备、功能或服务。

[来源：ISO/IEC 27040:2015，定义3.43]

3.5.4

存储介质 storage media

承载电子数据的各类载体或设备，包括但不限于计算机硬盘、磁带、软盘、光盘、各种形式的存储卡等。

[来源：GB/T 31500—2015，定义3.2]

3.6管理体系相关术语[3)]

3.6.1

管理体系 management system

组织建立方针和目标以及实现这些目标的过程的相互关联或相互作用的一组要素。

注1：一个管理体系可以针对单一的领域或几个领域，如信息安全、隐私、合规或质量管理。

注2：管理体系要素规定了组织的结构、岗位和职责、策划、运行、方针、惯例、规则、理念、目标，以及实现这些目标的过程。

注3：管理体系的范围可能包括整个组织、组织中可被明确识别的职能或可被明确识别的部门，以及跨组织的单一职能或多个职能。

[来源：GB/T 19000—2016，定义3.5.3]

3.6.2

方针 policy

（组织）由最高管理者正式发布的组织的宗旨和方向。

[来源：GB/T 19000—2016，定义3.5.8]

3.6.3

目标 objective

要实现的结果。

注1：目标可以是战略性的、战术的和/或操作层面的。

注2：目标能与不同方面（诸如财务、健康与安全及环境的目标）相关，且能应用于不同层面，如战略层、整个组织、项目、产品和过程。

注3：目标能用其他方式表达，如：预期结果、目的、操作准则，作为合规目标或使用具有相似含义的其他词汇（如：目的、终点或标的）。

注4：在合规管理体系中，合规目标由组织确定，与合规方针保持一致，以实现特定的结果。

[来源：GB/T 35770—2017，定义2.9]

3) 本文件的规范性引用文件 GB/T 29246—2017 给出了信息安全管理体系，GB/T 19000—2016 给出了管理体系通用术语。如果本文件中使用了在本文件中未改写或抄录的管理体系术语，并且上述两个规范性引用文件中对同一术语给出了不同的定义时，GB/T 29246—2017 的定义优先于 GB/T 19000—2016。

3.6.4

风险 risk

不确定性的影响。

注1：影响是指偏离预期，可以是正面的或负面的。

注2：不确定性是一种对某个事件，或是事件的局部的结果或可能性缺乏理解或知识方面的信息的情形。

注3：通常，风险是通过有关事件（GB/T 23694—2013 中的定义，4.5.1.3）和后果（GB/T 23694—2013 中的定义，4.6.1.3）或两者的组合来描述其特性的。

注4：通常，风险是以某个事件的后果（包括情况的变化）及其发生的可能性（GB/T 23694—2013 中的定义，4.6.1.1）的组合来表述的。

注5：“风险”一词有时仅在有负面后果的可能性时使用。

[来源：GB/T 19000—2016，定义3.7.9]

3.6.5

信息安全 personal information security

保持、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[来源：GB/T 25069—2010，定义2.1.52]

3.6.6

保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[来源：GB/T 25069—2010，定义2.1.1]

3.6.7

完整性 integrity

3.6.8确保资产准确性和完整性的特性。

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[来源：GB/T 25069—2010，定义2.1.20]

3.6.9

个人信息安全事件 personal information security incident

其后果将导致个人信息意外或未经授权泄露、篡改、毁损、丢失的信息安全事件。

注1：泄露是指个人信息暴露于对该个人信息不具有访问或接收权限的人或组织从而保密性受损的状态，如被内部或外部未经授权的人或组织访问、接收，也包括被窃取等个人信息处理者事实上已失去对该个人信息的访问或披露的控制；篡改是指个人信息被未经授权地修改而完整性受损的状态；毁损是指个人信息受到损坏而不再完整甚至不再可用的状态；丢失是指个人信息不再存在于信息系统或不再能被信息系统访问和使用可用性受损的状态。

注2：信息安全事件的定义见 GB/Z 20986—2007，信息安全技术 信息安全事件分类分级指南，定义 2.2。用于个人信息处理的信息系统发生有害程序事件、网络攻击事件、信息破坏事件、信息内容事件、设备设施故障、灾害性事件、其他事件等信息安全事件，导致个人信息发生意外或未经授权的泄露、篡改、毁损、丢失，则构成个人信息安全事件。

4个人信息处理法律合规性评估概述

4.1概述

本文件为个人信息处理法律合规性评估提供了一个高度灵活、可定制的框架，以适应不同类型的组织、基于不同目的与目标进行的的法律合规性评估活动。

当组织决定启动一个法律合规性评估项目时，首先需要确定的是法律合规性评估的目的与目标。目的是指组织预期的法律合规性评估结论的用途；目标是指组织希望通过法律合规性评估确定的内容及其程度。法律合规性评估的目的与目标，对规划和实施评估方案、报告评估发现与评估结论以及持续性地监控和周期性地再评估，都具有牵引性作用。法律合规性评估的目的与目标也影响了评估模式、评估主体及具体评估团队的选择。

本章描述了组织在启动一项法律合规性评估时如何考虑目的与目标，以及这些目的与目标的规范化表达。目的与目标的规范化表达有助于法律合规性评估的所有相关方之间清晰地沟通评估相关事项。对于一个选定的法律合规性评估目的，为确保其评估结论能够使组织实现预期用途，在评估模式、评估主体及其评估组的选择上需要作出相应的规划，本章对于这些主题提供了初步的指引。

4.2评估目的与目标

个人信息处理法律合规性评估可以帮助组织实现多种目的和用途。在开展评估前，组织宜确定法律合规性评估的目的，即评估结论的用途，并确定评估所要实现的目标，即有待确定的内容和程度。

通常，组织开展个人信息处理法律合规性评估的目的和目标可能包含以下情形的组合：

目标：确定组织的个人信息处理的合规现状		
目的	目的说明	用途示例
改进	发现组织当前存在的个人信息处理不合规，或支持组织在个人信息处理活动中维持或改进其合规状态。	— 作为组织的一种合规管理手段； — 作为履行个人信息处理可问责性的一种方式； — 接受第二方评估或第三方评估前发现差距并进行改进。
证明	向外部证明组织在个人信息处理活动中具备的合规状态。	— 面向顾客或社会做出合规现状的声明； — 向监管者或法庭举证证明合规现状； — 在证券发行、公司并购或数据交易中进行的尽职调查的一部分。
		— 获得认证。
目标：确定组织所具备的个人信息处理合规能力		
目的	目的说明	用途示例
改进	支持组织改进现有的个人信息保护能力，使其更加适应组织的个人信息处理合规目标。	— 确定组织现有的信息安全管理体系、等级安全保护能力在实现组织在个人信息处理活动上的合规目标方面的适宜性、充分性和有效性，识别差距和可能的改进空间，在成本集约的前提下实现组织的个人信息处理合规目标；
证明	向外部证明组织具备一定的合规能力。	— 在个人信息委托处理前，向供方证明组织所提供的服务能够确保顾客的合规；

		— 向监管者证明组织的个人信息处理能够满足监管者对合规能力的要求； — 在涉及个人信息出境、新产品或服务上线前，作为个人信息影响评估的一部分； — 在出现重大个人信息安全事件或违规后，证明组织在个人信息处理合规方面的尽职和善意程度； — 以组织的个人信息处理合规能力为核心关切的证券发行、公司并购等交易。
		— 获得认证。

表1评估目的与目标的说明和示例

4.3评估模式与评估组

法律合规性评估的模式可以分为第一方评估、第二方评估和第三方评估。

评估模式的选择将取决于评估目的（见表2）：

——以改进为目的的评估，通常宜选择第一方评估。但取决于被评估方自身的需求，也可以选择第二方评估或第三方评估。

——以证明—获得认证为目的的法律合规性评估，通常只能选择第三方评估。

——其他以证明为目的的法律合规性评估，通常宜选择第三方评估。但取决于接受证明一方的要求，也可以选择第二方评估或第一方评估。

目标/目的	改进	证明	认证
合规现状	宜第一方评估 可第二方或第三方评估	宜第三方评估 可第二方或第一方评估	仅第三方评估
合规能力			

表2法律合规性评估模式的选择

不同的评估模式在评估主体和评估团队组成方面的区别（见表3）包括：

——**第一方评估：**由作为评估对象的组织自行实施，也包括组织委托外部组织代表其利益实施法律合规性评估，此时该外部组织是为被评估方的利益实施法律合规性评估。评估员可以由被评估方的人员担任或由被评估方指派，但评估员的具体人员仍宜考虑适当的独立性和公正性，以确保法律合规性评估的过程和结果对组织有意义。通常不需要观察员、协调员等角色。

——**第二方评估：**由对评估对象享有利益或利益冲突的组织实施，也包括组织委托外部组织代表利益实施法律合规性评估。评估组中，评估员由评估主体的人员担任或由其指派，宜根据评估主体的具体要求确保评估员的适当独立性和公正性。通常需要被评估方指派协调员以协助评估员，协调员不宜对法律合规性评估的过程和结果施加不当影响和干预。

——**第三方评估：**由独立于评估对象且在评估对象中不享有利益或利益冲突的组织实施。评估组中，评估员由评估机构指派。通常需要被评估方指派协调员以协助评估员，在为评估目的必要

时，评估委托方、顾客、监管者、投资者或认证机构可以指派观察员，需确保协调员和观察员均不对法律合规性评估的过程和结果施加影响和干预。

评估组中的评估员宜由具备法律职业资格的人员担任，在必要时，可以通过技术专家补充能力，为评估员提供专业知识、技能和建议。

评估模式	评估主体	评估员	协调员	观察员
第一方评估	— 被评估方； — 被评估方委托的外部组织（代表被评估方兼评估委托方利益）。	— 被评估方人员； — 被评估方指派的外部人员。	不需要	不需要
第二方评估	— 对评估对象享有利益或利益冲突的组织； — 该组织（评估委托方）委托的外部组织（代表评估委托方利益）。	— 对评估对象享有利益或冲突的组织的人员； — 评估委托方指派的外部人员。	通常需要被评估方指派	通常不需要
第三方评估	— 独立于评估对象且在评估对象中不享有利益或利益冲突的评估机构。	— 评估机构指派。	被评估方指派	必要时可以指派

4.4评估范围

4.4.1概述

为实现法律合规性评估的目标并使其结果适应评估目的，宜界定法律合规性评估的范围。评估范围宜说明法律合规性评估的内容和界限，这要求确定评估对象的范围和边界以及评估准则。

无论法律合规性评估基于何种目标和目的，评估范围的界定都是保障评估过程和结果可靠性的前提。在以确定合规现状为目标的评估中，评估范围决定了在多大范围内确定合规状态，以及为此采用的诸如采样方法的设计。在“证明—合规现状”型评估中，评估范围还决定了评估主体能够确保评估发现和结论在多大范围内是可靠和可问责的。如果评估的目标与目的决定了将个人信息处理法律合规性评估视为是合规管理过程的一部分，评估范围的确定本身构成了当前组织的合规管理活动的覆盖面，也是组织后续合规管理活动的基础。

4.4.2评估对象的范围和边界

评估对象是法律合规性评估活动所针对的具体对象，评估对象范围和和边界的界定对法律合规性评估的顺利进行至关重要。组织宜尽可能全面、详细和准确地界定评估对象的范围和边界。

在组织决定启动评估项目时，可以将评估对象初步界定为组织的个人信息处理活动。组织可以通过场景来描述和界定评估对象，如产品场景、服务场景，也可以具体界定为一个或若干个人信息处理活动，或者可以组合上述三种形式。

——可以将评估对象界定为组织在提供信息技术产品的场景中进行的所有个人信息处理活动。例如，组织在面向消费者提供信息技术产品的过程中进行的个人信息处理活动，以及组织在信息技术产品交付后、最终用户使用信息技术产品的过程中进行的个人信息处理活动。

示例1：个人用信息技术产品的例子，包括但不限于：个人用计算机终端、移动智能终端、物联网感知终端（如智能可穿戴设备、智能音箱等）及这些终端的操作系统、应用软件和移动应用程序、数据存储系统、身份鉴别系统等。

示例2：信息技术产品可能是非个人用（如商用或公务用）信息技术产品，此时顾客并非大众消费者，但使用该信息技术产品的最终用户可能是个人信息主体，或者使用该信息技术产品的过程中可能产生对众多个人信息主体的个人信息处理。如商用或公务用人脸识别门禁设备、移动终端（如用于电子支付的近距离无线通信的移动终端）、物联网感知终端（如智能音视频采集设备）以及这些设备或终端的支持系统。

注：如果组织仅仅提供信息技术产品而不进行任何个人信息处理，如提供照相机、耳机等个人用（消费）信息技术产品，但组织并不通过该信息技术产品收集个人信息，则不适合作为法律合规性评估的评估对象。此类信息技术产品本身需在产品设计、默认设置等方面符合隐私、安全性等要求，属于合格评定的对象。

——可以将评估对象界定为组织在提供基于信息技术的服务的场景中进行的所有个人信息处理活动。基于信息技术的服务包括信息技术服务，也包括组织以信息技术为手段提供的任何其他服务，只要在服务的过程中产生个人信息处理活动。

示例：组织以信息技术为手段提供的任何其他服务的实例，如在健身房、餐厅、学校、剧院、公园等线下交付的服务中使用具有个人信息处理功能的信息系统，例如，门禁系统、办公系统、视频监控系统、预约或订票系统等。

——可以将评估对象具体界定为一个或若干个人信息处理过程，例如，信息技术产品或基于信息技术的服务当中的某些功能或个人信息处理环节，前提是这样界定的评估对象对于法律合规性评估目的而言是有意义的和自足的，这意味着评估对象通常应涵盖个人信息处理的整个生命周期（如从收集到删除或匿名化），或者将其中的某个个人信息处理环节排除在评估对象之外有合理的理由。

示例：例如，对于同时通过网页和移动应用程序提供在线票务预订的组织，仅为改进目的将评估对象界定为网页端的个人信息收集、传输、存储、使用、对外提供等环节，而没有包含个人信息的删除或匿名化等环节和移动应用程序端的任何环节是可接受的，但对于证明目的而言，所界定的评估对象可能难以向接受证明一方表明组织（甚至仅在线票务预订业务中）的个人信息处理活动达到合规。

——也可以将评估对象界定为由同一组织提供的若干信息技术产品、基于信息技术的服务或个人信息处理过程的组合，前提是在该组合内的信息技术产品、基于信息技术的服务或个人信息处理过程之间存在除同一组织作为供方以外的额外联结点，使得可以将该组合通过一定的线索联系起来视为一个具有整体目标的个人信息处理过程。

示例1：额外联结点，诸如该组合具有共同的应用场景，该组合处理的是同一组个人信息主体的同一组个人信息，个人信息处理流程需有连续性，使得可以将该组合视为一个完整的个人信息处理过程并便于进行法律合规性评估。

示例2：以应用场景为额外联结点的组合实例，如在同一个移动应用程序（信息技术产品）中提供的定位、导航、跟踪等位置服务（定义见 GB/T 35638—2017，4.1）以及网约车服务，该移动应用程序本身即是按照应用场景将若干基于信息技术的服务预先集成后提供的信息技术产品。

示例3：以同一组个人信息主体的同一组个人信息为联结点的组合实例，如可穿戴智能手表与配套使用的移动应用程序是两个产品的组合，处理的是同一组个人信息主体的一组个人信息。

注：通过组合界定评估对象的目的是适应同时提供多种产品、服务或过程的组织，通过组合界定的评估对象有助于对组织的个人信息处理活动进行完整的法律合规性评估并得出总体性的结论，并且可以合并法律合规性评估中的同类活动从而提高效率。但组合界定评估对象也可能导致法律合规性评估的深度降低，所适用的合规要求过于多样、复杂而难以确定评估准则，或在法律合规性评估项目中需要参与和协调的相关人员和组织过多增加评估项目的实施难度等。例如，在一个电子商务中提供的物流服务和电子支付服务，在应用场景、所处理的个人信息、所涉及的个人信息主体方面可能都满足额外联结点的要求，但该组合的供方可能涉及同一集团控制下的多个组织或同一组织内的多个独立部门。如果组合界定的评估对象最终将不利于法律合规性评估的顺利实施，不宜采用组合的方式，而宜分别界定为不同的评估对象或采用持续迭代的法律合规性评估方式。

界定评估对象时，宜识别组织的个人信息处理活动的对象和环境要素，如产品、服务、过程、程序、管理体系、信息处理设施、个人信息相关方及其他环境要素的集合。

——以下要素对于界定组织的个人信息处理活动而言是必不可少的要素：

- 评估对象中所包含的个人信息处理的目的、过程和程序；
- 所处理的个人信息的类型及其所涉及的个人信息主体的类型；
- 评估对象中的个人信息处理所采用的信息处理设施，包括信息系统，如用户登录和认证系统、操作系统、存储系统、路由器和防火墙、通信基础架构或网络访问等，外包服务，信息系统清单及其所在的地点；
- 作为个人信息处理者和/或个人信息处理受托人角色的组织。

——以下要素对于组织的个人信息处理活动具有重要影响，宜予以界定：

- 个人信息处理者和/或个人信息处理受托人的组织架构，以及两者之间的法律关系；
- 与评估对象中所包含的个人信息处理活动有关的组织内相关部门、人员及其相互间关系；
- 个人信息处理中存在的接口或界面，既可能是技术的接口或界面，如用户界面、API 等信息系统的接口，也可能是法律意义上的接口或界面，如与个人信息相关方之间的合同；
- 评估对象中所包含的组织的管理体系、信息安全保护能力，以及已经采取的控制措施。

组织在系统识别上述所有要素的基础上，宜通过文件界定评估对象的边界，包括某些被识别的要素被排除在评估对象范围之外的理由：

——个人信息处理活动边界；

——组织边界；

——网络边界；

——信息系统边界；

——物理边界。

组织宜集成上述所有边界的描述文件，最终得出有关评估对象范围和边界的文件。

4.4.3评估准则

评估准则是法律合规性评估中用来确定合规状态以及确定合规程度的依据，体现了评估的目标。评估准则中所包含的合规要求，由组织的合规义务和组织选择遵守的其他规定要求组成。

组织宜系统识别其合规义务。合规义务的来源包括法定要求、监管要求、司法要求以及组织的合规承诺。

——法定要求、监管要求、司法要求是从组织的外部施加的合规义务。

示例1：外部施加的合规义务的例子，包括但不限于：

——法律、法规和部门规章对个人信息处理活动的一般性的规定要求；

——组织所处的行业或所从事的业务所需要的许可、执照或其他形式的资格准入的监管要求；

——强制性的国家标准或行业标准。

——组织作出的合规承诺也构成了合规义务的来源。

示例2：组织作出的合规承诺的例子，包括但不限于：

——组织与个人信息相关方之间签订的合同；

——组织公开发布的个人信息保护政策；

——提供个人信息处理的产品或服务的说明书；

——合同、个人信息保护政策、产品或服务说明书中声明符合的自愿性的标准、原则或规程；

——组织向监管者作出的合规或整改承诺。

组织宜有成文信息列出被识别的合规义务，并有适当的过程持续地识别新的和变更的合规义务，包括评价已被识别的任何新的和变更的合规义务对组织的个人信息处理合规要求的影响。

在合规义务的基础上，组织宜考虑法律合规性评估的目标与目的，识别和选择纳入其他合规要求。如：

——T/CLAST 002.2—2021 给出的合规框架，提供了系统地分类和归纳组织个人信息处理合规要求的框架。组织可以选择将合规框架纳入合规要求，并根据所识别的全部合规义务和组织选择遵守的其他规定要求，调整合规框架中给出的合规维度和合规指标，最终确定评估准则；

——顾客或其他证明接受一方的合规要求；

——其他希望或追求符合的自愿性的标准、原则或行为准则。

组织宜集成上述所有合规要求，最终得出有关评估准则的文件。

在以确定合规能力为目标的法律合规性评估，组织在评估准则中还需确定合规能力评价的基准。组织宜考虑以下因素：

——T/CLAST 002.1—2021 给出的能力评价模型；

——顾客或其他证明接受一方确定的能力评价要求；

——其他希望或追求符合的自愿性的标准、原则或行为准则给出的能力评价模型。

4.5评估方法论

4.5.1评估流程和方法

组织宜根据确定的法律合规性评估目标与目的、评估对象的范围和边界、评估准则，选择和确定评估方法以有效和高效地实施法律合规性评估活动。

以确定合规现状为目标的评估与以确定合规能力为目标的评估，在评估流程方面是基本相同的。区别在于以确定合规能力为目标的法律合规性评估，在以确定合规现状为目标的法律合规性评估流程基础上，增加了赋值、评审和解释能力的过程作为必要流程。

在评估方法方面，获取客观证据的方法，如文件评审、访谈和事实陈述、记录、观察、测量、试验、检测、检查等基本方法是相同的。在获取客观证据后确认和验证是否符合评估准则的活动中，以确定合

规现状为目标的评估更关注对现状和差距的充分揭示，只要可能，所有被发现的差距无论是否在评估期内调整，均需要详细记录和提示，以促进改进、证明等法律合规性评估目的。以确定合规能力为目标法律合规性评估更关注对评估对象合规能力的优势、短板的揭示和描述，及其综合能力的评价，在赋值、评审和解释中可以增加基于风险的评价方法。

4.5.2评估结论

评估结论的形式取决于法律合规性评估的目标。

以确定合规现状为目标的法律合规性评估，可以得出符合或不符合评估准则的结论。符合意味着经过法律合规性评估，评估对象满足评估准则中的全部合规要求；不符合意味着经过法律合规性评估，评估对象与评估准则中的某项合规要求之间存在差距，并且通过调整和处置未能消除差距。

评估结论宜陈述诸如以下内容：

——评估对象是否履行或满足评估准则中的全部合规要求；

——在法律合规性评估中发现了哪些差距，被评估方对差距原因的解释，或者在法律合规性评估期内的调整；

——经调整后，可能残留的风险；

——评估员对于该差距和残留风险是否影响符合或不符合结论的评价及其理由。

以确定合规能力为目标的法律合规性评估，可以得出对合规能力的整体评价、单项维度或指标上符合或不符合的结果以及对该结果的解释和改进建议。在单项维度或指标上的符合或不符合的含义，与以确定合规现状为目标的法律合规性评估一致，这也表明合规能力的评价宜基于对合规现状的确定，在此意义上合规现状的确定构成了合规能力评价所依赖的客观证据。

评估结论宜陈述诸如以下内容：

——能力评价基准、赋值权重及其解释；

——能力评价基准满足程度的整体结论，对整体结论的解释、评审理由和改进空间等；

——单项维度或指标的满足程度，包括差距和差距对于满足程度结论的影响以及评审理由。

以确定合规能力为目标的法律合规性评估结论可视化呈现概念图见图 1-3。

图1合规能力评价模型（概念图）

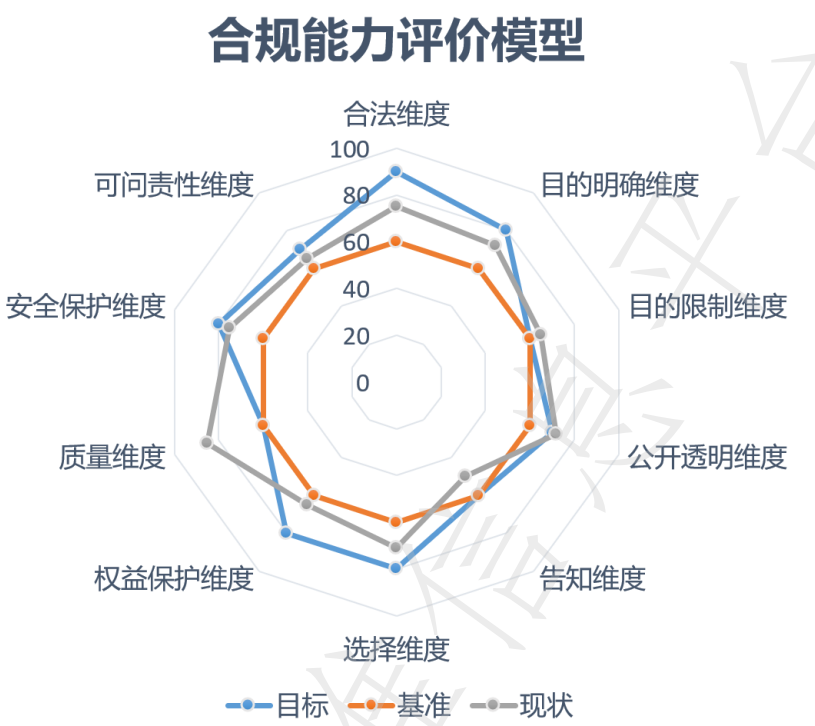
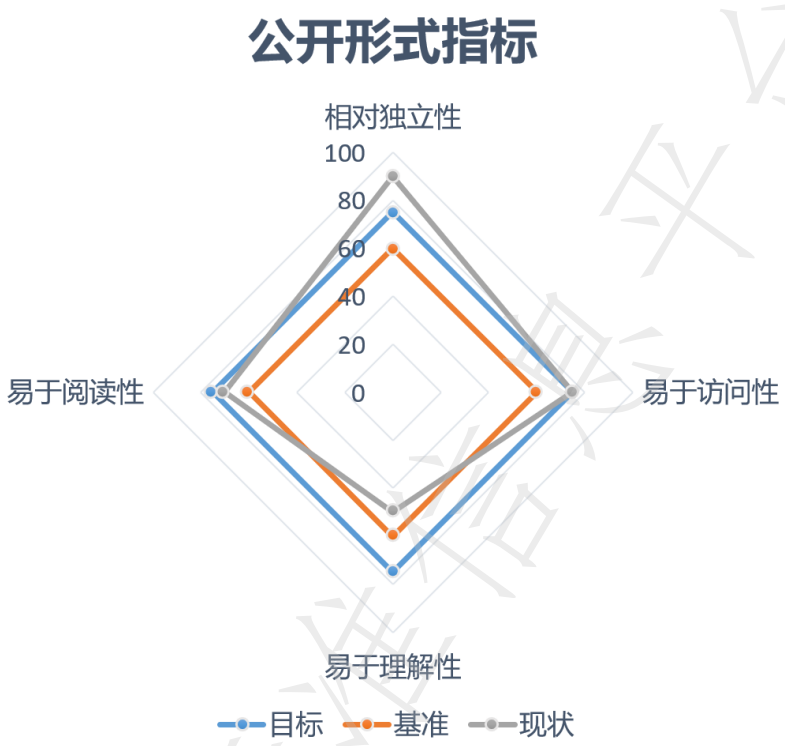


图2法律合规性评估维度（概念图）

图3法律合规性评估指标（概念图）



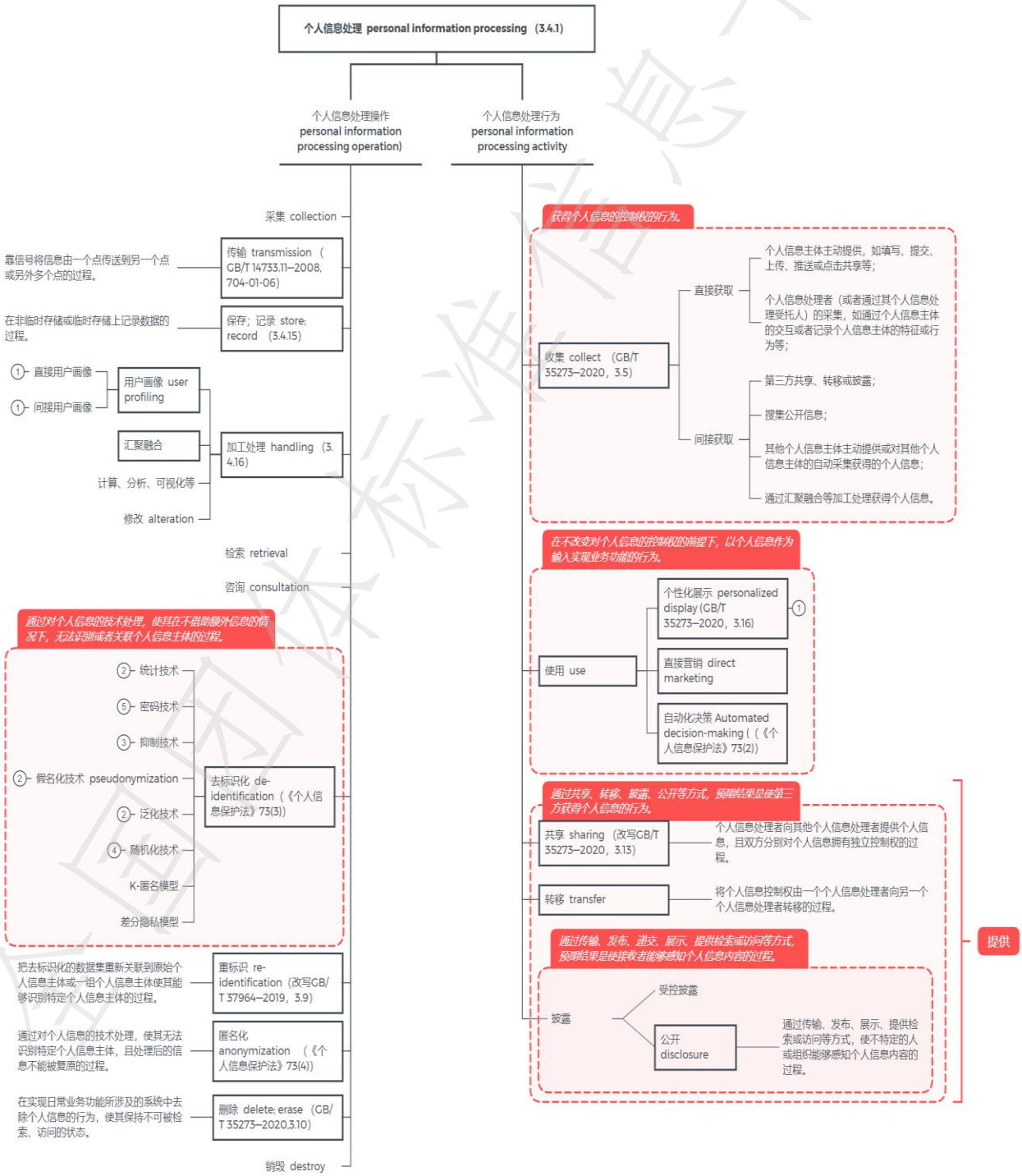
4.5.3可持续的评估

组织宜对其个人信息处理合规状态进行持续监控和周期性的再评估。

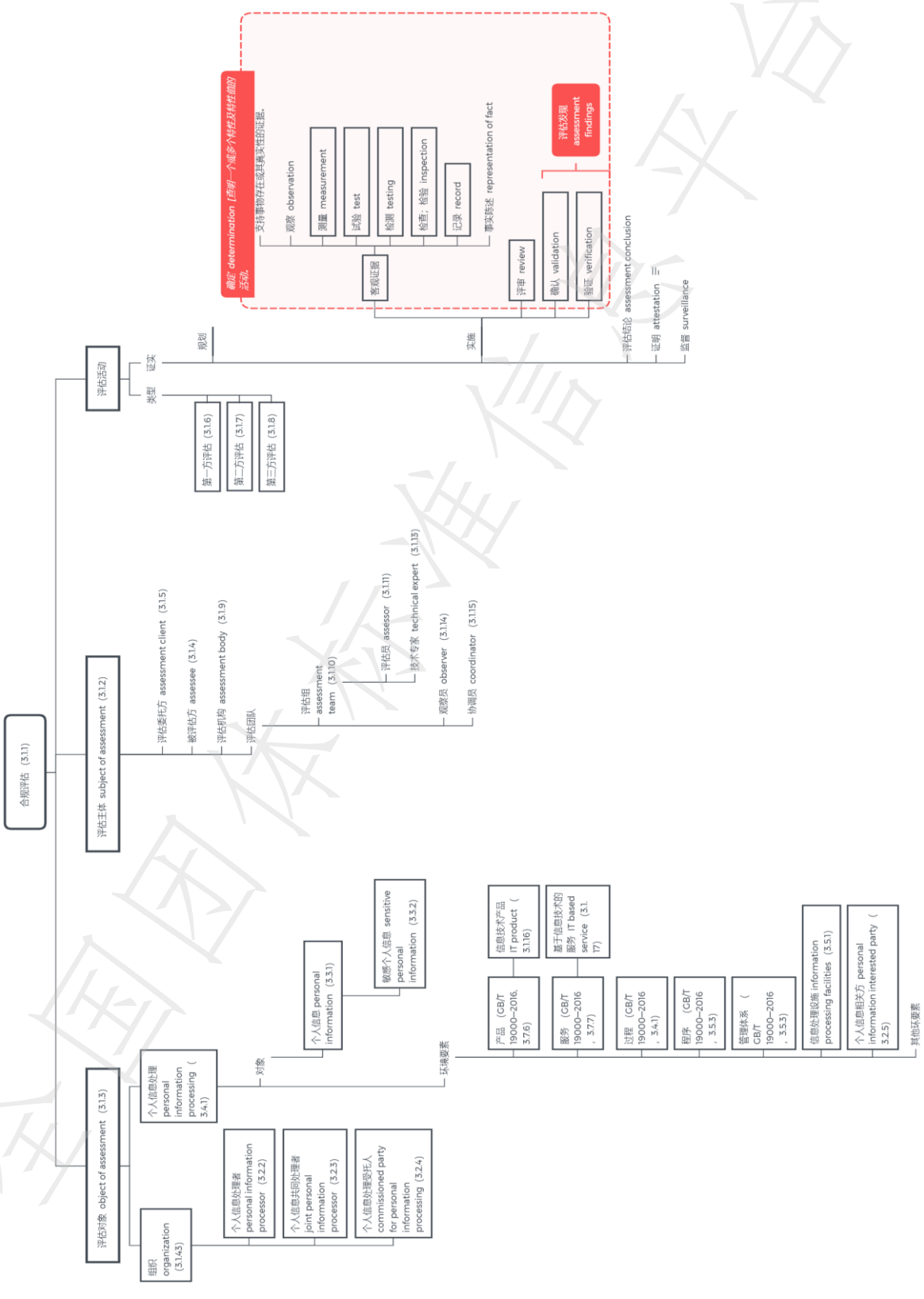
再评估的过程中，组织可以实现迭代的法律合规性评估活动，以便在一个持续性的过程中完善组织的合规状态与能力。这种迭代的法律合规性评估活动，可以通过在下一次的评估对象范围和边界中逐步纳入组织的更多个人信息处理产品、服务或过程来实现，也可以通过逐步纳入更多合规要求来实现，以及也可以随着内部环境或外部环境中对合规的期待与需求变化，逐步将法律合规性评估中的基准提高。这种迭代的法律合规性评估在持续的法律合规性评估—改进—监控/再评估—改进—监控/再评估的过程中拉近组织合规状态与组织合规目标之间的差距。

附录A
（资料性附录）
术语的概念关系图示

图A.1个人信息处理相关术语概念关系图示



图A.2法律合规性评估相关术语概念关系图示



T/CLAST

团　体　标　准

T/CLAST 002.2—2021

个人信息处理法律合规性评估指引
第 2 部分：合规框架

Guidelines for legal compliance assessment of processing of personal information—
Part 2：Compliance framework

2021－12－06 发布　　2022－01－01 实施

中 国 科 学 技 术 法 学 会 发 布

目　次

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国科学技术法学会提出并归口管理。

本文件主要起草单位：中国科学技术法学会、深圳市北鹏前沿科技法律研究院、中国法学交流基金会、中国法律咨询中心、北京大学法学院/知识产权学院、北京大学粤港澳大湾区知识产权发展研究院、平安科技（深圳）有限公司、上海携程商务有限公司、北京小桔科技有限公司、阿里巴巴(北京)软件服务有限公司、每日互动股份有限公司、深圳市和讯华谷信息技术有限公司、广东北源律师事务所、上海市锦天城律师事务所、北京市浩天信和律师事务所、北京市金杜律师事务所、中国信息通信研究院云计算与大数据研究所、北京北大英华科技有限公司、网易(杭州)网络有限公司、腾讯科技（深圳）有限公司、荣耀终端有限公司、华米科技、OPPO 广东移动通信有限公司、比亚迪股份有限公司、广州小鹏汽车科技有限公司、深圳市大疆创新科技有限公司、深圳市地铁集团有限公司、上海游昆信息技术有限公司、贝壳找房（北京）科技有限公司、深圳市迷你玩科技有限公司、百行征信有限公司、深圳依时货拉拉科技有限公司、广东小天才科技有限公司、安信证券股份有限公司、深圳市安证企业合规管理（集团）有限公司、杭州安信检测技术有限公司、杭州安恒信息技术股份有限公司、深圳市网安计算机安全检测技术有限公司。

本文件主要起草人：张平、毕马宁、南红玉、黄亚英、肖声高、徐美玲、时建中、李玉香、周辉、涂俊峰、谈建、周涛、任晓明、李伟民、崔亚冰、王心阳、赵怡冰、辜凌云、徐子淼、姬祥、牟晋军、周林、秦齐祺、张娜、徐彩曦、张铮、陈津来、陈光炎、植吕梅、梁艳芬、吴卫明、丁峰、田劼、冯红、吴涵、何为、李青、赵紫钰、包一明、石霖、何远琼、李川东、蒋仁熙、梁淳栋、孙海鸣、武杨、张辉、吴迪、王辉、彭星、高凤、杨小娟、林森才、许艳冰、林莹、彭伟、叶娟、白宝龙、张朝、谢晓勇、罗经华、覃江林、白雷、周俊华、陈天伟、李维春、李旻瑞、李良、龙军、黄伟杰、江鑫、洪跃腾、王水兵、何冠辉、杜文琦、倪荣、刘志乐、吴俊雄。

本文件由中国科学技术法学会、深圳市北鹏前沿科技法律研究院负责解释。

个人信息处理法律合规性评估指引　第 2 部分：合规框架

1范围

本文件规定了组织的个人信息处理应遵循的合规要求，这些合规要求构成了在个人信息处理法律合规性评估中确定评估准则的合规框架。本文件也规定了评估员在法律合规性评估中对这些合规要求的符合性进行确定时应遵循的评估要求和指引。

本文件适用于各种类型的组织规范其个人信息处理活动，也适用于各类组织对其个人信息处理合规性进行的第一方评估和管理，个人信息处理的相关方为采购、监管等特定目的进行的第二方评估，以及独立的评估机构进行的第三方法律合规性评估和咨询。

2规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/CLAST 002.1-2021　个人信息处理法律合规性评估指引　概述和术语

T/CLAST 002.3-2021　个人信息处理法律合规性评估指引　实施指南

GB/T 25069—2010　信息安全技术　术语

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 39335—2020　信息安全技术　个人信息安全影响评估指南

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

3术语与定义

T/CLAST 002.1-2021中界定的或规范性引用的术语和定义适用于本文件。

4概述

本文件给出了个人信息处理的合规框架。合规框架首先是对组织的合规要求，组织可以基于自愿遵守并使用本文件，以规范其个人信息处理活动。当与组织的其他合规要求相结合使用时，本文件通过“维度—指标”或“维度—指标—特性”建立的合规框架可以用来管理组织的各类合规要求，并确定组织应遵循的整体合规准则。

本文件也可以作为个人信息处理法律合规性评估中确定评估准则的基准。当本文件被用来进行法律合规性评估时，本文件中标明为“指标要求”或“特性要求”的内容作为法律合规性评估准则的基准，评估员可以根据适用于评估对象的其他合规义务和合规要求调整这些基准。本文件中标明为“评估要求”的内容是对评估员的要求，即评估员在确定指标要求或特性要求符合性时应遵循的规范。

本文件的结构如下：

第5章给出了个人信息处理和法律合规性评估的通用要求。第5章给出的通用要求采用了“维度—指标”或“维度—指标—特性”框架（见5.1）。

第6章按照不同个人信息处理环节给出了个人信息处理和法律合规性评估的扩展要求，这包括将第5章给出的维度、指标和特性适用到特定个人信息处理环节时所需要的具体化和变通。

附录A-E给出了使用本文件的资料性附录：

附录A（合规框架）

附录B（必要性、直接相关和合理关联性测试方法及示例）

附录C（合法利益的多因素平衡测试方法及示例）

附录D（比例性测试及示例）

附录E（风险评估方法及示例）

5通用要求

5.1通用要求概述

第5章给出了个人信息处理和法律合规性评估的通用要求，包括维度和指标。维度是对指标的类型化概括，表明该维度中的多个指标具有共同的合规和合规评估关注要点。维度也是个人信息处理的基本原则的规则化，通常适用于个人信息处理的全过程，涵盖至少两个以上的个人信息处理环节，或者并非特定于某一个个人信息处理环节。

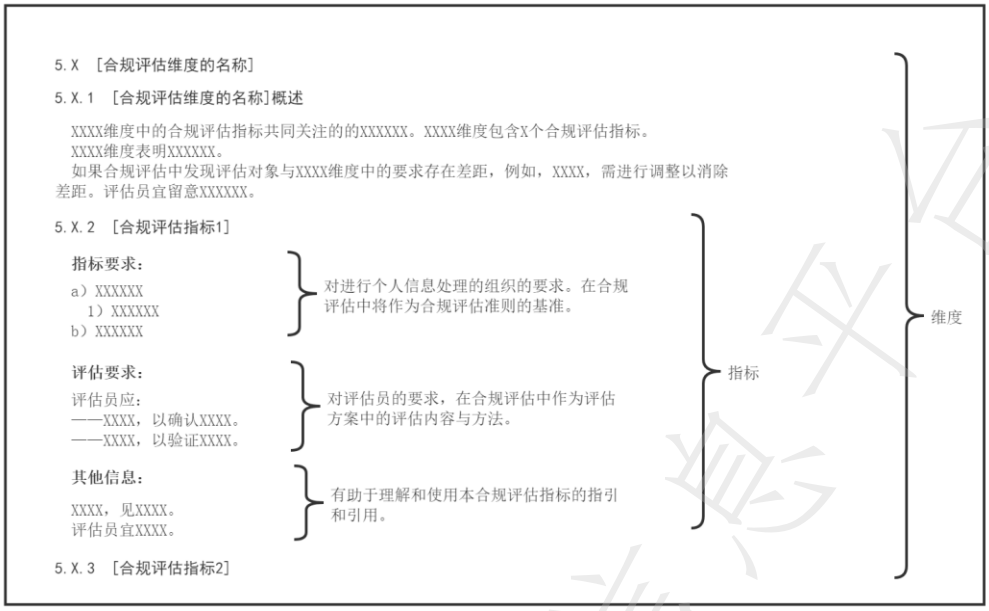
本章给出的每个维度的表述结构如下：

本章中每个一级条标题（如5.2或5.3）是维度的名称。

每个维度下第一个二级条标题（如5.2.1或5.3.1）给出了该维度的概述。概述说明了该维度中包含的指标数量，以及这些指标的共同关注要点。必要时，维度的概述部分还给出了更多指引，例如有助于理解该维度的其他信息，或者在法律合规性评估中发现评估对象与维度之间存在差距时，这些差距的适当调整或处置方法，以及这些差距的调整或处置如何影响法律合规性评估结论。

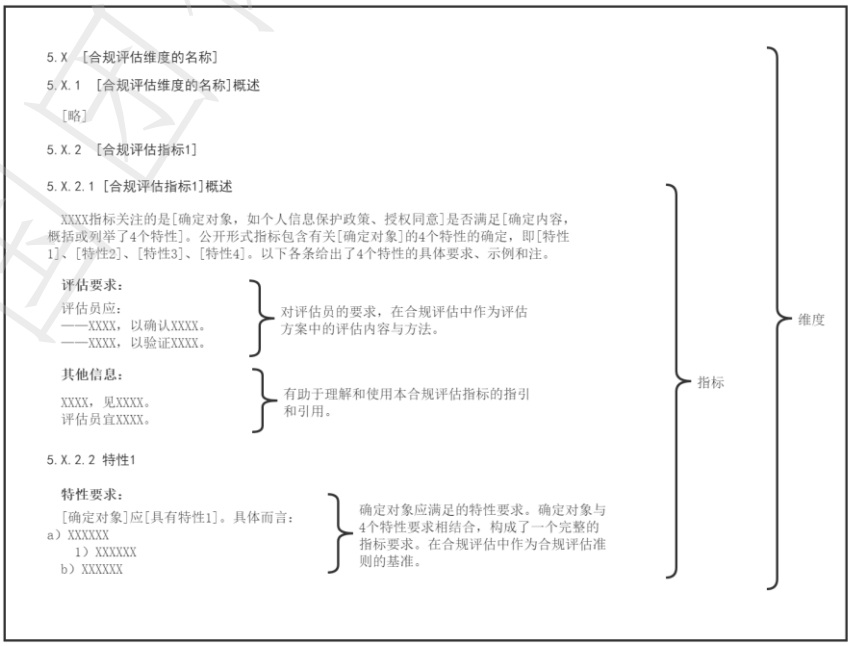
每个维度的第二个二级条标题（如5.2.2或5.3.2）开始，给出该维度中所包含的指标。一般情形下，指标是一个独立的要求，因此一个指标的表述结构一般是由“指标要求”、“评估要求”和“其他信息”组成的。

图1　维度-指标框架图示



但也存在一些例外情形，即有些指标的确定可能依赖于多个特性，例如，公开形式指标（见5.5.4）是对有关个人信息处理政策和实践信息的公开形式方面的要求，其中包含4个特性的确定，例如，相对独立性（5.5.4.2）、易于访问性（5.5.4.3）、易于理解性（5.5.4.4）及易于阅读性（5.5.4.5）。在一个指标包含多个必须被单独描述的特性时，本文件采用了三级条标题来表述这些特性。因此，在这种指标中，第一个三级条标题是概述，表明该指标的确定对象和确定内容，并给出“评估要求”和“其他信息”，第二个三级条标题开始是特性，给出了“特性要求”，也包括该特性要求的示例和注。确定对象与特性要求共同构成了一个完整的指标。

图2　维度-指标-特性框架图示



5.2合法维度

5.2.1合法维度概述

合法维度中的指标共同关注的是：个人信息处理是否符合可适用的法的强制性规范。

合法维度包含5个指标，即合法性基础指标、主体合法指标、程序合法指标、类型合法指标和来源合法指标，分别从个人信息处理的基础、主体、程序、对象类型与来源等方面，确定个人信息处理符合可适用的法的强制性规范。

合法维度中的指标都援引了可适用的法。这些指标在未充分识别评估对象的可适用的法的前提下是无法适用的，并且在可适用的法发生变化时，指标会受到该变化的影响。这要求组织持有一份合规义务清单以明确其可适用的法，并确保组织内存在一个管理机制使其能够持续更新合规义务清单。在法律合规性评估中，也要求评估员在评估期内采取审慎的步骤识别和确定评估对象的合规义务清单，并宜在评估法律意见书中将合规义务清单作为附件。评估员宜认识到该指标由于援引可适用的法而带来的固有的不确定性，并使法律合规性评估的所有相关方认识到这些指标的评估可能具有的局限性。

5.2.2合法性基础指标

指标要求：

个人信息处理者应在个人信息处理前明确识别可适用的合法性基础，并确保个人信息处理满足5.2.2.1-5.2.2.8的特性要求之一。

其他信息：

以下各条给出了8种可能的合法性基础及其特性要求。

在法律合规性评估中，由被评估方识别个人信息处理的合法性基础。评估员的任务是获取客观证据确定评估对象是否满足该合法性基础的特性要求。如被评估方识别的合法性基础经确定为不满足，评估员宜允许被评估方重新识别合法性基础，并再次确定评估对象是否满足重新识别的合法性基础。如果确定评估对象不满足任何一项合法性基础，或者未能确定评估对象满足任何一项合法性基础，该维度的评估结论为不符合。评估员宜审慎考虑这是否表明评估对象很可能已经不合法，并与评估委托方商定是否终止法律合规性评估。

5.2.2.1选择同意处理

特性要求：

个人信息处理是基于个人信息主体或其监护人的选择同意（见 5.7.2）。

评估要求：

评估员应确认被评估方征求同意的具体场景，以确定被评估方在个人信息处理前已获得有效的选择同意（见 5.7.2）。

其他信息：

参见《个人信息保护法》第 13 条第 1 款第 1 项。

本项可以采用抽样方法获取客观证据，评估员宜使法律合规性评估的所有相关方注意到

采用抽样方法评估的局限性。

选择以本项作为合法性基础时，需与选择同意指标（见 5.7.2）结合进行评估，个人信息处理符合选择同意指标（见 5.7.2）是符合本合法性基础的必要条件。

5.2.2.2合同必要处理

特性要求：

个人信息处理应是：

a) 为了履行个人信息主体作为一方的合同而必要的；或

b) 为了应个人信息主体的请求与之订立合同而必要的；

注：“为了订立……合同”不宜被宽泛地理解为涵盖未经个人信息主体的请求而主动做出的要约邀请或要约等，虽然要约邀请或要约本身对于合同订立而言具有必要性，但为此进行的未经同意的个人信息处理，可能被有权机关认定为是未经同意的商业营销目的。

评估要求：

评估员应评审被评估方提供的合同、产品/服务说明、产品/服务协议等文件，确认个人信息处理就该合同履行、订立目的而言具有必要性。

其他信息：

参见《个人信息保护法》第 13 条第 1 款第 2 项前半句。

合同必要处理的必要性确定方法及示例，见附录 B.3。

本项可以采用抽样方法获取客观证据，评估员宜使法律合规性评估的所有相关方注意到采用抽样方法评估的局限性。

5.2.2.3人力资源管理必要处理

特性要求：

a) 个人信息处理应是为了按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理而必要的；

b) 如果可适用的法规定了所涉及的个人信息和个人信息处理的类型、所涉及的个人信息主体、处理目的、存储期限、可接收该个人信息的第三方的，援引本项作为合法性基础的个人信息处理不应超出可适用的法规定的范围。

注：人力资源管理通常涵盖入职、在职、离职等各环节，但宜留意劳动规章制度、集体合同以及可适用的法的适用范围，尤其是对非在职个人信息主体的适用性。

评估要求：

评估员应：

——评审被评估方的劳动规章制度和集体合同，确认个人信息处理者已明示涉及个人信息处理的具体人力资源管理目的、方式和范围；

——评审个人信息处理者明示的目的、方式和范围，确认个人信息处理的方式和范围就已经明示的具体目的而言是必要的；

——确认个人信息处理的具体目的、方式和范围符合被评估方的劳动规章制度和集体合同中已经明示的处理目的、方式和范围；

——评审被评估方的劳动规章制度和集体合同，确认其符合可适用的法的规定，尤其是

符合可适用的法规定的有关个人信息处理的要求。

其他信息：

参见《个人信息保护法》第13条第1款第2项后半句。

用人单位与雇员、雇员候选人或前雇员之间为订立、履行合同而必要的处理，亦可能援引合同必要处理（5.2.2.2）作为合法性基础。

符合本合法性基础不意味着豁免个人信息处理者在合法维度的其他指标、目的明确、目的限定、告知等其他维度的合规要求。

5.2.2.4法定义务必要处理

特性要求：

a) 个人信息处理应是为了履行个人信息处理者和/或个人信息处理受托人的法定义务而必要的；
b) 应能够证明施加该义务的法定依据；
c) 如果该法定依据规定了所涉及的个人信息和个人信息处理的类型、所涉及的个人信息主体、处理目的、持有期限、可接收该个人信息的第三方的，援引本项作为合法性基础的个人信息处理不应超出该法定依据规定的范围。

评估要求：

评估员应：

——评审被评估方提出的法定依据，确认个人信息处理就履行法定义务而言是必要的；

——验证个人信息处理所涉及的个人信息和个人信息处理类型、所涉及的个人信息主体、处理目的、持有期限、接收该个人信息的第三方，以确定满足该法定依据中规定的条件。

其他信息：

参见《个人信息保护法》第13条第1款第3项。

法定义务处理的必要性确定方法及示例，见附录B.1。

如经确认不满足法定依据规定的条件，如所涉及的个人信息、个人信息处理类型、个人信息主体、处理目的、持有期限、接收该个人信息的第三方超出了法定依据规定的范围，应确定为差距。该差距的调整或处置可参照适用目的限制维度中有关超范围处理的调整或处置（见5.4.1）。

5.2.2.5公共利益必要处理

特性要求：

a) 个人信息处理应是为了实现或维护以下公共利益而必要的：
   1) 国家安全、国防安全、公共安全；
   2) 犯罪侦查、起诉、审判和执行判决；
   3) 应对突发公共卫生事件；
   4) 其他公共利益。
b) 应能够证明符合以下主体适格性要求之一：
   1) 被评估方根据可适用的法拥有进行该个人信息处理的职责或权限；

2) 被评估方是在符合 1)项要求的个人信息处理者的命令或委托之下进行该个人信息处理的。

c) 可适用的法规定了为此目的进行个人信息处理所涉及的个人信息类型、个人信息处理类型、个人信息主体类型、处理目的、存储期限、可接收该个人信息的第三方的，援引本项作为合法性基础的个人信息处理不应超出该范围。

评估要求：

评估员应：

——评审被评估方提出的法定依据，以确认个人信息处理就实现或维护所识别的特定公共利益而言是必要的；

——评审被评估方的主体资格类或其他文件，以验证被评估方的主体适格性；

——验证个人信息处理所涉及的个人信息和个人信息处理类型、所涉及的个人信息主体、处理目的、持有期限、接收该个人信息的第三方，以确定满足该法定依据中规定的条件。

其他信息：

参见《个人信息保护法》第13条第1款第3项（履行法定职责）、第4项（应对突发公共卫生事件）、第7项（法律、行政法规规定的其他情形）和第26条。

公共利益处理的必要性确定方法及示例，见附录B.2。

如经确认不满足法定依据规定的条件，如所涉及的个人信息、个人信息处理类型、个人信息主体、处理目的、持有期限、接收该个人信息的第三方超过法定依据规定的范围，应确定为差距。该差距的调整或处置可参照适用目的限制维度中有关超范围处理的调整或处置（见5.4.1）。

5.2.2.6公共信息公平处理

特性要求：

a) 应能够证明个人信息处理所涉及的个人信息是从公开信息中收集的，包括：

1） 个人信息主体自行公开的信息；

2） 从其他合法公开的信息中收集的，如合法的新闻报道、出版物或政府信息公开、政府数据共享等渠道。

b) 个人信息主体未事先明确声明拒绝该个人信息处理，并且拥有有效的选择退出机制（见 5.7.3）；

c) 援引本项作为合法性基础的个人信息处理，在其具体场景中不应是对个人信息主体的合法权益有重大影响的个人信息处理；

d) 援引本项作为合法性基础的个人信息处理，在其具体场景中不应超出可适用的法所允许的合理范围；

e) 个人信息处理符合来源合法指标（见 5.2.6）及其收集环节扩展要求（见 6.2.2.2）。

注：除个人信息主体的合法权益之外，在具体场景中个人信息处理可能为其他组织或个人的合法权益带来损害，如违反ROBOTS协议的爬虫、违反第三方API协议的数据获取等，有可能损害其他组织或个人对其数据享有的合法权益，从而面临《反不正当竞争法》《刑法》项下的责任，这些要求见来源合法指标收集环节扩展要求（见6.2.2.2）。

评估要求：

评估员应：

——评审有关个人信息来源或渠道的证明，以确认这些来源符合来源合法指标的要求；

——确认被评估方在实际开展大规模的公开信息收集活动前，是否通过个人信息保护影响评估或其他组织流程，审慎地评估所要收集的公开信息渠道、收集的合理限度，以及所计划的收集目的和后续使用目的可能对个人信息主体合法权益带来的影响，并根据评估结果采取适当的控制措施；

——确认选择退出机制的存在及其有效性。

其他信息：

参见《个人信息保护法》第13条第1款第6项和第27条。

个人信息被自行或合法公开的事实本身并不会改变个人信息的性质，也不会排除个人信息保护的相关义务与责任。对公开信息的收集可能豁免告知维度中的部分指标或特性要求[如政策告知指标和事件告知指标中的送达方式特性要求（见5.6.2.4和5.6.3.4），同步告知指标要求（见5.6.4.6）和选择同意指标要求（见5.7.2）]，但这取决于这些特定指标或特性要求中的具体条件的满足，同时，对这些从公开信息中获得的个人信息进行后续处理时，需要重新考虑这些要求是否仍然被满足。

评估员宜留意在法律合规性评估中，公开信息公平处理本身是一种要求利益平衡的评估，其中包含的“对个人信息主体的合法权益有重大影响”以及“合理范围”等条件是该合法性基础成立的必要条件，但其本身因采用了开放性、不确定性概念而保留了裁量空间。评估员宜使法律合规性评估的所有相关方认识到，该项合法性基础及其评估的固有局限性。例如，只能确定被评估方对于这些公开信息公平处理进行了审慎尽职的利益平衡，从而在必要时帮助被评估方证明其尽到了合理的注意义务，遵循了正当原则和可问责原则。评估员仅被要求验证和证明此种事实的存在，并根据可适用的法以及评估员的知识和经验，确认在此种审慎尽职的利益平衡中不存在明显不合理的情形。

5.2.2.7紧急必要处理

特性要求：

a) 应能够证明在个人信息处理的具体场景中，个人信息主体或其他个人的生命、健康和财产安全面临现实和即刻的危险；

b) 所进行的个人信息处理应是为保护个人信息主体或其他个人的生命、健康和财产安全等重大合法权益而必要的；

c) 应能够证明在当时的具体场景中，难以事先获得个人信息主体的选择同意；

d) 该个人信息处理不应对个人信息主体的合法权益带来不成比例的损害。

评估要求：

评估员应：

——验证评估对象中个人信息处理的具体场景，如重大合法权益的具体内容、是否面临现实和即刻的危险，以确定个人信息处理就保护个人信息主体、其他个人的重大合法权益而言具有必要性和紧急性；

——验证评估对象中个人信息处理的具体场景，以确定在该具体场景中难以事先获得个人信息主体的选择同意；

——验证评估对象中个人信息处理的具体场景，以确定该个人信息处理不会对个人信息主体的合法权益带来不成比例的损害。

其他信息：

参见《个人信息保护法》第13条第1款第4项后半句。

比例性确定方法及示例，见附 录D。

评估员宜留意在法律合规性评估中紧急必要处理所包含的比例性确定方法存在固有的局限性。例如，比例性确定在本质上是具体场景下的利益平衡，法律合规性评估只能确定被评估方对于这些紧急必要处理进行了审慎尽职的利益平衡，从而在必要时帮助被评估方证明其尽到了合理的注意义务，遵循了正当原则和可问责原则。这些利益平衡可能事后被有权机关认定为是不适当的，评估员宜使法律合规性评估的所有相关方认识到这些方法固有的局限性。

5.2.2.8合法利益公平处理

特性要求：

a) 个人信息处理是为了实现个人信息处理者所追求的合法利益而必要的；

b) 应具体识别其个人信息处理所追求的现实的和当下的合法利益；

注1：个人信息处理者所追求的合法利益的例子，诸如，行使个人信息处理者的合法权利，如知识产权、保护商业秘密、债权等，或者防止对产品或服务的欺诈、滥用，保护其信息系统、网络和信息安全，维护客户关系或商誉，营销、广告宣传或维护公共关系，更好地了解客户偏好和需求，研发新产品或服务或改进现有产品或服务，改进组织管理等，遵守监管部门的要求或控制合规风险等。

注2：个人信息处理所追求的合法利益也可能是属于第三方、公众或社会的合法利益，诸如，通过使用其持有的个人信息提供反欺诈核验服务，以协助第三方履行其反欺诈的法定义务；个人信息处理者通过对其持有的个人信息进行统计、分析和研究，发布诸如流行病预测、电信诈骗趋势报告等，可能使公众或社会因统计、分析和研究结果获得与主题有关的信息和知识；个人信息处理者为公共利益实施新闻报道、舆论监督等行为而进行个人信息处理。

c) 应能够有说服力地论证，为该合法利益所进行的个人信息处理，未超出可适用的法通常所允许的合理范围；

d) 应能够有说服力地论证在该个人信息处理的具体场景下，要求其事先获得选择同意将使其追求的合法利益无法实现或要求付出与收益不成比例的成本；

e) 应能够有说服力地论证（如通过个人信息保护影响评估等），在具体场景中，已采取有效的控制措施，足以确保该个人信息处理不会对个人信息主体的合法利益造成不成比例的损害；

f) 至少为个人信息主体提供行选择退出机制（见 5.7.3），且个人信息主体未明确拒绝或选择退出。

评估要求：

评估员应：

——验证评估对象中个人信息处理的具体场景，以确定个人信息处理者所追求的是否是现实的和当下的合法利益，且个人信息处理是否是为了实现该合法利益而必要的；

——验证评估对象中个人信息处理的具体场景，以确定被评估方有关选择同意的成本—收益比例性论证和利益—损害比例性论证是适当和充分的；

——验证评估对象中个人信息处理的具体场景，以确定个人信息处理未超出可适用的法允许的合理范围，以及被评估方的论证是适当和充分的；

——确认至少存在选择退出机制，并且个人信息主体的选择退出（见 5.7.3）得到执行。

其他信息：

参见《个人信息保护法》第13条第1款第5项、第7项、第34条。

合法利益公平处理的必要性，见附 录C。

比例性测试及示例，见附 录D。

评估员宜留意在法律合规性评估中合法利益公平处理包含的比例性确定和合理范围的确定存在其固有的局限性。比例性确定和合理范围的确定本质上是具体场景下的利益平衡，法律合规性评估只能确定被评估方对于这些合法利益公平处理进行了审慎尽职的利益平衡，从而在必要时帮助被评估方证明其尽到了合理注意，遵循了正当原则和可问责原则。这些利益平衡可能事后被有权机关认定为是不适当的，评估员宜使法律合规性评估的所有相关方认识到这些方法固有的局限性。

5.2.3主体合法指标

指标要求：

可适用的法对所涉及的个人信息处理要求行政许可等主体资格的，应符合这些主体资格要求。

示例：可适用的法设定主体资格准入要求的例子，如设立经营个人征信业务的征信机构，须经国务院征信业监督管理部门批准。个人征信业务，即对个人的信用信息进行采集、整理、保存、加工并向信息使用者提供的活动；征信机构是指依法设立，主要经营征信业务的机构。参见《征信业管理条例》第 2 条、第 5 条和第 6 条。

评估要求：

评估员应在确定合规义务清单的基础上，评审被评估方的主体资格类文件，以确认被评估方具备所要求的主体资格。

其他信息：

参见《个人信息保护法》第5条（合法原则）。

5.2.4程序合法指标

指标要求：

可适用的法要求就所涉及的个人信息处理履行行政审批等特定程序要求的，应符合这些程序要求。

示例：可适用的法要求审批程序的例子，如《中华人民共和国人类遗传资源管理条例》虽未禁止外国组织、个人及其设立或者实际控制的机构利用我国人类遗传资源（包括人类遗传资源信息和人类遗传资源材料）开展科学研究活动，但第 21-22 条要求应采取与我国科研机构、高等学校、医疗机构、企业合作的方式，并经国务院科学技术行政部门批准。

评估要求：

评估员应在确定合规义务清单的基础上，评审被评估方提供的行政审批等文件，以确认评估对象履行了这些程序要求。

其他信息：

参见《个人信息保护法》第5条（合法原则）。

5.2.5类型合法指标

指标要求：

不应对可适用的法禁止处理的个人信息类型进行处理。

示例：如《非银行支付机构网络支付业务管理办法》（中国人民银行公告(2015)第43号）第20条禁止非银行支付机构存储客户银行卡的磁道信息或芯片信息、验证码、密码等敏感信息。

评估要求：

评估员应：

——确定评估对象中包含的所有个人信息类型，包括评估对象中每一个个人信息处理过程输入和输出的个人信息类型，见T/CLAST 002.3—2021，8.2.1 a）3）；

——在确定合规义务清单和其中包含的对个人信息类型的禁止性规定的基础上，验证评估对象是否对可适用的法禁止处理的个人信息类型进行处理。

其他信息：

参见《个人信息保护法》第5条（合法原则）。

5.2.6来源合法指标

指标要求：

所处理的个人信息应具有可被证明的合法收集来源，该合法收集来源满足收集环节的扩展要求（见6.2.2.2）。

评估要求：

评估员应：

——确定评估对象中包含的所有个人信息类型及其来源，包括评估对象中每一个个人信息处理过程输入和输出的个人信息类型，见T/CLAST 002.3—2021，8.2.1 a）3）；

——确定评估对象中的所有个人信息类型均具有明确的收集来源；

——确定这些来源是否符合来源合法指标收集环节扩展要求（见6.2.2.2）。

其他信息：

参见《个人信息保护法》第5条（合法原则）。

通常评估对象中必须包含个人信息收集，但本指标并不仅仅适用于收集环节。宜留意在评估对象中可能包含多个个人信息处理环节，而在收集以外的个人信息处理中可能有额外的个人信息类型作为输入，此时对于新增输入还需确定其具有合法收集来源。因此本指标所涵盖的范围要大于收集环节对来源合法指标的扩展要求。

5.3目的明确维度

5.3.1目的明确维度概述

目的明确维度中的指标共同关注的是：个人信息处理是否具有具体/特定的、明示的、合理的处理目的。处理目的表明一个或一组相互关联或相互作用的个人信息处理过程所要实现的预期结果或目标。处理目的是个人信息处理合规的起点，用以确定个人信息处理是否具

有适当的合法性基础以及需采取何种控制措施。目的明确维度也是适用目的限制维度、质量维度的前提条件。

目的明确维度包含3个指标，即目的具体/特定指标、目的明示指标和目的合理指标。

如果法律合规性评估中发现评估对象与目的明确维度中的要求之间存在差距，例如，未识别或未明示处理目的，或者明示的处理目的不够具体、过于模糊抽象，或者处理目的之间不一致、有歧义，或者明示的处理目的具有误导性，需进行调整以消除差距。这些差距并不必然导致不合规（例如隐瞒处理目的、掩盖真实处理目的，窃取或者以欺诈、诱骗或误导方式处理个人信息等）。不合规的判定还需考虑所有相关事实，尤其是差距本身的严重程度、所导致的结果，以及个人信息处理者是否具有隐瞒或掩盖的行为和对后果具有主观故意或严重疏忽。但当这些差距被发现时，评估员宜如实记录发现的情况，同时与评估委托方商榷处置方案，包括是否可接受被评估方在法律合规性评估期间及时调整差距，或在评估法律意见书揭示已经存在的风险，由被评估方选择进行风险接受或进行其他合理处置。

5.3.2目的具体/特定指标

指标要求：

所识别的个人信息处理目的，就所要处理的个人信息类型而言，应足够具体和/或特定。

示例：处理目的过于模糊抽象而不够具体的例子，如“提升服务质量”、“改善用户体验”、“加强安全性”或“研发新产品或服务”，又如“为了履行法定义务”。

注1：处理目的是否足够具体宜在场景中确定，如在个人信息保护政策或者在征求同意前的同步告知中，接收到该信息的一般受众能否根据所告知的处理目的合理确定个人信息将被用于哪些个人信息处理或哪些应用，或者是为了履行哪些法定义务。如被评估方进行多个相互关联的个人信息处理操作或行为，宜识别个人信息处理过程的总体目的，并适当列出该总体处理目的之下所包含的多个处理操作或行为。

注2：对于敏感个人信息而言，处理目的不仅需足够具体，还需足够特定。处理目的特定是关于处理目的个别化（或单独性）方面的要求，即在个人信息保护政策或者在征求同意前的同步告知场景中，接收到该信息的一般受众能否根据所告知的处理目的，合理确定敏感个人信息将被用于哪一个个人信息处理目的。一个敏感个人信息的处理目的可能包含多个服务于该处理目的的个人信息处理操作，应确保这些处理操作中的每一步对于处理目的而言都是必不可少的。

评估要求：

评估员应评审个人信息保护政策、产品/服务说明或协议、产品/服务设计文档、与个人信息处理相关方之间的合同等文件，以确定处理目的具体和特定程度。

其他信息：

参见《个人信息保护法》第6条第1款前半句和第28条第2款。

公开形式指标中的易于理解性特性要求（见5.5.4.4）和同步告知指标的形式适当性特性要求（见5.6.4.4），均包含向个人信息主体沟通处理目的时的具体和特定程度方面的要求。评估员在法律合规性评估过程中可以一并评估这些要求。但评估员宜留意目的具体/特定指标中，处理目的信息的受众也可能不仅限于个人信息主体，还包含其他个人信息相关方，例如，被评估方的员工或个人信息处理受托人。

5.3.3目的明示指标

指标要求：

处理目的应充分明示，即以清晰和明显的方式予以披露、解释或表达，以使个人信息处理者及其人员、个人信息处理受托人、个人信息主体、监管部门等所有个人信息处理相关方能够对处理目的获得确定性的预期和共识。

注：明示处理目的的方式并不限于向个人信息主体进行的政策告知和同步告知，还可以包括向个人信息处理受托人沟通的有关处理目的的要求或合同条款，向监管部门提交的书面申请或其他书面声明等。

评估要求：

评估员应评审个人信息保护政策、产品/服务说明或协议、产品/服务设计文档、与个人信息处理相关方之间的合同等文件，以确定处理目的的明示方式和明示程度。

其他信息：

参见《个人信息保护法》第7条。

处理目的之间不一致或有歧义（如政策中公开的或向个人信息主体同步告知的处理目的、向组织的员工或个人信息处理受托人披露的处理目的，以及向监管部门报告的处理目的之间），或者处理目的的表达方式可能具有误导性（如明示的处理目的与实际处理实践不符），宜将这些情形确定为差距，调整或处置的方法见5.3.1。

5.3.4目的合理指标

指标要求：

个人信息处理目的应具有合理性。

注1：个人信息处理具有合法性基础（见5.2.2）并不必然等同于处理目的具有合理性并不必然等同于个人信息处理的合法性基础。前者是指个人信息处理具有可获得承认的合法基础，如具有权利、特许或自由、义务、授权、权力、职责等；而目的合理是指处理目的在更宽泛的意义上符合所有可适用的法所承认的价值，如非歧视、尊重人格尊严、生命、健康等，从而具有实质正当性。表明合法与合理之间的差异的示例，如为了防止保险欺诈行为收集既往病史，可能是基于防止保险欺诈的法定义务或者个人信息处理者的合法利益，从而具有合法性基础。但如果在具体场景中所涉及的是为相同目的收集遗传信息、基因检测资料，则隐含地存在基因歧视等不公平因素，从而在这一具体场景中不具有合理性。又如，为了建立员工名录、考察员工的岗位适格性等人力资源管理目的进行必要的个人信息处理，通常具备合法性基础，但为评估岗位适格性的目的收集婚姻、生育、乙肝病原携带情况的信息，通常需要特别考虑处理目的的合理性，例如是否涉及特殊工种或特殊工作环境等。

注2：可能引发合理性质疑的常见情形，如歧视性的用户画像标签、算法歧视、操纵价格或滥用市场支配地位、就业歧视等。

评估要求：

评估员应结合个人信息处理的具体场景，评审确定处理目的不具有明显违反被可适用的法所承认的价值的因素。

其他信息：

参见《个人信息保护法》第5条（正当原则）、第6条前半句（合理的目的）、第24条第1款。

当法律合规性评估中发现评估对象的处理目的与目的合理指标的要求之间存在差距时，评估员宜如实记录发现的事实，并与评估委托方商榷处置方案，包括是否建议被评估方尽可能在评估期间调整这些差距或在评估法律意见书中如实揭示这些风险，并由评估委托方进行风险接受或进行其他合理处置。

评估员宜留意在法律合规性评估中目的合理指标的确定存在其固有的局限性。目的合理性的确定本质上是在具体场景下对处理目的与可适用的法所承认的价值之间的一致性进行的判断。法律合规性评估中，评估员只能根据可适用的法所承认的价值以及评估员对可适用的法的知识和经验，确认处理目的不存在明显不合理的情形。因此，评估员宜通过评估团队集体评审、与评估委托方和被评估方的充分沟通，以及必要时引入问卷调查等客观证据的方式，尽可能保障本指标评估的客观性。同时，法律合规性评估过程和结论本身，以及有效的权益行使机制，将有助于帮助被评估方证明其在处理目的的合理性方面进行了审慎尽职的评估。这些评估结论可能事后被有权机关认定为是不适当的，或者由于环境的变化而不再适当，评估员宜使法律合规性评估的所有相关方认识到这些方法固有的局限性。

5.4目的限制维度

5.4.1目的限制维度概述

目的限制维度中的指标共同关注的是：在实际收集个人信息时，以及在所有后续个人信息处理过程中，个人信息处理者是否以明示的目的为限制进行个人信息处理。

目的限制维度包含2个指标，包括最小必要指标和目的兼容指标。

5.4.2最小必要指标

指标要求：

个人信息处理应：

a) 与明示的处理目的直接相关；

b) 采取对个人信息权益影响最小的方式；

c) 限于实现明示的处理目的所需的最小必要范围。

评估要求：

评估员应：

——确认评估对象的个人信息处理是否都与明示的处理目的直接相关；

——根据评估对象的流程、规程，确定个人信息处理的范围未明显超出实现处理目的所需的最小必要范围，尤其是个人信息处理的类型、数量、频度等；

——确定评估对象中的个人信息处理所选择的方式，尤其是其技术特点，是否是在若干能够实现收集目的的可比较方式中选择对个人信息主体的权益影响最小的方式；

其他信息：

《个人信息保护法》第5条（必要原则）、第6条。

本指标通用于各种个人信息处理环节，但在收集、持有环节有扩展要求。

个人信息处理与处理目的之间的直接相关测试方法及示例，见附录B.3。

可比较方式中对个人权益影响最小的方式，往往取决于成本约束条件以及其他具体场景的考量，在法律合规性评估中评估员宜允许被评估方对该要求作出充分的解释，并在此基础上得出独立的评估发现。

最小必要处理是可适用的法（如《个人信息保护法》第6条）和现有标准（如GB/T 35273—2020）中常见的要素，这使得最小必要指标中出现的差距很可能表明较高的风险程度。对于已超范围处理个人信息的事实，评估员宜如实记录所发现的事实并揭示风险，并与评估委托方商榷处置方案，包括是否建议被评估方在评估期间调整这些差距，或在后续的评估法律意见书中如实披露相关的风险，由评估委托方进行风险接受或进行其他额外处置。

5.4.3目的兼容指标

指标要求：

收集个人信息后的任何后续处理目的，应与所明示的收集目的具有合理关联（兼容性）。

注1：如果所计划的后续处理目的与收集目的不具有合理关联（兼容性），在明示收集目的时应单独列出与收集目的不具有合理关联（兼容性）的后续处理目的，并分别就收集目的（包含与收集目的具有合理关联的后续处理目的）和非合理关联后续处理目的识别合法性基础。

注2：在收集以后,拟进行的后续处理目的与收集目的不具有合理关联（兼容性）的，视为处理目的变更。个人信息处理者应：

——识别可适用于后续处理目的的合法性基础，在必要时进行同步告知并重新获得选择同意；

——在以新的处理目的进行个人信息处理前更新个人信息保护政策并进行政策告知。

注3：与最初的收集目的不具有合理关联的后续处理目的是否需要同步告知并重新获得选择同意，取决于对后续处理目的可援引的合法性基础。例如，无论最初的收集目的所援引的合法性基础，当后续处理目的可援引的合法性基础为合同必要处理（5.2.2.2）、人力资源管理必要处理（5.2.2.3）、法定义务必要处理（5.2.2.4）、公共利益必要处理（5.2.2.5）、公开信息公平处理（5.2.2.6）、紧急必要处理（5.2.2.7）时，个人信息处理的合法性并不取决于选择同意，这些情形（取决于具体分析）通常也可能符合免于同步告知的情形；当后续处理目的可适用的合法性基础为合法利益公平处理（5.2.2.8）时，该合法性基础的适用本身以证明难以获得事先选择同意为前提，同时也可能符合免于同步告知的情形。个人信息处理者也可以直接选择对后续个人信息处理援引选择同意处理（5.2.2.1）作为合法性基础。

评估要求：

评估员应：

——确认后续处理目的与收集目的具有合理关联（兼容性）；

——如果不具有合理关联，通过抽样方法选择与最初收集目的不兼容的后续处理，并确认在该次目的转用时是否存在相应的个人信息保护政策更新和告知；

——评审被评估方对于后续处理目的识别的合法性基础,并按照相应的合法性基础确认符合性；

——如被评估方直接以选择同意处理（5.2.2.1）作为合法性基础，应通过抽样方法验证在每一种与最初收集目的不兼容的后续处理前,是否存在同步告知和选择同意步骤。

其他信息：

《个人信息保护法》第6条、第14条、第17条。

合理关联（兼容性）确定方法及示例，见附录B.4。

除评估要求所规定的对被评估方实际做法的抽样确认之外,评估员宜评审被评估方的流程是否有助于确保：在以任何新的处理目的进行个人信息处理前，经过合规部门的评审以确

认合理关联（兼容性），并决定是否同步地更新个人信息保护政策和进行告知。这一流程的存在将影响所需抽样的数量。

对于明显超范围使用个人信息（或称目的转用）的行为及可能带来的违法违规风险，评估员宜如实记录所发现的事实并揭示风险，并与评估委托方商榷进一步的处置方案。

如果法律合规性评估中发现评估对象以与明示的收集目的不具有兼容性的目的进行后续个人信息处理，而在这些差距发生前，被评估方未识别可适用的合法性基础，首先宜验证在这种差距发生前，被评估方是否更新了个人信息保护政策或与个人信息收集使用有关的规则并进行有效告知，如果也未更新和告知，则此种差距很可能已经构成超范围使用（或称目的转用）。

如果已经进行个人信息政策更新和告知，宜进一步进行合法性基础的识别，并根据具体情形决定调整或处置方式：

——如果超出明示收集目的的后续个人信息处理经识别符合不需要获得选择同意的合法性基础，包括合同必要处理（5.2.2.2）、人力资源管理必要处理（5.2.2.3）、法定义务必要处理（5.2.2.4）、公共利益必要处理（5.2.2.5）、公开信息公平处理（5.2.2.6）、紧急必要处理（5.2.2.7）或合法利益公平处理（5.2.2.8），需进一步评估是否需要就后续个人信息处理目的变更进行同步告知（5.6.4），如果需要同步告知而未告知的，则此种差距很可能已经构成超范围使用；

——后续个人信息处理可适用的合法性基础为选择同意处理（5.7.2），此种差距很可能已经构成超范围使用。

对于上述差距，被评估方宜通过更新个人信息保护政策和进行政策告知、同步告知和选择同意等方式调整，以消除差距。差距很可能已经构成超范围使用从而产生被识别的风险，即“违反法律、行政法规的规定和双方的约定”使用个人信息可能导致的行政责任风险；如果后续个人信息处理是将个人信息披露、转移或提供给第三方或公开，根据具体情形还可能导致刑事责任。因此事后更新个人信息保护政策、政策告知、同步告知和选择同意，难以将已经发生的违规予以合法化从而彻底消除风险，否则将使目的明确维度与目的限制维度丧失意义。此时宜进行的额外处置，包括由评估委托方进行风险接受，或者由被评估方向监管部门咨询确定可能的处置方案，例如，主动向监管部门进行报告后作出整改承诺，必要时向受影响的个人信息主体进行事件告知和进行适当补偿等。

5.5公开透明维度

5.5.1公开透明维度概述

公开透明维度中的指标共同关注的是：有关个人信息处理政策与实践的信息是否以符合透明度原则的方式被公开并提供给个人信息主体，以保障个人信息主体的知情权和其他合法权益的行使。

公开透明维度包含3个指标，包括信息充分指标、公开质量指标、公开形式指标，分别关注有关个人信息处理政策与实践的信息公开是否满足充分、真实、准确、完整、及时、相对独立、易于访问、易于理解、易于阅读等特性。

通常宜将公开透明维度的所有指标作为整体进行法律合规性评估，这些指标所评估的对象，通常是对于所有个人信息相关方可见的信息，当评估对象与这些指标之间存在差距，是容易被感知并带来实质性风险的。这些差距通常可以并且宜在法律合规性评估期内得到调整。

评估员在法律合规性评估的过程中有可能感知到或发现在评估对象之外存在的差距，对于这些差距视而不见很可能削弱法律合规性评估结论的可信度。评估员宜在发现差距时及时

与评估委托方沟通，若评估委托方同意将该差距及时披露给被评估方，则评估员宜使被评估方认识到这些差距的存在并进行调整，但评估员宜使法律合规性评估的所有相关方认识到对于评估对象的范围和边界外的差距识别和风险提示并非法律合规性评估的范围。

5.5.2信息充分指标

指标要求：

个人信息处理者应公开与其个人信息处理政策与实践有关的充分的信息，包括：

a) 所公开的信息的适用范围，例如，适用于哪些产品、服务、组织等；

b) 个人信息处理者的身份，包括公司名称和具体联系方式；

1) 如果有个人信息共同处理者，应包含个人信息共同处理者的身份，以及在个人信息安全方面自身和其他个人信息共同处理者分别承担的责任和义务；

2) 如果有个人信息处理受托人，应包含个人信息处理受托人的身份或类型；

c) 收集个人信息的目的、方式、范围和相关处理规则；

注：具体见信息充分指标收集环节扩展要求（见6.2.5）。

d) 所收集的个人信息的后续处理目的、方式、范围和相关处理规则：

注1：后续处理目的宜包含收集个人信息后预计进行的所有后续处理，对于与收集目的具有合理关联（兼容性）的后续处理目的，通常可以通过“总体目的+该总体目的之下的后续个人信息处理环节”的方式给出；对于与收集目的可能不具有合理关联的后续处理目的，应单独明示后续处理目的、方式和范围以及该后续处理目的之下将包含的个人信息处理环节。

注2：收集目的和后续处理目的以满足目的具体/特定指标（见 5.3.2）和目的明示指标（见 5.3.3）的方式得到描述和明示后，通常可以识别该目的中是否会包含提供、公开、转移、向境外提供等对个人信息的保密性产生重要影响的个人信息处理环节。如果预期普通受众可能很难从收集目的和后续处理目的的表达中合理确信其个人信息将被提供、公开、转移或向境外提供，宜具体和明确地指出这些内容，具体见信息充分指标在特定环节的扩展要求。

e) 个人信息的存储地域、存储期限以及存储期限届满时的处理方式；

f) 个人信息主体合法权益的行使方式、条件或程序，如查询、更正、删除、获取个人信息副本、对自动决策结果进行投诉的方法等，以及选择退出机制；

g) 个人信息主体询问或投诉的渠道（如电子邮件、电话、在线表单、在线客服等）、具体联系方式和处理机制（如处理时限）；

h) 提供个人信息后可能存在的安全风险，发生个人信息安全事件时的处置或补救措施，以及事件告知方式；

i) 个人信息处理者所遵循的个人信息安全原则或法律、法规、标准、协议等，具备的信息安全能力，以及采取的个人信息安全保护措施；

注1：个人信息安全保护措施可包括，诸如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等；

注2：必要时可公开信息安全和个人信息保护相关的认证证明或评估报告等，以说明个人信息处理者所具备的信息安全能力。

j) 外部纠纷解决机构及联络方式；

k) 发布或生效日期和更新规则。

注：“更新规则”应界定必须更新的重大变更事项的范围，应纳入对个人信息处理的范围（如主体、对象、目的和方式）或个人信息主体合法权益行使能力与方式产生实质影响的事项，至少应包括b)-h)。

评估要求：

评估员应评审个人信息处理者所公开的有关个人信息处理政策与实践的信息，以确认其提供的信息具有充分性。

其他信息：

参见《个人信息保护法》第7条、第17条，以及其他标准，如GB/T 35273—2020，5.5。

5.5.3公开质量指标

指标要求：

个人信息处理者应确保信息充分指标（见5.5.2）所记载的信息真实、准确和完整地体现了组织的个人信息处理政策与实践，并在发生重大变更时及时更新信息。

注1：重大变更的范围由个人信息处理者在其公开的信息中自行界定（见 5.5.2 1）及其注），但无论是否以及如何界定，在发生个人信息处理范围（如主体、对象、目的和方式）的实质变更或者对个人信息主体合法权益行使能力与方式产生实质影响的变更时，应及时更新信息以使其保持真实、准确和完整。

注2：变更涉及须获得个人信息主体选择同意的事项时，宜在实际变更发生前且就该事项征求同意前更新；不涉及须获得个人信息主体选择同意的事项时，宜不晚于变更事项实际发生或生效后的一个月。

评估要求：

评估员应：

——在法律合规性评估的过程中比较评估对象与本指标的符合性，并在法律合规性评估结论前，整体评审确定本指标的符合性。

——当确定评估对象与本指标之间存在差距时，进一步评审该差距的重要性，是否可能导致评估对象中的个人信息处理在具有误导性或欺诈性的信息公开基础上进行的。

其他信息：

参见《个人信息保护法》第5条（正当原则、诚信原则和该条后半句）和第17条。

公开质量指标关注的是被评估方实际发生的个人信息处理政策和实践，与被评估方对外公开的信息之间是否一致，这种一致性需要在整个法律合规性评估过程中得到反复评估和确认。当评估对象中的个人信息处理政策和实践与公开的信息之间存在不一致时，这种差距并不必然表明被评估方存在误导、欺诈、隐瞒等违规甚至违法。但这些差距的存在已经表明风险被识别。评估员宜进一步评审确定差距的重要性是否很可能导致：评估对象中的个人信息处理是在具有误导性或欺诈性的信息公开基础上进行的。评估员宜在发现差距时及时与评估委托方沟通，并将这些差距的调整作为出具评估法律意见书的前提，并且明确提示差距调整前已经存在的风险，由评估委托方考虑进行风险接受或其他处置。

目的明确维度和目的限制维度中的差距，很可能同时导致在本指标项下的差距。在其他维度或指标项下的差距需要通过修改或更新个人信息保护政策予以调整时，宜按照特定维度或指标项下给出的调整指引进行。

5.5.4公开形式指标

5.5.4.1公开形式指标概述

公开形式指标关注的是：个人信息处理政策与实践的信息是否以有助于透明度和公正性的形式进行公开。

公开形式指标包含个人信息处理政策与实践信息的4个特性的确定，即相对独立性、易于访问性、易于理解性和易于阅读性。以下各条给出了4个特性的具体要求、示例和注。

评估要求：

评估员应评审个人信息处理保护政策，以验证个人信息保护政策满足相对独立性、易于访问性、易于理解性和易于阅读性的特性要求。

其他信息：

参见《个人信息保护法》第17条，以及其他标准，如GB/T 35273—2020，5.5。

5.5.4.2相对独立性

特性要求：

应通过制定相对独立的文件提供信息充分指标（见5.5.2）所述信息，其呈现形式应：

a) 能够明显区分于用户注册与使用协议、服务协议等并非聚焦于个人信息处理的文件；

b) 能够明显区分同一组织提供的不同产品或服务；

c) 能够明显区分适用于不满十四周岁未成年人个人信息的处理规则。

注1：此类文件的常用名称，如个人信息保护政策、隐私政策、个人信息收集使用规则、隐私声明、隐私通知、常见问答等。无论文件采用何种名称，须综合性地体现并且相对独立地存在。在本文件中统称为个人信息保护政策。

注2：为符合公开透明维度而提供的有关个人信息处理政策与实践的文件（如个人信息保护政策）与约定权利义务的用户协议或服务协议具有不同的目的与效力，后者可能被可适用的法或有权机关认定为格式合同；而个人信息处理的合法性基础并非仅限于个人信息主体的选择同意或与个人信息主体之间的合同，个人信息的收集方式亦涵盖间接获取的情形，在此情形下个人信息主体不受用户协议或服务协议的约束，因此个人信息保护政策需要涵盖用户以外的更大范围的群体。

注3：宜就同一组织提供的不同产品或服务，如多款移动应用程序分别制定单独的文件，而不是仅制定一份适用于组织全部产品或服务的一般性文本，以确保所提供的信息（尤其是个人信息处理目的、方式、范围、和规则等信息）足够具体/特定。如同一组织提供的产品或服务数量相对有限，或个人信息处理的目的、方式、范围和规则同质性程度较高，使得不必制定单独的文件就能够实现足够具体的信息提供，宜在文本中视必要性和适当性明显区分不同产品或服务。

5.5.4.3易于访问性

特性要求：

个人信息保护政策应公开发布且易于访问。具体而言：

a) 任何拥有网站的组织均应在其产品或服务网站主页醒目位置用常用名称（如个人信息保护政策或隐私政策等）设置可直接访问个人信息保护政策的链接；

b） 移动应用程序等软件，应在下载界面（如官方下载网页、应用商城等）、安装界面以及安装后的移动应用程序用户界面的醒目位置（如菜单栏、设置菜单等）提供文件或直接访问个人信息保护政策的链接；

c） 带有屏幕的硬件产品，如物联网设备、移动智能终端设备等，应在产品首次注册或开启界面和用户界面（如菜单栏、设置菜单等）的醒目位置展示个人信息保护政策或直接访问个人信息保护政策的链接；

d） 不带有屏幕的硬件产品，可以在产品在线销售界面提供个人信息保护政策或直接访问个人信息保护政策的链接，并应在产品包装或说明书中提供个人信息保护政策全文或提供可访问个人信息保护政策全文的二维码或个人信息保护政策所在网页的链接地址。

注1：易于访问是指结合产品或服务的具体使用场景和行业内的通用实践，个人信息主体在需要查阅时无需进行繁琐的搜索和跳转等动作，即可在产品或服务有关的直观和醒目位置访问个人信息保护政策。

注2：可适用的法可能规定了适用于特定产品或服务的底线要求，如《APP 违法违规收集使用个人信息行为认定办法》规定“如进入 App 主界面后，需多于 4 次点击等操作才能访问到”为难以访问。

5.5.4.4易于理解性

特性要求：

个人信息保护政策应采用具体、清晰和易于理解的语言。具体而言：

a） 应避免使用过于笼统抽象的语言从而无法提供有关个人信息处理的有意义的信息，以及避免采用模棱两可从而容易产生歧义的语言；

b） 应符合通用的语言习惯，使用标准化的数字或图示等；

c） 应采用平实的语言，避免晦涩难懂的语言，如使用大量专业术语。

示例：笼统抽象和模棱两可的例子，如“为了更好地提供服务和升级产品，我们可能会将您的某些个人信息提供给合作伙伴用于统计分析”，“我们采用行业通行的安全技术和严格的管理制度来保护您的个人信息安全”的表述，过于笼统抽象，从而未能提供有关个人信息处理的有意义的信息；而“合作伙伴”的术语在未经定义的前提下，难以确定是指委托的个人信息处理受托人还是向第三方提供或转移；“我们可能会收集……”等模棱两可的表达难以确定是否收集。

5.5.4.5易于阅读性

特性要求：

个人信息保护政策应易于阅读，并对其中的重要信息采用突出显示。

注1：易于阅读宜关注呈现格式、形式或语言等方面，如字号、颜色、行间距等排版格式不会造成阅读困难，文件过长时宜提供目录、摘要或超链接等以便查找和定位。呈现格式、形式或语言等方面，宜充分考虑受众特点、呈现场景等因素的影响，如产品或服务的计划受众主要是儿童、视觉障碍人士或老年群体时，适应受众特点选择呈现格式或提供音视频等多媒体形式。

注2：突出显示宜关注突出显示的信息与非突出显示的信息的区分程度，如采用字体加粗、标星号、下划线、斜体、颜色或表格中的单独一列等。

注3：需突出显示的信息取决于可适用的法的规定，通常包括敏感个人信息、涉及出境的个人信息类型等。

5.6告知维度

5.6.1告知维度概述

告知维度关注的是：个人信息处理者在个人信息处理的过程中，是否不仅仅是通过个人信息保护政策公开信息，还通过与个人信息主体的适时沟通与互动，将信息主动提供给个人信息主体，使个人信息处理的规则、事件、变化对个人信息主体而言具有适当透明度。适当的告知，将促进个人信息主体知情权、决定权的实现，并有助于增进个人信息主体对个人信息处理者尽责性的理解。

告知维度与公开透明维度、选择维度具有密切的联系，有时告知维度和选择维度被统称为告知同意。但告知并不仅仅是在征求同意的语境下才需要的，尤其在不以选择同意作为合法性基础的个人信息处理中，以及在采取选择退出机制的场景中，将不同的告知与选择同意的场景区别开来加以规划和评估，将有助于避免在个人信息主体突然发现其个人信息被处理时可能引发的对处理合规性的质疑和争端。

告知维度包含3个指标，涵盖3种不同类型的告知，即政策告知、事件告知以及同步告知。

法律合规性评估中发现被评估方实际进行的告知与本维度中的指标之间存在差距的，并不必然表明个人信息处理不合法，但在差距较为重大时可能表明个人信息处理有违合法性原则或正当性原则，并容易因此引发与个人信息主体之间的纠纷以及其他行政责任。评估员宜将这些差距及其可能的风险充分揭示给评估委托方，由评估委托方考虑进行风险接受或处置。在法律合规性评估中宜允许被评估方对微小的差距进行及时的调整。

5.6.2政策告知指标

5.6.2.1政策告知指标概述

政策告知指标关注的是：在公开透明维度的基础上，个人信息处理者是否还采取积极的步骤将个人信息保护政策有效地提供给个人信息主体，包括主动引导个人信息主体访问，以促进个人信息主体的理解和知情的选择同意。

政策告知指标包含3个特性的确定，即政策告知的时机、形式和送达方式的适当性。以下各条给出了3个特性的具体要求、示例和注。

评估要求：

评估员应：

——在评估对象的实际安装、使用场景中，验证首次政策告知的时机与本指标的符合性；

——评审被评估方间接获取个人信息时进行政策告知的方式和时机，验证政策告知是在后续个人信息处理前或间接获取个人信息后的合理期限中较早截至的时机前进行的；

——采用抽样方法验证个人信息处理者在个人信息保护政策文件更新时已进行重新告知；

——评审个人信息处理者的规章制度、操作规程和配套的报告记录模板，确认个人信息处理者所建立的制度、规程和业务流程能够确保个人信息保护政策更新时重新进行政策告知。

其他信息：

参见《个人信息保护法》第17条，以及其他标准，如GB/T 35273—2020，5.5。

政策告知与本指标中的特性要求存在差距的，个人信息处理者应通过修改消除差距。未进行政策的首次告知和重新告知的，需对调整前的风险进行揭示，由评估委托方进行风险接受。

5.6.2.2时机适当性

特性要求：

a） 首次政策告知时机应不晚于首次打开产品、首次使用服务、安装软件或移动应用程序、注册账号时；

b） 间接获取个人信息的，应在进行任何后续个人信息处理前或者间接获取个人信息后的合理期限内尽早进行首次政策告知；

示例：间接获取后进行的后续个人信息处理的示例，如利用间接获取的个人信息与个人信息主体进行首次通信，将间接获取的个人信息与个人信息处理者已经持有的个人信息进行汇聚融合，存储至可以访问间接获取的个人信息以进行用户画像、个性化展示、自动决策等的业务系统中，以及委托处理、向第三方提供、转移、公开间接获取的个人信息等。

注1：不应等到间接获取的个人信息后续处理即将要超出间接获取时已获得的选择同意范围，从而需要重新征求个人信息主体选择同意时，才进行首次政策告知。首次政策告知与选择同意并不具有必然关联。但如果在间接获取时或在间接获取之前，个人信息主体已经获得政策告知并且其中已经包含与间接获取的个人信息的处理范围和个人信息主体合法权益的行使有关的信息，则不必再次告知。

注2：合理期限宜不晚于间接获取个人信息后的一个月。

c） 个人信息保护政策文件更新时，应重新进行政策告知。

5.6.2.3内容适当性

特性要求：

政策告知应：

a） 采用明显方式提醒阅读，并附个人信息保护政策的全文或链接；

注：可供选择的明显方式包括弹窗、显著标识（如字体加粗、标星号、下划线、斜体、颜色等）的文字说明、勾选框、填写框、提示条、提示音等。

b） 个人信息保护政策因以下重大变更而更新时，除附个人信息保护政策的全文或链接外，政策告知应采用明显方式提示发生变更的内容：

1） 个人信息处理范围（如主体、对象、目的和方式）发生实质变更；

2） 对个人信息主体合法权益行使能力与方式产生实质影响的变更；

3） 个人信息处理者所公开的信息中自行界定的其他重大变更。

注1：重大变更的范围见 5.5.2 1）及其注。

注2：在政策告知中提示变更内容的明显方式，如在政策告知中包含变更内容摘要，或者在所附个人信息保护政策全文中突出显示变更内容。

5.6.2.4送达方式适当性

特性要求：

个人信息保护政策的首次告知和重新告知应逐一送达个人信息主体；当成本过高或有显著困难时，可以公告形式发布。

注1：逐一送达方式，如弹窗、电子邮件、信函、电话、推送通知等方式。

注2：逐一送达成本过高或有显著困难的例子，如在非在线交互环境下面向非特定的个人信息主体自动采集个人信息，难以获得个人信息处理者的联系方式，或缺乏与个人信息主体建立联系的机制等。

5.6.3事件告知指标

5.6.3.1事件告知指标概述

事件告知指标关注的是：当发生可能给个人信息主体的合法权益造成严重危害的个人信息安全事件或其他个人信息处理违规行为后，是否通过及时、透明与尽责的事件告知，为个人信息主体提供警示、建议和补救。

评估要求：

评估员应：

——通过评审个人信息安全事件记录，确定评估对象是否发生过可能给个人信息主体的合法权益造成严重危害的个人信息安全事件或其他个人信息处理违规行为；

——通过抽样方式确定在这些事件发生后，被评估方是否及时进行适当事件告知；

——评审个人信息处理者的规章制度、操作规程和配套的报告记录模板，确认适用于评估对象的制度、规程和业务流程界定了进行事件告知的条件，这些条件能确保在其得到遵守时被评估方满足本指标。

其他信息：

参见《个人信息保护法》第57条第2款，以及其他标准，如GB/T 35273—2020，10.2。

评估对象与本指标中的特性要求存在差距的，宜要求调整消除差距。对调整前的风险，宜向评估委托方进行揭示由其进行风险接受或其他处置，例如由被评估方向监管部门咨询确定可能的补救方案。

5.6.3.2时机适当性

特性要求：

个人信息安全事件或其他个人信息处理违规行为可能给个人信息主体的合法权益造成严重危害的，如敏感个人信息的泄露，应尽快向个人信息主体进行事件告知。

注1：有些个人信息处理违规行为，如违反最小必要指标（见 5.4.2）或目的兼容指标（见 5.4.3）从而超范围进行的个人信息收集或后续个人信息处理，有可能会导致未经个人信息主体授权的个人信息泄露，但这一泄露并不是未经个人信息处理者授权的泄露，因此不属于信息安全事件。当个人信息安全事件以外的其他个人信息处理违规行为可能给个人信息主体的合法权益造成严重危害的，也应进行事件告知。

注2：事件告知的时机不应有不合理的拖延，在发现或合理地确信个人信息安全事件或其他个人信息处理违规行为很可能已经发生后，如果可行，宜在 72 小时内。

5.6.3.3内容适当性

特性要求：

事件告知内容应包括：

a) 个人信息安全事件或其他个人信息处理违规行为的内容和对个人信息主体的影响；
b) 已采取或将要采取的处置措施；
c) 个人信息主体自主防范和降低风险的建议；
d) 针对个人信息主体提供的补救措施；
e) 组织中被指定的个人信息保护负责人和个人信息保护工作机构的联系方式。

5.6.3.4送达方式适当性

特性要求：

事件告知应逐一送达受影响的个人信息主体；当逐一送达有显著困难，应采取合理、有效的方式发布必要的警示信息。

注：逐一送达方式，如包括弹窗、电子邮件、信函、电话、推送通知等方式。

5.6.4同步告知指标

5.6.4.1同步告知指标概述

同步告知指标关注的是：个人信息处理者是否根据个人信息处理环节或征求个人信息主体同意的进程，分阶段、即时同步地向个人信息主体告知与个人信息处理最密切相关的信息，以促进知情或知情同意。

同步告知指标包含4个特性要求，涵盖同步告知的时机、内容、形式和送达方式的适当性，另外，5.6.4.6给出了免于同步告知的情形。

同步告知指标在收集、使用、存储、公开、提供、转移等环节，以及在向境外提供、共同处理、委托处理、第三方管理等特殊个人信息处理类别中均有扩展要求。这些扩展要求主要给出了同步告知的适当时机与适当内容。

评估要求：

评估员应：

——在评估对象的具体运行环境中，验证在 5.6.4.2 所规定的时机将出现同步告知；

——在评估对象的具体运行环境中，确认同步告知内容、形式和送达方式的适当性特性要求得到满足。

其他信息：

参见《个人信息保护法》第17条、第18条、第22条、第23条、第30条、第35条、第39条。

5.6.4.2时机适当性

特性要求：

同步告知至少应在以下适当时机出现：

a) 同步告知的扩展要求列出的时机；
b) 可适用的法要求单独告知的时机；
c) 个人信息处理者征求单独同意或书面同意时。

5.6.4.3内容适当性

特性要求：

同步告知应提供与触发本次同步告知的个人信息处理最密切相关的信息。

注：最密切相关信息一般包含触发本次同步告知的个人信息处理的目的、方式、所涉及的个人信息类型和个人信息处理者的身份。在根据同步告知的场景可以明确知晓个人信息处理者身份的，可以省略该信息。在涉及个人信息处理者之外的其他个人信息相关方时，最密切相关信息还包括该个人信息相关方的身份（如姓名或名称），必要且适当时可包括该相关方的联系方式。

5.6.4.4形式适当性

特性要求：

同步告知在形式上应：

a） 采用简洁、清晰和平实的语言或通用图标；

b） 单独呈现最密切相关的信息；并且

c） 附带进一步访问详细信息的便捷方式。

注1：仅提供个人信息保护政策，未单独呈现最密切相关信息的，不是同步告知。

注2：允许个人信息主体进一步访问详细信息的便捷方式，如：

- 链接—跳转/下载：在同步告知中设置一个或多个链接，允许个人信息主体通过点击链接直接跳转至或者下载更详细的信息，如更详细的说明或个人信息保护政策。采用链接—跳转方式的，宜跳转至对应条款或段落；
- 分层展示：在同步告知中设置一个或多个按钮，个人信息主体点击按钮时展开或弹出更详细的信息；
- 分区展示：在同步告知中或者在同步告知的同时，用单独区域（如文本框或网页界面）直接展示更详细的信息，如更详细的说明或个人信息保护政策；
- 扫码获取：在同步告知中附带二维码，个人信息主体扫描二维码时展示更详细的信息；宜仅适用于非在线交互环境中或者展示空间受限的同步告知。
- 在非在线交互的环境中播放预录制音频或视频、提供纸质文件、提供访问地址等方式。

5.6.4.5送达方式适当性

特性要求：

同步告知应是以逐一送达至个人信息主体的方式提供的。具体而言：

a） 在移动应用程序、软件和移动智能终端等允许在线交互的环境中应是推送方式；

注：推送方式如弹窗、文本框、站内消息、预录音频或视频等。弹出或跳转至权限管理界面、隐私仪表盘、隐私菜单等交互界面，宜视为是推送方式。

b） 在非在线交互的环境中，可以是纸质文件、电子邮件、电话、短信、信件、警示牌、标准化图标、二维码、预录音频或视频等。

5.6.4.6免于同步告知的情形

特性要求：

a） 个人信息主体已经就相同的个人信息类型、处理目的、个人信息处理和所涉及的第三方获得至少一次同步告知，并且未发生需要重新获得同意的变化；

b） 个人信息处理者能够证明：

1） 可适用的法规定不需要向个人告知，

2） 可适用的法或有权机关要求保密，或者

3) 同步告知将导致特定合法性基础所追求的合法利益无法实现或严重受损。

c) 特定个人信息信息处理的合法性基础是紧急必要处理（5.2.2.7），并且个人信息处理者能够证明：

1) 在该具体场景中因情况紧急无法及时向个人信息主体进行同步告知；

2) 该无法及时告知的情况尚未消除。

d) 个人信息是间接获取的，并且个人信息处理者能够证明：

1) 提供同步告知不可能实现，或者

2) 相比于该特定个人信息处理对个人信息主体的影响而言，同步告知将要求不成比例的成本。

注：不可能实现既包括同步告知在客观上不可能实现，也包括如果要求提供同步告知将使个人信息所追求的合法利益无法实现；为了统计和研究目的处理个人信息，例如在个人信息处理者组织范围内进行并且在发布成果时已经进行适当去标识化处理的统计研究，公开信息公平处理（见5.2.2.6）通常涉及众多与个人信息处理者不具有直接联系的个人信息主体，这些情形宜推定为要求个人信息处理者提供同步告知很可能要求不成比例的成本；但如果间接获取的个人信息被用来与个人信息主体进行直接联系时，不宜再推定要求不成比例的成本。

5.7选择维度

5.7.1选择维度概述

选择维度关注的是：除可适用的法或所援引的合法性基础不允许个人信息主体行使选择的情形外，个人信息处理者是否通过易于理解和易于访问的机制，使个人信息主体能够行使有关其个人信息处理的决定权。

选择维度包含2个指标，即选择同意指标和选择退出指标。宜留意两个指标并不必然是二选一的，在选择同意指标中自由度特性在考虑个人信息主体是否拥有真实的选择自由时，可以将选择退出机制的存在作为考量因素之一，因此两个指标可以并用，此时选择退出机制也被称为撤回同意。在某些不以选择同意作为条件的合法性基础中，例如，公开信息公平处理（见5.2.2.6）、合法利益公平处理（见5.2.2.8），选择退出机制的存在则是必要条件，而选择同意指标则不是必要的。

5.7.2选择同意指标

5.7.2.1选择同意指标概述

选择同意指标关注的是：个人信息处理者是否在必要时以及适当且可行时获得有效的同意。

选择同意指标包含4个特性要求，涵盖同意的自由度、具体性、知情度、明确性等特性要求。

选择同意指标在收集、使用、存储、公开、提供、转移等环节，以及在向境外提供、共同处理、委托处理、第三方管理等特殊个人信息处理类别中均有扩展要求。这些扩展要求主要给出了获得同意的具体性（如是否应是单独同意）、明确性（如是否应是明示同意，以及如采用明示同意，是否应是书面同意）等方面的特殊要求。

评估要求：

评估员应：

——在评估对象征求同意的具体场景中确定个人信息主体给出的选择同意满足 4 个特性要求，即自由度、具体性、知情度和明确性。

其他信息：

参见《个人信息保护法》第5条（合法原则和正当原则，不得“胁迫”）、第14条、第15条、第16条、第22条、第23条、第25条、第26条、第27条、第29条、第31条、第39条和第44条（决定权）。

4个特性要求给出了对这些特性的具体解释和示例，评估员宜留意除非评估对象的可适用的法存在具体的强制性规范，单独符合或不符合其中某一个示例并不必然意味着评估对象构成违法或违规，但被发现的差距宜充分记录并提示给被评估方以供调整。评估员宜在充分考虑4个特性的前提下，综合评定这些差距是否会使得被评估方按照现状获得的同意被认定为无效。

当评估对象的范围和边界包含多个产品或服务等情形时，评估员可以采用抽样方式进行确定，但宜使法律合规性评估的所有相关方认识到抽样方法带来的局限性。如果可行，抽样应涵盖收集、目的转用、公开、提供、转移、向境外提供等关键环节。

5.7.2.2自由度

特性要求：

选择同意应是在个人信息主体有真实的选择和自由的基础上给出的。这意味着：

a) 在征求同意的具体场景中，不应存在强迫个人信息主体给出同意的设定；

b) 在征求同意的具体场景中，不应存在欺诈、误导、夸大不利影响的陈述或表示。

注1：是否存在强迫个人信息主体给出同意的设定需在具体场景中确定，通常宜考虑以下因素：

- 合同的签订、履行或者提供产品或服务基本业务功能，是否以个人信息主体对非最小必要的个人信息处理给出同意为条件；
- 是否将基本业务功能和扩展业务功能捆绑在一起征求同意，并且未对扩展业务功能提供拒绝同意的选项；
- 是否不适当地合并或捆绑多个处理目的一并征求同意；
- 是否不适当地合并或捆绑多个个人信息处理操作一并征求同意；
- 拒绝同意、关闭或退出特定业务功能后，是否除了使个人信息主体不再获得该特定业务功能之外，还受到其他不利影响，如暂停个人信息主体自主选择和保留的其他业务功能，降低其他业务功能的服务质量，在同意之前无法访问任何的公开信息或业务功能；
- 拒绝同意、关闭或退出特定业务功能后，是否频繁地征求个人信息主体的同意，以至于对其他被自主选择或保留的业务功能使用造成干扰；
- 是否仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意。

注2：欺诈、误导、夸大不利影响均需具体场景中存在具有虚假性的陈述或表示，并因此导致个人信息主体很可能基于错误认识、混淆或无意识前提下做出同意的动作。

5.7.2.3具体性

特性要求：

选择同意应足够具体。这意味着：

a) 应适当区分不同处理目的和不同处理环节，以就具体处理目的和处理环节逐步征求个人信息主体的同意。

b） 可适用的法要求获得单独同意的，所获得的同意应是针对特定处理目的、特定处理环节和/或特定个人信息类型等特定内容所作出的。

注1：单独同意是对同意的意思表示所针对的对象或内容的个别化要求。同意的意思表示应针对特定处理目的、特定处理环节和/或特定个人信息类型或其他特定内容作出，取决于可适用的法在规定单独同意时设定的条件。

示例：例如，可适用的法要求公开获得单独同意是针对公开这一特定处理环节而言，但由于可适用的法也要求在征求同意的场景中明示处理目的，因此单独同意应是针对“特定处理环节+具体处理目的”作出的。又如，可适用的法要求向境外提供获得单独同意也是针对向境外提供这一特定处理环节而言，但可适用的法也要求在征求同意的场景中向个人告知境外接受方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人想境外接收方行使权利的方式和程序等事项，因此单独同意应是针对“特定处理环节+特定境外接收方+具体处理目的+具体个人信息类型”作出的。再如，可适用的法要求处理敏感个人信息获得单独同意是针对特定敏感个人信息而言，同时可适用的法要求处理敏感个人信息应具有特定的目的，因此在此情形下的最低要求应是“特定敏感个人信息+特定处理目的”，但当所涉及的个人信息处理环节要求获得单独同意，需根据可适用的法所设定的条件增加“特定处理环节”“特定接收方”等条件。

注2：具体性特性要求宜在根据可适用的法和本文件确定合规准则的前提下，结合同步告知指标，在征求同意的具体场景中加以评估。

5.7.2.4知情度

特性要求：

选择同意应是在知情前提下给出的。这意味着：

a） 个人信息主体在被征求同意时能够获得同步告知；

b） 只要可行，在征求同意时应向个人信息主体提供：

1） 同步告知指标（见 5.6.4.2）所要求的最密切相关信息；

1） 有关其合法权益及其保障的信息；

2） 有关同意或拒绝同意的影响或后果的信息。

注：知情度特性要求宜在根据可适用的法和本文件确定合规准则的前提下，结合同步告知指标，在征求同意的具体场景中加以评估。

5.7.2.5明确性

特性要求：

选择同意应是明确的意思表示。这意味着：

a） 只要可行，征求同意的场景设计应要求或引导个人信息主体做出明示同意，包括：

1） 主动作出积极行为，如通过书面、口头等方式主动做出纸质或电子形式的声明。其中：

——可适用的法明确要求书面同意的，应获得个人信息主体以纸质或者电子形式签字以表示同意的文件。

2） 自主做出肯定性动作，如主动勾选、主动点击、主动填写或提供等积极行为。

b） 只要可行，应避免需要将消极行为推定为默示同意的场景设计；

c） 处理不满十四周岁未成年人的个人信息，应由未成年人的父母或者其他监护人作出上述明确的意思表示。

注1：默认勾选的对话框或默认开启的权限不应被视为是明确的意思表示。

注2：通常沉默只有在有法律规定、当事人约定或者符合当事人之间的交易习惯时，才可以被视为是意思表示。不宜将默示同意作为同意的一般原则或默认设定。

注3：明确性特性要求宜在根据可适用的法和本文件确定合规准则的前提下，在征求同意的具体场景中加以评估。

5.7.3选择退出指标

5.7.3.1选择退出指标概述

选择退出指标关注的是：除可适用的法不允许个人信息主体行使选择的情形外，个人信息处理者是否为个人信息主体提供有效的选择退出机制，即通过便捷的机制受理和及时响应个人信息主体以积极行为做出的希望不再进行特定个人信息处理的意思表示，从而保障个人信息主体的决定权。选择退出指标包含3个特性要求，涵盖选择退出的便捷性、自由度和及时响应性等特性要求。

选择退出指标在存储、公开、提供、转移、向境外提供等环节/类别均有扩展要求。这些扩展要求主要给出了在具体环节或特殊类别中选择退出机制的具体表现形式以及执行选择退出的具体要求。这些扩展要求主要是对便捷性和及时响应性特性的扩展。

评估要求：

评估员应：

——在评估对象选择退出的具体场景中确定选择退出机制满足 3 个特性要求，即便捷性、自由度和及时回应性。

其他信息：

参见《个人信息保护法》第15条、第44条和第47条。

5.7.3.2便捷性

特性要求：

选择退出机制应具有便捷性。这意味着：

a) 选择退出机制应与选择同意一样易于理解；

b) 选择退出机制应与选择同意一样易于访问；

c) 个人信息处理的合法性基础为的选择同意处理的，应提供撤回同意形式的选择退出机制。

注1：选择退出的具体表现形式可以是撤回同意、关闭或退出特定业务功能、注销账户、向指定途径发送停止个人信息处理的请求等，以积极行为做出的希望不再进行特定个人信息处理的意思表示。

注2：选择退出与选择同意宜具有合理可比性，例如，在同时存在选择同意与选择退出机制（如撤回同意）的场景下，选择同意为即刻执行，选择退出的执行机制为人工处理时，通常需要合理的理由。

注3：权限的含义得到清楚易理解的表示、权限得到适当设置、个人信息主体可以自主选择开启或关闭权限且指令自动得到执行的交互式隐私面板，可能同时符合选择同意和选择退出指标。

5.7.3.3自由度

特性要求：

选择退出机制应具有自由度。这意味着：

a) 选择退出机制不应设置不合理条件或其他障碍，增加选择退出的难度或阻碍个人信息主体自由的选择退出；

b) 选择退出机制应验证个人信息主体的身份，验证所要求提交的身份鉴别信息应以实现身份验证目的的最小必要为限。

c) 在选择退出的具体场景中，不应存在欺诈、误导、夸大不利影响的陈述或表示。

注1：选择退出的自由度特性可以参考选择同意的自由度特性要求。通常可能被视为不具有自由度的选择退出机制，如将多个不具有必要关联的产品或服务绑定在一起，一旦选择退出其中一个产品或服务将导致其他不具有必要关联的产品或服务无法使用、服务质量明显下降或受到其他不利影响，或者在选择退出的场景中存在欺诈、误导、夸大不利影响的陈述或表示。

注2：在撤回同意或注销账户的场景下，如果多个产品或服务之间存在必要关联，例如，一旦注销某个产品或服务的账户或者停止某项个人信息处理，将导致其他产品或服务的基本业务功能无法实现或者服务质量明显下降的，宜具体和客观地向个人信息主体进行说明。

5.7.3.4及时响应性

特性要求：

选择退出的机制应具有及时响应性。这意味着：

a) 应建立相应程序确保在以下时限内及时响应或执行个人信息主体的选择退出：

——个人信息处理者承诺的时限；

——可适用的法规定的时限；

——经协商，个人信息主体同意延长的时限。

注：个人信息处理者承诺的时限应不晚于可适用的法规定的时限，但同时需考虑选择退出与选择同意的合理可比较性。例如，在同时存在选择同意与选择退出机制（如撤回同意）的场景下，选择同意为即刻执行，选择退出的执行机制为人工处理时，通常需要合理的理由。如人工处理选择退出的请求，宜在合理期限内得到响应和执行。

b) 个人信息主体通过身份验证的，只要可适用的法没有限制个人信息主体行使选择，应执行选择退出的请求；

c) 个人信息处理者无法执行或决定不执行个人信息主体的请求的，应向个人信息主体告知理由，并提供投诉的途径；

d) 收到选择退出的请求或指令后至执行选择退出请求前，除为了执行选择退出所必要的处理、在人工处理选择退出请求期间按照原定个人信息处理过程不可避免地自动执行和履行法定义务外，不应再对选择退出的个人信息进行继续处理或额外处理；

e) 执行选择退出的请求或指令后，应停止对该个人信息主体进行被选择退出的个人信息处理；

f) 对于在执行选择退出的请求或指令前已经处理的个人信息：

1) 应及时进行删除或匿名化；

2) 可适用的法规定的存储期限尚未届满或者删除在技术上难以实现的，应停止除存储和采取必要的安全保护措施（如匿名化）之外的处理。

注：个人信息主体的选择退出（如撤回同意），可能伴随删除机制下的删除请求（见5.8.6），或可能导致个人信息处理者终止对这些个人信息的处理（见7.3）。在必要且适当时，个人信息处理者需同时考虑选择退出与其他合规要求之间的衔接。

5.8权益保障维度

5.8.1权益保障维度概述

权益保障维度也是体现个人信息主体参与的一个维度，关注的是：个人信息处理者是否向个人信息主体提供能够询问、参与和沟通有关个人信息处理的政策与实践的有效机制，并确保这些机制能够在适当和必要时对个人信息主体的请求进行适时回应。这些机制包括保障个人信息主体行使其查询、获取副本和转移、更正、删除等合法权益的机制，以及接收一般性的询问、投诉和举报的渠道。

权益保障维度包含6个指标，其中第1个指标是通用指标，描述了有效的权益保障机制应具备的特性。随后的4个指标是适用于查询、获取副本和转移、更正、删除等个人信息合法权益行使机制的指标要求，尤其是关于响应和执行条件的要求，这些个人信息合法权益行使机制通常是合规义务的一部分。第6个指标是关于一般性的投诉举报问询机制的指标要求。

评估要求：

评估员应：

——验证 5 种合法权益保障机制的存在和满足通用指标的要求；

——验证 5 种机制在法律合规性评估期内是否得到响应；

——确认这些机制的提供方式，如自动化或人工，以及响应程度。

5.8.2合法权益行使机制通用指标

指标要求：

a) 个人信息处理者提供的行使其合法权益的机制：

1) 应易于理解、易于访问和有效响应；

注：采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其合法权益。

2) 应建立相应程序确保在以下时限内及时响应或执行个人信息主体提出的请求：

——个人信息处理者承诺的时限；

——可适用的法规定的时限；

——经协商，个人信息主体同意延长的时限。

注：个人信息处理者承诺的时限应不晚于可适用的法规定的时限，不宜超过15个工作日。在难以在承诺时限或可适用的法规定的时限内及时响应时，可经协商后延长时限。

3) 不应收取费用，但对一定期间内多次重复的请求，可视情况收取一定成本费用；

4) 应建立相应程序验证个人信息主体的身份，所要求的个人信息不应超过注册和使用环节收集的个人信息；

注：为响应或执行个人信息主体行使合法权益的请求而采取的身份验证所需信息，宜以实现身份验证目的最小必要信息为限。

5) 应公布已经死亡的个人信息主体的近亲属等，依法或依死者生前安排对该个人信息主体的个人信息行使查询、获取副本、更正、删除等权利的条件、规则和程序。

6) 应避免设置不必要或不合理的程序，以阻碍个人信息主体合法权益的行使。

b) 对于个人信息主体提出的查询、获取副本和转移、更正、删除等请求，存在以下情形时可以不执行请求：

1) 个人信息处理者进行个人信息处理的合法性基础属于法定义务必要处理（见5.2.2.3）或公共利益必要处理（见 5.2.2.5），并且依据该合法性基础的性质，个人信息处理者不能执行个人信息主体的具体请求，或执行个人信息主体的具体请求将导致难以实现该合法性基础所追求的目标；
2) 执行个人信息主体的请求将导致个人信息处理者违反可适用的法施加的义务，或将导致个人信息处理者承担法律责任；
3) 执行个人信息主体的请求将导致泄露个人信息处理者的商业秘密；
4) 执行个人信息主体的请求将直接导致其他个人或组织的合法权益受到损害；
5) 个人信息处理者有充分证据表明个人信息主体存在主观恶意或滥用权利。

c) 个人信息处理者决定不执行个人信息主体的请求的，应向个人信息主体告知该决定的理由，并提供投诉的途径；

d) 直接执行个人信息主体的请求需要个人信息处理者付出高额成本或存在其他显著困难的，个人信息处理者应向个人信息主体提供替代方法以保障个人信息主体的合法权益。

5.8.3查询机制指标

指标要求：

a) 个人信息处理者应向个人信息主体提供查询其个人信息的方法；

b) 除非具有以下情形之一，个人信息处理者应向个人信息主体反馈查询结果：
1) 向个人信息主体反馈查询结果将导致个人信息处理者违反可适用的法施加的义务（包括保密义务），或将导致个人信息处理者承担法律责任；
2) 个人信息处理的合法性基础为法定义务必要处理，且向个人信息主体反馈查询结果将妨碍国家机关履行法定职责；
3) 可适用的法规定不需要告知。

c) 个人信息主体请求查询其个人信息并通过身份验证的，向个人信息主体提供的查询结果应包含以下信息：
1) 其所持有的关于该个人信息主体的个人信息或个人信息的类型；
2) 上述个人信息的来源、处理目的和合法性基础；
3) 已经获得上述个人信息的第三方身份或类型。

d) 个人信息主体请求查询非其主动提供的个人信息时，个人信息处理者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，做出是否响应的决定。

注：通过用户信息管理、隐私管理或授权管理等交互界面提供自主查询时，在交互界面已经提供查询的范围内不必人工响应个人信息主体的查询请求，宜通过个人信息保护政策、查询界面自动回复等方式告知查询方法。

其他信息：

参见《个人信息保护法》第45条第1款和第2款。

5.8.4获取副本和转移机制指标

指标要求：

根据个人信息主体的请求，个人信息处理者应为个人信息主体提供获取个人信息副本的方法，或在符合可适用的法规定条件的前提下直接将个人信息转移至个人信息主体指定的第三方。

其他信息：

参见《个人信息保护法》第45条。

5.8.5更正机制指标

指标要求：

a) 个人信息处理者应向个人信息主体提供更正其个人信息的方法；

b) 个人信息主体通过身份验证，并且符合以下条件时，应执行更正请求：

1) 个人信息主体能够合理地证明个人信息确有错误；

2) 个人信息主体合理地主张个人信息不完整；

3) 个人信息主体的更正请求符合可适用的法规定的其他条件，包括但不限于：

——个人信息处理者有侵犯个人信息主体合法权益的其他行为；

——个人信息处理者根据可适用的法有义务采取更正措施的。

示例1：如《民法典》第 1028 条规定了民事主体有证据证明报刊、网络等媒体报道的内容失实，侵害其名誉权的，有权请求该媒体及时采取更正、删除等必要措施。

示例2：如《民法典》第 1029 条规定了民事主体发现信用评价不当的，有权提出异议并请求采取更正、删除等必要措施。信用评价人应当及时核查，经核查属实的，应当及时采取必要措施。

c) 个人信息处理者已经向个人信息共同处理者、个人信息处理受托人或其他第三方提供个人信息的，应在执行更正请求时向上述各方发送更正通知，或在与个人信息共同处理者或个人信息处理受托人共同使用的数据库中进行一并更正。但以下情形除外：

1) 个人信息主体明示豁免的；

2) 个人信息处理者在综合考虑不发送更正通知或一并更正可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现成本等因素后，决定不发送更正通知或一并更正的，应向个人信息主体给出解释说明和已经通过个人信息处理者获得上述个人信息的第三方身份和联系方式。

其他信息：

参见《个人信息保护法》第45条。

5.8.6删除机制指标

指标要求：

a) 个人信息处理者应向个人信息主体提供删除其个人信息的方法；

b) 符合以下条件时，个人信息处理者应执行删除请求：

1) 个人信息处理违反可适用的法；

2) 个人信息处理违反个人信息主体与个人信息处理者之间的约定；

示例：如违反最小必要指标（见 5.4.2）、目的兼容指标（见 5.4.3）。

3) 个人信息处理目的已经实现或者无法实现；

4) 就个人信息处理者明示的处理目的而言，该个人信息已不再必要；
5) 个人信息处理者停止提供产品或者服务；
6) 个人信息的存储期限已经届满；
7) 个人信息主体已经注销账户或撤回同意；
8) 个人信息主体的删除请求符合可适用的法规定的其他条件，包括但不限于：
——个人信息处理者有侵犯个人信息主体合法权益的其他行为；
——个人信息处理者根据可适用的法有义务采取删除措施的。

示例1：如《民法典》第 1195 条规定，网络用户利用网络服务实施侵权行为的，权利人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。通知应当包括构成侵权的初步证据及权利人的真实身份信息。

示例2：见 5.8.5 b) 3)的示例 1 和示例 2。

c) 个人信息处理者已经向个人信息共同处理者、个人信息处理受托人或其他第三方提供个人信息的，应在执行更正请求时向上述第三方发送删除通知，或在与个人信息处理者或个人信息处理受托人共同使用的数据库中进行一并删除。但以下情形除外：
1) 个人信息主体明示豁免的；
2) 个人信息处理者在综合考虑不发送删除通知或一并删除可能对个人信息主体合法权益带来的风险和损害，以及技术和业务可行性、实现成本等因素后，决定不发送删除通知或一并删除的，应向个人信息主体给出解释说明和已经通过个人信息处理者获得上述个人信息的第三方身份和联系方式。

其他信息：
参见《个人信息保护法》第47条。

5.8.7投诉举报问询机制指标

指标要求：
a) 个人信息处理者应建立并公布：
1) 个人信息投诉举报渠道，以便通过个人信息主体的参与及时发现其个人信息处理中的个人信息安全事件、违法或违规等事项并采取必要措施和改进；
2) 个人信息处理规则问询渠道，以便受理个人信息主体对其个人信息处理规则的问询并及时对其个人信息处理规则进行解释说明。
b) 个人信息处理者应建立处理投诉、举报、问询的程序，例如在组织内分配处理人员、职责、流程与时限等，以确保投诉、举报、问询能够得到及时的处理，并在可行时能够适当地与个人信息主体沟通或反馈处理过程或结果。

其他信息：
参见《个人信息保护法》第 48 条。

5.9质量维度

5.9.1质量维度/指标

质量维度仅包含一个同名指标。在个人信息保护语境下，质量维度/指标关注的是：个人信息处理者是否采取适当的技术、管理或必要措施，确保所处理的个人信息就其处理目的

而言足够准确、完整和必要时保持最新，从而降低因个人信息不够准确、完整或及时给个人信息主体合法权益带来负面影响。

指标要求：

a） 应在个人信息处理过程中采取适当的技术和管理措施，以确保所处理的个人信息就其处理目的而言是准确、完整的，并在必要时保持最新；

注1：处理目的中包含可能直接对个人信息主体的合法利益带来显著影响的个人信息处理，例如，全部或部分自动化决策、用户画像，宜在规划设计阶段或首次投入使用前，评估处理目的对数据质量的需求并采取相适应的质量控制措施。事前开展的个人信息保护影响评估以及根据评估结果采取适当的控制措施，可视为此类处理目的的一项必要措施。允许对自动化决策的结果进行人工复核，通过 5.8.5 的更正机制或一般性的投诉举报机制接受个人信息主体对决策结果的质疑，也可以视为一项必要措施。

注2：在其他处理目的中，允许个人信息主体对自动采集的个人信息进行确认、复核或修改，在组织中明确指定人员定期检查或维护信息质量等，均可以是必要措施之一。

b） 应在持续的管理过程中定期检查和维护信息质量，及时删除或更正不准确、不完整或失去时效性的信息。

评估要求：

评估员应：

——确认必要措施、定期检查维护的存在及其类型，综合评审以确定这些措施对于确保就处理目的而言的准确、完整和及时性具有充分性。

其他信息：

参见《个人信息保护法》第8条。

对于质量维度/指标尚不存在统一标准，对于个人信息处理而言，质量维度/指标并非对质量结果的保证。评估对象与质量维度/指标存在差距的，评估员宜在评估法律意见书中指出这些差距。

5.10安全保护维度

5.10.1安全保护维度概述

安全保护维度关注的是：组织的个人信息处理是否采取适当的技术、管理或其他必要措施，以确保对个人信息完整性、保密性和可用性的适当水平的保护，防止违法的个人信息处理以及未经授权的和意外的篡改、毁损、丢失、访问、泄露。

安全保护维度包含3个指标，即安全保护能力指标、事件管理指标和数据最小化指标。

评估员宜留意，安全保护维度并非旨在建立不同于现有网络安全和信息安全标准的安全要求，安全保护维度的法律合规性评估目的在于确认组织的网络安全和信息安全保护措施被适当地运用到个人信息处理当中，并考虑到个人信息处理的特殊需求进行了适当的调整和适应。

5.10.2安全保护能力指标

指标要求：

a) 个人信息处理信息系统应满足其信息安全保护等级所对应的管理规范和技术标准要求；

b) 应在个人信息处理的各环节中采用适当的技术、管理或其他必要措施，以确保个人信息保密性、完整性和可用性。这些技术、管理或其他必要措施应与个人信息处理中的安全风险相匹配。其中：

1) 在传输环节应采取以下安全控制措施：

——安全控制措施可包括采用安全传输通道、数据加密等措施；

——通过公共网络传输敏感个人信息，应采用加密通道或数据加密；

——在传输或接受传输前，应对通信双方进行身份鉴别和认证；

——应采用校验技术或密码技术确保在传输过程中的完整性，传输的接收方在接收个人信息后，应进行完整性校验；

——采用程序编程接口传输个人信息时，应采取措施防止未经授权的应用程序编程接口访问和使用。

注：传输通常是其他个人信息处理环节（如收集、使用、公开、提供、转移等）附带的一项个人信息处理操作。从法律合规性评估的角度而言，对传输环节的关注要点仅在于安全保护。

c) 应通过持续的信息安全风险管理，定期评审和重新评估所采取的技术、管理或其他必要措施的有效性，并解决已被识别的安全缺陷、漏洞、网络侵入、病毒等风险和脆弱性。

评估要求：

评估员应：

——确认评估对象范围和边界内的个人信息处理信息系统已经完成等级保护测评工作；

——确认在各环节中所采用的技术、管理或其他必要措施的内容，及其是否与该特定环节中的安全风险相匹配。

其他信息：

参见《个人信息保护法》第9条、第51条和第59条。

信息安全管理体系评审或等级保护测评的结果，对于法律合规性评估的目的而言都是可接受的客观证据，只要能够适当确认这些评审或测评的范围已经涵盖评估对象范围和边界中的个人信息处理设施或信息系统。在接受这些已经存在的评审或测评结果时，评估员宜留意评估对象范围和边界的重合性，以及已经进行的评审或测评的时效性，宜充分听取技术专家的意见以及被评估方的解释。如果评审或测评的范围没有完全覆盖到评估范围内的个人信息处理活动，这些被遗漏的部分需要技术专家重新进行信息安全风险评估。

5.10.3事件管理指标

指标要求：

a) 信息安全事件应急预案中所界定的信息安全事件范围应能够涵盖个人信息安全事件（见 T/CLAST 002.1—2021，定义 3.6.9），应急预案内容应有明确的处置流程和岗位职责，该处置流程和岗位职责应能够确保在发生个人信息安全事件后，合规团队可以及时获知并有机会就事件对个人信息主体的影响、处置和事件告知给出建议；

b) 应定期组织内部相关人员开展应急预案相关培训和应急演练；

c) 在发生个人信息安全事件后，应根据应急响应预案采取包括但不限于以下处置措施：

1) 记录事件内容，包括但不限于发生事件的时间、地点和人员，所涉及的个人信息及人数，发生事件的信息系统名称，对其他互联系统的影响，以及是否联系相关执法或监管部门；
2) 评估事件可能造成的影响，应包括对个人信息主体的影响，如是否会导致或已经导致身份盗用、电信欺诈等，并采取必要措施控制事态和消除隐患；
3) 根据可适用的法的有关规定及时报告，报告事项包括但不限于个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，以及已经采取的或即将采取的处置措施，事件处置相关人员联系方式；
4) 经合规团队评估认为必要时，应进行事件告知。

评估要求：

评估员应：

——评审信息安全事件应急预案，以确认应急预案适当地涵盖个人信息安全事件；

——评审培训记录和演练记录等，以验证存在定期培训和演练；

——评审事件记录，以确认是否满足处置措施的要求。

其他信息：

参见《个人信息保护法》第51条第5项、第57条，以及其他标准，如GB/T 35273—2020，10.1。

5.10.4数据最小化指标

5.10.4.1数据最小化指标概述

数据最小化指标与目的明确维度（见5.3）和目的限制维度（见5.4）都密切相关，但更进一步地关注组织是否通过产品、服务的流程和信息系统的设计或默认设置，将个人信息处理所涉及的数据最小化，从而降低对个人信息安全性的风险和影响。

数据最小化指标包含2个特性要求，即最小化技术和最小化访问控制。

5.10.4.2数据最小化技术

特性要求：

a) 应适当采用有助于数据最小化的技术，如匿名化、去标识化等，以确保以可识别个人信息主体的形式进行的个人信息处理被最小化；
b) 宜制定相关安全策略和数据分类分级标识管理制度，并根据相关安全策略和数据分类分级标识管理制度，对个人信息进行匿名化、去标识化处理。

评估要求：

评估员应：

——评审评估对象的匿名化、去标识化等规程，以确定被评估方是否要求对评估对象中的个人信息处理采用匿名化、去标识化等技术；

——确定评估对象所采用的匿名化、去标识化的方法及其所涉及的个人信息处理环节；

——确认被评估方所采用的匿名化、去标识化等技术是否与其处理的个人信息类型、个

人信息处理环节的风险程度相匹配，从而具有适当性；

——通过抽样方法检测匿名化、去标识化在评估对象中按照规程得到实施。

其他信息：

参见《个人信息保护法》第51条。

常见的去标识化技术及其优缺点，见GB/T 37964—2019。

关于匿名化、去标识化等最小化技术适当性的确定，宜充分听取技术专家的建议。此外，评估对象的流程与规程中存在定期评审重标识风险的要求等持续型的风险管理机制，可以作为确定最小化技术适当性的积极考量因素。

5.10.4.3访问最小化控制

特性要求：

a) 个人信息处理过程应采取适当的访问权限控制措施，最小化被赋予个人信息访问权限的人员和相关方数量；

b) 拥有访问权限的人员和相关方被赋予的权限，应仅为履行其被赋予的职责或者履行合同约定的处理目的所必要的最小权限。

评估要求：

评估员应：

——评审评估对象的访问权限控制规程，以确定被评估方是否对评估对象中的个人信息处理采用访问权限控制；

——评审访问权限控制策略是否符合访问权限最小化访问的目标，以及是否与被评估方确定的个人信息分类分级相适应；

——确认访问权限控制策略是否得到定期的评审，批量修改、下载、复制、对外提供等敏感权限是否得到特别控制；

——通过抽样方法检测访问权限控制策略在评估对象中按照规程得到的实施，是否存在未被清理的冗余权限，被赋予的访问权限明显超出职责所必要的最小权限等情况。

其他信息：

参见《个人信息保护法》第51条。

关于访问权限控制措施的适当性的确定，宜充分听取技术专家的建议。此外，当评估对象已经完成信息安全管理体系审核、等级保护测评时，在能确定这些审核或测评范围已经覆盖到评估对象、在法律合规性评估期内得到执行的前提下，评估员可以根据技术专家的建议考虑避免全部或部分重复性的确定活动，但宜考虑这些控制措施在个人信息处理具体场景中的适当性，尤其是个人信息访问权限的控制水平通常宜不低于组织界定的重要数据的访问权限控制水平。在个人信息处理具体场景中的访问控制措施要求，见GB/T 35273—2020,7.1。

5.11可问责性维度

5.11.1可问责性维度概述

可问责性维度关注的是：个人信息处理者是否以负责任的方式进行个人信息处理并能够证明其尽责程度。可问责性是个人信息处理者的态度、行动与能力的综合体现，包括：是否明确界定并履行与其所享有的权利（或权限）相一致的个人信息保护的义务与责任；是否通

过适当的文件和日志记录等管理措施，确保个人信息处理者有能力证明其个人信息处理的合规性；以及在进行个人信息处理的过程中尽职、审慎地评估和管理风险，并通过持续的改进来完善其合规体系。

可问责性维度包含5个指标，包括合规管理体系指标、权责一致指标、文件管理指标、合规审计指标和影响评估指标。

5.11.2合规管理体系指标

5.11.2.1合规管理体系指标概述

合规管理体系指标的关注点在于：合规是否作为组织的一项目标被嵌入到有关个人信息处理和信息安全的管理体系当中。

合规管理体系指标包含了3个特性要求，包括管理架构、方针与制度、意识与培训。

合规管理体系指标并不要求组织在现有的个人信息保护机构或信息安全管理体系之外建立全新的架构和体系，与个人信息处理合规相关的这些特性要求完全可以通过改进现有体系来实现。对于法律合规性评估而言，重要的是评估组织内与个人信息处理有关的管理体系是否有能力保障组织持续地实现和改进个人信息处理的合规状态与目标。如果在法律合规性评估中发现被评估方现有的个人信息处理的管理未充分关注和体现合规目标，宜在评估法律意见书中予以提示由法律合规性评估的委托方予以考虑。

其他信息：

参见《个人信息保护法》第 51 条、第 52 条、第 58 条。

5.11.2.2管理架构

特性要求：

个人信息处理者应建立旨在促进个人信息处理合规的管理架构，并具备以下要素：

a) 合规管理机构及其职责：在组织的最高管理层中指定一名或多名人员组成个人信息处理合规管理机构，领导组织个人信息处理活动的合规管理工作。该合规管理机构的职责中应至少包含以下事项：
   1) 批准建立并持续监督旨在保障其个人信息处理合规的管理体系；
   2) 任命或提名对个人信息处理合规负有职责的团队，并为合规团队提供充分的人力、财力、物理资源与工作支持；
   3) 及时审议合规团队的意见和建议，并对个人信息处理中的不合规实践进行制止和采取必要的纠正措施；
   4) 通过明确的承诺和持续的管理过程支持在组织内建立旨在保障组织个人信息处理合规的制度与文化，并鼓励员工遵守这些合规制度与文化；
   5) 支持合规团队将合规绩效纳入组织的现有业务实践和程序，以及将合规绩效纳入个人信息处理相关部门与人员的绩效考核范围。
b) 识别相关部门与人员：该管理架构应明确识别组织内与个人信息处理合规工作密切相关的部门与人员，包括法务、信息安全、开发与销售等，并确保合规管理机构被赋予充分的职责与权限协调组织内个人信息处理合规工作相关部门与相关人员；
c) 合规团队及其职责：应组建或明确指定对个人信息处理的合规工作负有职责的团队及其负责人，其职责至少涵盖：
   1) 协助合规管理机构制定并统筹实施旨在保障其个人信息处理合规的管理体系；

2) 负责建立、维护、定期评审和更新组织在个人信息处理方面的合规义务与合规要求清单，定期对组织个人信息处理的合规绩效进行评估或审计；
3) 通过制定、组织实施、定期评审和更新个人信息保护政策、相关规章制度与操作规程，将所识别的合规义务与合规要求转化为组织内可执行的制度、程序和过程；
4) 为员工提供或组织实施个人信息处理合规方面的培训；
5) 通过组织内的咨询热线、举报系统或其他适当机制，为组织内的相关人员提供个人信息处理合规相关的资料、规章制度和意见，调查处理被举报或被识别的个人信息处理不合规实践；
6) 识别来自组织内的和个人信息相关方的合规风险，并及时向相关人员进行警示，在必要时向合规管理机构报告并建议采取制止或纠正措施。

d) 应通过组织流程确保合规团队及其负责人在以下有关个人信息处理的重要事项前能够获得报告，并有机会就这些重要事项的决策提供有关合规方面的意见与建议：
1) 组织内涉及个人信息处理的新产品、服务的上线，以及新的个人信息处理过程的上线，如个人信息的提供、转移、委托处理、跨境转移、公开等；
2) 现有产品与服务中涉及个人信息处理的重大决策及其重大变更，如个人信息处理者、个人信息处理受托人、处理目的、方式（如对象、手段与来源）与范围、信息安全能力和信息安全控制措施；
3) 个人信息保护影响评估的开展、过程及其结果；
4) 个人信息安全事件与违规的处置。

e) 应建立合规团队与组织内个人信息处理合规的其他相关部门之间的信息通报与沟通流程，例如，通过组织流程确保在个人信息处理事项上，合规团队能够获得同步或定期的信息通报，并且在合规工作需要时有权限接触完整的信息；

注：组织可以将合规团队的职责与权限分配给组织内的现有部门和人员兼任，但需确保承担组织合规团队职责与权限的部门和人员在履行其职责方面具有充分的专业性和独立性，以避免潜在的利益冲突影响组织合规管理体系的有效性，合规管理机构宜为合规团队提供充分支持。

f) 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应存在主要由外部成员组成的独立机构对个人信息保护情况进行监督。

评估要求：

评估员应：

——评审组织内存在明确的个人信息处理的管理架构，确认在这一管理架构中指定和分配了合规相关的角色与职责、建立了适当的组织流程，这些流程在组织运行中得到遵守。

5.11.2.3方针与制度

特性要求：

个人信息处理者的组织应建立旨在促进个人信息处理合规的管理方针和制度体系，并具备以下要素：

a) 组织内应有明确表达的持续改善个人信息处理合规状态与能力的目标和管理层承诺；
b) 组织内应具备个人信息处理的制度体系，这些管理制度体系应适应组织的合规目标，并至少涵盖以下主题：

1) 个人信息处理合规的原则与目标（或称为方针）；
2) 个人信息处理合规管理架构、人员及其职责、权限等；
3) 旨在促进和实现个人信息处理合规的规章制度、操作规程和配套的报告记录模板，至少应涵盖以下主题：
——个人信息分级分类；
——个人信息处理合法/合规管理；
——个人信息保密管理；
——访问控制、密码管理；
——备份与恢复；
——物理环境安全；
——安全存储和存储介质管理；
——安全传输、通信安全、网络使用；
——安全投诉与举报管理；
——个人信息合法权益行使请求的处理；
——个人信息安全事件管理与预案；
——匿名化、去标识化等技术措施。

c) 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，其个人信息处理合规制度体系还应满足可适用的法的要求（如有），例如，关于规范平台内产品或服务提供者的个人信息处理活动及其合规性的制度或平台规则。

5.11.2.4意识与培训

特性要求：

a) 个人信息处理者的合规管理机构、合规团队和合规工作相关的部门及其相关人员，均应具备适当的个人信息处理合规意识与能力。组织应确保定期向所有相关部门及其相关人员提供合规意识和知识培训，并将合规意识、知识、技能与行为纳入这些相关部门与人员的绩效考核当中；

注：合规意识与能力可以通过教育、培训或工作经历等方式获得和证明。

b) 对于组织内的其他员工，组织应确保在其任职时以及在任职期间，通过培训、会议和员工守则等被适时和充分地强调和告知在工作中遵守组织的个人信息处理合规制度和文化的重要性，尤其是对用户个人信息的严格保密与安全保护。

评估要求：

评估员应评审相关的部门与人员的人事资料、培训记录、考核表、员工手册等记录，以及采取抽样访谈等形式，确认与个人信息处理合规工作相关的部门、岗位人员具备相应的合规意识和能力。

5.11.3权责一致指标

5.11.3.1权责一致指标概述

权责一致指标的关注点在于：个人信息处理者是否根据其个人信息处理的规模、业务类型和对社会的重要性，适当履行与其权利与权力相适应的责任。

权责一致指标包含了3个特性要求，包括共同处理、委托处理、平台/第三方管理。

通常而言，在没有采取共同处理、委托处理、平台/第三方接入等方式时，个人信息处理者满足可问责性维度的其他指标即可视为尽到了与其权利与权力相适应的责任。当个人信息处理者采取共同处理、委托处理、平台/第三方接入等方式时，除其他指标外，个人信息处理者还应满足共同处理指标、委托处理指标和平台/第三方管理指标的要求。

5.11.3.2共同处理

特性要求：

当存在个人信息共同处理者时：

a) 个人信息共同处理者之间应通过合同等成文信息形式确定个人信息处理的目的、方式和合法性基础，共同确定个人信息处理应满足的合规要求，以及各自在合规方面承担的义务和责任；

b) 应分别或者由至少一个个人信息共同处理者通过个人信息保护政策等方式向个人信息主体明确告知个人信息共同处理者的存在、身份、各自的义务和责任，尤其是个人信息主体行使合法权益的方式。

评估要求：

评估员应：

——评审个人信息共同处理者之间的合同，以确认个人信息共同处理者之间通过合同等成文信息形式确定了合规要求、各自的义务和责任；

——评审个人信息保护政策，确认已进行明确告知。

5.11.3.3委托处理

特性要求：

个人信息处理者应：

a) 在委托处理前进行个人信息保护影响评估，确保个人信息处理受托人具备就委托的个人信息处理而言充分的数据安全能力，能够提供充分的安全保护水平；

b) 与个人信息处理受托人签订委托协议，明确规定双方的责任与义务。委托协议应能够涵盖以下事项：

   1) 明确约定委托处理的范围，包括委托处理的个人信息的类型。委托处理范围不应超出个人信息处理者有权进行的个人信息处理范围；
   2) 明确规定委托的个人信息处理目的以及遵守该处理目的的要求；
   3) 委托处理的方式以及期限，以及提前终止委托或委托期限届满时个人信息的处理方式，如返还或删除等；
   4) 个人信息处理者的控制和监督权利与方式，应能够确保个人信息处理者有权对委托的个人信息处理进行审计和定期评估委托处理的风险；
   5) 转委托时事先征求委托方同意的要求，以及对儿童个人信息的转委托进行限制；
   6) 明确要求受托人按照法律、行政法规的规定和个人信息处理者的要求处理个人信息，协助个人信息处理者履行其合规义务；
   7) 约定在个人信息处理者要求时协助个人信息处理者响应个人信息主体请求的约定；
   8) 约定采取措施保障信息安全的义务和具体要求；

9) 约定发生个人信息安全事件时及时向个人信息处理者报告的义务；

c) 向受托人明示委托的处理目的、合法性基础及其要求以及个人信息控制者的合规义务清单，以明确合规要求，避免因受托人的行为导致个人信息处理者违反其自身的合规义务；

d) 在委托处理的过程中定期对委托的个人信息处理进行审计，定期评估委托处理的风险与合规性；

e) 在发现个人信息处理受托人未按照委托协议的约定处理个人信息，或可能导致个人信息处理者违反合规义务的情形，采取必要措施予以制止、要求纠正或采取补救措施；

f) 在委托处理终止时，确保个人信息处理者及时返还或删除从个人信息处理者处获得的个人信息；

g) 保留一份完整和最新的个人信息处理受托人清单，包含个人信息处理受托人的身份和委托事项，并确保个人信息保护政策中公开的信息保持最新。

评估要求：

评估员应：

——评审个人信息保护影响评估报告和委托协议，以确认被评估方在委托处理前进行了审慎的影响评估，并且其委托协议已经对影响其自身合规状态或能力的重要事项进行约定，从而使被评估方在发现不合规时有能力进行制止和干预；

——确认影响个人信息处理者自身合规的重要事项，如处理目的、方式、合法性基础、合规义务等已向个人信息处理受托人明示；

——确认在委托处理的过程中个人信息处理者存在定期的审计和评估活动，并及时制止可能使其自身不合规的违约或其他违规行为；

——（如适用）确认个人信息处理者在委托处理终止时要求返还或删除；

——确认个人信息处理者清单与个人信息保护政策的一致性。

5.11.3.4平台/第三方管理

特性要求：

个人信息处理者提供重要互联网平台服务，应制定公开、公平、公正的平台规则，以及产品、服务、插件接入机制和工作流程。该规则、机制和工作流程应能够确保：

a) 在提供重要互联网平台服务或接入产品、服务、插件之前进行影响评估，并采取适当的控制措施；

b) 在必要时要求接入的平台的产品、服务、插件提供者进行事前合规检测、评估、审计，或影响评估；

c) 通过用户协议和平台规则或者其他合同等形式，明确各自的合规义务与责任边界；

d) 明确平台内产品、服务、插件提供者的个人信息处理合规要求，例如，向个人信息主体进行政策告知、同步告知和获得选择同意等要求，并定期进行合规检测、评估或审计；

e) 明确自身向个人信息主体公开平台内产品、服务、插件提供者身份或类型，以及各自的安全义务与责任的规程；

f) 发现平台内的产品、服务或插件提供者违反用户协议、平台规则、合同约定或存在其他个人信息处理违规行为，或者多次收到个人信息主体的投诉表明其存在违规行为的，立即要求该平台内产品、服务、插件提供者停止相关行为，自行采取或要求

平台内产品、服务、插件提供者采取有效补救措施（如更改口令、回收权限、断开网络连接等）；

g) 对严重违反可适用的法进行个人信息处理的平台内产品、服务、插件提供者，在必要时停止向该平台内产品、服务、插件提供者提供服务，并要求其及时删除从个人信息处理者处获得的个人信息。

评估要求：

评估员应：

——评审被评估方的用户协议、平台规则和合同，确认其中已明确：各自的合规义务与责任边界；平台内产品、服务、插件提供者的合规要求；个人信息处理者在发现违约或违规行为时的处置方式，这些处置方式足以确保个人信息处理者有权利、权力和能力采取特性要求中涉及的处置行为；

——评审个人信息处理者的平台规则、接入机制和工作流程，确认这些规则、机制和流程足以确保：个人信息处理者在提供重要互联网平台服务或接入产品、服务、插件之前进行影响评估并采取适当的控制措施；在必要时要求平台内产品、服务、插件提供者进行事前合规检测、评估、审计或影响评估。

——采用抽样方法验证这些规则、机制和工作流程被有效执行。

5.11.4文件管理指标

指标要求：

个人信息处理者应建立并持续维护与个人信息处理有关的活动记录和文件，以便在必要时能够及时举证以证明其合规性。

注：与个人信息处理有关的活动记录和文件包括但不限于：（1）有关其个人信息处理合法性基础的成文信息；（2）有关其个人信息处理目的的成文信息；（3）个人信息保护政策的历次版本，以及在版本更新时进行政策告知的适当证明；（4）有关其个人信息处理过程和程序的成文信息；（5）所处理的个人信息的信息资产清单；（6）个人信息处理设施和信息系统清单；（7）合规义务与合规要求清单；（8）能够证明其个人信息来源与流向的记录以及所涉及的第三方清单；（9）有关其为保护个人信息而采取的技术措施、管理措施和其他必要措施的成文信息；（10）所进行的个人信息保护影响评估的记录和报告；（11）有关个人信息处理合规的管理制度与规程；（12）获得个人信息主体同意的流程及其适当的证明；（13）与个人信息相关方之间的合同。

评估要求：

评估员应：

——在法律合规性评估的整个过程中确认被评估方的文件管理能够确保在其必要时可以及时提出证明其合规性的证据。

其他信息：

参见《个人信息保护法》第55条、第56条第2款、第63条和第69条第1款。

在首次法律合规性评估后所形成的文件清单、被采纳的客观证据清单等文件，通常已经能够表明组织为证明其个人信息处理的合规性所需要保留和维护的文件和证据。组织可以通过持续地更新和维护这些客观证据库以证明满足本指标的要求。

5.11.5合规审计指标

指标要求：

a) 个人信息处理的信息系统应启用日志功能，以确保能够对个人信息处理活动进行监测、记录和合规审计；

注：个人信息处理的信息系统，宜包括网络边界、重要网络节点、服务器和终端设备等设备资产以及业务应用系统。

b) 日志所记录的事件类型应覆盖个人信息的全部处理过程；

c) 日志应能够记录个人信息的来源（包括第三方提供）和流向（包括向第三方提供），包括所涉及的个人信息主体和/或其个人信息类型、第三方身份、授权或操作用户、时间；如果日志功能难以完全自动记录本项的，应采用人工记录予以补充；

d) 日志或记录应涵盖每个信息系统用户，记录事件所涉及的个人信息主体和/或其个人信息类型、日期和时间、用户、事件类型、事件是否成功以及其他与合规审计相关的信息；

e) 应为日志配置保存期限，配置的保存期限应与个人信息处理者的合规方针相符，并至少配置为六个月或者可适用的法规定的期限；

f) 为日志配置的保存期限届满后应予以删除，该操作宜通过配置自动进行；

g) 应对日志或记录采取与其他个人信息相同的安全保护措施，定期备份，避免日志或记录受到未预期的泄露、篡改或覆盖、毁损或丢失；

h) 应对日志进程进行保护以避免未经授权的中断，应在组织内部明确分配锁定或关闭日志事件的权限，锁定或关闭日志事件应被记录；

i) 应在组织内指定审计管理员在合规团队指导下定期对日志或记录进行合规审计；

j) 应跟踪和记录个人信息的加工处理、分析、挖掘等处理过程，建立适当的溯源机制，确保能够重现相应处理过程以支持合规审计要求。

评估要求：

评估员应：

——确认评估对象范围和边界内的信息系统启用了日志功能并可供持续地监测、记录和进行合规审计；

——确认所采用的日志记录配置满足上述记录要求；

——确认日志或记录得到被采取适当的安全保护措施和管理，能够避免因日志或记录管理不当导致的个人信息泄露、篡改、毁损、丢失等不利后果；

——确认被评估方定期对日志或记录进行合规审计，并及时对可疑或违规事件进行处置。

其他信息：

参见《个人信息保护法》第 54 条、第 64 条。

5.11.6影响评估指标

指标要求：

a) 个人信息处理者应建立个人信息保护影响评估的制度或流程，以确保在发生以下情形前，能够进行个人信息保护影响评估并依据评估结果采取适当的控制措施：

1) 处理敏感个人信息；

2) 利用个人信息进行自动化决策；

3) 委托处理个人信息；

4) 向其他个人信息处理者提供个人信息；

5) 公开个人信息；

6) 其他对个人权益有重大影响的个人信息处理活动。

注：本指标在公开、共享提供、转移环节以及向境外提供时有扩展要求，这些扩展要求给出了需要进行个人信息保护影响评估的具体情形。

b) 应定期地以及在现有的个人信息处理环境及其风险发生重大变化时，重新评审或再评估以持续改进控制措施。

注：个人信息处理环境极其风险发生重大变化的情形宜包括：（1）产品或服务的业务功能发生重大变化；（2）业务模式、信息系统或运行环境发生重大变化；（3）法律法规发生重大变化。

评估要求：

评估员应：

——确认被评估方是否存在个人信息保护影响评估的制度或流程；

——这些制度或流程是否能够确保被评估方可以根据个人信息处理所涉及的风险的变化，持续地改进对个人信息主体的风险以及合规风险的控制；

——这些制度或流程是否被定期评审和再评估。

其他信息：

参见《个人信息保护法》第55条和第56条。

个人信息保护影响评估的内容、方法和实施流程，见GB/T 39335—2020。

6特定处理环节的扩展要求

6.1特定处理环节的扩展要求概述

在个人信息处理的不同环节，个人信息主体的合法权益和个人信息安全主要面临的风险类型及其程度不尽相同。第5章确立的通用要求可能在某些特定的个人信息处理环节并不适用，或在适用时有必要具体化或变通适用。

第5章给出的通用要求均是在假定被评估方为个人信息处理者的前提下给出的。个人信息处理受托人可能仅提供单个环节或若干环节的个人信息处理服务，在个人信息处理者委托处理语境下，个人信息处理受托人应满足的合规要求将取决于两个因素：一是受委托的个人信息处理环节以及来自可适用的法对该特定个人信息处理环节的合规义务；二是委托模式和个人信息处理者的合规要求。例如，个人信息处理者可能委托个人信息处理受托人代为进行政策告知、同步告知、事件告知等事项。在个人信息处理受托人未履行这些合规要求时，最终可能由个人信息处理者承担法律责任，因此个人信息处理者的权责一致指标委托处理特性中包含了向个人信息处理受托人提供合规义务清单并明确其合规要求的内容（见5.11.3.3）。在此情形下，个人信息处理者可以通过在委托协议中引用本文件的维度、指标、特性名称或编号的形式，向个人信息处理受托人明示合规要求。在法律合规性评估中评估对象为个人信息处理受托人时，考虑上述因素并且明确识别合规义务清单和合规要求清单以确定适用的法律合规性评估准则至关重要。

在本章中给出了第5章规定的通用要求在适用于特定个人信息处理环节时的扩展要求。这些扩展要求包括指标在特定处理环节的具体化和必要变通，以及特定个人信息环节的被评估方为个人信息处理受托人时必要的变通要求。这些扩展要求并不构成一个新的指标，而应视为第5章指标的一部分。

本章的结构安排如下：

本章的每个一级条标题区分了个人信息处理的不同环节，如“6.2 收集”、“6.3 使用”。

每个一级条标题项下的第一个二级条标题（如6.2.1和6.3.1）是概述，给出了第5章的维度在该特定个人信息处理环节中的适用情况等信息。

第二个二级条标题（如6.2.2和6.3.2）开始按第5章给出的维度名称命名，表明该二级条标题所属的维度。在该维度中的指标有扩展要求时，设置三级条标题。其他特殊情形的区分，如对特定个人信息类型、特定个人信息处理设施或信息系统、个人信息处理者或个人信息处理受托人等，不再额外设置条标题。

注1：对于特定的个人信息处理环节，第 5 章给出的维度不适用或者无扩展要求时，仍然保留对应该维度的二级条标题，并在二级条标题项下的段中给出明确说明。

注2：评估对象中不包含特定个人信息处理环节时，无需将本章中该特定个人信息处理环节的扩展要求纳入评估范围。

6.2收集

6.2.1收集环节概述

有关个人信息处理的合规义务多数是对个人信息收集环节的要求。在第5章给出的通用要求中，所有维度和指标均适用于收集环节。

在法律合规性评估中，收集环节是评估对象范围和边界中必不可少的个人信息处理环节，否则将导致个人信息处理法律合规性评估的结论难以可靠地说明个人信息处理的合规性。

6.2.2合法维度

6.2.2.1合法性基础指标（5.2.1）收集环节扩展要求

扩展要求：

a) 收集个人信息前，个人信息处理者应明确识别可适用的合法性基础并确认是否满足合法性基础的要求；
b) 个人信息处理者应将所识别的合法性基础转化为成文信息，并提供给个人信息处理受托人；
c) 个人信息处理受托人接受委托为个人信息处理者收集个人信息的，应要求个人信息处理者提供收集个人信息的合法性基础文件；
d) 个人信息处理受托人应审查个人信息处理者提供的合法性基础文件，以确保合法性基础的要求至少在形式上均已具备，文件中不存在明显欠缺合法性基础要求的情形。

6.2.2.2来源合法指标（5.2.6）收集环节扩展要求

扩展要求：

个人信息处理者应从合法来源收集个人信息，包括但不限于：

a) 个人信息主体主动提供的，应确保在要求个人信息主体主动提供的具体场景中，至少已明示个人信息的收集目的，且不存在明显的欺诈、诱骗个人信息主体主动提供的虚假陈述或表示；
b) 从个人信息主体自动采集个人信息时，应确保在自动采集的具体场景中，至少已明示正在自动采集的事实；在开启自动采集的权限或功能的具体场景中，不存在明显的欺诈、诱骗个人信息主体开启自动采集权限或功能的虚假陈述或表示；
c) 搜集公开信息的，应能够证明确定的搜集来源，且在搜集公开信息的具体场景中，不存在违反 ROBOTS 协议爬取、违反 API 使用协议调取或其他技术手段绕开或破解搜集来源信息系统授权访问机制的情形；
d) 通过第三方的提供、转移间接获取的，应要求该第三方提供个人信息的合法来源并对合法来源进行确认，应确认第三方能够提供个人信息主体对提供、转移的选择同意，以及第三方收集个人信息具有合法来源。

6.2.3目的明确维度

6.2.3.1目的明示指标（5.3.3）收集环节扩展要求

扩展要求：

a) 收集个人信息前，个人信息处理者应明确收集目的，并单独明示可能与收集目的不具有合理关联（兼容性）的后续处理目的；
b) 个人信息处理者应将其收集和后续处理目的转化为成文信息，以在必要时提供给个人信息处理受托人等个人信息处理相关方；
c) 个人信息处理受托人接受委托为个人信息处理者收集个人信息时，应要求个人信息处理者提供处理目的文件，并按照个人信息处理者明示的处理目的进行收集。

6.2.4目的限制维度

6.2.4.1最小必要指标（5.4.2）收集环节扩展要求

扩展要求：

a） 实际收集的个人信息类型应与实现产品或服务的业务功能直接相关；
b） 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；
c） 间接获取个人信息的数量应是实现产品或服务的业务功能所需的最少数量；
d） 实际收集个人信息的方式，应是能够实现收集目的的若干可行收集方式中对个人信息主体权益影响最小的方式。

其他信息：

被评估方在收集环节出现与扩展要求a）-c）的差距，表明有超范围收集（过度收集）的违规风险。如果实际收集的个人信息类型与明示的收集目的之间被确定为没有直接相关，宜考虑删除或匿名化超范围收集的个人信息，并调整评估对象收集个人信息的类型、数量、频度和方式等设置，以消除这些差距。如果被评估方认为仍需保留这些已收集的个人信息或保留评估对象的原有设置，则需要调整其明示的收集目的，并重新征求个人信息主体的选择同意。但对于已经超范围收集个人信息的事实及其可能的行政责任等风险，评估员宜如实记录其发现并揭示这些风险，并与评估委托方商榷处置方案，包括是否建议被评估方尽可能调整这些差距，或者在评估法律意见书中如实披露相关的风险，由评估委托方是进行风险接受或进行其他合理处置，如要求被评估方向监管部门进行咨询以确定补救方法。

6.2.5公开透明维度

6.2.5.1信息充分指标（5.5.2）收集环节扩展要求

扩展要求：

a） 个人信息的收集目的应包括收集个人信息的具体业务功能以及该业务功能中包含的主要个人信息处理环节；
b） 应根据合法性基础或收集目的分别列举所收集的个人信息类型和方式；
c） 收集敏感个人信息的，应明确标识或突出显示；
d） 对于收集目的而言并非最小必要的个人信息类型、范围，以及与收集目的不具有合理关联的后续处理目的，应明确标识或突出显示；
e） 应根据合法性基础或收集目的，告知拒绝特定个人信息的收集可能产生的影响；
f） 收集方式应具体，如主动填写、自动采集或间接获取，如涉及自动采集应包含采集的方式和频率；
g） 应包含个人信息主体可以选择退出的方式和规则。

6.2.6告知维度

6.2.6.1同步告知指标（5.6.4）收集环节扩展要求

扩展要求：

a） 个人信息处理者关于收集的同步告知应包括以下最密切相关的信息：
   1） 收集个人信息的目的、方式和类型；
   2） 个人信息的存储时间；
   3） 拟对个人信息进行的非合理关联后续处理目的。
b） 收集敏感个人信息的，最密切相关信息除 a）项之外，还应包括：
   1） 处理敏感个人信息的必要性；
   2） 对个人权益的影响。

c） 在收集环节向个人信息主体同步告知（见 5.6.4）的时机：

1） 应是在请求个人信息主体主动提供个人信息的同时；

注：如在请求个人信息主体提供电话号码、住址等个人信息的交互界面或纸质表单中，用文字说明、图示、图标等进行告知；在人与人通过面对面、电话或在线互动的环境中，请求个人信息主体口头提供个人信息的，可以进行口头告知、文字说明或播放提前录制的告知。

2） 一次性自动采集个人信息的，应在实施自动采集前；

3） 间隔性或持续性自动采集个人信息的，应在请求或实际开启可自动采集个人信息的权限或实施首次自动采集前；

4） 因个人信息主体进入自动采集的物理空间而自动采集个人信息的，应在个人信息主体进入该自动采集区域前。

注：通常在线交互环境中宜通过弹窗、文字说明、推送通知等交互界面完成同步告知；无屏幕的智能终端或物联网设备，可在产品配置说明或在配置界面（如配套使用的移动应用程序等）中提供同步告知，或者通过提示音、图标等方式提供同步告知；在进入自动采集空间入口，用显著的文字说明、图示、图标等方式进行告知。

d） 通过在公共场所安装的图像采集、个人身份识别设备，采集为维护公共安全所必需的图像、身份识别信息的，同步告知：

1） 应采用能够表明以下最密切相关信息的提示标识：

——该设备所采集的个人信息类型；

——采集是为维护公共安全所必需的事实；

——采集方式。

2） 该提示标识应采用显著的形式；

3） 该提示标识应出现在个人信息主体进入采集区域前。

注1：采集的目的或范围并非为维护公共安全所必需、将采集到的维护公共安全所必需的个人信息用于其他目的，根据《个人信息保护法》第 26 条，应取得个人信息主体的单独同意。此种情形应采用与上述提示标识相独立的、满足 a）-c）项的同步告知。

注2：采集方式和个人信息类型的简洁表示方式，如“拍照”、“实时录像”、“刷脸”、“刷身份证”、“扫码”、“采集（按）指纹”等文字或相应的图。

注3：提示标识可采用浅显易懂的图标、图示、文字、音频或视频等形式。宜根据受众类型选择具体形式或组合多种形式，宜通过调整提示标识的大小、颜色、音量等，使提示标识对其主要受众的认知能力而言具备显著性。例如，预计主要受众为视觉障碍者的，宜采取或组合可通过听觉感知的提示标识。

6.2.7选择维度

6.2.7.1选择同意指标（5.7.2）收集环节扩展要求

扩展要求：

a） 当适用于个人信息收集的合法性基础要求获得同意，个人信息处理者应：

1） 在收集一般个人信息前，获得个人信息主体的选择同意；

2） 在收集敏感个人信息前，获得个人信息主体以单独和明示方式作出的选择同意；

3） 在收集个人生物识别信息前，获得个人信息主体以单独和明示方式作出的选择同意；

4） 在收集儿童个人信息应获得监护人以明示方式作出的选择同意，收集年满 14 周岁的未成年人个人信息前，获得未成年人或其监护人以明示明示方式作出的同意；

b） 所获得的同意应满足选择同意指标的特性要求。

6.2.8权益保障维度

权益保障维度（见5.8）并非特定于单个处理环节，在收集环节适用但无扩展要求。

6.2.9质量维度

质量维度/指标（见5.9.1）适用于收集环节，但无扩展要求。

6.2.10安全保护维度

6.2.10.1安全保护能力指标（5.10.2）收集环节扩展要求

扩展要求：

a） 个人信息为主动提供、自动采集的，应制定平台规范制度或接口规范制度，并对个人信息的数据字段格式进行定义；

b） 个人信息为主动提供、自动采集的，输入个人信息或通过通信接口输入个人信息的数据格式或长度应符合系统设定要求，并能够实现对恶意数据的过滤；

c） 间接获取个人信息的，应对获取个人信息的平台或接口进行全过程控制。

6.2.11可问责性维度

6.2.11.1合规管理体系指标（5.11.2）收集环节扩展要求

扩展要求：

应有明确的制度、规章或组织流程要求相关部门或人员在以新的目的收集个人信息前，以及实质性改变现有个人信息收集范围（如收集的个人信息类型、频率、数量）或收集方式前，向合规团队咨询：

a） 新的收集目的是否具有合法性基础；

b） 是否需要采取额外的政策告知、同步告知或选择同意等措施；

c） 实质性变更后的个人信息收集范围是否仍然满足最小必要指标的要求。

6.2.11.2文件管理指标（5.11.4）收集环节扩展要求

扩展要求：

收集环节应保留的证明合规性的文件包括但不限于：

a） 有关收集环节合法性基础的成文文件；

b） 有关收集目的的成文文件；

c） 收集环节政策告知的记录或适当证明；

d） 收集环节同步告知和选择同意的记录或适当证明；

e） 委托处理收集的，包括委托协议；

f） 有关收集合法来源的成文文件以及相应的证明；

g） 收集环节的日志记录。

6.3使用

6.3.1使用环节概述

个人信息的使用环节包含了多种多样的使用目的，在第5章给出的通用要求中所有维度和指标均适用于使用环节。

通常，在使用目的与收集目的具有合理关联（兼容性）时，使用环节法律合规性评估的核心关注点在于合法维度、目的合理维度、目的限制维度、公开透明维度、权益保障维度、安全保护维度和可问责性维度。但当个人信息的使用目的与收集目的不具有合理关联时，还会触发有关新的使用目的的合法维度、公开透明维度、告知维度、选择维度和可问责性维度等的关注。

6.3.2合法维度

6.3.2.1合法性基础指标（5.2.1）使用环节扩展要求

扩展要求：

在以与收集目的不具有合理关联的新的目的使用个人信息前，应再次识别合法性基础并确定满足相应合法性基础的要求。

6.3.2.2来源合法指标（5.2.6）使用环节扩展要求：

扩展要求：

在业务活动中所使用的个人信息应具有合法的收集来源。

注：宜留意在个人信息使用环节中作为输入的个人信息类型及其来源的合法性。

6.3.3目的明确维度

6.3.3.1目的合理指标（5.3.4）使用环节扩展要求：

扩展要求：

a) 以用户画像目的使用个人信息时，应遵守 GB/T 35273—2020，7.4 a)-c)的要求。

b) 使用个人信息进行自动化决策，应保证决策的透明度和结果公平、公正性，不应对个人在交易上实行不合理的差别待遇。

6.3.4目的限制维度

6.3.4.1目的兼容指标（5.4.3）使用环节扩展要求：

扩展要求：

个人信息的使用目的应与收集目的具有合理关联。

6.3.5公开透明维度

6.3.5.1信息充分指标（5.5.2）使用环节扩展要求

扩展要求：

a) 个人信息保护政策中列出的后续处理目的应包括任何与收集目的不具有合理关联的使用目的，以及该使用目的项下包含的主要个人信息处理环节；

b） 对于与收集目的不具有合理关联的使用目的，应根据合法性基础或使用目的分别列举所使用的个人信息类型和方式；
c） 以与收集目的不具有合理关联的目的使用敏感个人信息的，应明确标识或突出显示；
d） 应根据合法性基础或收集目的，告知拒绝特定个人信息的使用可能产生的影响；
e） 应包含个人信息主体可以选择退出的途径和规则。

6.3.6告知维度

6.3.6.1同步告知指标（5.6.4）使用环节扩展要求

扩展要求：

个人信息处理者变更已收集的个人信息使用目的的同步告知：
a） 应在变更使用目前的合理期限内作出；
b） 应包含以下最密切相关信息：
1） 新的使用目的、方式、个人信息种类和范围；
2） 选择退出机制。

6.3.7选择维度

6.3.7.1选择同意指标（5.7.2）使用环节扩展要求

扩展要求：

a） 基于选择同意处理个人信息的，在使用目的、方式和个人信息种类发生变更前，应重新获得个人信息主体的选择同意；
c） 除可适用的法或所识别的合法性基础不允许个人信息主体行使选择的情形外，以与收集目的不具有合理关联的目的使用个人信息前，应获得个人信息主体的选择同意。其中，以下使用应获得单独同意：
1） 将在公共场所安装的图像采集、个人身份识别设备所采集的图像、身份识别信息，用于维护公共安全以外的其他目的；
2） 使用已公开个人信息且使用方式对个体权益有重大影响。
3） 使用敏感个人信息，其中可适用的法明确要求获得书面同意的，应获得书面同意。
b） 个人信息处理者在进行以下使用前，应获得个人信息主体的单独同意：
1） 将在公共场所安装的图像采集、个人身份识别设备所采集的图像、身份识别信息，用于维护公共安全以外的其他目的；
2） 使用已公开个人信息的方式对个体权益有重大影响。
c） 可适用的法明确要求获得同意的使用，应获得个人信息主体的选择同意。

注：通常在收集时的选择同意已经能够涵盖与收集目的具有合理关联的使用，但在目的转用时以及某些可适用的法要求选择同意的特殊类型使用，需要额外考虑选择同意指标（见5.7.2）。

6.3.7.2选择退出指标（5.7.3）使用环节扩展要求

扩展要求：

a） 基于选择同意处理合法性基础使用个人信息的，个人信息处理者应至少提供撤回同意方式的选择退出机制。

b） 使用个人信息以自动化决策方式提供信息推送、商业营销的，个人信息处理者应提供选择退出机制；

注：在通过自动化决策方式提供信息推送、商业营销的具体场景中，选择退出宜单独或结合采用以下便捷方式：

— 显著区分：向个人信息主体提供商品或搜索结果的个性化展示的，同时提供非个性化展示的内容，显著区分以自动化决策方式提供的个性化展示内容与非个性化展示内容，如通过不同栏目、板块、页面的分置进行区分；

— 退订：在信息推送、商业营销信息的同时附带退订按钮或链接，或者提供推定方法的说明；关闭权限：通过隐私设置、权限管理、隐私仪表盘、隐私菜单等交互界面，提供关闭、停用个性化信息推送、商业营销信息发送的选项；

c） 可适用的法明确要求提供选择退出机制的，个人信息处理者应提供选择退出机制。

注：宜留意可适用的法可能对某些特殊类型的使用要求提供选择退出机制。

6.3.8权益保障维度

6.3.8.1投诉举报机制指标（5.8.7）使用环节扩展要求

扩展要求：

业务运营所使用的信息系统具备自动决策机制，并且该自动化决策可能对个人信息主体的合法权益带来重大影响的：应向个人信息主体提供对自动决策结果的投诉举报问询机制，向个人信息主体提供关于该自动决策过程和结果的公平公正性、目的合理性的解释说明，并支持对自动决策结果的人工复核。

注：对个人信息主体的合法权益有重大影响的决定，如自动决定个人征信和贷款额度，用于面试人员的自动筛选等。

6.3.9质量维度

6.3.9.1质量指标（5.9.1）使用环节扩展要求

扩展要求：

在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

6.3.10安全保护维度

6.3.10.1数据最小化指标（5.10.4）使用环节扩展要求

扩展要求：

a） 涉及通过界面展示个人信息的，个人信息处理者应采用适当的去标识化或匿名化技术措施，避免直接显示个人信息，降低个人信息的泄露风险；仅在被授权或经过身份验证的前提下展示全文。

b） 将为不同目的收集的个人信息汇聚融合存储的，应确保存储汇聚融合后的个人信息的数据库系统与具体进行个人信息使用的业务信息系统的分离，以及不同业务信息系统之间的适当分离，并对汇聚融合的个人信息转移至使用个人信息的业务信息系统设置严格的访问控制措施。

注：在首次将汇聚融合的个人信息转移至新的使用个人信息的业务信息系统之前，需进行个人信息保护影响评估，见6.3.11.3。

c） 对个人信息存储介质（如磁盘、磁带、固态硬盘等）采取访问控制措施并留存访问记录。

6.3.11可问责性维度

6.3.11.1合规管理体系指标（5.11.2）使用环节扩展要求

扩展要求：

应有明确的制度、规章或组织流程要求相关部门或人员在以新的目的使用个人信息前，以及实质性改变现有个人信息使用范围（如使用的个人信息类型、频率、数量）或使用方式前，向合规团队咨询：

a） 新的使用目的是否与收集目的具有合理关联；
b） 新的使用目的是否具有合法性基础；
c） 是否需要采取额外的政策告知、同步告知或选择同意等措施；
d） 实质变更后的个人信息使用范围是否仍然满足最小必要指标的要求。

6.3.11.2文件管理指标（5.11.4）使用环节扩展要求

扩展要求：

使用环节应保留的证明合规性的文件包括但不限于：

a） 有关使用环节合法性基础的成文文件；
b） 有关使用目的的成文文件；
c） 有关使用环节变更事项的政策告知记录或适当证明；
d） 使用环节要求同步告知和选择同意的，相关记录或适当证明；
e） 使用环节所包含的个人信息处理过程被委托处理的，包括委托协议；
f） 有关使用的个人信息合法收集来源的成文文件以及相应的证明；
g） 使用环节的日志记录。

6.3.11.3影响评估指标（5.11.6）使用环节扩展要求

扩展要求：

a） 业务运营所使用的信息系统具备自动化决策机制，并且该自动化决策可能对个人信息主体的合法利益带来直接影响的，应在信息系统规划阶段或首次使用前以及投入使用后定期（至少每年一次）开展个人信息保护影响评估，并依据评估结果采取并持续改进有效的保护个人信息主体的措施。
b） 在对汇聚融合后的个人信息首次转移至使用目的与收集目的不具有合理关联的业务系统之前，以及投入使用后定期（至少每年一次）开展个人信息保护影响评估，并依据评估结果采取并持续改进有效的保护个人信息主体的措施。

6.4存储

6.4.1存储环节概述

在第5章给出的通用要求中所有维度和指标在个人信息存储环节均可以适用。

但除非评估对象是以个人信息的存储作为核心的产品、服务或过程，存储环节法律合规性评估的主要关注点可以聚焦于存储期限、存储期限届满时的处理，以及特殊的个人信息类型，如人类遗传资源、

银行卡磁道信息或芯片信息、验证码、密码等敏感信息，或者个人生物识别信息的存储合法性、必要性和安全性等方面。

6.4.2合法维度

6.4.2.1合法性基础指标（5.2.1）存储环节扩展要求

扩展要求：

在存储对于收集使用目的而言已不再必要或者超出个人信息保护政策声明的存储期限的前提下继续存储个人信息，又不进行匿名化或删除操作的，应再次识别合法性基础并确定满足相应合法性基础的要求。

6.4.2.2主体合法指标（5.2.3）存储环节扩展要求

扩展要求：

a） 可适用的法对个人信息存储设定了主体资格要求的，应符合主体资格要求。

注：在存储环节，主体合法指标与类型合法指标有可能是重叠的，因为可适用的法通常只会对特定类型的个人信息存储设定主体资格要求。例如，《人类遗传资源管理条例》第7条禁止外国组织、个人及其设立的或者实际控制的机构在我国境内采集、保藏人类遗传资源（包括人类遗传资源材料和人类遗传资源信息）。又如，《非银行支付机构网络支付业务管理办法》第20条禁止非银行支付机构存储客户银行卡的磁道信息或芯片信息、验证码、密码等敏感信息。这些特定类型的个人信息存储是以具备一定的主体资格为条件。

b） 可适用的法对特定个人信息处理者设定了境内存储要求的，符合该主体资格条件的个人信息处理者应在中华人民共和国境内存储个人信息。

注：在存储环节，主体合法指标包含对可适用的法境内存储要求的满足。例如，《个人信息保护法》第36条对国家机关处理的个人信息规定了境内存储的要求。个人信息处理者是国家机关或者为国家机关处理的个人信息提供存储的，需在境内存储。又如，根据《个人信息保护法》第40条，关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，需将境内收集和产生的个人信息存储在境内。这些境内存储要求均是以具备一定的主体资格为条件。

6.4.2.3类型合法指标（5.2.5）存储环节扩展要求

扩展要求：

a） 个人信息处理者不应对可适用的法禁止存储的个人信息类型进行存储。

注：在可适用的法并非以主体资格作为存储特定类型个人信息的条件，而是在一般情形下禁止所有类型的个人信息处理者存储特定类型的个人信息时，宜适用类型合法指标。在一般性禁止和例外允许存储的情形下，宜确认被评估方符合例外的情形。

b） 可适用的法对特定个人信息类型设定了境内存储要求的，个人信息处理者应将该个人信息类型存储在境内。

6.4.3目的明确维度

目的明确维度（见5.3）适用于存储环节。通常而言，个人信息的存储目的是由个人信息的收集目的所决定的，或者是由可适用的法所决定的，当个人信息的存储期限超出收集目的的最小必要时，则需要具体、明示和合理的存储目的。

6.4.4目的限制维度

6.4.4.1最小必要指标（5.4.2）存储环节扩展要求

扩展要求：

a） 个人信息的存储期限应为实现明示的收集目的所必需的最短时间，可适用的法另有规定或个人信息主体另行选择同意时除外；

b） 在个人信息保护政策中规定的最小必要持有期限届满时应安全地删除或匿名化；

c） 当可适用的法要求继续存储该个人信息而没有个人信息主体的选择同意时，应锁定或将个人信息存入存档系统，以使个人信息免于除存储以外的进一步的处理。

6.4.5公开透明维度

公开透明维度（5.5）适用于存储环节，但在存储环节无扩展要求。

6.4.6告知维度

6.4.6.1事件告知指标（5.6.3）存储环节扩展要求

扩展要求：

所存储的个人生物识别信息发生泄漏的，个人信息处理者应进行事件告知。

6.4.6.2同步告知指标（5.6.4）存储环节扩展要求

扩展要求：

延长个人生物识别信息的存储期限或改变存储期限届满时的处理方式，应向个人信息主体进行同步告知。

注：根据GB/T 35273—2020,5.4 c)的要求，在收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。该要求已经被本文件6.2.6.1a)和b）所涵盖。

6.4.7选择维度

6.4.7.1选择同意指标（5.7.2）存储环节扩展要求

扩展要求：

a） 除非可适用的法要求继续存储，个人信息处理者在个人信息的存储期限届满而不进行删除或匿名化，或者延长存储期限的，应获得个人信息主体的选择同意；

b） 延长个人生物识别信息的存储期限或改变存储期限届满时的处理方式前，应获得个人信息主体以明示方式作出的选择同意。

6.4.7.2选择退出指标（5.7.3）存储环节扩展要求

扩展要求：

除非可适用的法明确要求保留个人生物识别信息，个人信息处理者对于所存储的个人生物识别信息应提供选择退出机制，并在选择退出时进行删除。

6.4.8权益保障维度

权益保障维度（见5.8）适用于存储环节，但在存储环节无扩展要求。

6.4.9质量维度

质量维度（见5.9）适用于存储环节，但在存储环节无扩展要求。

6.4.10安全保护维度

6.4.10.1安全保护能力指标（5.10.2）存储环节扩展要求

扩展要求：

a） 应将去标识化后的信息与可用于重标识的标识符分别存储，并加强对标识符的访问和使用权限管理；

b） 应将个人生物识别信息与一般个人信息分别存储，并加强对生物识别信息的访问和使用权限管理；

c） 除非有可适用的法定义务要求存储原始个人生物识别信息（如图像或样本），否则不应存储原始个人生物识别信息（如图像或样本），只存储个人生物识别信息的摘要信息；

注：其他可被采用的措施也可包括在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能，或者在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。见GB/T 35273—2020,6.3 c)。

d） 敏感个人信息应加密存储；

注：密码技术应符合适用的密码管理相关国家标准。

e） 应建立异地个人信息（或其数据）备份措施，并根据业务应用场景需求及时进行备份；

f） 备份存储安全保护措施应与业务应用系统存储保护措施一致；

g） 备份过程中应保障备份数据的完整性、保密性；

h） 应定期对备份数据进行恢复测试，以确保备份数据的可用性。

6.4.11可问责性维度

6.4.11.1文件管理指标（5.11.4）存储环节扩展要求

扩展要求：

存储环节应保留的证明合规性的文件包括但不限于：

a） 有关存储环节的合法性基础的成文文件；

b） （如适用）有关存储目的的成文文件；

c） 存储期限或存储期限届满时处理方式变更的同步告知和选择同意等的记录或适当证明；
d） 将存储环节委托处理的，包括委托协议；
e） 存储环节的日志记录。

6.5公开

6.5.1公开环节概述

第5章给出的通用要求中的所有维度和指标在个人信息公开环节均可以适用。

个人信息的公开往往涉及个人信息保密性的较高程度的侵入，尤其当所公开的个人信息为隐私权所保护的私密信息，或者敏感个人信息时，公开将伴随着更高的违规风险。鉴于个人信息公开的敏感性和高风险，除选择同意处理（5.2.2.1）以外，可适用的法较少能够为公开提供合法性基础，甚至在某些情形下可能明确禁止公开。因此，对公开环节的法律合规性评估宜更加聚焦于合法维度、选择维度，以及与个人信息主体行使选择有关的公开透明维度和告知维度。

其他信息：

参见《个人信息保护法》第25条、第27条、第55条第3项。

6.5.2合法维度

6.5.2.1合法性基础指标（5.2.1）公开环节扩展要求

扩展要求：

在进行一项新的公开前，个人信息处理者应明确识别合法性基础并确定满足相应合法性基础的要求。

注：除选择同意处理之外，其他合法性基础可能包含公开，但宜根据公开的具体目的、个人信息类型、具体场景等进行个案综合判断。例如，为公共利益实施新闻报道、舆论监督等行为通常包含对个人信息的一定程度的公开。但该情形下公开是否属于在合理范围内的个人信息处理，则高度依赖于可适用的法。例如，在实施新闻报道、舆论监督的过程中公开刑事案件证人、鉴定人、被害人等的真实姓名、住址和工作单位、外貌、真实声音等，很可能给个人信息主体的人身安全带来较高程度的风险。又如，公开信息公平处理中所涉及的个人信息本身已经是公开信息，但该公开信息的再公开或经加工后的公开，仍然可能因具体目的、个人信息类型、具体场景等因素的影响，而对个人信息主体的合法权益有重大影响。因此，凡是涉及个人信息的新的公开，仍需要重新明确识别合法性基础并确定满足。

6.5.2.2类型合法指标（5.2.5）公开环节扩展要求

扩展要求：

a） 不应公开个人生物识别信息；
b） 不应公开我国公民的种族、民族、政治观点、宗教信仰等敏感个人信息的分析结果。

6.5.3目的明确维度

6.5.3.1目的具体/特定指标（5.3.2）公开环节扩展要求

扩展要求：

在公开个人信息前，应识别明确的公开目的：

a） 公开目的应具体到产品或服务中涉及公开的具体业务功能，并区分基本业务功能和扩展业务功能；

b） 所识别的公开目的应形成成文信息并可用。

6.5.4目的限制维度

目的限制维度（见5.4）适用于公开环节，但在公开环节无扩展要求。

6.5.5公开透明维度

6.5.5.1信息充分指标（5.5.2）公开环节扩展要求

扩展要求：

个人信息处理者所公开的与其个人信息处理政策与实践有关的充分信息，应包括：

a） 是否会公开个人信息的说明；

b） 公开个人信息的目的、方式、类型和范围。

注1：公开目的的具体程度宜参考目的具体指标公开环节扩展要求（6.5.3.1）。公开个人信息的方式宜结合已识别的合法性基础加以说明，例如表明将在何种条件下公开个人信息以及个人是否享有选择同意或选择退出机制。公开的个人信息类型的具体程度宜考虑是否为敏感个人信息，如为敏感个人信息，宜尽可能逐项列出。公开个人信息的范围宜考虑可访问被公开个人信息的受众范围，例如是否仅注册用户或好友可访问，抑或全网可访问等。

注2：信息的充分性可根据个人信息主体的选择权以及在具体场景中的合理期待加以调整，例如，在社交应用程序等场景中，公开一定程度的个人信息符合个人信息主体的合理期待，尤其是当个人信息主体可以自行选择公开哪些个人信息以及公开范围时，在信息充分指标中的信息可适当简略。

6.5.6告知维度

6.5.6.1同步告知指标（5.6.4）公开环节扩展要求

扩展要求：

个人信息处理者公开个人信息的同步告知：

a） 应在就公开向个人信息主体征求选择同意时作出；

b） 应包含以下最密切相关的信息：

1） 将公开个人信息的事实；

2） 公开个人信息的目的和个人信息类型。

注：根据《个人信息保护法》第25条和第55条，公开个人信息应获得单独同意并在事前进行个人信息保护影响评估。在公开个人信息前的同步告知中，宜尽可能包含为确保个人信息主体知情同意所需的其他相关信息，例如，公开可能对个人信息主体权益带来的影响，拒绝公开的影响、选择退出（包括撤回同意）的方式以及个人信息主体合法权益的行使方式等。

6.5.7选择维度

6.5.7.1选择同意指标（5.7.2）公开环节扩展要求

扩展要求：

个人信息处理者在公开个人信息前，应获得个人信息主体以单独且明示的方式作出的选择同意。

6.5.7.2选择退出指标（5.7.3）公开环节扩展要求

扩展要求：

a) 基于选择同意公开个人信息的，个人信息处理者应为个人信息主体提供至少包含撤回同意在内的选择退出机制：
   1) 个人信息主体撤回同意的，应停止对该个人信息主体个人信息的公开。
b) 公开个人信息的合法性基础并非选择同意处理的，除非该合法性基础不允许个人信息主体行使选择，个人信息处理者应：
   1) 提供选择退出机制。
   2) 有效的删除机制可视为存在选择退出机制；
   3) 个人信息主体选择退出的，应停止对该个人信息主体个人信息的公开。

6.5.8权益保障维度

6.5.8.1删除机制指标（5.8.6）公开环节扩展要求

扩展要求：

个人信息处理者违反可适用的法的规定或违反与个人信息主体的约定公开个人信息，或者依据可适用的法产生删除义务的其他情形，个人信息主体要求删除的，个人信息处理者应立即停止公开、自行删除，并发送通知要求个人信息处理相关方删除相应信息。

注：宜留意即使并非个人信息处理者直接违反可适用的法的规定或个人信息主体的约定，在某些特定情形下也可能基于“通知—删除”规则等导致需删除个人信息的情形。例如，《民法典》第1195条规定，网络用户利用网络服务实施侵权行为的，权利人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。通知应当包括构成侵权的初步证据及权利人的真实身份信息。

6.5.9质量维度

6.5.9.1质量维度/指标（5.9.1）公开环节扩展要求

扩展要求：

在公开个人信息前，宜根据公开的目的进行必要的个人信息准确性、完整性和及时性的确认，以避免因公开的个人信息就公开的目的而言不够准确、完整和及时而可能导致的索赔。

6.5.10安全保护维度

6.5.10.1安全保护能力指标（5.10.2）公开环节扩展要求

扩展要求：

公开个人信息的，应采用完整性校验等技术措施确保个人信息传输的完整性。

6.5.11可问责性维度

6.5.11.1合规管理体系指标（5.11.2）公开环节扩展要求

扩展要求：

个人信息处理者应有明确的制度、规章或组织流程要求相关部门或人员在以新的目的公开个人信息，以及实质性改变现有个人信息公开范围（如个人信息类型、数量等）、公开方式前，向合规团队咨询：

a） 新的公开是否具有合法性基础；

b） 是否需要采取额外的政策告知、同步告知或选择同意等措施；

c） 实质变更后的个人信息公开范围是否仍然满足最小必要指标的要求。

6.5.11.2文件管理指标（5.11.4）公开环节扩展要求

扩展要求：

个人信息处理者关于公开环节应保留的证明合规性的文件包括但不限于：

a） 有关公开环节的合法性基础的成文文件；

b） （如适用）有关公开目的的成文文件；

c） 有关公开披露的个人信息保护政策历次版本、同步告知和选择同意等的记录或适当证明；

d） 为公开所进行的个人信息保护影响评估文件；

e） 个人信息的公开情况的准确记录，包括公开的日期、规模、目的和公开范围等。

6.5.11.3影响评估指标（5.11.6）公开环节扩展要求

扩展要求：

个人信息处理者在公开前应事先开展个人信息保护影响评估，并依评估结果采取有效的保护个人信息主体的措施。

6.6提供

6.6.1提供环节概述

第5章给出的维度在个人信息提供环节均可以适用。

个人信息提供往往并不像公开一样直接导致个人信息保密性的丧失，但提供通常使得个人信息的接收者获得对个人信息的独立的控制权，其结果也必然包含对个人信息享有访问权限的组织或个人的范围扩大，从而对个人信息的保密性带来风险。相比于公开，个人信息提供可能适用的合法性基础涵盖较广，并且以具体、明示、合理的目的提供的个人信息在某些情形下可能服务于个人信息处理者合法利益的同时，为个人信息主体带来便利。但缺乏透明度、选择与可问责性的个人信息提供，容易导致个人信息主体丧失对其个人信息的控制，从而引发更多的担忧，并且在违规提供时很可能导致严格的行政责任甚至刑事责任。考虑到提供环节的上述特性，所有法维度和指标在提供环节的法律合规性评估中都是相关且重要的，但尤其需要关注合法性基础、目的限制、公开透明、选择和和可问责性维度。

6.6.2合法维度

6.6.2.1合法性基础指标（5.2.1）提供环节扩展要求

扩展要求：

在进行一项新的个人信息提供之前，应明确识别合法性基础并确定满足相应合法性基础的要求。

6.6.3目的明确维度

目的明确维度（见5.3）适用于提供环节，但在提供环节无扩展要求。

6.6.4目的限制维度

目的限制维度（见5.4.1）适用于提供环节，但在提供环节无扩展要求。

6.6.5公开透明维度

6.6.5.1信息充分指标（5.5.2）提供环节扩展要求

扩展要求：

a) 产品或服务中接入收集个人信息的第三方产品、服务或插件，并且该第三方直接向个人信息主体收集个人信息并获取选择同意的，个人信息处理者所公开的与其个人信息处理政策与实践有关的充分信息，应包括：
   1) 涉及此类第三方的业务功能；
   2) 第三方类型以及各自的安全和法律责任，包括个人信息处理者所采取的第三方接入管理流程或安全保护措施。

注：应在进入此类产品或服务前设置同步告知或明确的警示标志。

b) 产品或服务中接入或嵌入的第三方产品、服务或插件通过个人信息处理者间接获取个人信息，并且：
   1) 个人信息处理者与该第三方将分别对个人信息享有控制并各自承担责任的，个人信息处理者所公开的与其个人信息处理政策与实践有关的充分信息，应包括：
      ——涉及此类第三方的业务功能和提供目的；
      ——第三方类型以及各自的安全和法律责任，包括个人信息处理者所采取的第三方接入管理流程或安全保护措施；

   注：个人信息处理者应通过查询机制提供通过个人信息处理者获得个人信息的第三方身份和个人信息类型（见6.6.8.1）；在提供前应进行同步告知（见6.6.6.1b)），并获得个人信息主体对提供的单独同意（见6.6.7.1）。个人信息处理者应满足权责一致指标平台/第三方管理特性要求（见5.11.3.4）。

   2) 如第三方不单独向个人信息主体征求同意的，在个人信息处理者的提供与第三方的收集环节为个人信息共同处理者，个人信息处理者所公开的与其个人信息处理政策与实践有关的充分信息，应包括：
      ——此类第三方的名称或姓名和联系方式；
      ——该第三方的收集目的和后续处理目的；
      ——该第三方的处理方式和个人信息类型；
      ——各自的安全和法律责任。

   注：此种情形的示例，如产品或服务的过程中部署的收集个人信息的第三方插件，例如统计分析工具、软件开发工具包SDK、调用地图API接口。如果个人信息处理者没有充分公开有关此类第三方的信息，很可能

导致个人信息处理者承担非法提供的法律责任，并可能因该第三方的个人信息处理不合规而共同承担或替代承担法律责任。

6.6.6告知维度

6.6.6.1同步告知指标（5.6.4）提供环节扩展要求

扩展要求：

a） 对于产品或服务中接入的直接向个人信息主体收集个人信息的第三方产品或服务，应在个人信息主体通过个人信息处理者的产品或服务进入到第三方产品或服务时，同步告知或设置明显标识提示正在进入第三方产品或服务的事实；

b） 接入通过个人信息处理者间接获取个人信息的第三方产品、服务或插件，或者以其他方式向第三方提供个人信息的，应在提供前同步告知：

1） 第三方的名称或者姓名、联系方式；

2） 提供目的、方式和个人信息的类型；

3） 可适用的法有明确要求的，还包括提供可能产生的后果、拒绝提供的影响、选择退出方式、第三方的数据安全能力等。

注：根据《个人信息保护法》第23条和第55条，个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应取得单独同意并在事前进行个人信息保护影响评估。在提供个人信息前的同步告知中，无论可适用的法是否有明确要求，宜尽可能包含为确保个人信息主体知情同意所需的所有相关信息，例如，提供可能对个人信息主体权益带来的后果，拒绝提供的影响，选择退出方式，第三方的数据安全能力，以及个人信息主体合法权益的行使方式等。

c） 向第三方提供敏感个人信息，向个人信息主体作出的同步告知应：

1） 单独列出敏感个人信息类型；

2） 包含特定的提供目的；

3） 包含提供敏感个人信息的充分必要性；

4） 包含提供对个人权益的影响。

6.6.7选择维度

6.6.7.1选择同意指标（5.7.2）提供环节扩展要求

扩展要求：

个人信息处理者向第三方提供个人信息前，应获得个人信息主体的单独和明示方式作出的选择同意。

6.6.7.2选择退出指标（5.7.3）提供环节扩展要求

扩展要求：

个人信息处理者向第三方提供个人信息的，应：

a） 向个人信息主体提供选择退出机制，如撤回同意；

b） 个人信息主体选择退出（如撤回同意）的，个人信息处理者应停止向第三方提供，并向第三方发送通知要求告知选择退出的事实，要求第三方停止已经被选择退出的个人信息处理。

注：个人信息主体的选择退出（如撤回同意），可能伴随删除机制下的删除请求（见5.8.6和6.6.8.2），或

可能导致个人信息处理者终止对这些个人信息的处理（7.3）。在必要且适当时，个人信息处理者需同时考虑选择退出与其他合规要求之间的衔接。

6.6.8权益保障维度

6.6.8.1查询机制指标（5.8.3）提供环节扩展要求

扩展要求：

向第三方提供个人信息的,应提供查询机制以允许个人信息主体查询通过个人信息处理者提供获取个人信息的第三方身份、个人信息类型。

6.6.8.2删除机制指标（5.8.6）提供环节扩展要求

扩展要求：

个人信息处理者违反法律法规规定或违反与个人信息主体的约定向第三方提供个人信息,个人信息主体要求删除的，应及时停止提供并通知第三方删除。

6.6.9质量维度

质量维度/指标（见5.9.1）适用于提供环节，但在提供环节无扩展要求。

6.6.10安全保护维度

安全保护维度（见5.10）适用于提供环节，但在提供环节无扩展要求。

6.6.11可问责性维度

6.6.11.1权责一致指标（5.11.3.4）提供环节扩展要求

扩展要求：

个人信息处理者的产品或服务中接入第三方产品、服务、插件的，应建立第三方产品、服务、插件接入管理机制和工作流程，该机制和工作流程应满足平台/第三方管理特性要求（5.11.3.4）。

6.6.11.2文件管理指标（5.11.4）提供环节扩展要求

扩展要求：

提供环节应保留的证明合规性的文件包括但不限于：

a） 有关提供环节的合法性基础的成文文件；
b） 有关提供目的的成文文件；
c） 有关提供的个人信息保护政策历次版本、同步告知和选择同意等的记录或适当证明；
d） 为提供所进行的个人信息保护影响评估文件；
e） 第三方接入有关的合同、第三方接入清单和相关日志或记录；
f） 第三方管理指标所要求的管理机制和工作流程等文件。

6.6.11.3合规审计指标（5.11.5）提供环节扩展要求

扩展要求：个人信息处理者应在其产品或服务与第三方的产品或服务的边界启用日志记录功能，持续记录和定期审计第三方接口和数据使用情况，必要时设置自动警报机制，以便及时发现通过接口违规获取数据的行为。

6.6.11.4影响评估指标（5.11.6）提供环节扩展要求

扩展要求：

计划通过公开开放或协议开放API接口等方式允许个人信息共同处理者、个人信息处理受托人以外的第三方通过接入其产品、服务直接向个人信息处理者收集个人信息，或者通过其产品或服务间接获取个人信息的，应在首次开放前以及在此后定期进行个人信息保护影响评估。

6.7转移

6.7.1转移环节概述

第5章给出的通用要求中所有维度和指标在个人信息转移环节均可以适用。

由于个人信息的无形性、易复制特征，绝大多数个人信息控制权变动是通过提供实现的，即在向第三方提供个人信息后，提供方与接收方共同或分别享有个人信息控制权。提供方将个人信息控制权转移给第三方的同时使自身丧失该个人信息控制权的情形较为有限。转移通常是伴随着作为个人信息处理者的合并、分立、解散、被申请破产或申请破产重整等组织变更一并发生的，否则除选择同意处理和合法利益公平处理之外也较少有合法性基础能够为个人信息的转移赋予确定性的合法性基础。转移对个人信息保密性的风险程度与提供环节类似，转移的合规要求通常与提供环节一并得到规定。但宜特别留意脱离具体、明示、合理目的（例如脱离产品或服务的业务功能场景），而仅将个人信息交易作为转移目的往往更容易产生行政责任甚至刑事责任的风险。鉴于转移环节的上述特性，在转移环节尤其具有相关性和重要性的是合法维度、目的明确维度、选择维度和可问责性维度。

6.7.2合法维度

6.7.2.1合法性基础指标（5.2.1）转移环节扩展要求

扩展要求：

除非已识别的合法性基础或者已经明示的处理目的中已包含转移，在进行一项新的个人信息转移之前，应明确识别合法性基础并确定满足相应合法性基础的要求。

注：极少有可适用的法直接为个人信息的转移赋予合法性基础，基于选择同意处理、合同必要处理和合法利益公平处理可能是最为相关的。其中，合并、分立、解散、被申请破产或申请破产重整等组织变更所导致的个人信息转移，通常可以视为是为实现个人信息处理者的合法利益而必要的，并且要求选择同意容易导致合并、分立、解散、被申请破产或申请破产重整等组织变更遇到难以确定估值和难以交割等障碍，提供选择退出机制并且确保后续的个人信息处理者按照原定方式履行原个人信息处理者的义务和责任、在破产无承接方时妥善安全删除，通常可以有效降低转移对个人信息主体的合法利益的影响。

6.7.3目的明确维度

目的明确维度（见5.3）适用于转移环节，但在转移环节无扩展要求。

6.7.4目的限制维度

目的限制维度（见5.4）适用于转移环节，但在转移环节无扩展要求。

6.7.5公开透明维度

6.7.5.1信息充分指标（5.5.2）转移环节扩展要求

扩展要求：

个人信息处理者所公开的与其个人信息处理政策与实践有关的充分信息，应包括：

a） 是否进行个人信息转移；

b） 转移目的；

c） 涉及的个人信息类型；

d） 接收方的名称或姓名和联系方式；

e） 各自的安全和法律责任等信息。

6.7.6告知维度

6.7.6.1政策告知指标（5.6.2）转移环节扩展要求

扩展要求：

因合并、分立、解散、被申请破产或申请破产重整等导致个人信息处理者发生增加、减少或变更，和/或导致个人信息主体行使其合法权益的方式发生变更的，应在完成合并、分立、解散、被申请破产或申请破产重整的合理期限内及时更新个人信息保护政策并进行政策更新告知。

6.7.6.2同步告知指标（5.6.4）转移环节扩展要求

扩展要求：

a） 个人信息处理者因合并、分立、解散、被申请破产或申请破产重整等原因需要进行个人信息转移的，同步告知：

1） 应在实际转移前的合理期限内一次性或分阶段作出；

2） 应包含以下最密切相关信息：

——因合并、分立、解散等原因将转移个人信息的事实；

——接受方的名称或者姓名和联系方式；

——接收方将继续履行个人信息处理者义务的事实。

注1：同步告知的时机宜同时考虑可行性与合理性。通常在做出合并、分立、解散的决议时，接收方及其他最密切相关信息均已确定，个人信息处理者宜在做出决议后尽早进行同步告知。个人信息处理者被宣告破产的，通常在破产财产变价经债权人会议通过或经法院裁定后才可能确定接收方，个人信息处理者宜在接收方确定后尽早进行同步告知。同步告知宜适当早于实际转移，以便个人信息主体在实际转移前有合理的时间对将要发生个人信息处理者或其他重大变更做出反应。

注2：个人信息处理者解散或破产清算且无个人信息接收方的，应对个人信息进行删除，在完成删除后应通过同步告知或公告向个人信息主体告知该事实。

b） 非因合并、分立、解散、被申请破产或申请破产重整破产等原因需要进行个人信息转移的，同步告知：

1） 应在转移前的合理期限内一次性或分阶段作出；

2） 应包含以下最密切相关信息：

——转移个人信息的目的；

——接收方的名称或者姓名和联系方式；

——转移方式和个人信息的种类。

注：在转移个人信息前的同步告知中，无论可适用的法是否有明确要求，宜尽可能包含为确保个人信息主体知情同意所需的所有相关信息，例如，提供可能对个人信息主体权益带来的后果，拒绝提供的影响，选择退出方式，第三方的数据安全能力，以及个人信息主体合法权益的行使方式等。

c） 无论因何种原因转移敏感个人信息的，同步告知中应：

1） 单独列出涉及转移的敏感个人信息类型；

2） 包含特定的转移目的并说明转移敏感个人信息的充分必要性；

3） 说明转移敏感个人信息对个人权益的影响；

4） 可适用的法有明确要求的，还包括提供可能产生的后果、拒绝提供的影响、选择退出方式、接收方的数据安全能力等。

d） 无论因何种原因转移个人信息的，应单独列出或另行同步告知：

1） 将在实际转移前发生的处理目的、处理方式变更，以及与需获得选择同意的其他重大变更最密切相关的信息；

2） （如适用）将在实际转移时发生的处理目的、处理方式变更，以及其他需获得选择同意的重大变更最密切相关的信息；

注：重大变更的范围见5.5.2k）及其注。在实际转移前发生处理目的变更，或其他需要获得个人信息主体选择同意的重大变更，原个人信息处理者仍需履行相应义务。根据《个人信息保护法》第22条和第23条，接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。但接收方在实际转移同时变更处理目的、处理方式的，在实际转移前接收方很可能不具有自行同步告知并获得选择同意的可行性。单独列出或另行同步告知宜与征求选择同意相结合，以便获得适格的选择同意。

6.7.7选择维度

6.7.7.1选择同意指标（5.7.2）转移环节扩展要求

扩展要求：

a） 非因合并、分立、解散、被申请破产或申请破产重整等原因转移个人信息的，应获得个人信息主体以单独且明示的方式作出的选择同意；

b） 在实际转移前发生处理目的、处理方式变更以及需获得选择同意的其他重大变更的，应获得个人信息主体的选择同意；

c） 在实际转移的同时发生处理目的、处理方式变更以及需获得选择同意的其他重大变更，且接收方在该实际变更前无法获得个人信息主体选择同意的，个人信息处理者应获得选择同意；

d） 涉及敏感个人信息转移的，应获得个人信息主体以单独且明示的方式作出的选择同意。

6.7.7.2选择退出指标（5.7.3）转移环节扩展要求

扩展要求：

在向个人信息主体告知将要转移个人信息的事实起至完成转移期间，应确保选择退出机制保持有效运行，并及时响应个人信息主体选择退出的请求。

6.7.8权益保障维度

6.7.8.1合法权益行使机制通用指标（5.8.2）转移环节扩展要求

扩展要求：

在向个人信息主体告知将要转移个人信息的事实起至完成转移期间，应确保个人信息主体行使其合法权益的方法有效运行，并及时响应个人信息主体行使其合法权益的请求。

6.7.8.2删除机制指标（5.8.6）转移环节扩展要求：

扩展要求：

个人信息处理者违反法律法规规定或违反与个人信息主体的约定向第三方转移个人信息，个人信息主体要求删除的，应立即停止转移并通知第三方及时删除。

6.7.9质量维度

质量维度/指标（见5.9.1）适用于转移环节，但在转移环节无扩展要求。

6.7.10安全保护维度

6.7.10.1安全保护能力指标（5.10.2）转移环节扩展要求

扩展要求：

数据整体迁移的过程中，应采取措施防止数据残留。

6.7.11可问责性维度

6.7.11.1合规管理体系指标（5.11.2）转移环节扩展要求

扩展要求：

应有明确的制度、规章或组织流程要求相关部门或人员在个人信息转移前，向合规团队咨询：

a） 所涉及的转移是否具有合法性基础；

b） 是否需要采取额外的政策告知、同步告知或选择同意等措施。

6.7.11.2文件管理指标（5.11.4）转移环节扩展要求

扩展要求：

转移环节应保留的证明合规性的文件包括但不限于：

a） 有关转移环节的合法性基础的成文文件；

b） 有关转移目的的成文文件；

c） 有关转移的个人信息保护政策历次版本、同步告知和选择同意等的记录或适当证明；

d） 为转移所进行的个人信息保护影响评估文件；

e） 有关转移的合同等文件，其中明确规定数据接收方的责任和义务；

f） 个人信息的转移情况的准确记录，包括转移的日期、规模、目的以及数据接收方的基本情况等。

6.7.11.3影响评估指标（5.11.6）转移环节扩展要求

扩展要求：

在个人信息转移前，应事先开展个人信息保护影响评估，并依评估结果采取有效的保护个人信息主体的措施。

7特殊的个人信息处理类型

7.1特殊的个人信息处理类型概述

本章给出了向境外提供和终止等3类特殊的个人信息处理类型的扩展要求。这些个人信息处理类型的特殊性是源于其通常不具有独立性，或者可能是若干处理环节的类型化（如向境外提供的实现方式可能是提供、转移、存储至境外等），或者是作为一个个人信息处理生命周期中的终点（如删除、停止运营等）。这些特殊性使得第5章给出的维度和指标并非全部适用，而仅适用其中一个或若干个维度和指标。

本章的结构安排如下：

本章的每个一级条标题区分了特殊的个人信息处理类型，如“7.2 向境外提供”、“7.3 终止”等。

每个一级条标题项下的第一个二级条标题是概述，描述了该特定的个人信息处理类型在合规要求方面的特殊性，以及由此导致的在法律合规性评估中的主要关注点。

第二个二级条标题开始给出适用于该特定个人信息处理类型并且具有扩展要求的指标所属的维度名称，然后在该二级条标题项下的三级条标题给出具体指标的扩展要求。

7.2向境外提供

7.2.1向境外提供概述

向境外提供个人信息的具体实现方式可能是向境外提供、转移、存储至境外等。当向境外提供个人信息涉及提供、转移、存储等环节时，适用第5章给出的维度、指标及其相应的特定处理环节扩展要求。

在法律合规性评估中被评估方涉及向境外提供个人信息的，除相应特定处理环节的要求外，特殊的关注要点主要包括合法维度、目的限制维度、公开透明维度、告知维度、选择维度、可问责性维度等。

7.2.2合法维度

7.2.2.1程序合法指标（5.2.4）向境外提供环节扩展要求

扩展要求：

将在中国境内运营中收集和产生的个人信息向境外提供的，应遵循可适用的法的程序要求，尤其包括必要的安全评估程序和批准程序。

注：宜留意，可适用的法可能对特定个人信息处理者或者对特定个人信息处理者所处理的个人信息设定安全评估等程序要求，例如，关键信息基础设施运营者和达到可适用的法规定数量的个人信息处理者，又如，国家机关处理的个人信息。可适用的法也可能对向特定境外接收方的提供设定批准程序，如《个人信息保护法》第41条规

定的向外国司法或执法机构提供存储于境内的个人信息。

7.2.2.2类型合法指标（5.2.5）向境外提供环节扩展要求

扩展要求：

可适用的法禁止向境外提供特定类型的个人信息的，不应向境外提供该个人信息类型。

7.2.3目的限制维度

7.2.3.1最小必要指标（5.4.2）向境外提供环节扩展要求

扩展要求：

a） 跨境传输的个人信息类型应与跨境传输的目的或业务功能直接相关；
b） 向境外自动传输的个人信息频率应是向境外传输目的所需的最小频率；
c） 向境外传输的个人信息数量应是实现向境外传输目的所需的最小数量。

7.2.4公开透明维度

7.2.4.1信息充分指标（5.5.2）向境外提供环节扩展要求

扩展要求：

个人信息处理者所公开的与其个人信息处理政策与实践有关的充分信息：
a） 应包括是否涉及向境外提供个人信息，包括跨境传输和跨境提供、转移；
b） 如有，应根据信息充分指标特定环节扩展要求包含相关信息。

7.2.5告知维度

7.2.5.1同步告知指标（5.6.4）向境外提供环节扩展要求

扩展要求：

个人信息处理者向境外提供个人信息的同步告知：
a） 应在提供前的合理期限内一次性或分阶段作出；
b） 应包含以下最密切相关信息：
    1） 境外接收方的名称或者姓名、联系方式；
    2） 个人信息的类型；
    3） 向境外提供的目的和提供方式；
    4） 境外接收方的后续处理目的和处理方式；
    5） 向境外接受方行使合法权益的方式和程序等规则。

7.2.6选择维度

7.2.6.1选择同意指标（5.7.2）向境外提供环节扩展要求

扩展要求：

向境外提供个人信息，应获得个人信息主体以单独和明示方式作出的选择同意。根据向境外提供的方式，选择同意还应满足特定环节扩展要求。

7.2.6.2选择退出指标（5.7.3）向境外提供环节扩展要求

扩展要求：

向境外提供个人信息，应向个人信息主体提供选择退出机制，如撤回同意。

7.2.7可问责性维度

7.2.7.1文件管理指标（5.11.4）向境外提供环节扩展要求

扩展要求：

应妥善留存向境外提供个人信息有关的合同、境外接收方清单和相关日志或记录。

7.2.7.2影响评估指标（5.11.6）向境外提供环节扩展要求

扩展要求：

计划向境外提供个人信息的，应在首次向境外提供前以及在此后定期进行个人信息保护影响评估。

注：向境外提供个人信息时的保护影响评估的内容，应遵守可适用的法以及相关国家标准。

7.3终止

7.3.1终止概述

完整的个人信息处理生命周期由个人信息的收集开始，并以个人信息的删除、销毁、匿名化等方式终止。终止仅是对个人信息处理中一个阶段的描述，其中可能包含删除、销毁、匿名化等个人信息处理操作。导致个人信息处理终止的原因可能是多方面的，例如，因个人信息主体选择退出、行使删除权、存储期限届满，又如个人信息处理者破产且无承接方、清算，停止运营其产品或服务等，均可能导致个人信息处理的终止。

在法律合规性评估中对个人信息处理终止环节的关注点仅在于告知维度、安全保护维度和可问责性维度。

7.3.2告知维度

7.3.2.1事件告知指标（5.6.3）终止环节扩展要求

扩展要求：

当个人信息处理者停止运营其产品或服务时，应及时将停止运营的通知以逐一送达或公告的形式通知个人信息主体。

7.3.3安全保护维度

7.3.3.1安全保护能力指标（5.10.2）终止环节扩展要求

扩展要求：

a） 删除个人信息的，个人信息处理者应确保删除是彻底和不可逆的；

注1：应采取技术、管理或其他必要措施避免在执行删除的过程中无意地创建副本或保留备份。

注2：删除意味着从实现日常业务功能所涉及的系统中去除个人信息，使其保持不可被检索、访问的状态。个人信息处理者有合法性基础继续持有个人信息的，如履行可适用的法规定的义务等，可在确保日常业务功能所涉及的系统中去除，而在另外的存档系统中保留。

b） 销毁个人信息的，应建立基于数据分类分级的数据销毁机制，并明确销毁方式和销毁要求；

c） 应在境内对数据进行删除或销毁。

7.3.4可问责性维度

7.3.4.1合规管理体系指标（5.11.2）终止环节扩展要求

扩展要求：

a） 应有明确的删除、销毁或匿名化的制度、规章或组织流程或操作规程，要求相关部门或人员在终止个人信息前安全删除或匿名化个人信息；

b） 这些制度、规章、组织流程或规程，应能够涵盖以下情形下的个人信息处理终止和删除、销毁或匿名化：

1） 执行个人信息主体的选择退出，如撤回同意；

2） 执行个人信息主体的删除请求；

3） 存储期限届满；

4） 委托处理终止；

5） 用于个人信息处理的信息处理设施或信息系统被退出使用；

6） 组织终止；

7） 个人信息处理者停止运营产品或服务。

7.3.4.2文件管理指标（5.11.4）终止环节扩展要求

扩展要求：

个人信息处理者应妥善留存终止个人信息处理时采取删除、销毁、匿名化等操作的相关日志或记录。

附 录A
（资料性附录）
合规框架

通用要求（维度/指标）	特定处理环节的扩展要求						特殊的个人信息处理类型	
	收集	使用	存储	公开	提供	转移	向境外提供	终止
5.2合法维度	6.2.2	6.3.2	6.4.2	6.5.2	6.6.2	6.7.2	7.2.2	
5.2.2合法性基础指标	6.2.2.1	6.3.2.1	6.4.2.1	6.5.2.1	6.6.2.1	6.7.2.1		
5.2.3主体合法指标	适用	适用	6.4.2.2	适用	适用	适用		
5.2.4程序合法指标			适用				7.2.2.1	
5.2.5类型合法指标			6.4.2.3	6.5.2.2			7.2.2.2	
5.2.6来源合法指标	6.2.2.2	6.3.2.2	适用	适用				
5.3目的明确维度	6.2.3	6.3.3	6.4.3	6.5.3	6.6.3	6.7.3		
5.3.2目的具体/特定指标	适用	适用	适用	6.5.3.1	适用	适用		
5.3.3目的明示指标	6.2.3.1			适用				
5.3.4目的合理指标	适用	6.3.3.1						
5.4目的限制维度	6.2.4	6.3.4	6.4.4	6.5.4	6.6.4	6.7.4	7.2.3	
5.4.2最小必要指标	6.2.4.1	适用	6.4.4.1	适用	适用	适用	7.2.3.1	
5.4.3目的兼容指标	适用	6.3.4.1	适用					
5.5公开透明维度	6.2.5	6.3.5	6.4.5	6.5.5	6.6.5	6.7.5	7.2.4	
5.5.2信息充分指标	6.2.5.1	6.3.5.1	适用	6.5.5.1	6.6.5.1	6.7.5.1	7.2.4.1	
5.5.3公开质量指标	适用	适用		适用	适用	适用		
5.5.4公开形式指标								
5.6告知维度	6.2.6	6.3.6	6.4.6	6.5.6	6.6.6	6.7.6	7.2.5	7.3.2
5.6.2政策告知指标	适用	适用	适用	适用	适用	6.7.6.1		

5.6.3事件告知指标			6.4.6.1			适用		7.3.2.1
5.6.4同步告知指标	6.2.6.1	6.3.6.1	6.4.6.2	6.5.6.1	6.6.6.1	6.7.6.2	7.2.5.1	
5.7选择维度	**6.2.7**	**6.3.7**	**6.4.7**	**6.5.7**	**6.6.7**	**6.7.7**	**7.2.6**	
5.7.2选择同意指标	6.2.7.1	6.3.7.1	6.4.7.1	6.5.7.1	6.6.7.1	6.7.7.1	7.2.6.1	
5.7.3选择退出指标	适用	6.3.7.2	6.4.7.2	6.5.7.2	6.6.7.2	6.7.7.2	7.2.6.2	
5.8权益保障维度	**6.2.8**	**6.3.8**	**6.4.8**	**6.5.8**	**6.6.8**	**6.7.8**		
5.8.2合法权益行使机制通用指标	适用	适用	适用	适用	适用	6.7.8.1		
5.8.3查询机制指标					6.6.8.1	适用		
5.8.4获取副本和转移机制指标					适用			
5.8.5更正机制指标								
5.8.6删除机制指标				6.5.8.1	6.6.8.2	6.7.8.2		
5.8.7投诉举报问询机制指标		6.3.8.1		适用	适用	适用		
5.9质量维度	**6.2.9**	**6.3.9**	**6.4.9**	**6.5.9**	**6.6.9**	**6.7.9**		
5.9.1质量指标	适用	6.3.9.1	适用	6.5.9.1	适用	适用		
5.10安全保护维度	**6.2.10**	**6.3.10**	**6.4.10**	**6.5.10**	**6.6.10**	**6.7.10**		**7.3.3**
5.10.2安全保护能力指标	6.2.10.1	适用	6.4.10.1	6.5.10.1	适用	6.7.10.1		7.3.3.1
5.10.3事件管理指标	适用		适用	适用		适用		
5.10.4数据最小化指标		6.3.10.1						
5.11可问责性维度	**6.2.11**	**6.3.11**	**6.4.11**	**6.5.11**	**6.6.11**	**6.7.11**	**7.2.7**	**7.3.4**
5.11.2合规管理体系指标	6.2.11.1	6.3.11.1	适用	6.5.11.1	适用	6.7.11.1		7.3.4.1
5.11.3权责一致指标	适用	适用		适用	6.6.11.1	适用		
5.11.4文件管理指标	6.2.11.2	6.3.11.2	6.4.11.1	6.5.11.2	6.6.11.2	6.7.11.2	7.2.7.1	7.3.4.2
5.11.5合规审计指标	适用	适用	适用	适用	6.6.11.3	适用		
5.11.6影响评估指标		6.3.11.3		6.5.11.3	6.6.11.4	6.7.11.3	7.2.7.2	

附 录B
（资料性附录）
必要性、直接相关和合理关联性测试及示例

个人信息保护并非绝对的，个人信息主体的同意也并非个人信息处理的唯一合法性基础，正如《民法典》第1036条所表明的，在必要时个人信息保护需让位于公共利益和他人的合法利益。个人信息处理对于特定目的或所追求的特定利益而言具有必要性（或直接相关），是援引合同必要处理（5.2.2.2）、人力资源管理必要处理（5.2.2.3）、法定义务必要处理（5.2.2.4）、公共利益必要处理（5.2.2.5）、紧急必要处理（5.2.2.7）或合法利益公平处理（5.2.2.8）作为合法性基础的准入门槛。但必要性本身可能多种含义，其含义可能介于以下两端之间：在其最严格的一端，必要性是指对实现特定目的或特定利益而言“不可避免”“必不可少”，在其最松散的一端，必要性仅仅是指“有助于”实现特定目的或特定利益。在具体场景中确定必要性的含义及其判断标准，宜考虑个人信息处理所涉及的合法性基础，包括个人信息处理者和/或个人信息处理受托人与个人信息主体之间的关系，以及可适用的法为这种关系下的个人信息处理所设定的规则和原则。本资料性附录给出了各种合法性基础场景下的必要性测试及其示例。

B.1法定义务必要处理中的必要性及其示例

法定义务处理中的必要性，是指如果没有该特定的个人信息处理，个人信息处理者和/或个人信息处理受托人将无法履行其特定的法定义务。因此，为确认法定义务必要处理，宜采用的必要条件测试（but-for test）。

常见的法定义务必要的个人信息处理示例如下：

B.1.1实名制服务义务

示例：《中华人民共和国网络安全法》第 24 条第 1 款要求网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

B.1.2反欺诈义务

示例：《商业银行互联网贷款管理暂行办法》（中国银行保险监督管理委员会令[2020]9 号）第 19 条和《互联网保险业务监管暂行办法》（保监发[2015]69 号）第 20 条为商业银行和保险机构规定了反欺诈监控、调查、分析等义务。但不具有可适用的法规定的反欺诈义务的个人信息处理者，为防止身份冒用或其他交易欺诈进行个人信息处理，则需考虑是否存在其他合法性基础。

B.1.3反洗钱义务

示例：《中华人民共和国反洗钱法》第 3 条为金融机构和特定非金融机构规定了反洗钱义务，要求识别客户身份、保存客户身份资料和交易记录。

B.1.4税收征管义务

示例1：支付所得的单位或个人作为个人所得税的扣缴义务人，为办理预扣预缴或汇算清缴收集并向税务机关提供身份证号码或纳税人识别号、收入信息、合同信息等。

示例2：《中华人民共和国电子商务法》第 28 条为电子商务平台经营者规定了向市场监督管理部门报送平台内经营者身份信息的义务，以及向税务部门报送平台内经营者身份信息和与纳税有关的信息的义务。

B.1.5社会保险费申报和缴纳义务

示例：《中华人民共和国社会保险法》（2018 修正）为用人单位规定了为其职工办理社会保险登记、申报和缴纳社会保险费的义务。

B.2公共利益必要处理中的必要性及其示例

为实现公共利益而对个体权利和利益进行的必要侵入，在总体上受到比例原则的约束。比例原则的“手段—目的”分析框架并不要求手段对于目的而言必不可少，而仅要求手段与目的之间具有关联性，即手段“有助于”实现目的。但同时，比例原则的另外两个子原则缓和了相对宽松的关联性要求对个体权利与利益带来的损害程度，即要求存在多个有助于实现目标的可选手段时，采用对个体权利和利益侵入性最小的手段，所选择的手段对个体权利和利益造成的损害与其所要实现的目的之间具有均衡性。

在公共利益必要处理的场景中，特定个人信息处理被作为实现特定公共利益的手段，同样也受到比例原则的约束。在比例原则视域下，个人信息处理（手段）与处理目的之间的关系不宜采用最严格的必要条件测试（but-for-test），而是更接近于“有助于”实现特定目的或特定利益一端。

但同时，公共利益处理中的必要性测试，宜留意个人信息处理是否的确是基于“具体的”和“迫切的”公共利益的需要，而不是仅仅抽象地指向某个公共利益。公共利益处理中的必要性测试并非是对所要实现的公共利益本身是否足够重要的目的合理性审查，尤其是在可适用的法已经对某些重要的公共利益作出了规定并明确选择了个人信息处理作为追求该公共利益的手段时，宜假定目的合理性和个人信息处理作为手段的适当性已经得到适当评估。因此，在法定义务必要处理中

可适用的法通常将实现某项公共利益的具体职责和权限授予给了国家机关等公共机构，但并不意味着该合法性基础与作为非公共机构的个人信息处理者和/或个人信息处理受托人无关。除个人信息处理者和/或个人信息处理受托人本身作为可适用的法的授权主体之外，许多可适用的法中规定了组织或个人为公共机构履行其职责提供协助和支持的义务。当个人信息处理是可适用的法赋予的职权或权限进行时，

或者（作为个人信息处理受托人）在可适用的法授权主体的控制之下进行时，这些合法性基础是可能被满足的。

公共利益处理中的必要性测试可以考虑以下因素：

——所要实现或维护的公共利益具体而言是什么；

——是否有可适用的法规定了该公共利益的实现或维护方式；

——在具体场景中是否出现了迫切的实现或维护公共利益需要，如问题的严重性、发生时间，社会对该问题的态度或解决问题的需求；

——所采取的个人信息处理是否的确能够解决该公共利益的迫切需要；

——所采取的个人信息处理是否是若干方式中最小损害的；

——所采取的个人信息处理是否确定了清晰的目标和明确的目的；

——评估现有措施和替代措施；

——所涉及的个人信息具有充分性和相关性，而不是过度的；

——确定了明确的持有期限；

——个人信息控制是能够提供相关和充分的理由和论证。

B.2.1国家安全、国防安全、公共安全

国家安全、国防安全、公共安全可构成进行个人信息处理的迫切的公共利益需要。

示例：国家安全的迫切需要的示例，如《国家安全法》第 77 条第 2 项规定了组织和个人及时报告危害国家安全活动的线索、如实提供所知悉的涉及危害国家安全活动的证据、为国家安全工作提供便利条件或者其他协助，向国家安全机关、公安机关和有关军事机关提供必要的支持和协助的一般性义务。当个人信息处理者和/或个人信息处理受托人发现危害国家安全活动的线索或知悉涉及危害国家安全活动的证据时，以及被国家安全机关、公安机关和有关军事机关请求为具体的国家安全工作提供便利条件、支持和协助时，才能视为产生向有权机关提供已经收集的个人信息，或者在有权机关控制之下进行个人信息处理的迫切的需要。

B.2.2犯罪侦查、起诉、审判和执行判决

犯罪侦查、起诉、审判和执行判决，可构成进行个人信息处理的迫切的公共利益需要。通常，犯罪侦查、起诉、审判和执行判决，均由公安机关、检察机关、人民法院和监狱、看守所、未成年犯管教所等执行机关依据法定权限和程序进行。《网络安全法》第28条规定了网络运营者应当为公安机关依法侦查犯罪的活动提供技术支持和协助，《刑事诉讼法》第152条第4款要求有关单位和个人配合公安机关依法采取的技术侦查措施。因此，当个人信息处理是依据犯罪侦查、起诉、审判和执行判决的法定权限，或者在具有法定权限的有权机关控制之下依法进行的，可以构成个人信息处理的合法性基础。

示例1：《刑事诉讼法》第 150 条规定了可以采取技术侦查措施的三种情形。当个人信息处理者和/或个人信息处理受托人被有权机关要求配合技术侦查措施，则需要在有权机关的控制之下进行个人信息处理。但可适用的法（如《刑事诉讼法》第 151-152 条）和技术侦查措施的批准决定可能规定了具体的限制条件，如批准的措施种类、适用对象和期限，并要求采取侦查措施获取的材料，只能用于对犯罪的侦查、起诉和审判，不得用于其他用途；获取的与案件无关的材料必须及时销毁，并要求配合单位和个人予以保密。

示例1：《刑事诉讼法》第 144 条规定了检察机关和公安机关根据侦查犯罪的需要，可以依照规定查询、冻结犯罪嫌疑人的存款、汇款、债券、股票、基金份额等财产，有关单位和个人应当配合。当个人信息处理者和/或个人信息处理受托人被有权机关要求配合查询和冻结，则需要在有权机关的控制之下提供查询和冻结。

示例2：《反恐怖主义法》第 50 条规定公安机关调查恐怖活动嫌疑，可以依照有关法律规定……可以提取或者采集肖像、指纹、虹膜图像等人体生物识别信息和血液、尿液、脱落细胞等生物样本，并留存其签名。第 51 条规定，公安机关调查恐怖活动嫌疑，有权向有关单位和个人收集、调取相关信息和材料。有关单位和和个人应当如实提供。

B.2.3公共卫生领域的公共利益

传染病防治可构成个人信息处理所追求的公共卫生领域的公共利益。

示例1：《传染病防治法》第 31 条规定任何单位和个人发现传染病病人或者疑似传染病病人时，应当及时向附近的疾病预防控制机构或者医疗机构报告。发现传染病病人或者疑似传染病病人构成迫切需要，向疾病预防控制机构或医疗机构报告是个人信息处理目的，所必要的个人信息处理包括提供。但在发现传染病病人或者疑似传染病病人之前，迫切需要并不存在。

示例2：《结核病防治管理办法》第 8 条和第 9 条分别规定了结核病定点医疗机构和非定点医疗机构在结核病防治工作中履行的职责。结核病定点医疗机构的职责包括负责肺结核患者报告、登记和相关信息的录入工作，对传染性肺结核患者的密切接触者进行检查等；非结核病定点医疗机构的职责包括负责结核病患者和疑似患者的转诊工作。结核病定点医疗机构和非定点医疗机构在履行该法定职责时，需要进行的个人信息处理是必要的，并且在流动人口肺结核患者转出地和转入地结核病定点医疗机构之间交换该患者的信息，以确保落实患者的治疗和管理措施（第 30 条）；基层医疗机构应当对居家治疗的肺结核患者进行定期访视、督导服药等管理。但上述法定职责的必要中不包含故意泄露涉及肺结核患者、疑似肺结核患者、密切接触者个人信息的有关信息、资料。

示例3：根据《突发公共卫生事件应急条例》，突发公共卫生事件，是指突然发生、造成或者可能造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒以及其他严重影响公众健康的事件。国家建立了突发事件应急报告制度。《突发公共卫生事件应急条例》第 40 条规定了传染病爆发、流行时，街道、乡镇以及居民委员会、村民委员会协助卫生行政主管部门和其他有关部门、医疗卫生机构进行疫情信息的收集和报告。

示例4：要求填写个人健康申报表。收集联防联控所必需的个人信息，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上的歧视。为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。鼓励有能力的企业在有关部门的指导下，积极利用大数据，分析预测确诊者、疑似者、密切接触者等重点人群的流动情况，为联防联控工作提供大数据支持。

B.2.4其他重大公共利益

示例：如《通信短信息服务管理规定》第17条规定，短信息服务提供者按照有关部门的提前申请或在紧急情况下，应根据电信管理机构的协调向其用户发送公益性短信息，尤其是涉及自然灾害、事故灾难、公共卫生事件和社会安全事件预警和处置等应急公益性短信息。自然灾害、事故灾难、公共卫生事件和社会安全事件预警和处置是公共利益的迫切需要，利用个人联系方式向其发送应急性短信息宜被确定为是必需的。

B.3最小必要指标中的直接相关测试与合同必要处理、人力资源管理必要处理中的必要性测试

个人信息处理的必要原则以及在最小必要指标（5.4.2）中的“必要”一词，在《个人信息保护法》第6条中被进一步表述为是个人信息处理与处理目的直接相关。如上所述，必要或必需的含义可能介于对实现特定目的或特定利益而言“不可避免”“必不可少”到“有助于”实现特定目的或特定利益之间。相比于法定义务必要处理中的必要条件测试（but-for-test）和公共利益必要处理中依据比例原则综合考虑个人信息处理作为手段的适当性，关于最小必要指标中的必要性或直接相关，现有的标准化文件采取了相对较宽松的标准。

涉及最小必要指标的直接相关测试已经在现有标准化文件（如GB/T 35273—2020，5.2 a)和附录C.2；TC260-PG-20191A《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》（v.1.0-201906））中得到了丰富的阐释和发展。作为运用在私法意思自治领域的概念，直接相关测试可以具有比法定义务必要处理中的必要性测试相对宽松的范围，在意思自治得到确实保障（如选择维度）前提下，需要更多地尊重在市场中的需求、习惯与通用实践。

同样地，合法性基础中的合同必要处理和人力资源管理必要处理，尽管采用的表达为履行、订立合同或人力资源管理的“必要”，但更适宜采用最小必要指标中的直接相关测试。宜考虑合同的实质和根本目标，个人信息主体对产品或服务的根本期待和最主要需求。个人信息处理须是为合同的正常履行最小必要的，如为了向员工支付工资必要的银行账户信息收集、持有和提供。但为了查证员工是否违反劳动合同中的义务，如保密、竞业禁止或工作职责，或采取法律诉讼等行动而访问员工邮箱、终端设备中的上网信息或查询员工财产信息，则不属于本项所指必要范围，从而需考虑是否存在其他合法性基础。当然在考虑合同必要处理的必要性时，也可以考虑合同的明确约定和附随义务。

产品或服务基本业务功能及其必要的个人信息处理，可参考GB/T 35273—2020附录C.2和TC260-PG-20191A《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》（v.1.0-201906）给出的指引。

示例1：为了向个人信息主体交付其在电子商务网站购买的产品，将个人信息主体的姓名或昵称、手机号码、地址等信息提供给承运商，是为了履行买卖合同而必要的。

示例2：为了应个人信息主体的请求与之订立合同而必要的个人信息处理的例子，如为了应个人信息主体的请求与之订立贷款合同，评估借款人还款能力和授信审批而必要的个人财产或信用信息收集；为了应个人信息主体的请求与之订立保险合同，评估保险费用或提供保险咨询所必要的个人信息收集。

示例3：为了向个人信息主体提供产品或服务的基本业务功能而必要的个人信息处理的例子，如对于一款将自身服务定位和宣传为个性化展示新闻资讯或短视频的移动应用程序而言，个性化展示属于基本业务功能，为此收集用户在该移动应用程序中关注的账号列表、标签或浏览操作记录，用来分析用户兴趣并进行个性化展示。但读取其他移动应用程

序或用户终端设备中的浏览操作记录、购物记录等，则不宜认定为基本业务功能必要的个人信息处理，从而需考虑是否存在其他合法性基础。

B.4目的兼容指标中的合理关联测试

确定后续处理目的是否与收集目的具有合理关联的测试方法，可以是从最初收集目的出发的形式测试，即考察根据通用实践和通用理解收集目的是否明显或默示地涵盖后续处理目的；也可以是多因素平衡测试以确定后续处理目的是否与最初收集目的相兼容。

B.4.1形式测试方法

形式测试方法相对简单，但所识别的合理关联范围相对严格。

示例1：最初收集目的是金融机构基于履行反洗钱义务的必要进行客户身份信息留存，将大额交易和可疑交易信息与该客户身份信息报告给中国反洗钱分析中心，是《反洗钱法》明确规定的后续处理。无论个人信息主体是否实际知晓该规定，或者个人信息处理者是否明示该后续处理，此类后续处理是收集目的明显涵盖的。

示例2：如果网络运营者履行通讯或信息发布服务实名制义务而收集的真实身份信息，后续被用于找回密码、开通新业务功能、个人信息主体合法权益请求的受理或反馈等场景下的用户身份核验，无论是否在收集时逐一明示所有此类场景，鉴于真实身份核验这一关联性，应视为收集目的所隐含的后续处理。

B.4.2多因素平衡测试方法

多因素测试方法相对复杂，但可以通过后续处理对个人信息主体的影响和适当保护措施“补偿”对最初收集目的的偏离度，从而使所识别的合理关联范围相对宽泛和灵活。

多因素平衡测试宜充分考虑以下因素：

a） 后续处理目的与最初收集目的之间的关联性程度；

b） 个人信息主体的合理预期：如结合个人信息被收集时的具体背景和个人信息处理者与个人信息主体之间的关系，后续处理目的是否符合个人信息主体的合理预期；

c） 后续处理所涉及的个人信息的类型，尤其是是否涉及敏感个人信息；

d） 后续处理对个人信息主体可能带来的正面的或负面的影响；

e） 是否存在适当的保护措施，例如，使信息系统功能分离，采用最小化技术或访问最小化控制等。

B.4.3示例

对于已经收集的个人信息，以下后续处理目的通常宜视为具有合理关联，但受制于具体处理方式和适当保护措施：

——已经建立的客户关系的管理，前提是对于利用所收集的个人信息与客户进行联系时提供选择退出机制；

——履行监管部门的合规要求；

——个人信息处理者的内部的行为审计、安全和防止欺诈；

——个人信息处理者内部的大数据统计、分析和研究；

——依法行使个人信息处理者对个人信息主体享有的法律权利，如债权、知识产权等。

对于已经收集的个人信息，以下后续处理目的通常不宜视为具有合理关联，但受制于具体处理方式和适当保护措施：

——与尚未建立合同或服务关系的个人信息主体进行营销联系；

——用户画像、精准营销广告、对个人产生影响的自动化决策；

——向第三方提供、转移或公开。

附 录C
（资料性附录）
合法利益的多因素平衡测试方法及示例

C.1合法利益的识别

利益是相关方对个人信息处理所享有的利害关系或从个人信息处理中获得的收益。合法利益是可以被法律所承认或保护的利益。个人信息处理者所识别的合法利益不宜过于宽泛，如仅仅宽泛地表明为了组织业务的发展、提高服务品质等，宜具体表明如开发某项新的业务，或改进某项现有产品或服务的某项功能。符合本项的合法利益不宜是过于远期的计划或设想，如为了促进组织向大数据平台的业务转型或探索数据商业化利用等。

个人信息处理所追求的合法利益的类型（如经营自由、表达自由、财产权等基本权利与自由，或者经济利益、竞争利益等）、属性（如仅仅是个人信息处理者或第三方的个体利益，还是也服务于更广泛的公众或社会利益）以及合法利益得到法律、文化、社会普遍承认的程度。

个人信息主体的合法利益宜被尽可能全面考虑和宽松解释，尤其不宜理解为仅包含个人信息权和隐私权。例如，个人信息处理者收集和使用个人购物信息所追求的合法利益可能是更好地了解用户偏好和满足用户需求以提高利润，个人信息主体通过该个人信息处理获得的收益可能是降低搜寻成本以提高消费者剩余，但同时也可能面临因歧视性定价或杀熟等策略付出更高价格的风险。当这一风险确实发生，则可能对个人信息主体的合法利益造成不合理的损害。

应具体识别个人信息处理对个人信息主体的合法利益带来的影响，包括正面影响和负面影响。

C.2合法利益的比较

合法利益公平处理（或合理使用）就其本质而言是基于具体场景的多因素利益平衡，即个人信息处理并非基于5.2.1.1-5.2.1.8的合法性基础时，仍然可能存在合法利益公平处理的合法性基础。当决定援引合法利益公平处理作为合法性基础时，宜尽可能全面地考察与个人信息处理有关并影响个人信息主体合法利益的所有因素：

——所涉及的个人信息的类型与特点，如所处理的个人信息是否为私密信息等隐私，或者是敏感个人信息，或者是具有社会属性的姓名、电话号码等，是否曾被公开；

——所涉及的个人信息处理的方式与特点，如个人信息处理是否为长期的、频繁的、涉及大范围个人信息主体的、大量的，或者是临时的、偶然或一次性的、涉及小范围个人信息主体的、少量的；是否会涉及个人信息的公开、提供或转移、跨境转移等；

——个人信息主体在个人信息被收集时的合理预期，如根据个人信息被收集时提供的信息或具体场景，个人信息主体是否可能合理预见到该个人信息处理；

——个人信息处理者和个人信息主体的地位和关系，如个人信息处理者是否为提供公共服务的组织；所涉及的个人信息主体是否为儿童或老年人，或者是否为个人信息处理者的客户、员工或其他相关方。

采取个人信息保护措施可以降低这些损害的规模或其发生概率，个人信息处理者可以通过其采取的个人信息保护措施论证其个人信息处理不会对个人信息主体的合法利益造成不合理的损害。

附 录D
（资料性附录）
比例性测试及示例

个人信息处理法律合规性评估语境下，至少存在两种比例性测试：

D.1合法性基础指标中的比例性测试

在公共利益处理中，为了实现公共利益所采取的手段（即个人信息处理）对个人信息主体权利的侵害性与所要追求的目的而言，应当是成比例的。这是公法中比例原则的体现，在合法性基础的比例性测试中宜予以考虑。

D.2告知与选择维度中的比例性测试

告知与选择维度的比例性测试则更偏向于在私法领域的成本-收益分析，即所付出的成本就所要实现的收益而言是成比例的。否则，当成本过高而超出收益时，一般没有理由继续进行这种个人信息处理。如果个人信息处理者的个人信息处理产生未能内部化的社会收益，即外部收益，则通常宜考虑如果逐一告知或选择同意的要求对于某些产生外部收益的行为而言负担过重，原本对社会有利可图的信息处理可能受到抑制，例如，较为典型的情形是学术研究。成本-收益比例性的另一种考虑可以是，相比于个人信息处理对个人信息主体带来的影响和效果而言，机械适用逐一告知或选择同意将给个人信息主体带来不成比例的成本。这些比例性测试不可能在所有情形下都实现严格的量化，这种要求本身就会带来不成比例的成本。

但在比例性测试中可以特别考虑以下因素：所涉及的个人信息主体的数量、个人信息的年代，可能表明更高的搜寻成本。所采取的保护措施，如个人信息保护影响评估、数据最小化技术、收集和存储期限最小化等，可以有效降低个人信息处理对个人信息主体带来的影响和效果，从而补偿不提供同步告知导致的风险。

附 录E
（资料性附录）
风险评估方法及示例

E.1风险管理维度的风险评估

适当的信息安全保护水平，应考虑现有技术、实施的成本，个人信息处理的性质、范围、环境和目的，以及对个人权利和自由的风险的变动的可能性与严重性，例如未经授权的或不合法的处理，以及意外丢失、毁损或破坏。

E.2事件告知维度的风险评估

事件告知维度中的风险评估，即个人信息安全事件或其他个人信息处理违规给个人信息主体带来的后果评估，目的是为了确定是否需要向个人信息主体进行事件告知，以及指导个人信息处理者和/或个人信息处理受托人采取适当的补救措施。

风险评估通常可以采用定性和定量的测度，或者两者的结合。但鉴于事件告知维度的风险评估所受到的时间和成本约束，除非个人信息处理者和/或个人信息处理受托人在事前建立的风险评估的模型或方法采用的是定量测度，例如，在组织的信息安全事件报告和处置管理制度、运维管理制度、应急预案等制度文件中，或者在组织的信息安全风险准则或信息安全风险评估过程成文信息（见GB/T 22080—2016，6.12；或者ISO/IEC 27701，5.4.1.2的改进）中，否则个人信息安全事件或其他个人信息处理违规的风险评估不必采用严格的定量测度。

个人信息安全事件或其他个人信息处理违规的风险评估模型或方法，可以参考GB/T 31722—2015、ISO/IEC 27005—2008附录E.2。考虑到信息安全风险评估的关注点在于信息安全事件给组织或其资产带来的风险，在评估个人信息安全事件或其他个人信息处理违规给个人信息主体的合法权益带来的后果大小和可能性时，宜特别考虑以下因素。

E.2.1后果的类型

个人信息安全事件或其他个人信息处理违规的后果包括直接后果和间接后果。直接后果是泄露、篡改、毁损、丢失导致的个人信息本身的保密性、完整性和可用性受损的结果；间接后果是个人信息安全事件所伴生的，如因身份盗用、窃取、诈骗、敲诈勒索、歧视性待遇等导致的财产损失，个人信息保密性、完整性受损带来的名誉损失、精神损害、歧视性待遇等，或者个人健康生理信息、财产信息等的可用性受损导致的生命、健康损害或机会损失等。对于间接损失，从责任追究的目的而言，个人信息安全事件或其他个人信息处理违规与间接后果之间的因果关系是必须得到证明的，但就进行风险评估以确定是否有必要向个人信息主体进行事件告知（尤其是事件告知的主要目的是警示和降低后果）而言，则宜尽可能宽松地考虑因果关系，以对可能的后果进行更全面的考虑。

E.2.2影响后果大小和可能性的因素

个人信息安全事件或其他个人信息处理违规为个人信息主体的合法权益带来的风险程度取决于两个变量，即后果及其可能性。以下因素可能影响个人信息安全事件或其他个人信息处理违规为个人信息主体的合法权益带来的后果大小和可能性。

a） **个人信息安全事件或其他个人信息处理违规的类型**

通常情况下，保密性受损的泄露可能比完整性或可用性受损的篡改、毁损、丢失带来更严重的后果。但即使是同样的个人信息泄露，当未经授权的接收者或访问者是特定的人或组织时，通常更容易采取返还、销毁等补救措施，从而有效降低个人信息安全事件或其他个人信息处理违规给个人信息主体带来后果的可能性。

b） **所涉及的个人信息的类型、敏感性和规模**

通常个人信息的类型越是具有敏感性，可能导致的后果越严重。如敏感个人信息的定义本身是根据一旦泄露、非法提供或滥用可能造成的危害后果界定的。即使是一般的个人信息，当个人信息安全事件或个人信息处理违规涉及的是多种类型或巨大规模的个人信息时，也可能带来比单一类型或少量个人信息带来更严重的后果。在个人信息泄露的情形下，经加密、假名化等去标识化的个人信息，通常可以降低个人信息安全事件或其他个人信息处理违规给个人信息主体带来后果的可能性。

c） **所涉及的个人信息主体的类型和规模**

个人信息安全事件或其他个人信息处理违规所涉及的个人信息主体人数众多时，通常可能带来更严重的后果，但少数个人信息主体的高度敏感的个人信息类型可能对受影响的个人信息主体带来严重后果。当个人信息主体是儿童或其他弱势人群，如容易受到电信诈骗影响的群体，通常可能具有更高的可能性。

d） **个人信息处理者和/或个人信息处理受托人的类型和已采取的措施**

通常个人信息处理者和/或个人信息处理受托人的身份类型将体现个人信息安全事件或其他个人信息处理违规所涉及的个人信息类型、敏感性、规模、个人信息主体的类型和规模，例如，医疗机构、金融机构、电信运营商等。个人信息处理设施或信息系统本身是否为关键信息基础设施或其信息系统的等级评定结果可能提供了有关信息，但宜考虑上述评定并非完全聚焦于对个人信息主体的后果，而主要考虑社会性的影响。个人信息处理设施或信息系统本身的等级评定也可能提供了有关个人信息处理者和/或个人信息处理受托人在个人信息安全事件发生前已经采取的信息安全保护措施，如加密、备份等，这些信息安全保护措施的存在可以较为有效地降低后果的可能性。

e） **已采取的补救措施**

个人信息安全事件或其他个人信息处理违规发生后，个人信息处理者和/或个人信息处理受托人采取的补救措施可能已经有效降低对个人信息主体带来的后果大小或可能性。例如，已经从备份中恢复毁损或丢失的个人信息，已经联系未经授权的接收者采取适当的返还或销毁措施等。个人信息安全事件或其他个人信息处理违规的风险评估应考虑采取补救措施后的剩余风险。

f） **已被报告的案例**

个人信息安全事件或其他个人信息处理违规发生后，如果个人信息处理者和/个人信息处理受托人通过个人信息主体的询问、投诉或其他渠道获悉，已经出现多起因个人信息安全事件导致的身份冒用、诈骗、敲诈勒索、经济损失等案例，结合本次个人信息安全事件或其他个人信息处理违规所涉及的个人信息主体规模，可以较为简易地测算后果的可能性，但应考虑被报告的案例很可能明显低于实际发生的案例。尤其是，当已经有上述迹象表明后果的可能性较高，且所涉及的个人信息主体规模较大，不管已被报告的案例是否造成的实际损失或其大小，个人信息处理者和/或个人信息处理受托人宜尽快发出事件告知，以警示个人信息主体避免进一步的损失。

E.2.3后果评价

个人信息处理者和/或个人信息处理受托人应在其信息安全风险准则、信息安全事件报告和处置管理制度、运维管理制度、应急预案等制度文件中补充，或者单独制定个人信息安全事件或其他个人信息处理违规对个人信息主体带来后果的分级，以确定严重等级。严重等级宜参照信息安全事件给组织带来的风险分级，如组织的重要数据或客户数据测度。可适用的法或监管部门对个人信息安全事件或其他个

人信息处理违规规定了分级要求的，个人信息处理者和/或个人信息处理受托人确定的分级应符合可适用的法或监管部门的要求。

如果个人信息处理者和/或个人信息处理受托人没有可供参照的信息安全事件给组织带来的风险分级，如其信息安全事件报告和处理管理制度、运维管理制度、应急预案等制度文件仅参照信息安全事件的社会影响分级，宜参照确定是否已构成等级为较大或较严重（含）以上。所涉及的个人信息类型为敏感个人信息时，除非有F.2.2所述的其他因素明显降低后果的大小或可能性，否则宜推定较大或较严重的信息安全事件很可能给个人信息主体的合法权益带来严重后果并应进行事件告知。

T/CLAST

团　体　标　准

T/CLAST 002.3—2021

个人信息处理法律合规性评估指引
第3部分：实施指南

Guidelines for legal compliance assessment of personal information processing—
Part 3：Implementation guidance

2021-12-06 发布　　2022-01-01 实施

中国科学技术法学会发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国科学技术法学会提出并组织专门机构归口管理。

本文件主要起草单位：中国科学技术法学会、深圳市北鹏前沿科技法律研究院、中国法学交流基金会、中国法律咨询中心、北京大学法学院/知识产权学院、北京大学粤港澳大湾区知识产权发展研究院、平安科技（深圳）有限公司、上海携程商务有限公司、北京小桔科技有限公司、阿里巴巴(北京)软件服务有限公司、每日互动股份有限公司、深圳市和讯华谷信息技术有限公司、广东北源律师事务所、上海市锦天城律师事务所、北京市浩天信和律师事务所、北京市金杜律师事务所、中国信息通信研究院云计算与大数据研究所、北京北大英华科技有限公司、网易(杭州)网络有限公司、腾讯科技（深圳）有限公司、荣耀终端有限公司、华米科技、OPPO 广东移动通信有限公司、比亚迪股份有限公司、广州小鹏汽车科技有限公司、深圳市大疆创新科技有限公司、深圳市地铁集团有限公司、上海游昆信息技术有限公司、贝壳找房（北京）科技有限公司、深圳市迷你玩科技有限公司、百行征信有限公司、深圳依时货拉拉科技有限公司、广东小天才科技有限公司、安信证券股份有限公司、深圳市安证企业合规管理（集团）有限公司、杭州安信检测技术有限公司、杭州安恒信息技术股份有限公司、深圳市网安计算机安全检测技术有限公司。

本文件主要起草人：张平、毕马宁、南红玉、黄亚英、肖声高、徐美玲、时建中、李玉香、周辉、涂俊峰、谈建、周涛、任晓明、李伟民、崔亚冰、王心阳、赵怡冰、辜凌云、徐子淼、姬祥、牟晋军、周林、秦齐祺、张娜、徐彩曦、张铮、陈津来、陈光炎、植吕梅、梁艳芬、吴卫明、丁峰、田劼、冯红、吴涵、何为、李青、赵紫钰、包一明、石霖、何远琼、李川东、蒋仁熙、梁淳栋、孙海鸣、武杨、张辉、吴迪、王辉、彭星、高凤、杨小娟、林森才、许艳冰、林莹、彭伟、叶娟、白宝龙、张朝、谢晓勇、罗经华、覃江林、白雷、周俊华、陈天伟、李维春、李旻瑞、李良、龙军、黄伟杰、江鑫、洪跃腾、王水兵、何冠辉、杜文琦、倪荣、刘志乐、吴俊雄。

本文件由中国科学技术法学会、深圳市北鹏前沿科技法律研究院负责解释。

个人信息处理法律合规性评估指引　第3部分：实施指南

1　范围

本文件描述了个人信息处理法律合规性评估的基本原则和过程，给出了个人信息处理法律合规性评估的基本原则和法律合规性评估过程概述，对从项目启动阶段、计划准备阶段、现场实施阶段到评估法律意见书阶段所需进行的活动提供了相应的指引。

本文件适用于各种类型的组织对其个人信息处理的合规状态或合规能力进行第一方评估和管理，个人信息相关方为采购、监管等特定目的进行的第二方评估，以及评估机构进行的第三方法律合规性评估和咨询。

2　规范性引用文件

下列文件中的内容通过本文件中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅注日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/CLAST 002.1-2021　个人信息处理法律合规性评估指引　概述和术语

T/CLAST 002.2-2021　个人信息处理法律合规性评估指引　合规框架

3　术语与定义

T/CLAST　002.1-2021中界定的或规范性引用的术语和定义适用于本文件。

4　概述

本文件描述的法律合规性评估基本场景是由第三方评估机构受委托实施的第一方评估、第二方评估或第三方评估，并且被评估方是初次进行法律合规性评估。当被评估方并非初次进行法律合规性评估时，第三方评估机构可以根据实际情况调整部分活动。由第三方评估机构以外的组织自行实施第一方评估和第二方评估时，评估委托方宜理解为组织的管理层，并可以根据实际情况调整适用。

本文件的结构安排如下：

第5章　明确法律合规性评估的基本原则

第6章　对法律合规性评估过程进行总体概述

第7章　项目启动阶段

第8章　计划准备阶段

第9章　现场实施阶段

第10章　评估法律意见书阶段

5　基本原则

5.1 概述

个人信息处理法律合规性评估需要遵循一定的基本原则。该基本原则是个人信息处理法律合规性评估能够得到公平客观的、对法律合规性评估目的而言有意义的评估结论的前提，也是确保相同或不同的评估主体在多个项目或多次法律合规性评估中得出可比较、可问责的评估结论的前提。

5.2 独立

无论采用何种评估模式，所选择的评估员应被确保相对于评估对象的独立性，在评估对象中不享有可能影响其法律合规性评估活动与结论的利益或利益冲突，对评估对象不带有偏见。法律合规性评估组的组成、法律合规性评估方案的制定与实施中，应时刻考虑保障评估员的工作不受来自商业、财务和其他压力的影响和干预。

注：不同的法律合规性评估模式对评估员独立性的需求不尽相同。在第一方法律合规性评估中，独立性意味着评估员不应是对作为评估对象的个人信息处理活动的绩效负有直接责任的人员；在第二方法律合规性评估中，宜考虑评估主体自身的要求，如评估主体的采购、执法等廉洁性和独立性保障程序与纪律；在第三方法律合规性评估中，应遵守认证机构的要求和/或第三方评估机构自身的执业纪律。

5.3 客观

法律合规性评估发现和评估结论应基于客观证据和客观评价，并有能力确保事后可被验证和追溯。

评估员和技术专家在法律合规性评估方案的制定与实施中，应避免过度依赖任何一方的陈述等言词证据，在可行的前提下应优先选择物证、书证、音像证据、记录等可靠稳定的客观证据。在法律合规性评估过程中的发现与评估结论均应在有客观证据支持的基础上得出。

5.4 保密

评估员、观察员和协调员应审慎地使用和保护在法律合规性评估中获得的信息，不应以违反保密协议和执业纪律的方式使用法律合规性评估中获得的信息。尤其在第二方评估和第三方评估中，应尊重被评估方的信息安全规定和要求，在法律合规性评估组的组成、法律合规性评估方案的制定与实施中，应时刻考虑信息的沟通、报告方式，不致因法律合规性评估本身导致被评估方保密信息的泄露。

注：在第二方评估和第三方评估中的项目协议与法律合规性评估方案均应事先考虑法律合规性评估中信息的沟通与报告渠道。在确保法律合规性评估的过程与结论可追溯、可被评审的前提下，所获得的客观证据的保管和法律合规性评估法律意见书中的引用宜尽可能考虑被评估方的信息安全需求，并减少法律合规性评估本身带来的风险。

5.5 专业

评估员和技术专家应在所要确定的内容所属领域具备充分的知识、技能和经验以及必要的资格证书。法律合规性评估组的组成应考虑评估员、技术专家等角色的人员在专业能力方面的的互补性。

注：个人信息处理的法律合规性评估本身是一项跨学科的确认活动，无论是确认现状还是确认能力，必不可少的是在法律领域的专业性，客观证据的获取可能有赖于技术专家的支持，尤其是信息技术与信息安全领域的专业性，能力评估还需要考虑经济学或管理学领域的能力。

6 法律合规性评估过程概述

个人信息处理法律合规性评估过程由项目启动阶段（第7章）、计划准备阶段（第8章）、现场实施阶段（第9章）、评估法律意见书阶段（第10章）组成。

第7-10章给出的法律合规性评估过程的描述结构如下：

——每章的第 1 条是概述，给出该阶段所要达到的总体目标、主要输入、活动和输出。

——每章的第 2 个条款开始的每个条款依次给出该阶段主要活动的具体描述，包括该活动的输入、活动、实施指引和输出。

——输入：进行该活动所需的任何信息；通常，上一项活动的输出是本项活动的输入。

——活动：简要描述活动。

——实施指引：为执行该活动提供指引。

——输出：描述了执行完成活动后得到的结果或可交付项，例如一个文件。

——其他信息：提供了可能有助于完成该活动的补充信息，例如，对其他标准的引用。

每一阶段的主要活动和输出，如图1所示。

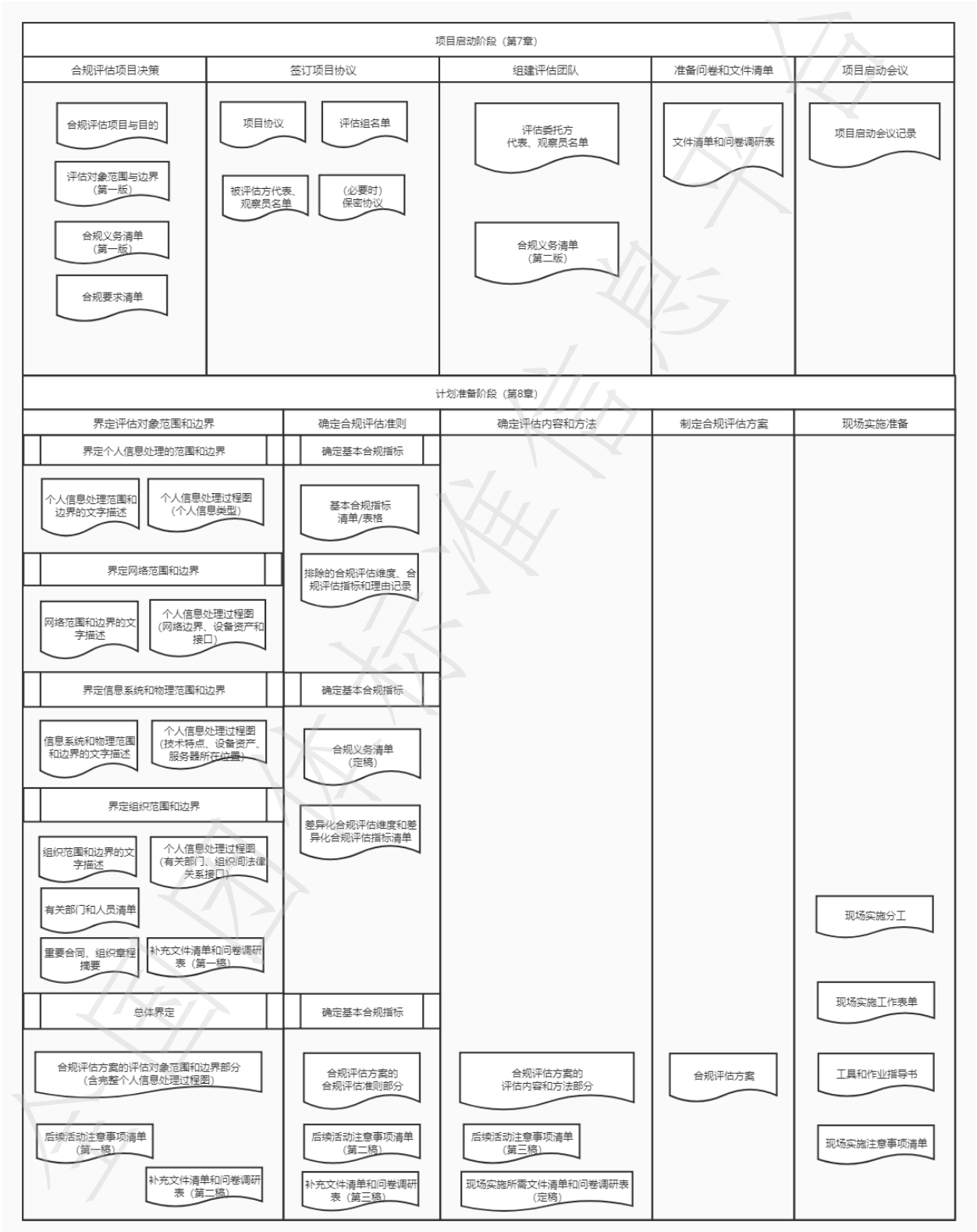
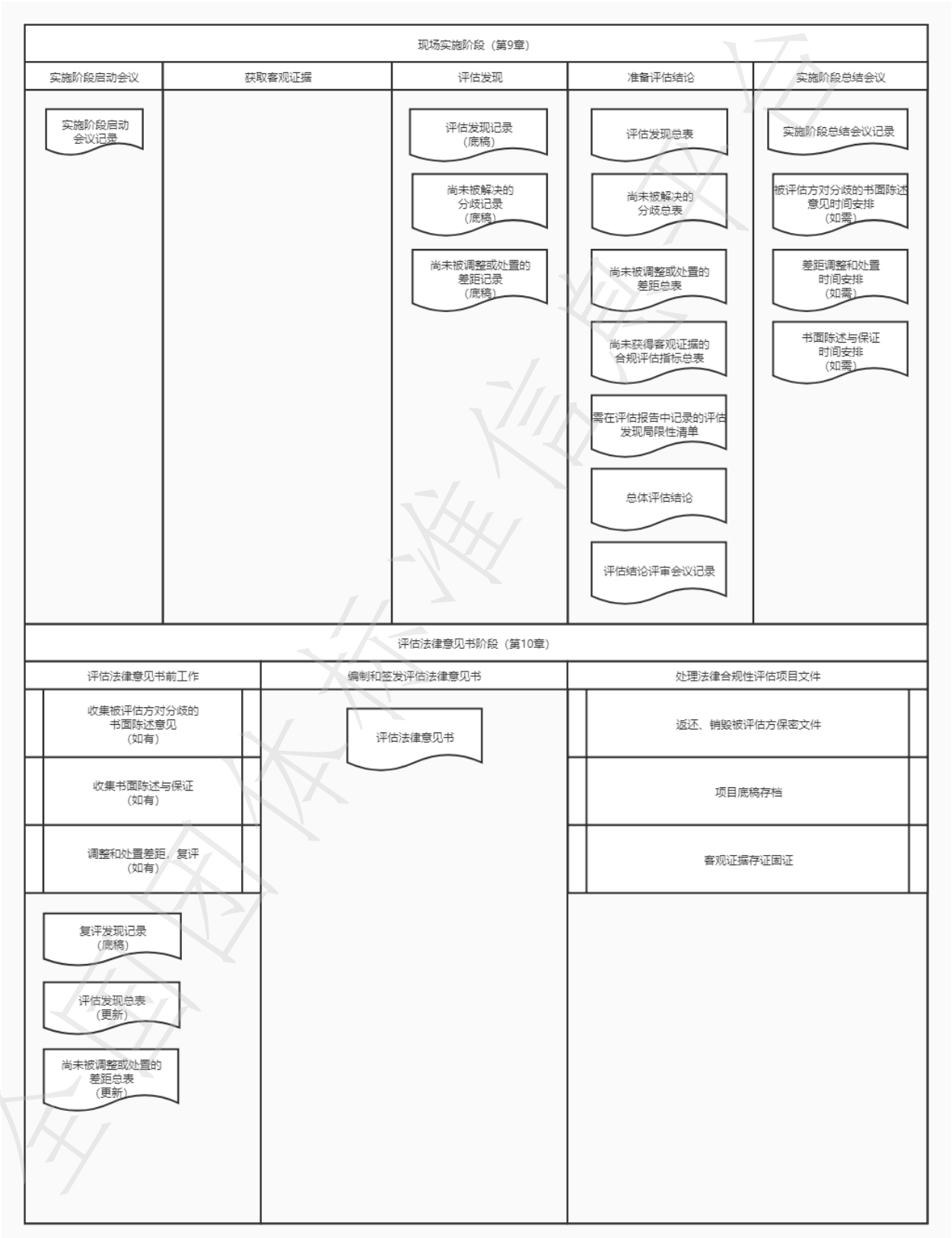


图1　法律合规性评估过程活动与输出


现场实施阶段（第9章）
实施阶段启动会议
获取客观证据
评估发现
准备评估结论
实施阶段总结会议
实施阶段启动会议记录
评估发现记录（底稿）
尚未被解决的分歧记录（底稿）
尚未被调整或处置的差距记录（底稿）
评估发现总表
尚未被解决的分歧总表
尚未被调整或处置的差距总表
尚未获得客观证据的合规评估指标总表
需在评估报告中记录的评估发现局限性清单
总体评估结论
评估结论评审会议记录
实施阶段总结会议记录
被评估方对分歧的书面陈述意见时间安排（如需）
差距调整和处置时间安排（如需）
书面陈述与保证时间安排（如需）
评估法律意见书阶段（第10章）
评估法律意见书前工作
编制和签发评估法律意见书
处理法律合规性评估项目文件
收集被评估方对分歧的书面陈述意见（如有）
收集书面陈述与保证（如有）
调整和处置差距，复评（如有）
评估法律意见书
返还、销毁被评估方保密文件
项目底稿存档
客观证据存证固证
复评发现记录（底稿）
评估发现总表（更新）
尚未被调整或处置的差距总表（更新）

7 项目启动阶段

7.1 概述

法律合规性评估项目启动阶段的主要任务是：

——在评估委托方、第三方评估机构、被评估方代表之间就法律合规性评估的可行性、目标与目的、初步的评估范围达成一致；

——签订评估项目协议；

——组建评估项目组，并确定观察员、协调员等角色指派需求与人选，确认所有人员的选择符合本文件第 5 章的基本原则；

——建立沟通机制，沟通确认法律合规性评估的过程与时间安排，获取为制定法律合规性评估方案所需的文件与信息。

7.2 法律合规性评估项目决策

输入：

对于组织启动法律合规性评估项目的决策与准备有意义的所有信息。

活动：

组织作出启动法律合规性评估项目的决策，选定评估机构和评估组长。

实施指引：

当组织考虑启动法律合规性评估项目时，需提前考虑以下事项并作出决策和准备：

a） 确定组织通过法律合规性评估所要实现的目标与目的；

b） 初步选定法律合规性评估对象，并识别与法律合规性评估对象有关的以下问题：

1） 拟纳入法律合规性评估对象的组织单元；

2） 拟纳入法律合规性评估对象的个人信息处理活动，如产品、服务、过程或其组合；

3） 法律合规性评估对象所涉及的信息处理设施及其所在地点，以确定法律合规性评估组的规模以及是否可能涉及多个地点；

4） 法律合规性评估对象所采用的信息系统和信息资产清单及其技术特点；

5） 所涉及的个人信息~~控制者~~处理者、个人信息处理~~受托人者~~和其他个人信息相关方之间的接口和法律关系，是否有必要将其他组织纳入法律合规性评估范围；

6） 评估对象是否被组织现有的管理体系、信息安全保护能力及其采取的控制措施所涵盖，或法律合规性评估的目的是否是为了改进现有管理体系、信息安全保护能力以使其适应个人信息处理合规的需要。

注：本阶段的初步界定是为了组建适当规模和组成的评估组，评估对象的范围和边界可以在评估组成立后进一步识别和界定。

c） 选择法律合规性评估模式，如第一方评估、第二方评估或第三方评估；

d） 选定评估机构和评估组长；

e） 识别并确定组织的合规义务清单和其他选择纳入评估准则的合规要求清单；

注：组织宜参考T/CLAST 002.1—2021的4.4.3，尽可能详细识别合规义务清单，尤其是组织考虑法律合规性评估的目标和目的选择纳入评估准则的合规要求清单，以便评估组成立后进一步识别和确定评估准则。

f） 评估委托方应在启动法律合规性评估项目决策前确定法律合规性评估的可行性，尤其是被评估方的充分合作、法律合规性评估方案的制定所需的充分和适当的信息、时间和资源的可获得性。评估委托方应保障被评估方能够充分展示与评估对象有关的客观事实、客观情况，并有效配合

评估组、评估员基于评估方案采取的评估方法。评估过程中对被评估方故意隐瞒、恶意掩盖有关客观事实和客观情况的，评估委托方应有能力采取应对措施；

g) 评估对象的范围和边界以及评估准则由评估组长按照本文件第 8 章的要求进一步确定。评估目标与目的、评估范围（包括评估对象的范围和边界以及评估准则）的任何变化宜由评估委托方与评估组长协商一致，必要时宜获得被评估方的同意。

输出：

本活动的可交付项是：

——法律合规性评估目标与目的文件；

——初定的评估对象及介绍；

——合规义务清单（第一版）；

——合规要求清单。

其他信息：

确定法律合规性评估目标与目的，见T/CLAST 002.1—2021的4.2；

界定评估对象的范围与边界，见T/CLAST 002.1—2021的4.4.2；

合规义务清单与合规要求清单，见T/CLAST 002.1—2021的4.4.3。

7.3 签订项目协议

输入：

法律合规性评估项目决策（见7.2）活动的输出。

活动：

评估机构与评估委托方签订项目协议，以明确法律合规性评估的目标与目的、范围、人员组成、双方的责任和义务。

实施指引：

决定项目协议的签订主体和应包含的约定内容，宜参考以下因素：

a) 法律合规性评估模式；

b) 如适用，法律法规、合同、认证机构的要求；

c) 保密义务的需求；

d) 评估组对法律合规性评估过程与结果的沟通和报告渠道。

输出：

项目协议。

7.4 组建评估团队

输入：

法律合规性评估项目决策（见7.2）活动的输出；

项目协议（见7.3）。

活动：

签订项目协议后，评估组长确定法律合规性评估组的人选，由评估委托方决定是否需指派观察员，向被评估方申请确认协调员人选。

实施指引：

在以下7.4.1-7.4.3中给出。

7.4.1 评估组

a) 评估组的规模和组成宜考虑以下因素：

1） 评估目标与目的、评估范围所需要的评估组的整体能力需求；
2） 法律合规性评估模式所决定的评估组的组成要求；
3） 如适用，法律法规、合同或认证机构的对评估组组成的要求；
4） 本文件第 5 章所述的基本原则，尤其是保障法律合规性评估独立、客观、保密、专业性的需求；
5） 法律合规性评估所涉及的地点、语言和文化背景需求；
6） 在评估组、被评估方与评估委托方之间有效沟通与协作的能力；
7） 是否涉及特定专业的检测、试验等活动。

注1：法律合规性评估模式及评估组组成参考 T/CLAST 002.1—2021 的 4.3。

注2：评估组在特定专业领域的知识和技能，可以通过选任技术专家予以补充。

b） 评估员的人选宜考虑：
1） 评估员具备律师执业证，宜具有胜任评估项目的从业经验和能力；
2） 如适用，评估员的能力须符合法律法规、合同或认证机构的要求；
3） 实习评估员可以在评估员指导下工作；
4） 评估组长宜确定评估员符合本文件第 5 章所述的基本原则，包括确认评估员不存在利益或利益冲突并遵守适当的保密义务。

c） 技术专家的人选宜考虑：
1） 当法律合规性评估所要确定的事实或特性要求具备特定专业领域的知识和技能时，可以通过选任技术专家来补充评估组所需的能力，技术专家须具备相应的资格证书，比如注册信息安全专业人员（Certified Information Security Professional）/信息系统安全认证专业人员（Certification for Information System Security Professional）；
2） 在评估组中技术专家并非评估员，技术专家在评估员的指导下工作，对所获得的客观证据作出技术解释，对合规要求的符合性提供技术意见，并出具相应的技术报告，由评估员参考和确认；
3） 技术专家人选符合本文件第 5 章所述的法律合规性评估基本原则，尤其是确保技术专家遵守与评估员同等程度的保密义务。

d） 在遵守本文件第 5 章所述基本原则的前提下，评估委托方和被评估方可基于合理理由向评估组长申请更换评估组成员。

示例：合理理由可包括利益冲突、对评估员能力或职业道德的考虑。

7.4.2 观察员

当法律合规性评估是由被评估方以外的组织委托，或者法律法规、认证机制有要求时，评估委托方或认证机构可以选择指派观察员以监督法律合规性评估的过程和结果，就观察员的参与与被评估方达成一致意见。

a） 观察员遵守与评估员同等程度的保密义务；
b） 观察员并非评估组成员，观察员不对法律合规性评估过程和结果造成不当影响和干预；

7.4.3 协调员

a） 被评估方指派适当数量的协调员以协助评估组实施法律合规性评估。
b） 协调员并非评估组成员，协调员不对法律合规性评估过程和结果造成不当影响和干预。
c） 协调员的主要职责包括：
1） 协调安排访谈人员与时间；
2） 协调安排对个人信息处理设施的访问；

3） 应评估员的请求提供文件，澄清信息；
4） 向评估员介绍组织的信息安全规定并确保遵守。

输出：

本项活动的可交付项包括：

——评估组名单，包含评估组长、评估员、技术专家等评估组成员；
——评估委托方代表、观察员名单；
——被评估方代表、协调员名单；
——必要时，上述人员签署的保密协议。

7.5 准备问卷和文件清单

活动：

评审评估委托方提供的所有现有资料，进行独立的信息调查，了解和分析初步选定的评估对象，制定为界定评估对象的范围和边界所需要的文件清单和问卷调研表。

实施指引：

a） 评估组宜审阅评估委托方提供的所有现有资料，尤其是：
1） 法律合规性评估项目决策（见 7.2）活动的输出；
2） 被评估方的个人信息保护政策、产品或用户协议；
3） 产品、服务或过程简介或说明文档。
b） 评估组宜独立调查：
1） 就初步界定的评估对象可获得的公开资料；
2） 独立调查可能适用于初步选定的评估对象的所有法定义务、监管义务和司法义务，以补充完善评估委托方提供的合规义务清单。
c） 评估组宜梳理的文件清单，包括：
1） 评估对象的产品、服务或过程设计文档；
2） 评估对象的业务流程图、数据流程图、网络拓扑图、系统架构图；评估对象所包含的设备资产清单，包括但不限于设备编号、所在位置、管理部门和人员等信息，并与业务流程图一一匹配；
3） 最近一次的信息安全等级保护测评报告、个人信息安全管理体系审核报告，以及现有的信息安全保护/控制措施对评估对象的覆盖范围说明、法律风险评估报告/评估法律意见书；
4） 评估对象所涉及的业务部门、支持部门和人员清单。

输出：

本项活动的可交付项包括：

——为界定评估对象的范围和边界所需要的文件清单和问卷调研表；
——合规义务清单（第二版）。

7.6 项目启动会议

输入：

准备问卷和文件清单（见7.5）活动的输出。

活动：

评估组、被评估方、委托评估方之间进行项目启动会议。

实施指引：

启动会议的主要任务在于：

a) 与被评估方代表建立沟通渠道；
b) 通过被评估方的介绍了解评估对象；
c) 沟通法律合规性评估的目标与目的和初步选定的法律合规性评估范围，包括评估对象的范围、边界和评估准则；
d) 沟通确认法律合规性评估的过程和时间安排；
e) 提出和说明为制定法律合规性评估方案所需的文件清单和问卷调研表，并商定反馈时间和形式。

输出：

本项活动的可交付项包括：

——项目启动会议记录。

8 计划准备阶段

8.1 概述

计划准备阶段的总体目标是完成现场实施阶段所需的准备。

开启计划准备阶段的主要输入，除项目启动阶段的全部输出之外，还包括被评估方反馈的问卷调研表和按照文件清单准备的文件。如发现所提供的文件和获得的信息不充分或不适用，评估组长可以通知评估委托方和被评估方，共同商定在文件和信息问题得到解决前，推迟或暂停法律合规性评估。

计划准备阶段的主要活动包括：

——界定评估对象范围和边界；
——确定评估准则；
——确定评估内容和方法；
——制定法律合规性评估方案；
——现场实施准备。

计划准备阶段的主要输出包括：

——法律合规性评估方案；
——现场实施分工；
——现场实施工作表单；
——现场实施注意事项清单；
——工具和作业指导书。

8.2 界定评估对象范围和边界

组织启动法律合规性评估项目的决策是基于初步界定的评估范围和边界。在项目启动会议后基于第一次文件评审所获得的信息对评估对象范围与边界进行详细界定，是高效确定评估准则、制定和实施法律合规性评估方案的关键因素，也是保障法律合规性评估全面、充分和可靠的基础。

输入：

——评估对象的范围和边界文件（第一稿）（见 7.2）；
——项目启动会中被评估方提供的介绍和会议记录（见 7.6）；
——被评估方反馈的问卷调研表和按照文件清单准备的文件。

活动：

界定评估对象范围和边界，所需进行的活动包括：

a) 界定个人信息处理范围和边界；
b) 界定网络范围和边界；
c) 界定信息系统和物理范围和边界；
d) 界定组织范围和边界；
e) 集成上述基础性的范围和边界，以获得评估对象的范围和边界。

8.2.1 界定个人信息处理的范围和边界

实施指引：

a) 界定个人信息处理的范围和边界，宜通过回答以下问题的方式进行：
   1) 评估对象的产品或服务；
   2) 该产品或服务的业务功能、业务场景及流程；
   3) 该产品或服务中包含的个人信息类别、来源和对应的处理活动及流程；
   4) 个人信息处理活动所涉及的个人信息~~控制者或~~处理者或个人信息处理受托人；
   5) 其他与个人信息处理活动有关的信息。
b) 在通过文件评审得到解答上述问题的信息后，评估组宜制作一份文件描述所获得的信息，并在业务流程图的基础上通过修改或绘制评估对象的个人信息处理过程图，在其中表述作为输入和输出的个人信息类型。

输出：

本项活动的可交付项包括：
——个人信息处理范围和边界的文字描述；
——标注个人信息类型的个人信息处理过程图。

8.2.2 界定网络范围和边界

实施指引：

a) 通过分析评估对象的网络拓扑图，区分网络边界，识别和梳理评估对象所涉及的网络安全设备、网络设备、服务器、存储、备份等所有设备资产，并描述整体网络情况，包含但不限于具体的外联区域、链路、安全措施等。
b) 评估组宜制作一份文件描述所获得的信息，并在业务流程图（见 8.2.1）上标注网络边界和设备资产，以及与其他网络区域的接口。

输出：

本项活动的可交付项包括：
——网络范围和边界的文字描述；
——标注网络边界、设备资产和接口的个人信息处理过程图。

8.2.3 界定信息系统和物理范围和边界

实施指引：

a) 通过分析系统架构图，识别和梳理用于评估对象的主要设备、设备所承载的软件、其他组件以及设备之间的连接情况等，并标注出每个设备对应的物理位置；
b) 在 8.2.2 所得出的个人信息处理过程图中，标注信息系统的设备资产、组件，包括结合被评估方反馈的问卷调研表，在个人信息处理过程图中标注设备资产清单；
c) 对于个人信息存储，需识别服务器（包括数据库服务器、中间件服务器、日志服务器、备份服务器等）的位置，存储介质（如磁盘、光盘、磁带）、终端等的使用情况，在个人信息处理过程图中标注存储所在位置。

输出：

本项活动的可交付项包括：

——信息系统和物理范围和边界的文字描述；

——标注技术特点、设备资产、服务器所在位置的个人信息个人信息处理过程图。

8.2.4 界定组织范围和边界

实施指引：

a) 界定组织范围和边界，宜通过回答以下问题的方式进行：
   1) 被评估方的哪些部门和人员对评估对象产品或服务负责，例如，开发、运营和销售；
   2) 被评估方的哪些部门和人员参与或支持这些个人信息处理过程，例如，安全、网络管理、设备管理、法务合规；
   3) 除被评估方之外，这些个人信息处理过程中有哪些组织参与其中，例如，顾客、外包服务的供方、第三方等；
   4) 被评估方与这些组织之间存在哪些合同或其他法律关系，例如，委托处理、共享、转移~~让~~、运行维护、云服务、关联关系等；
   5) 在这些个人信息处理过程和与其他组织的关系中，被评估方处于什么地位。
b) 对被评估方已经提供的合同、组织章程等文件进行评审，识别和分析合同和法律关系，明确被评估方的地位；
c) 在通过文件评审得到解答上述问题的信息后，评估组宜制作一份文件描述所获得的信息，并在个人信息处理过程图中标注有关部门，组织间法律接口；
d) 检查组织间法律接口与已经标注的技术接口之间的一致性，分析差异原因，以准备补充文件清单和问卷调研表。

输出：

本项活动的可交付项包括：

——组织范围和边界的文字描述；

——纳入评估对象的被评估方有关部门和人员清单；

——重要合同、组织章程摘要；

——标注有关部门、组织间法律接口的个人信息处理过程图；

——补充文件清单和问卷调研表（第一稿）。

8.2.5 总体界定

输入：

8.2.1-8.2.4活动的所有输出。

活动：

总体界定评估对象的范围和边界。

实施指引：

a) 综合 8.2.1-8.2.4 活动的所有输出，综合分析个人信息处理、网络、信息系统、组织范围和边界，界定评估对象的范围和边界；
b) 分析评估对象的范围和边界对于后续活动的影响，如确定评估准则、确定评估内容和方法、制定法律合规性评估方案、现场实施准备时的注意事项；
c) 修改拟向被评估方发送的补充文件清单和问卷调研表。

输出：

本项活动的可交付项包括：

a) 法律合规性评估方案的评估对象范围和边界部分，包含一份完整的个人信息处理过程图；
b) 后续活动注意事项的清单（第一稿）；
c) 补充文件清单和问卷调研表（第二稿）。

其他信息：

见T/CLAST 002.1—2021的4.4.2。

8.3 确定评估准则

输入：

界定评估对象范围和边界（见8.2）活动的全部输出；
合规义务清单（第二版）（见7.5）；
T/CLAST 002.2—2021文件。

活动：

确定评估准则。

实施指引：

见以下8.3.1-8.3.3。

8.3.1 确定基本法律合规性评估指标

实施指引：

a) 评估组宜对照描述和界定评估对象的范围和边界的文件与合规框架（T/CLAST 002.2—2021），依次选取：
   1) 第 5 章（法律合规性评估维度）中的全部法律合规性评估指标，除非经评估员分析认为其中的单个法律合规性评估维度或单个法律合规性评估指标不适用，可以排除并记录理由；
   2) 根据评估对象的范围和边界中包含的个人信息处理，从合规框架第 6 章和第 7 章中选取适用的全部扩展要求。
b) 将选取的法律合规性评估指标的基本要求和扩展要求进行组合，形成基本法律合规性评估指标清单/表格。

输出：

本项活动的可交付项包括：
——基本法律合规性评估指标清单/表格；
——适用性声明，包括排除的法律合规性评估维度、法律合规性评估指标和理由。

8.3.2 确定差异化法律合规性评估指标

实施指引：

a) 评估员宜根据评估对象的范围和边界，重新检索是否存在尚未被识别的合规义务，尤其宜留意可能影响合规义务的以下要素：
   1) 产品或服务的业务场景；
   2) 个人信息处理类型；
   3) 所适用的个人信息类型；
   4) 被评估方组织所属行业的监管要求；
   5) 被评估方组织和个人信息处理设施所在地域；
   6) 评估对象所采用的技术特征；
   7) 评估对象所采用的信息系统和网络结构。
b) 根据重新检索的合规义务，确定合规义务清单。

c） 分析合规义务清单和选择纳入的其他规定要求，将其与基本法律合规性评估指标清单/表格中的要求进行比较，以确定：

1） 所识别的合规要求和其他规定要求是否涵盖基本法律合规性评估指标未提及的差异化法律合规性评估维度；

2） 所识别的合规要求与其他规定要求涵盖与基本法律合规性评估指标相同的法律合规性评估维度，但存在差异化指标，包括：

——就相同法律合规性评估维度提出了高于基本法律合规性评估指标的要求；

——就相同法律合规性评估维度提出比基本法律合规性评估指标更具体的要求；

——明示减轻或免除基本法律合规性评估指标中某个法律合规性评估维度的要求。

输出：

本项活动的可交付项包括：

——合规义务清单（定稿）；

——差异化法律合规性评估维度和差异化法律合规性评估指标清单。

8.3.3 确定评估准则

实施指引：

a） 根据差异化法律合规性评估维度和差异化法律合规性评估指标清单，调整基本法律合规性评估指标清单/表格，包括：

1） 标注差异化合规维度和差异化法律合规性评估指标；

2） 记录减轻和免除基本法律合规性评估指标中某个法律合规性评估指标的理由和依据。

b） 分析确定的评估准则对于后续活动的影响，如确定评估内容和方法、制定法律合规性评估方案、现场实施准备时的注意事项；

c） 修改拟向被评估方发送的补充文件清单或问卷调研表。

输出：

本项活动的可交付项包括：

——法律合规性评估方案的评估准则部分，附：

- 合规义务清单（定稿）；
- 排除的法律合规性评估维度、法律合规性评估指标及其理由；
- 减轻或免除基本法律合规性评估指标中某个法律合规性评估指标的理由依据记录。

——后续活动注意事项清单（第二稿）；

——补充文件清单和问卷调研表（第三稿）。

8.4 确定评估内容和方法

输入：

法律合规性评估方案的评估对象范围和边界部分（见8.2.5）；

法律合规性评估方案的评估准则部分（见8.3.3）；

后续活动注意事项清单（第二稿）；

补充文件清单和问卷调研表（第三稿）（见8.3.3）。

活动：

确定评估内容和方法，制定现场实施所需文件清单和问卷调研表。

实施指引：

a) 将评估准则与评估对象的范围和边界结合起来，将法律合规性评估指标或所属的法律合规性评估维度映射到各评估对象上，结合评估对象的特点，说明所要确认或验证的内容，所采取的获取客观证据的方法。

b) 对于其中需要进行文件评审的，修改补充文件清单和问卷调研表（第三稿），以确定现场实施所需文件清单和问卷调研表（定稿）。

输出：

本项活动的可交付项包括：

——法律合规性评估方案的评估内容和方法部分；

——后续活动注意事项清单（第三稿）；

——现场实施所需文件清单和问卷调研表（定稿）。

8.5 制定法律合规性评估方案

输入：

前述活动的全部可交付项。

活动：

制定和分发法律合规性评估方案，便于在评估委托方、评估组和被评估方之间就法律合规性评估的实施达成一致，并就评估活动的日程进行协调。

向被评估方提供现场实施所需文件清单（定稿），必要时提供说明并确认可获得的时间。

实施指引：

法律合规性评估方案宜包含以下内容：

a) 法律合规性评估的目标和目的；

b) 法律合规性评估对象的范围和边界；

c) 评估准则；

d) 法律合规性评估内容和方法；

e) 法律合规性评估组的具体构成和职责；

f) 实施法律合规性评估的时间计划和地点；

g) 实施法律合规性评估所需的资源，包括被评估方的协调员，所需设备、场地等后勤安排、文件提供、访谈、会议等沟通安排等。

注1：对于首次法律合规性评估和后续法律合规性评估，以及根据法律合规性评估的目标和法律合规性评估模式，法律合规性评估方案的内容和详略程度可以有所不同。

注2：法律合规性评估方案宜保留一定的灵活性，评估组长根据法律合规性评估的进展可以进行必要的调整。

注3：在第二方评估和第三方评估中，法律合规性评估方案的制定应与被评估方充分协商和沟通，并将最终的法律合规性评估方案文件提供给被评估方。对法律合规性评估方案的重大调整，在评估组长与被评估方的协调员，必要时包括观察员之间协商确定。

输出：

本项活动的可交付项包括：

——法律合规性评估方案。

8.6 现场实施准备

输入：

法律合规性评估方案；

后续活动注意事项清单（第三稿）；

现场实施所需文件清单和问卷调研表（定稿）。

活动：

准备现场实施所需的工作表单和工具。

实施指引：

现场实施阶段之前的准备工作包括：

a) 评估组长与评估组成员商定，对每名成员在现场实施中的工作任务（包括具体负责的过程、场所、活动等）进行分配，并就成员相互之间的配合进行部署；

注：工作任务的分配宜考虑评估组成员各自的独立性、能力、资源的高效利用，以及评估员、实习评估员与技术专家等不同角色和职责。在现场实施中可以根据评估过程的需要灵活地调整。

b) 评估组成员评审与其所承担的评估工作有关的文件和信息，并预备现场实施阶段必要的工作表单，用于现场评估过程中参考或记录；

示例：这些工作表单包括：

——各类检查表、作业指导书、问题清单等；

——用于记录客观证据、访谈、会议、评估发现的表格。

注1：评估活动的内容不应受限于既定工作表单，可以随着评估中的发现而有灵活的调整。

注2：评估组成员应妥善保管含有保密和知识产权信息的工作表单。在法律合规性评估结束时，工作表单的处理方式见 10.4。

c) 评估组成员评审与其所承担的评估工作有关的文件和信息，预备现场实施阶段必要的测量、试验、检测工具，并制定作业指导书；

d) 根据准备情况更新后续活动注意事项清单，形成现场实施注意事项清单。

输出：

本项活动的可交付项包括：

——现场实施分工；

——现场实施工作表单；

——现场实施注意事项清单；

——工具和作业指导书。

9 现场实施阶段

9.1 概述

现场实施阶段的总体目标是获得被客观证据所支持的评估发现和评估结论，并为评估法律意见书的编制收集和准备文件。

现场实施阶段的主要输入，除计划准备阶段的主要输出之外，还包括被评估方根据现场实施所需文件清单和问卷调研表（定稿）准备的文件。如发现被评估方准备的文件或者现场实施准备阶段的主要输出不充分或不适用，评估组长可以通知评估委托方和被评估方，共同商定在文件和准备问题得到解决前，推迟或暂停法律合规性评估。

现场实施阶段的主要活动包括：

——实施阶段启动会议；

——获取客观证据；

——确认和验证客观证据得出评估发现；

——根据评估发现，评审得出评估结论；

——实施阶段总结会议。

现场实施阶段的主要输出包括：

——已经使用的现场实施工作表单，记录了客观证据和评估发现；
——评估发现记录总表（定稿）；
——需在评估法律意见书中记录的评估发现局限性清单；
——尚未被解决的分歧记录总表（定稿）；
——尚未被调整或处置的差距总表（定稿）；
——尚未获得客观证据的法律合规性评估指标总表；
——总体评估结论；
——启动会议、评估组评审会议和总结会议记录。

9.2 实施阶段启动会议

输入：

法律合规性评估方案。

活动：

召开实施阶段启动会议。

实施指引：

a) 实施阶段启动会议的与会者宜包括：
   1) 评估组成员；
   2) 被评估方的管理层和协调员，以及被评估方指定的人员，如相关部门的负责人；
   3) 观察员（如有）；
   4) 评估委托方的代表（如有）。
b) 实施阶段启动会议的目的是：
   1) 确认所有与会者对法律合规性评估方案达成理解与一致；
   2) 介绍评估组成员及其职责；
   3) 介绍协调员以及被评估方其他与会者的职责；
   4) 确保法律合规性评估方案的实施能够得到所有与会者的充分支持。
c) 实施阶段启动会议的议程宜考虑：
   1) 概述法律合规性评估的目标、目的和范围；
   2) 概述法律合规性评估的程序，必要时介绍评估准则及其中的能力评价基准；
   3) 确定法律合规性评估的时间计划，以及实施法律合规性评估所需资源的可获得性；
   4) 实施法律合规性评估的过程中需遵守的纪律和规定，包括评估组的纪律，以及被评估方有关场地或信息安全的规定和注意事项；
   5) 确定评估组与被评估方之间的沟通渠道，尤其是有关法律合规性评估实施安排的日常沟通，以及对法律合规性评估中的评估发现、评估结论的正式沟通方法。

   注：根据评估的范围和复杂性，有必要对评估组内部以及评估组与被评估方之间的沟通作出正式的安排。评估组长宜定期与被评估方、评估委托方通报评估进展和有关信息。尤其是：

   ——法律合规性评估中发现有证据表明可能已经发生重大不合规或不符合时，评估组长宜视情况决定何时向被评估方通报，必要时向评估委托方通报；

   ——法律合规性评估中发现在评估对象的范围和边界之外，但可能影响法律合规性评估发现和结论的问题，宜随时向评估组长报告，如有必要，评估组长宜向被评估方与评估委托方通报；

   ——在法律合规性评估中获得的客观证据表明无法实现法律合规性评估目的，评估组长应向评估委托方和被评估方通报理由，以商定适当的措施。如修改法律合规性评估方案、改变法律合规性评估目的、法律合规性评估范围或终止法律合规性评估。
d) 实施阶段启动会议由评估组长主持，并为所有与会者提供提问的机会，应保留会议记录。

输出：

本项活动的可交付项包括：

——项目概述；

——实施阶段启动会议记录。

9.3 获取客观证据

获取客观证据的方法包括文件评审、访谈、记录、测量、试验、检测、检查。方法的选择取决于信息源和待确认事实的类型。

在法律合规性评估中，可以根据法律合规性评估目的、范围和评估准则的具体要求，通过抽样的方式收集客观证据。

对于采用T/CLAST 002.2—2021中的法律合规性评估指标，建议的方法如下。如评估准则中包含其它合规要求，可参照适用。

9.3.1 文件评审

输入：

被评估方按照文件清单提供的文件；

问卷调研表。

活动：

评审被评估方提供的文件。

实施指引：

a) 实施文件评审者宜包括评估员和技术专家；

b) 评审文件目的是获取客观证据和确定访谈及检测事项；

c) 评审的文件范围，宜包括被评估方的以下文件：

1) 公司营业执照及资质文件；
2) 问卷调研表的回复内容及附件；
3) 个人信息保护政策、产品或用户协议；
4) 评估对象产品、服务或过程简介或说明文档；
5) 评估对象的业务流程图、数据流程图、网络拓扑图、系统架构图等文件；
6) 与第三方签署的与评估对象个人信息处理活动有关的合同（个人信息主体授权同意文件，如有）和保密协议等法律文件；
7) 最近一次的信息安全等级保护测评报告和信息安全管理体系审核报告，以及现有的信息安全保护/控制措施对评估对象的覆盖范围说明、法律风险评估报告/评估法律意见书；
8) 与个人信息处理有关的制度，包括制度的执行记录文件；
9) 与个人信息处理或安全有关的认证证书文件；
10) 个人信息处理管理组织及人员有关的文件，如组织架构图、权责说明书等文件；
11) 与个人信息安全管理有关的文件，如事件应急预案和事件报告等文件；与个人信息处理或数据安全有关的其他文件。

d) 文件评审过程中宜注意：

1) 文件的有效性，如是否为正式签发的文件等；
2) 摘录文件的关键信息时不宜过多摘抄文件原文，注意商业秘密的保护；梳理问题项以及待进一步确认或提供信息或文件的待办事项。

输出：

本项活动的可交付项包括：

——评审文件摘录；
——待办事项清单（第一稿）；
——访谈提纲；
——后续活动注意事项清单（第三稿）。

9.3.2 访谈

输入：
访谈提纲。
活动：
与相关人员进行访谈。
实施指引：
a) 宜根据访谈提纲内容合理安排相应的被访谈人员，向被评估方确定不同业务部门，如业务、信息安全研发等部门的被访谈代表；
b) 访谈应得到完整详细的记录，宜要求被访谈人员对其陈述内容进行确认和签字，或要求被评估方对访谈记录进行确认并盖章，或经被评估方及被访谈人员允许对访谈进行录像或录音记录；如被评估方拒绝前述要求，需在访谈纪要中载明该情况及其原因；
c) 访谈过程中宜注意：
   1) 确保被访谈人员的适格性和独立性，以确保访谈能够获得相关、客观的回答；
   2) 访谈提纲涉及技术问题时，应安排具备信息安全技术领域知识和技能的评估员或技术专家在场。
输出：
本项活动的可交付项包括：
——访谈记录；
——待办事项清单（第二稿）。

9.3.3 检测

输入：
问卷调研表；
技术检测清单；
验证方案。
活动：
对评估对象进行技术检测。
实施指引：
a) 现场实施前将技术检测清单发送给被评估方，以确保具有检测所需环境及条件；
b) 与被评估方沟通可实施检测事项，不能检测的内容需要被评估方提供备选的事实确认方案，如提供文件资料或出具声明；
c) 现场实施前准备检测所需工具；
d) 实施检测者应为技术专家，同时评估员应在现场；
e) 应如实记录检测过程及检测发现，由技术专家对检测发现发表技术意见，出具技术分析报告；
f) 检测宜注意及时与被评估方沟通双方对技术检测的有效性和检测结果的分歧，及时调整差距，并如实记录调整情况。
输出：
本项活动的可交付项包括：

——技术分析报告；
——待办事项清单（第三稿）。

9.4 评估发现

输入：

获得的客观证据（见9.3）活动的输出。

活动：

评估员将所获取的客观证据与评估准则进行比较，验证规定要求是否得到满足，确认特定的预期用途或应用是否得到满足，并据以得出评估发现。当法律合规性评估目的有要求时，评估发现也需表明可能的改进空间。

实施指引：

a) 评估员宜及时记录评估发现，记录事项包括但不限于：
   1) 所涉及的法律合规性评估指标；
   2) 是否满足法律合规性评估指标；
   3) 所采用的获取客观证据的方法及其局限性；
   4) 客观证据（如名称、编号等）；
   5) （如存在差距）理由；
   6) （如存在差距）差距的严重程度；
   7) 记录人；
   8) 记录时间；
   9) 后续调整或处置建议。
b) 评估组内部宜定期沟通以交换在各自负责的工作中获得的客观证据和评估发现；
c) 评估组长宜定期汇总和评审评估组成员的评估发现记录，以确定法律合规性评估现场实施的进展，需要时重新分配评估组成员的工作；
d) 对于表明评估对象与评估准则存在差距的评估发现，评估组宜优先与被评估方沟通，使被评估方及时理解该差距；
   1) 如被评估方对客观证据的准确性提出质疑，评估组长宜允许被评估方提出理由，如有必要，可以决定调整获得客观证据的方法或安排另一名评估员按相同方法重新获得客观证据；
   2) 如被评估方对评估发现提出质疑，评估组长宜允许被评估方提出理由，并进行记录。
e) 在现场实施阶段宜尽可能解决评估组与被评估方之间对客观证据有效性和评估发现的分歧，以及可以立即调整的差距，汇总和记录尚未被解决的分歧和尚未被调整的差距。

输出：

本项活动的可交付项包括：
——评估发现记录（底稿）；
——尚未被解决的分歧记录（底稿）；
——尚未被调整的差距记录（底稿）；
——待办事项清单（第四稿）。

9.5 准备评估结论

输入：

评估准则（定稿）；
评估发现（见9.4）活动的输出。

活动：

评估组共同评审所获得的全部评估发现记录，逐项对照评估准则，整理分歧和差距并得出评估结论。

实施指引：

在实施阶段总结会议前，评估组宜共同评审以下内容：

a) 对比全部评估发现和评估准则（定稿），评审评估准则中的法律合规性评估指标是否已经全部得到有客观证据支持的评估发现。
   1) 如果是，已经得到的客观证据是否由于采用了抽样方法，导致评估发现存在方法本身带来的局限性，宜汇总和记录这些局限性，作为评估法律意见书的单独一部分内容；
   2) 如果有部分法律合规性评估指标未得到有客观证据支持的评估发现，并且是由于法律合规性评估指标的原因，导致评估组无法获得任何客观证据，评估组可以决定放弃对该法律合规性评估指标作出评估结论，或者接受被评估方的书面陈述与保证作为该法律合规性评估指标的评估结论所依赖的证据，这些法律合规性评估指标需被单独汇总和记录，作为评估法律意见书的单独一部分内容；
   3) 如果有部分法律合规性评估指标未得到有客观证据支持的评估发现，并且是由于评估对象的原因，如评估对象在法律合规性评估期内未提供客观证据，评估对象未保留任何客观证据，评估组宜评审这一事实本身是否表明评估对象不满足某项法律合规性评估指标（如可问责性维度的法律合规性评估指标或其他）。
      ——如果是，将该事实确定为尚未被解决的差距；
      ——如果不是，评估组可以决定放弃对该法律合规性评估指标作出评估结论，或者接受被评估方的书面陈述与保证作为该法律合规性评估指标的评估结论所依赖的证据，这些法律合规性评估指标需被单独汇总和记录，作为评估法律意见书的单独一部分内容。

b) 对于评估发现中表明的差距，是否已经在现场实施阶段得到调整或处置。如果还有尚未被调整或处置的差距，评估组宜汇总和记录这些差距；如果评估的目标和目的有要求，宜预备建设性的调整或处置意见；

c) 评估组与被评估方之间对客观证据有效性和评估发现的分歧，是否已经在现场实施阶段得到解决。如果还有尚未被解决的分歧，评估组宜评审该评估方就该分歧提出的理由，确定评估发现并汇总和记录这些分歧、理由和经评审后的评估发现；

d) 评估组宜综合考虑全部评估发现及其局限性、未被调整的差距（和调整或改进意见）、未被解决的分歧和经评审后的评估发现，确定总体性的评估结论，包括：
   1) 基于现有的全部评估发现（包括经评审后的评估发现）并考虑其局限性，对评估结论达成一致；
   2) 考虑法律合规性评估目标与目的，对未被调整的差距完成后续调整或处置是否作为出具评估法律意见书的前提。

输出：

本项活动的可交付项包括：

——评估发现总表；

注1：含法律合规性评估指标（或编号）、客观证据名称或编号、评估发现记录（底稿）编号、评审组成员、单项评估结论；

注2：如有决定放弃或决定接受书面陈述与保证，需在评估发现记录总表中简要标注理由（如法律合规性评估指标原因或评估对象原因）。

——需在评估法律意见书中记录的评估发现局限性清单；

注：宜按照方法或存在局限性的理由归类，无需就每一项法律合规性评估指标单独声明。

——尚未被解决的分歧总表；

注：宜包含法律合规性评估指标（或编号）、客观证据名称或编号。

——尚未被调整或处置的差距总表；

注：宜包含法律合规性评估指标（或编号）、客观证据名称或编号、评估发现记录（底稿）编号、评审组成员、是否作为出具评估结论的前提及理由、（如有）调整或处置建议。

——尚未获得客观证据的法律合规性评估指标总表；

注：宜包含法律合规性评估指标（或编号）、理由、评估组的决定（如放弃或接受书面陈述与保证）。

——总体评估结论；

——评估结论评审会议记录等其他文件。

9.6 实施阶段总结会议

输入：

现场实施阶段的全部输出。

活动：

召开实施阶段总结会议，目标是：

a) 确认所有与会者对评估发现、评估结论及其局限性达成理解与一致；

b) 讨论现场实施阶段中尚未被解决的分歧；

c) 讨论现场实施阶段中尚未被调整或处置的差距，（如需要）后续调整、处置、复评安排；

d) 保障评估组最终得出的评估结论能够获得所有相关方的充分认同和理解。

实施指引：

a) 实施阶段总结会议的与会者包括：

1) 法律合规性评估组成员；

2) 评估委托方的代表和/或观察员；

3) 被评估方管理层和协调员，以及由被评估方指定的人员，如相关部门的负责人。

b) 实施阶段总结会议的议程内容宜考虑：

1) 简要总结现场实施阶段的工作情况，重要评估发现、总体评估结论，说明局限性；

2) 提出尚未被解决的分歧和问题，评估组的评审意见，听取被评估方的意见；

3) 提出评估发现尚未被调整或处置的差距，对评估结论的影响；

——如果根据法律合规性评估目标和目的，差距调整和处置是出具评估法律意见书的前提，讨论后续差距调整和处置的时间安排；

——如果根据法律合规性评估目标和目的，差距调整和处置并非出具评估法律意见书的前提，确定出具评估法律意见书的时间安排；

4) 提出未获得客观证据的法律合规性评估指标，说明理由并提出放弃或接受书面陈述与保证的建议，获得评估委托方和被评估方同意，（如有）确定出具的时间安排。

c) 实施阶段总结会议由评估组长主持，并为所有与会者提供提问或发言的机会，保留会议记录；

d) 被评估方与评估组之间关于评估发现、必要的调整或处置以及可能的评估结论存在分歧，尽可能在实施阶段总结会议中解决，未能解决的分歧应予以记录；

e) 评估组宜允许被评估方在总结会议结束后的指定时间内提交书面意见陈述，书面意见陈述作为评估法律意见书的一部分，但评估组独立作出评估结论。

输出：

本项活动的可交付项包括：

——实施阶段总结会议记录；

——如需要，对后续差距调整和处置时间安排；

——如有，总结会议结束后被评估方提交对分歧的书面陈述意见以及书面陈述与保证的时间安排。

10 评估法律意见书阶段

10.1 概述

评估法律意见书阶段的总体目标是完成评估法律意见书的编制、签发和妥善终止法律合规性评估项目。

评估法律意见书阶段的主要输入，除现场实施阶段的主要输出之外，还包括（如有）被评估方根据实施阶段总结会议的时间安排提交的书面意见陈述、（如有）书面陈述与保证，以及（如需要）后续差距调整和处置证据。如发现这些主要输入不充分或不适用，评估组长可以通知评估委托方和被评估方，共同商定在得到解决前，推迟或暂停本阶段的法律合规性评估。

评估法律意见书阶段的主要活动包括：

——评估法律意见书前的工作；

——编制和签发评估法律意见书；

——终止法律合规性评估项目。

现场实施阶段的主要输出包括：

——个人信息处理法律合规性评估法律意见书；

——评估发现记录总表（定稿）；

——客观证据、工作底稿。

10.2 评估法律意见书前工作

输入：

法律合规性评估实施阶段的全部输出。

活动：

收集被评估方对分歧的书面陈述意见（如有）；

收集书面陈述与保证（如有）；

调整和处置差距，以及复评（如有）。

实施指引：

a) 如被评估方要求对分歧进行书面意见陈述并在约定时间内提交，评估组宜评审是否影响评估结论，如不影响，评估组宜将被评估方的意见陈述作为书面评估法律意见书的附件或在正文中进行摘录；

b) 如被评估方同意并在约定时间内提交书面陈述与保证，评估组宜评审书面陈述与保证的充分性；如在约定时间内未提交评估组认为充分的书面陈述与保证，评估组宜依据现有的客观证据得出法律合规性评估法律意见书；

c) 在以确定合规现状为目标的法律合规性评估中，评估组对于评估发现中差距的处理宜保留充分的裁量权，并可以选择将差距调整和复评作为出具评估法律意见书的前提条件。由于在法律合规性评估期内未得到调整的差距很可能已经表明评估对象与评估准则之间已经存在确定的不符合，如果在法律合规性评估法律意见书出具前未得到适当调整，对于该评估准则的结论应是不符合；

1) 在第一方评估中，评估组通常可以按照现状出具评估法律意见书，并在评估法律意见书中尽可能详细地描述存在的差距及其可能的风险，差距调整及其风险处置的决策和执行可以由委托其实施法律合规性评估的评估委托方（也是评估对象）自行完成；

2) 在第二方评估和第三方评估中，评估组宜考虑其代表的评估委托方的利益、自身的执业风险和责任以及作为评估机构的行为准则。评估组可以选择：

——在第二方评估中听取评估委托方的建议，在评估法律意见书中详细揭示差距及其可能的风险，由评估委托方自行决策是否要求被评估方做出调整或进行其他风险处置；

——在第三方评估中遵循评估机构的行为准则和评估机构管理层的决策，接受部分差距调整，并对于调整后仍然残留风险的部分进行记录以免除其自身的风险和责任。

d) 在以确定合规能力为目标的法律合规性评估中，评估法律意见书是对整体能力的评价，评估组通常按照实施阶段终止时的状态编制评估法律意见书，并可以将差距调整和风险处置留待报告后进行，并作为下一次法律合规性评估的确定内容。

输出：

本项活动的可交付项包括：

——评估组对书面陈述意见的评审结论和处理方法的建议；

——评估组对书面陈述与保证的评审结论，以及对法律合规性评估法律意见书的建议；

——复评发现记录（底稿），并在评估发现记录总表（定稿）中更新复评发现并进行特殊标记。

10.3 编制和签发评估法律意见书

输入：

法律合规性评估实施阶段的全部输出；

评估法律意见书前工作的全部输出（如有）。

活动：

编制和签发评估法律意见书。

实施指引：

a) 评估组长负责编制书面评估法律意见书，并对书面评估法律意见书的内容负责；

b) 评估法律意见书应提供有关以下内容的真实、准确、完整和清晰的信息：

1) 评估委托方的主体信息和代表；
2) 评估机构的主体信息和评估组长；
3) 被评估方的主体信息和协调员；
4) 评估组成员；
5) 法律合规性评估模式；
6) 评估的目标和目的；
7) 评估对象的范围和边界；
8) 评估准则；
9) 法律合规性评估期间；
10) 法律合规性评估过程中关键性事件及其时间节点；
11) 法律合规性评估结论的局限性声明，包括：
——由于抽样等评估方法固有的不确定性带来的局限性；
——放弃法律合规性评估指标或接受书面陈述与保证的情况；
——必要的风险提示。
12) 法律合规性评估总体结论、理由和客观证据：
——如总体结论为合规或符合，可以给出简要的评审理由，并附评估发现记录总表（定稿）以表明法律合规性评估结论所依据的评估发现、客观证据等；
——如总体结论为不合规或不符合，宜在报告中给出相对更为详细的评审理由和分析。
13) 评估发现中的重要差距，包括：
——是否在法律合规性评估期间得到调整和处置；
——（如有）调整和处置后的复评发现和结论；

——必要的风险提示；

——附复评的评估发现记录，或特别标注复评发现的评估发现记录总表（定稿）。

14）尚未被解决的分歧，以及被评估方提交的书面意见摘要、评审结论。

15）如有：

——对评估法律意见书后差距调整和风险处置的建议；

——对监督和持续评估的建议；

——对评估法律意见书后管理层评审或专家评审的建议。

c） 在评估法律意见书正式签发前，评估组长宜按照评估机构的组织程序，将编制完成的评估法律意见书提交管理层评审或履行适当的批准或签发程序。如法律合规性评估的目标和目的有要求，或者评估委托方、监管机构或认证机构要求，可以进行必要的专家评审；

d） 评估法律意见书宜按照商定的时间表提交。如可能发生迟延，评估组长向评估委托方通报迟延的理由，并就新的提交时间达成一致。

10.4 处理法律合规性评估项目文件

输入：

法律合规性评估项目的全部输入和输出。

活动：

对法律合规性评估项目文件进行返还、销毁、存证、固证、归档等处理。

实施指引：

通常，当法律合规性评估方案中的所有活动均已完成并正式签发评估法律意见书时，法律合规性评估项目即告终止。评估组宜在签发评估法律意见书后，履行适当的措施，妥善处理法律合规性评估项目文件，包括：

a） 按照被评估方的要求，返还或销毁被评估方在法律合规性评估项目期间提供的文件；

b） 按照相关法律法规的要求、评估项目协议或保密协议的约定，保存和固定在法律合规性评估项目中获得的客观证据。如客观证据中含有被评估方商业秘密或其他保密信息，应被评估方请求和委托协议的约定，宜通过可信时间戳、区块链等防篡改的方式存证固证，并可以由被评估方继续保管客观证据；

c） 对于在法律合规性评估过程中由评估机构制作的评估方案、底稿、评估发现记录总表和评估法律意见书及其附录，评估组宜按照相关法律法规以及评估机构项目管理的要求进行存档。按照评估协议的要求，对于可能记录有被评估方商业秘密和其他保密信息的工作底稿，可以与客观证据一并进行存证固证，以供在必要时可以查验。此时，评估组宜保留评估发现记录总表，其中含有法律合规性评估指标（或编号）、客观证据名称或编号、评估发现记录底稿（编号）、评估组成员、单项评估结论，以及评估法律意见书和附录，但评估组不得以违反保密协议（委托协议中的保密条款）约定的方式使用和披露。

输出：

返还、销毁被评估方文件的确认函；

存证固证的客观证据（和底稿）目录。