ICS 35.040
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术 个人信息安全影响评估指南

Information security technology -

Security Impact Assessment Guide of Personal Information

征求意见稿

2017-09

- XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准依据GB/T 1.1-2009给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准的附录A是资料性附录。

本标准起草单位：

本标准主要起草人：

引　言

本标准是《个人信息安全规范》的配套标准，将借鉴美、欧等国家和地区在个人信息安全影响评估（国际上习惯称为隐私影响评估（PIA））方面最新的法律规定、制度设计、实践做法，以国内现有立法、行政法规、标准要求为出发点，提出科学有效符合、信息化发展需要、具有明确实施指导意义的个人信息安全影响评估指南。指南将针对机构、企业提出个人信息安全影响评估的基本框架、方法和流程，供其自评估使用，同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据。

。

信息安全技术 个人信息安全影响评估指南

1 范围

本标准规定了个人信息安全影响评估的基本概念、框架、方法和流程。

本标准适用于各类组织自行开展个人信息安全影响评估工作。同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据。

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 35273-2017 信息安全技术 个人信息安全规范

3 术语

GB/T 25069-2010、GB/T 35273-2017确立的以及下列术语适用于本标准。

3.1 个人信息安全影响评估 personal information security 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。

4 评估基本原理和框架

4.1 概述

个人信息安全影响评估是个人信息控制者实施风险管理的重要组成部分，旨在发现、处置和持续监控个人信息处理过程中的安全风险。一般情况下，个人信息控制者必须在收集和处理个人信息前开展个人信息安全影响评估，明确个人信息保护边界，根据评估结果实施适当的安全控制措施，降低收集和处理个人信息的过程对个人信息主体权益造成的影响；另外，个人信息控制者还需按照要求定期开展个人信息安全影响评估，根据业务现状、威胁环境、法律法规、标准要求等情况持续修正个人信息保护边界，调整安全控制措施，使个人信息处理过程处于风险可控的状态。

4.2 评估价值

通常情况下，实施个人信息安全影响评估可以达到以下目的。

a）识别对个人权益造成的影响，安全风险和相关的责任。

b）为产品和业务设计阶段的个人信息保护理念落地提供支撑。

c）评审新上线信息系统在处理个人信息时的安全风险。

d）向个人信息主体提供加强个人信息安全的建议。

e）维护和更新信息系统新增功能可能对所处理个人信息安全的影响。

f）向相关方共享安全风险并采取风险处置措施。

g）向合规部门反馈证据。

个人信息安全影响评估通常被视为一种预警机制，它为组织提供一种安全风险发现方法，用于发现个人信息的处理过程中存在的安全风险，继而帮助组织在项目实际处理之前实施预防措施和专项保护措施，如果安全风险的影响非常严重且无法预防或保护，整个项目都可能被撤销。因此，个人信息安全影响评估有助于在早期识别个人信息安全问题，通过尽早考虑个人信息安全问题降低时间管理成本、法律费用以及潜在的媒体或公众担忧。

个人信息安全影响评估不仅是简单的合规性检查，还可以帮助组织在持续合规性审计或调查中证明其遵守了相关个人信息与数据保护法律、法规和标准要求。如果发生个人信息安全风险或违规事件，个人信息安全影响评估报告可提供证据证明组织已经采取适当措施试图阻止上述情况发生，这可以有助于减轻、甚至免除相关责任和名誉损失。此外，恰当的个人信息安全影响评估还可以向组织的用户或民众证明，该组织尊重他们的隐私并会回应他们所担忧的个人信息安全问题，用户或民众更倾向于信任执行个人信息安全影响评估的组织。

信任建立在透明的基础上，而个人信息安全影响评估是一项提倡开放式交流、共同认知及透明度的纪律性活动。执行个人信息安全影响评估流程的组织可以向其员工和承包商证明，组织将严肃对待个人信息保护问题，也期望他们能够采取相同的处理方式。此外，通过个人信息安全影响评估，组织还可以对员工进行个人信息保护教育，使之警惕可能导致组织受损的个人信息安全问题。此外，个人信息安全影响评估还是肯定组织本身价值的一种方式，可看作是尽职调查的一种形式，从而减少客户审计次数。

4.3 评估报告的使用对象

个人信息安全影响评估报告应能支持以下功能：

a）提供清单，确保特定的相关方始终了解已识别的受影响部门、受影响环境及受影响部门的周期性个人信息安全风险（包括固有风险和已经得到减缓的风险）。

b）作为一种持续性工作追踪机制，用于追踪改善和/或解决已识别为存在个人信息安全风险的行动/任务。同时，需要对评估报告信息的分发或发布的敏感性进行明确评估和分类（私有、机密、公开等）。

基于这些功能，个人信息安全影响评估报告可以给个人信息主体、个人信息控制者、监管机构、组织的合作伙伴或服务商带来以下帮助：

对于个人信息主体，个人信息安全影响评估是一种工具，可确保个人信息主体的个人信息得到有效保护。

对于个人信息控制者，评估报告的使用场景可能包括以下方面：

a）个人信息安全影响评估是一种工具，用于管理个人信息安全风险、提升意识、建立责任制度；确保组织内部处理个人信息的风险可视性、管理潜在风险与影响；

b）在项目初始阶段执行个人信息安全影响评估流程，有助于更加透彻地理解个人信息保护要求，确保在职能与非职能要求中加入个人信息保护要求（可实现、可行、可追踪），进而为产品或服务设计与交付提供风险维度的决策依据；

c）在产品或服务交付后，产品功能、互联网安全环境、法律法规变更时，对个人信息安全影响评估结果进行审核和修订，有助于组织及时跟踪产品或服务的安全风险，及时防范或弥补，避免对组织或用户带来更大的损失。

对于监管机构，个人信息安全影响评估报告可提供证据，证明某组织遵守适用法律、法规和标准要求。此外，如发生个人信息方面的违规、投诉等情况，个人信息安全影响评估可提供组织已进行尽职调查的相关证据。

对于组织的合作伙伴或服务商，个人信息安全影响评估是一种工具，用于评估个人信息处理者正在处理个人信息的方式是否会对个人信息安全带来不良影响，同时也可以作为合同义务的履行证据。

4.4 评估责任主体

通常，应由组织内部的安全职能部门对程序或信息系统执行个人信息安全影响评估流程，或者由客户组织或非政府组织对流程、信息系统或程序进行个人信息安全影响评估。

一般情况下，确保执行个人信息安全影响评估流程的责任首先应由负责保护个人信息的人员承担，或者由研发可能对隐私造成影响的新技术、服务或其他提案的项目经理承担。

应由最高级别的个人信息安全影响评估管理员负责确保评估流程的执行及结果的质量。经指派负责进行个人信息安全影响评估的人员可选择自行执行评估流程，或请求其他内部和/或外部相关方提供帮助，或将个人信息安全影响评估流程外包给独立第三方，上述方法都有各自的优缺点，可适当搭配使用。

当由组织自行进行个人信息安全影响评估时，监管机构和客户可以要求独立审计机构来核证评估活动的合理性。

组织应确保其已经明确个人信息安全风险管理的责任，包括个人信息安全风险管理流程的执行与维护，以及确保所有控制措施的适当性与有效性等。组织应指定人员负责个人信息安全风险管理框架的制定、执行与维护，安全控制措施的维护，以及相关个人信息安全影响和风险相关的报告。

4.5 评估规模

个人信息安全影响评估的规模往往取决于受到影响的个人信息主体范围和程度。如果影响的对象仅为组织内部员工时，可以仅针对员工的典型代表开展小规模的评估；如果政府部门希望为公民福利建议一个新的标识符管理系统，则需要实施一个更大范围的个人信息安全影响评估活动，同时涵盖外部的相关方。

通常，组织还会对其业务处理的个人信息实施自评估，以满足法律法规的需要，其中，个人信息的总量、类别、敏感程度、涉及个人信息主体的数量，能访问个人信息的人员等都会成为影响实际评估规模的重要因素。

中小企业实施个人信息安全影响评估时，应把握适当的评估规模，评估宜由相应的安全管理岗位人员完成，而非聘用专职从事个人信息安全影响评估的人员，选取外部专家进行评估也是一种可行路径。

4.6 评估原理

个人信息安全影响评估的基本原理如下图。

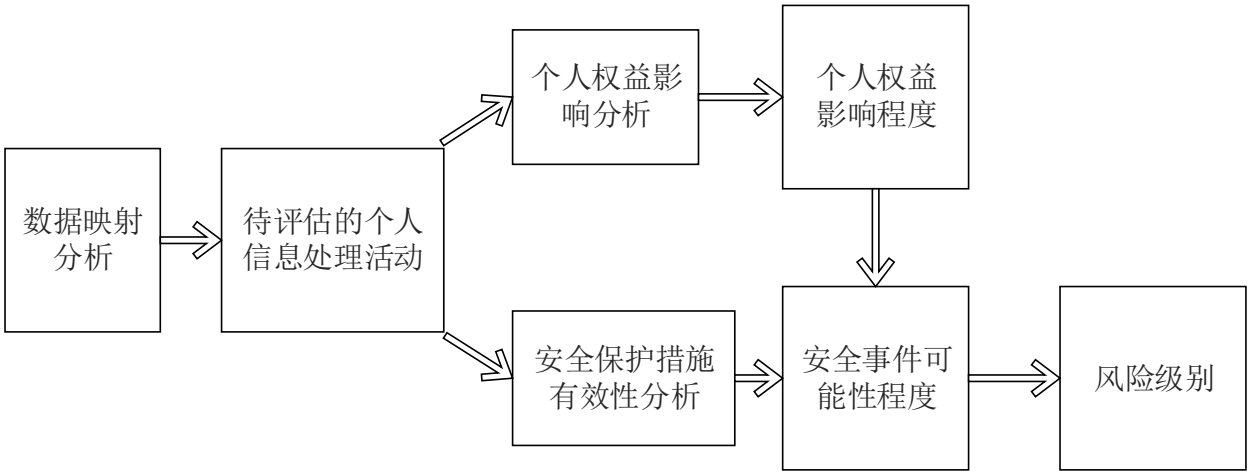

图1 评估原理示意图

评估前，对个人信息控制者的个人信息处理过程进行全面的调研，形成清晰的数据清单及数据映射图表。同时结合个人信息处理的具体场景，初步判定所处理的个人信息哪些属于个人敏感信息，梳理出待评估的个人信息处理活动。

评估过程中，首先，分析个人信息处理活动对个人权益造成的影响，并判定相应的影响程度；其次，对个人信息处理活动涉及的特点、安全措施、相关方、规模等进行分析，判定相应影响相关安全事件发生的可能性。最后，综合分析影响程度和可能性两个要素，得出风险等级，并给出相应的改进建议，最终形成评估报告。

4.7 实施流程

介绍个人信息安全影响评估的基本实施流程包括：评估准备阶段、必要性分析阶段、数据映射分析阶段、个人权益影响分析阶段、安全事件可能性分析阶段、风险分析阶段、评估报告阶段、风险处置和持续改进阶段、评估报告发布阶段。

4.8 评估活动

在评估过程中，所采用的基本评估方法，包括但不限于以下三种：

访谈：指评估人员对信息系统相关人员进行谈话，以促进对信息系统中个人信息保护措施设计和实施情况的了解、分析或取证。访谈的对象为个人或团体，如产品经理、研发工程师、个人信息保护负责人、法务负责人员、系统架构师、安全管理员、运维人员、人力资源人员和用户等。

检查：指评估人员通过对管理制度、安全策略和机制、合同协议、安全配置和设计文档、运行记录等进行观察、查验、分析，以便理解、分析或取得证据的过程。检查的对象为规范、机制和活动，如个人信息保护策略规划和程序；系统的设计文档和接口规范；应急规划演练结果；事件响应活动；技术手册和用户/管理员指南；信息系统的硬件/软件中信息技术机制的运行等。

测试：指评估人员通过人工或自动化安全测试工具进行技术测试，获得相关信息，并进行分析以便获取证据的过程。测试的对象为机制和活动，如访问控制、身份识别和验证、安全审计机制；传输链路和保存加密机制；对重要事件进行持续监控；测试事件响应能力，以及应急规划演练能力等。

4.9 评估工作形式

个人信息安全影响评估分为自评估和检查评估两种形式，个人信息安全影响评估应以自评估为主，自评估和检查评估相互结合，相互补充。

自评估是指个人信息控制者自行发起对其个人信息处理行为的评估，自评估可以由本机构组织专门负责评估、审计的部门和角色开展，也可以委托外部专业机构开展评估工作。

检查评估是指个人信息控制者的上级机构组织或由国家职能部门依法开展的个人信息安全影响评估工作。检查评估也可以委托外部评估技术服务支持，应要求外部机构的评估结果对检查机构负责。

5 评估流程

5.1 必要性分析

组织应在新的产品或服务的开发、启动、发布等环节分析针对其开展新的个人信息安全影响评估工作的必要性，如有必要，则需要确定评估责任人员，界定评估范围、边界和评估的适用性，评估所依赖的技术文档，评估工具与计划流程，评估需调研人员，评估报告的种类与发布形式等。必要时，可以专门编制必要性分析报告，以推动组织内部按计划开展个人信息安全影响评估工作。

通常情况下，出现本标准第 6 章的情形时可开展新的或更新个人信息安全影响评估程序。

5.2 评估准备工作

准备阶段的工作主要包括：组建评估团队、制定评估计划、确定评估对象和范围、相关方咨询等。

5.2.1 组建评估团队

组织应确认并任命负责进行个人信息安全影响评估的人员（评估人）。此外，组织还应指定人员负责签署评估报告。

评估人应定义风险准则，确保高级管理层认可该用于评价风险严重程度的风险标准。该标准可能以现有标准要求所示内容为基础，或者由组织单独制定（以及评估影响程度及各等级风险的标准）。此外，评估人还应确认风险接受标准并确保管理层认可该标准。

风险准则应反映组织的价值、目标与资源。在制定风险准则时，评估人应考虑以下因素：

a）影响个人信息保护的法律与监管因素；

b）外部因素，如行业准则、职业标准、公司政策与客户协议；

c）由具体应用预先决定的因素、或者在特定用例情境下预先决定的因素；

d）会影响信息系统设计及相关个人信息保护要求的其他因素。

组织管理层应分别从个人信息主体的视角和组织的视角出发审视个人信息安全风险。为制定用于评价个人信息安全风险重要程度的规则，评估人应回答以下问题：

a）用于评估对个人信息主体与组织的影响程度的标准是什么？（例如，识别水平、泄露的个人信息的敏感程度、受影响的个人信息主体的数量、组织影响程度）。

b）用于评估可能性的标准是什么？（例如，支持资产的漏洞、风险源利用漏洞的能力。）

c）用于评估影响程度的标尺？

d）用于评估可能性的标尺？

e）用于评价风险的各种组合（影响程度与可能性）的重要程度？尤其重要的是，风险接受标准是什么？

f）适用于应对各种情况的策略是什么？尤其重要的是，用于确认风险是可接受的策略是什么？

g）处理个人信息优势将对策略产生怎样的影响？

注：上述准则应与组织内部使用的其他风险标准保持一致，同时，每次使用准则时应考虑是否有改进机会。

应综合以上考虑和问题，基于以下内容定义风险准则：

a）对产品、服务或系统使用者的伤害。此类伤害包括身体、经济、名誉损失，家庭生活被打扰或陷入尴尬境地。此外，当考虑个人信息安全风险对个人的影响时，组织应考虑不同类型的个人信息，例如人身信息、位置与空间信息、行为信息、通信内容、数据与图像信息、思想感情信息、以及交际信息；

b）法律与监管要求，以及合同义务；

c）相关方的期望与看法，对商誉及名誉的负面影响；

d）个人信息可用性、机密性及完整性在运营方面的重要性；

e）信息处理的战略价值，如信息处理产生现有价值和未来的机遇。

应清楚规定是否会进行公众咨询、个人信息安全影响评估报告将提交给谁、个人信息安全影响评估的名义预算及时间段、是否会公布评估报告或摘要。个人信息安全影响评估的最低要求应取决于法律或监管限制、或者组织认定的个人信息安全风险重要程度。

如有必要评估人应申请团队支持，例如由 ICT 部门、相关业务单位、及法律部门的代表构成的团队。组织内部个人信息安全影响评估需要组织管理层给予长期大力支持，管理层应确保为个人信息安全影响评估团队配置必要资源。

5.2.2 制定评估计划

评估计划应考虑待进行的评估活动的范围、如有必要应允许迭代进行，包括个人信息安全影响评估报告的迭代。当评估涉及大量资源时这一做法尤为有效，但针对复杂程度较低的小型提案时，非必要流程。此外，计划还应考虑到待评估提案中断的情况。

计划应清楚规定完成个人信息安全影响评估报告须进行的工作、相关工作具体由评估团队中的哪些成员负责、评估计划表、以及如果进行咨询、咨询的进行方式。计划应说明在某些具体情况下为什么咨询相关方是非常重要的、将咨询哪些人员、以及具体的咨询方式（例如通过公众意见调查、研讨会、焦点小组、公众听证会、线上体验等等）。

评估人完成评估计划的编制后，应评估执行成本、向组织的高级管理层申请基本预算及人力资源。根据具体计划，可能会上调高级管理层最初设定的名义预算，或者，负责进行个人信息安全影响评估报告的人员可能需要根据可用预算修订评估计划。

组织应为个人信息安全影响评估报告配置合适资源。具体操作时应考虑以下方面：

a）人员、技能、经验及能力；

b）执行各项任务所需时间；

c）进行评估每一步骤所需资源，如自动化的评估工具等。

5.2.3 确定评估对象和范围

应从以下三个方面描述评估的对象和范围。

a）描述系统需求信息，包括但不限于：

1）处理个人信息的类型目的；

2）对当前或未来将获得信息系统支持的业务流程的描述；

3）针对信息系统定义的职能要求清单及其义务或执行水平；

4）信息安全目标；

5）关于数据收集方式、收集对的数据的说明。说明中应阐明谁将有权访问个人信息，包括个人信息主体访问权限的相关参数；

6）如果预定与第三方共享信息系统或其中的个人信息，则应就信息系统或个人信息的共享人、以及共享目的提供详细信息及相关建议；

b）描述系统设计信息，包括但不限于：

1）功能（或逻辑）结构概览；

2）物理结构概览

3）包含个人信息的信息系统数据库、表格和字段的清单和结构；

4）按部分和接口划分的数据流示意图；

5）个人信息周期的数据流示意图，例如个人信息的生成、应用、转移和处理；

6）描述在什么时间通知个人信息主体、以及什么时间取得个人信息主体同意的工作流程图；

7）定义已连接个人信息主体及已转移数据字段的接口清单；

8）关于端口、协议、APIs、及加密的详细信息。

c）描述处理流程和程序信息，包括但不限于：

1）信息系统的身份与用户管理概念；

2）操作概念，包括信息系统或其中部分结构在现场运行、外部托管、抑或云外包，以及具体位置；

3）支持概念，非常重要的一点是列示参与信息系统支持的第三方名称、他们拥有的个人信息访问权限的大小、以及从哪些位置可以访问个人信息；

4）记录概念及已登入信息的保存计划；

5）备份与恢复计划；

6）元数据的保护与管理；

7）数据保存与删除计划及媒介的处置。

描述上述内容的方式可以有以下几种：可用于为评估执行人员提供必要的背景信息、可归入评估报告中、或者在咨询相关方时可用作简报。项目说明中应提供一些背景信息（例如执行项目的原因、目标市场的构成、所描述的技术、服务、系统或其他提案影响隐私的具体方式、将处理的个人信息以及用于处理个人信息的平台）。项目说明中应指明项目的负责人及重要的里程碑事件，尤其应说明在什么时候制定可影响项目设计方案的决策。

5.2.4 相关方咨询

相关方包括但不限于：

1）员工，例如人力资源、法律、信息安全、财务、业务运营职能、通信与内部审计（尤其是在监管环境下）相关人员；

2）个人信息主体；

3）消费者代表；

4）分包商；

5）业务合作伙伴；

6）系统开发人员；

7）系统运维人员；

8）对于评估有相应担忧的其他组织人员。

为保证评估流程的透明、实现评估解决安全风险的目标，评估执行负责人应详细确认与进入评估程序的流程、或者正在处理中的个人信息的保护具有利益关系、或受上述两者影响的内部或外部相关方。相关方可以是拥有或可能获取个人信息访问权限的所有个人信息主体。

评估人应确认相关方的各个种类、然后具体确认各类相关方中的具体个人，个人应尽可能具有代表性。个人信息的范围与规模，对于确定恰当的相关方非常重要。如果正在执行的是大型政府项目，可能存在许多相关方。在这种情况下，社会利益群体，例如消费者代表可能被确认为相关方，另外还需确认处理个人信息、以及为个人信息主体的相关方。相反，一些小型的商业流程，可能不需要确认这样宽泛的相关方清单。

制定咨询计划应明确不同的相关方所受影响、后果（如果已知）、以及所采取的管理措施等相关问题。计划中还应包含咨询规模及计划表，内容包括但不限于：

a）与相关方合作识别并评估个人信息安全影响；

b）就评估报告草案咨询相关方意见以确认报告草案是否充分反映他们对有关问题的关注。

c）将咨询的相关方的数量与范围，个人信息安全影响程度、安全事件的可能性、以及可能受到影响的个人信息主体数量进行假设。

例如，如果风险的波及范围仅限定于某一个组织的员工，则咨询范围仅限于该组织员工和/或其代表。然而，如果预期风险将影响到国家内的每一个人，组织应广泛咨询外部相关方的意见。如果，最初组织认为仅有小量相关方可能受到影响，但后续认识到受影响人员的数量可能要大得多且风险也要大得多，则组织应根据情况修订其咨询计划并尽力咨询大量相关方的意见。

相关方的反馈意见所确认的问题可能与风险感知有关、而非实际风险，但不应忽略这些意见、而是应该将这些意见放在更广泛的相关方管理问题中进行处理，为交流活动提供帮助。

对于许多独立、但却非常相似的项目而言，如果能够重复使用咨询结果，咨询相关方意见所造成的潜在重要影响可能降至最低。如果预计许多项目面临类似的个人信息保护问题，重复使用适用咨询结果可以为咨询设计提供有用信息。咨询范围不应过于宽泛，在合理判断下可实现对咨询结果的重复利用。对于新项目中的新问题，以递增方式进行咨询，有助于规避不当影响。

可根据领域专项准则，按市场领域调整相关方。在同一市场领域中的组织，可使用领域特有的准则作为基准来评估和应对隐私与安全风险。此类准则应与本文件原则保持一致，应基于特定市场领域的常见业务流程与服务明确风险和控制措施。

对于中小企业而言，咨询相关方的意见所带来的利益、可能与所消耗的时间和成本不成比例。对此类企业而言，当他们能够参考相应准则时，领域专项准则的理念可以改善个人信息安全影响评估的全面性及品质。

5.3 数据映射分析

组织应针对个人信息控制者的个人信息处理过程进行全面的调研，形成清晰的数据清单及数据映射图表（可参考附录 B 表 B-1 和表 B-2）。数据映射分析阶段需结合个人信息处理的具体场景，初步判定所处理的个人信息哪些属于个人敏感信息。

调研内容包括个人信息收集、存储、使用、对外提供、废弃环节涉及的目的和具体实现方式，以及个人信息处理过程涉及的资源和相关方（如策略和规程、合同和协议、内部信息系统、个人信息处理者、第三方、交易平台经营者、外部服务供应商、云服务商等）（可参考附录 B 表 B-3），调研过程中应考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。

梳理数据映射分析的结果，根据个人信息的类型、敏感程度、收集场景、处理方式、涉及相关方等

要素，对个人信息处理活动进行分类，并描述每类个人信息处理活动的具体情形，便于后续分类进行影响分析和风险评价。一般情况下个人敏感信息处理活动和普通个人信息处理活动不归于同一类。

5.4 个人权益影响分析

个人权益影响分析一般指根据不同的个人信息处理活动，分析其是否存在对个人信息主体权益产生影响。个人权益影响概括可分为“影响个人自主决定权”、“引发差别性待遇”、“个人名誉受损或遭受精神压力”、“个人财产受损”四个维度：

a）影响个人自主决定权。如，被强迫执行不愿执行的操作、缺乏相关知识或缺少相关渠道更正个人信息、无法选择推送广告的种类、被蓄意推送影响个人价值观判断的资讯、个人人身自由受限、可能引发人身伤害等；

b）引发差别性待遇。如，因疾病、婚史等信息泄露造成的针对个人权利的歧视；因个人消费习惯等信息的滥用而对个人公平交易权造成损害等；

c）个人名誉受损或遭受精神压力。如，被他人冒用身份、公开不愿为人知的事实（生活习惯、以往经历等），被频繁骚扰、监视追踪等；

d）个人财产受损。如，账户被盗、遭受诈骗、勒索等。

组织应根据本标准 5.3 所述过程识别的数据映射分析结果及梳理得到的个人信息处理活动，通过查阅支撑性文档、检查个人信息处理过程、测试相应的处理机制等方法，分析个人信息在数据流程以及个人信息处理活动全生命周期的范围内，评价组织的个人信息保护策略的执行情况、相关法律法规与政策标准的符合性情况，并审视是否存在侵害个人信息主体权益的风险。

注：支撑性文档包括（但不限于）各类需求和设计文档、管理制度和记录、数据库表单结构说明、个人信息保护协议等。

个人权益影响分析过程一般包含对个人信息处理过程弱点分析、问题确认，以及影响分析三个阶段。

在个人信息处理过程弱点分析阶段，组织应参照与国家有关法律法规和政策标准要求，依据数据映射分析与个人信息处理活动结果，对个人信息处理过程进行全生命周期、全流程的分析，识别个人信息处理过程中可能存在的薄弱环节。个人信息处理过程弱点分析应至少包含以下内容：

- 个人敏感信息的判定是否准确；
- 收集个人信息的目的是否正当、合法；
- 从第三方获得的数据是否得到正式的处理授权；
- 告知方式和告知的内容是否友好可达，是否所有的处理活动都征得了用户同意；
- 是否定义了个人信息最小元素集，是否收集了过多的个人信息；
- 是否提供便捷有效的个体参与的机制；
- 变更目的处理对个人信息主体产生的影响；
- 接收个人信息的第三方是否会变更目的使用个人信息；
- 去标识化（匿名化、假名化等）后的个人信息是否能够被识别；
- 是否提供及时有效的安全事件通知机制和应急处置机制；
- 是否提供有效的投诉和维权渠道等。

在个人信息处理活动问题分析阶段，组织应依据个人信息处理过程弱点分析的结果，对各弱点的潜在问题进行深入挖掘分析，寻找归纳引起弱点出现的根本性问题。个人信息处理活动问题分析应该至少包含以下内容：

- 私自变更目的使用数据；
- 散播不准确的数据或不完整的误导性数据；

- 诱导或强迫个人提供过多个人信息；
- 过多地追踪或监视个人行为造成影响；
- 意料之外的数据披露对个人造成影响；
- 无根据地限制个人控制其个人信息的行为等。

在个人权益影响分析阶段，组织应结合前两阶段的弱点分析与问题归纳结果，综合组织的个人信息处理活动各环节涉及的个人信息特征、敏感程度，分析上述弱点与问题对个人权益可能造成的影响，及其严重程度。个人权益影响程度评估可参考本标准附录 A.1。

实施个人权益影响分析时可参考附录 B 表 B-4。

5.5 安全事件可能性分析

决定个人信息安全事件发生的要素很多，就威胁源而言，有内部威胁源，也有外部威胁源；有恶意人员导致的数据被窃取等事件，也有非恶意人员无意中导致的数据泄露等事件，也有物理环境影响导致的数据毁损；有技术因素导致的数据泄露、篡改、丢失等事件，也有管理不当引起的滥用等事件。为简化安全事件可能性的分析过程，将与安全事件可能性相关的要素归纳为以下四个方面：

a）网络环境和技术措施。如，所处网络环境、与其他系统的交互方式、采取的加密、授权、访问控制、审计、备份等技术措施；

b）处理流程规范性。如，个人信息收集的规范性、个人信息保存的周期、个人信息使用的限制、个人信息对外提供的授权、个人信息保护机构设置合理性、收到的个人信息处理相关的投诉等；

c）参与人员与第三方。如，人员资格审核情况及具备的技能、涉及处理个人信息人员的安全意识、人员职责有效履行的情况、第三方处理个人信息过程的可控性等；

d）安全态势及处理规模。如，近期内遭受网络攻击或发生安全事件的情况、近期内收到过的安全相关的警示信息、当前或预计处理个人信息的规模、频率等。

组织应该对以上维度的相应内容进行充分了解，通过调研访谈、查阅支撑性文档、功能检查、技术测试等方式，识别已采取的措施与当前的状态。针对 5.4 中对个人权益影响分析的不同维度，从以上四方面导致安全事件发生的可能性进行综合评价，得到安全事件发生的可能性。安全事件可能性等级评估可参考本标准附录 A.2。

实施安全事件可能性分析时可参考附录 B 表 B-5。

5.6 风险分析

进行风险分析时，首先，应根据个人信息处理活动的目的、状态、相关个人信息的敏感程度，同时考虑个人信息主体数量、群体特征等要求，评价对个人权益影响的程度等级；其次，应根据个人信息处理活动涉及的特点、已实施的安全措施、相关方、处理规模等要素，同时考虑具备的事件处置经验、用户习惯、及预防性措施等，评价安全事件发生的可能性等级。最后，综合分析个人权益影响程度和安全事件可能性两个要素，得出风险等级。其中，风险分析的具体过程和风险等级的判定可参考附录A.3。

风险分析的实施过程可参考附录 B 表 B-6。

5.7 评估报告

评估报告的内容通常包括：个人信息保护专员的审批页面、评估报告适用范围、实施评估及撰写报告的人员信息、参考的法律、法规和标准、个人信息影响评估对象（应明确涉及的个人敏感信息）、评

估内容、涉及的相关方等，以及个人权益影响分析结果，安全保护措施分析结果、安全事件发生的可能性分析结果、风险判定的准则、合规性分析结果、风险分析过程及结果，风险处置建议等。

5.8 风险处置和持续改进

根据评估结果，选取并实施相应的安全控制措施进行风险处置。通常情况下，严重风险应立即处置，高风险应限期内处置，中风险应在权衡影响和成本后处置，低风险可选择接受。

个人信息控制者应持续跟踪风险处置的落实情况，评估剩余风险，将风险控制在可接受的范围内。此外，应将评估结果用于下一次个人信息安全影响评估工作。

5.9 评估报告发布

公开发布个人信息安全影响评估报告是促进自合规、配合监管、增加客户信任的重要方式，公开发布的个人信息安全影响评估报告可以在已有评估报告基础上予以简化，但其内容通常应不少于以下方面：收集和处理个人信息的必要性和给个人给来的益处、收集和处理的个人信息类型（个人敏感信息需单独强调）、个人信息处理的例外情况（法律法规规定）、合规性分析的概况、评估过程和结果概况、已实施和将要实施的风险处置措施概况、对个人信息主体的建议、实施评估责任部门或人员的联系方式和解答疑问的渠道等。

6 评估实施

6.1 合规性差距评估

6.1.1 整体合规性差距评估

个人信息控制者可根据所参考的个人信息保护相关法律、法规、政策及标准，直接分析当前执行的个人信息处理活动与其条款的差距（可参考附录 B 表 B-7）。该评估方式的应用场景包括但不限于以下情形：

a）产品或服务年度整体评估；

b）新产品或新服务（不限技术平台）设计阶段评估；

c）新产品或服务（不限技术平台）上线初次评估；

d）法律法规、政策、标准、外部环境等出现重变化时重新评估；

e）业务模式、信息系统、运行环境等发生重大变更重新评估；

f）发生重大个人信息安全事件后重新评估；

f）发生收购、兼并、重组等情形时。

对于合规差距分析过程中发现个人信息处理活动与法律、法规、政策、标准等的条款存在合规性差距的，可根据需要按照本标准第 5 章内容，启动相应的个人信息安全影响评估工作，评估该差距对个人信息主体权益可能造成的影响和风险。

6.1.2 局部合规性差距评估

个人信息控制者可根据所参考的个人信息保护相关法律、法规、政策及标准，对当前执行的个人信息处理活动中的部分子活动与相对对应条款的差距进行分析（可参考附录 B 表 B-7）。该评估方式的应

用场景包括但不限于以下情形：

a）新增功能需要收集新的个人信息时评估；

b）法律、法规、政策、标准出现部分变化时评估；

c）业务模式、信息系统、运行环境等发生变化时评估。

对于合规差距分析过程中发现个人信息处理活动与法律、法规、政策、标准等的条款存在合规性差距的，可根据需要按照本标准第 5 章内容，启动相应的个人信息安全影响评估工作，评估该差距对个人信息主体权益可能造成的影响和风险。

6.2 典型个人信息处理活动影响评估

6.2.1 典型评估场景

通常情况下，涉及以下针对个人信息的处理活动时，应实施个人信息安全影响评估：

a）个人信息出境前评估；

b）个人信息处理目的变更前评估；

c）个人信息委托处理、转让、共享或公开披露前或范围发生变化时评估；

d）个人信息匿名化和去标识化效果评估；

e）其他情形，包括但不限于：

1）需要对去标识化后的数据重标识使用时；

2）通过购买、从合作伙伴获得方式收集、使用个人信息时；

3）使用“征得同意例外”条款收集、使用个人信息时；

4）使用“默许同意”方式收集个人信息时；

5）对政府、监管部门、司法部门提供个人信息前；

6）出现用户申诉且纠纷未解决时。

6.2.2 个人信息出境安全评估

个人信息出境情场景的评估可参照 GB/T XXXX《信息安全技术 数据出境安全评估指南》中的相应内容。

6.2.3 个人信息处理目的变更前的影响评估

分析个人信息处理活动的影响时，需要考虑多种因素，以评估“与收集个人信息时所声称的目的具有直接或合理关联的范围”的影响为例，如果新设目的与原目的目的有直接或合理的关联，则不会为个人权益带来额外影响，无需再次告知用户并征得其明示同意。判断时是否有直接或合理的关联应至少需要考虑如下因素：

a）个人信息主体对原先目的、组织处理个人信息方式和方法的合理的理解程度；

b）个人信息收集时的场景，包括个人信息主体和个人信息控制者之间的关系、商品或服务的范围及使用的商标和名称、个人信息主体使用商品或服务的方式、商品或服务为个人信息主体提供的便利等；

c）特定场景中可合理预期的个人信息处理方式，如常规商业运营中，可预见到的将被使用的个人信息的类型，与个人信息主体之间直接互动的范围、频率、性质、历史，以及为提供商品或服务，或改进或推广商品或服务，可预见到的将被使用到的个人信息的类型。

如将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，应对结果中所包含的个

人信息进行去标识化处理，否则在对目的变更后的影响评估中可能会得出存在高风险的判断。

6.2.4 个人信息匿名化和去标识化效果评估

匿名化和去标识化对个人信息进行了技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体。但数据接收方可能会借助于额外的信息以及技术手段，进行重标识攻击，从而将去标识化的数据集归因到原始个人信息主体或一组个人信息主体。

常见的用于重标识的方法如下：

a） 隔离：基于是否能唯一确定一个个人信息主体，将属于一个个人信息主体的记录隔离出来；

b） 关联：将不同数据集中关于相同个人信息主体的信息关联；

c） 推断：通过其它属性的值以一定概率推断出一个属性的值。

评估个人信息匿名化和去标识化效果时，应充分考虑以下要素：

a） 个人信息匿名化和去标识化过程的规范性，所采用技术的通用性；

b） 匿名化后的个人信息是否为统计型结果；

c） 去标识化后的个人信息是否能够达到满足使用目的的最小元素集；

d） 匿名化和去标识化后的个人信息使用场景；

e） 数据处理者的安全保障能力；

f） 能否在公开渠道或数据交易机构获得类似的个人信息；

g） 未经处理保留的个人信息类型和内容的特殊性。

6.2.5 个人信息委托处理、转让、共享或公开披露前的影响评估

在对个人信息进行委托处理、转让、共享和公开披露前，应开展个人信息安全影响评估，评估的内容包括但不限于以下方面：

a） 个人信息的类型、数量、敏感程度等；

b） 是否向个人信息主体告知了转让、共享、公开披露的基本情况，并得到个人信息主体的明示授权同意；

c） 数据发送方的安全管理保障和安全技术保障能力；

d） 数据接收方的安全管理保障和安全技术保障能力（不包括公开披露）；

e） 数据接收方可能会开展的个人信息处理活动，或公开披露的个人信息可能会被使用的个人信息处理场景；

f） 个人信息是否进行过去标识化处理；

g） 发生个人信息安全事件后的补救措施；

h） 数据接收方所能响应个人信息主体的请求的范围，如：访问、更正、删除等。

6.2.6 个人信息安全事件影响评估

发生个人信息安全事件后，组织应及时评估事件可能造成的影响，并采取必要措施控制事态，消除隐患。评估影响时，应充分考虑以下因素：

a） 个人信息的类型、数量、敏感程度、涉及的个人信息主体数量等；

b） 发生事件的信息系统状况，对其他互联系统的影响；

c） 已采取或将要采取的处置措施及措施的有效性；

d） 对个人信息主体权益造成的直接影响和长期影响；

e） 向个人信息主体告知事件的方式和内容；

f） 是否达到《国家网络安全事件应急预案》等有关规定的上报要求。

6.3 可能产生高风险的个人信息处理活动影响评估

个人信息处理活动自身可能涉及对个人信息主体权益影响及相应风险较高的情况下，也应开展个人信息安全影响评估，可能产生高风险的场景包括但不限于：

a）涉及对个人信息主体评价、打分等直接画像行为，如进行负面标识、预测健康状态等；

b）使用个人信息进行自动分析给出司法裁定或其他对个人有重大影响的决定；

c）系统性的监控分析个人或个人信息，如在公共区域监控、采集个人信息等；

d）收集的个人敏感信息数量、比重较多，收集频率要求高，与个人经历、思想观点、健康、财务状况等密切相关；

e）数据处理的规模较大，如涉及50万人以上、持续时间久、在某个特定群体的占比高、涵盖的地理区域广泛或较集中等；

f）对不同处理活动的数据集进行匹配和合并，并应用于业务；

g）数据处理涉及弱势群体的，如未成年人、病人、老年人、低收入人群、文化水平偏低人群、寻求庇护人群等；

h）创新型技术或解决方案的应用，如生物特征识别、IoT、人工智能等；

i）处理个人信息可能导致个人信息主体无法行使权利、使用服务或得到合同保障等。

判断个人信息处理活动是否与上述情形相关，可在进行数据映射分析、合规性差距分析等过程中进行识别，一旦涉及上述情形，可针对以上场景评估影响和风险，同时应重视个人信息主体代表等相关方的咨询工作，保障评估的准确性。

附 录 A
（资料性附录）
个人信息安全影响评估参考方法

A.1 评估个人信息主体权益影响程度

个人权益影响程度评价可采用定性、半定量和定量的方式。个人权益影响程度判定原则见下表。

表A.1 个人权益影响程度判定原则

影响描述	影响程度
个人信息主体可能会遭受重大的，不可消除的，可能无法克服的影响。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等。	严重
个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等。	高
个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度。如付出额外成本、无法使用应提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等。	中
个人信息主体可能会 遭受一定程度的困扰，但尚可以克服。如被占用额外的时间、被打扰、产生厌烦和恼怒情绪等。	低

以定性方式为例，可从“影响个人自主决定权”、“引发差别性待遇”、“个人名誉受损和遭受精神压力”、“个人财产受损”四个维度，依据本标准表 A.1 的判定原则，对个人信息主体的权益进行影响程度评价。影响程度分为“严重”、“高”、“中”、“低”四个等级，影响程度判定可参考下表。

表 A.2 影响程度判定表

影响类别	影响程度判定原则	影响描述	影响程度
影响个人自主决定权	个人信息主体可能会遭受重大的，不可消除的，可能无法克服的影响。	如个人人身自由受限、遭受人身伤害。	严重
	个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大。	如，被强迫执行违反个人意愿的操作、被蓄意推送资讯影响个人价值观判断、可能引发个人人身自由受限或遭受人身伤害。	高
	个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度。	如，缺乏相关知识或缺少相关渠道更正个人信息、为使用应提供的产品或服务而付出额外的成本等。	中
	个人信息主体可能会 遭受一定程度的困扰，但尚可以克服。	如，被占用额外的时间。	低
引发差别性待遇	个人信息主体可能会遭受重大的，不可消除的，可能无法克服的影响。	如，因信息泄露造成歧视性对待以致被用人单位解除劳动关系。	严重
	个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大。	如，造成对个人合法权利的歧视性待遇、造成对个人公平交易权的损害（无法全部或部分使用应提供的产品或服务）。	高

影响类别	影响程度判定原则	影响描述	影响程度
	个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度。	如，造成误解、为使用应提供的产品或服务而需付出额外的成本（包含资金成本、时间成本等）。	中
	个人信息主体可能会 遭受一定程度的困扰，但尚可以克服。	如，被打扰、产生厌烦和恼怒的情绪等。	低
个人名誉受损和遭受精神压力	个人信息主体可能会遭受重大的，不可消除的，可能无法克服的影响。	如，名誉受损以致长期无法获得财务收入、导致长期的心理或生理疾病以至于失去工作能力、导致死亡等。	严重
	个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大。	如，名誉受损以致被用人单位解除劳务关系、导致心理或生理疾病以致健康遭受不可逆的损害等。	高
	个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度。	如，造成误解、名誉受损（通过澄清可全部或部分恢复）、产生害怕和紧张的情绪、导致心理或生理疾病（通过治疗或纠正措施，短期可痊愈）等。	中
	个人信息主体可能会 遭受一定程度的困扰，但尚可以克服。	如，被频繁打扰、产生厌烦和恼怒情绪等。	低
个人财产受损	个人信息主体可能会遭受重大的，不可消除的，可能无法克服的影响。	如，遭受无法承担的债务等。	严重
	个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大。	如，遭受金融诈骗、资金被盗用、征信信息受损等。	高
	个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度。	如，社会信用受损，为获取金融产品或服务需付出额外的成本等。	中
	个人信息主体可能会 遭受一定程度的困扰，但尚可以克服。	如，因个人信息更正而需执行额外的流程（或提供额外的证明性材料）等。	低

评估过程中，可先分析对某一个个人信息主体造成的影响程度，再根据处理活动的特征、群体性特征等要素修正影响等级，修正的条件可参考下表。

表 A.2 影响程度修正表

修正前影响程度	修正条件	修正后影响程度
严重	无	无
高	个人信息处理活动涉及个人敏感信息，且涉及的个人信息主体超过 10 万人。	严重
	个人信息处理活动涉及的个人信息主体超过 500 万人。	严重
	受影响个人信息主体群体抗财务风险能力差、心理承受能力差等情形。如未成年人、学生、老年人等。	严重
	其他不可控因素，如个人信息出境后保存地的法律、政策多变等。	严重
中	个人信息处理活动涉及个人敏感信息，且涉及的个人信息主体超过 500 万人。	严重

修正前影响程度	修正条件	修正后影响程度
	个人信息处理活动涉及个人敏感信息，且涉及的个人信息主体超过 10 万人。	高
	个人信息处理活动涉及的个人信息主体超过 500 万人。	高
	受影响个人信息主体群体抗财务风险能力差、心理承受能力差等情形。如未成年人、学生、老年人等。	高
	其他不可控因素，如个人信息出境后保存地的法律、政策多变等。	高
低	个人信息处理活动涉及的个人信息主体超过 500 万人。	中
	对个人信息主体造成困扰的频率过高时。	中

以半定量或定量方式为例，可根据个人权益受损对个人信息控制者付出的成本进行评价。成本一般包括：违规成本（如监管处罚、诉讼费用、整改费用等）、直接的业务损失（如流失客户减少了业务收入等）、名誉损失（如品牌形象受损、客户信任受损等）、内部企业文化损失(如企业执行力受损、价值观冲突引起员工积极性下降等)等。

A.2 评估安全事件发生的可能性

安全事件可能性等级评价可采用定性、半定量和定量的方式。安全事件可能性等级判定原则见下表。

表A.3 安全事件可能性等级判定原则

可能性描述	可能性等级
采取的措施严重不足，个人信息处理行为极不规范，安全事件的发生几乎不可避免。	很高
采取的措施存在不足，个人信息处理行为不规范，安全事件曾经发生过或已经在类似场景下被证实发生过。	高
采取了一定的措施，个人信息处理行为遵循了基本的规范性原则，安全事件在同行业、领域被证实发生过。	中
采取了较有效的措施，个人信息处理行为遵循了规范性最佳实践，安全事件还未被证实发生过。	低

以定性方式为例，可从“网络环境和技术措施”、“处理流程规范性”、“参与人员与第三方”、“安全态势及处理规模”等方面，依据本标准表 A.3 的判定原则，对安全事件可能性等级进行评价。可能性等级分为“很高”、“高”、“中”、“低”四个等级，安全事件可能性判定可参考下表。

表 A.4 可能性判定表

可能性描述	可能性等级
网络环境与互联网及大量信息系统有交互现象，基本上未采取安全措施保护个人信息安全。	很高
该个人信息处理行为为常态、不间断的业务行为，该行为已经对个人主体的权益造成了影响，或收到了大量相关的投诉，并引起了社会关注。	

任意人员可接触到个人信息，对第三方处理个人信息的范围无任何限制，或已出现第三方滥用个人信息的情形。	
威胁引发的相关安全事件已经被本组织发现，或已收到监管部门发出的相关风险警报。	
网络环境与互联网及其他信息系统有较多交互现象，采取的安全措施不够全面。	高
该个人信息处理行为为常态、不间断的业务行为，个人信息处理行为不规范，且收到了相关的投诉。	
对处理个人信息相关人员的管理松散，未对第三方处理个人信息的范围提出相关要求。	
威胁引发的相关安全事件曾经在组织内部发生过，或已在合作方已经发生，或收到过权威机构发出的相关风险预警信息，或处理个人信息的规模超过 1000 万人。	
网络环境与互联网及其他信息系统有交互现象，采取了一定的安全措施。	中
该个人信息处理行为为常态业务行为，个人信息处理行为规范性欠缺，且合作伙伴或同领域其他组织收到过相关的投诉。	
对人员提出了管理要求，对第三方处理个人信息的范围提出限制条件，但相应的管理和监督效果不明。	
威胁引发的相关安全事件已经同领域其他组织发现，或在专业机构相关报告中被证实已出现，或处理个人信息的规模超过 100 万人。	
网络环境比较独立，交互少，或采取了有效的措施的保护个人信息安全。	低
该个人信息处理行为非常态业务行为，个人信息处理行为符合规范，几乎没有出现关于该行为的投诉。	
对人员的管理和审核比较严格，与第三方合作时提出有效的约束条件并进行监督。	
威胁引发的安全事件仅被专业机构所预测。	

评估过程中，可根据事件自身的性质估计和经验数据评估其可能性，再根据个人信息控制者所实施的针对性安全控制措施，相关事件处置经验对可能性进行修正，修正的条件可参考下表。

表 A.4 可能性级别修正表

修正前可能性等级	修正条件	修正后可能性等级
很高	对相关的投诉有处置的经验，并得到了个人信息主体认同。	高/中
	针对安全事件的特征提前实施了有效的安全措施，或根据安全预警的内容及时提升了安全防护水平。	高/中
高	对相关的投诉有处置的经验，并得到了个人信息主体认同。	中
	针对安全事件的特征提前实施了有效的安全措施，或根据安全预警的内容及时提升了安全防护水平。	中
中	已实施了处理相关投诉问题的解决方案。	低
	针对安全事件的特征提前实施了有效的安全措施。	低
低	无	无

A.3 个人信息安全风险综合评估

综合分析个人权益影响程度和安全事件可能性两个要素，得出风险等级，并给出相应的改进建议，最终形成评估报告。风险等级可分为：严重、高、中、低四个等级。以定性分析为例，可参考下表。

表 A.5 风险等级判定表

风险等级		可能性级别			
		低	中	高	很高
影响级别	严重	中	高	严重	严重
	高	中	中	高	严重
	中	低	中	中	高
	低	低	低	中	中

附 录 B
（资料性附录）
个人信息安全影响评估常用工具表

表 B-1 基于系统组件的个人信息映射表

组件名	该功能是否收集、使用、存储个人信息	个人信息的类型	收集个人信息的方法	收集/使用个人信息的原因	实施的安全控制措施

表 B-2 基于个人信息生命周期的个人信息映射表

序号	个人信息的类型	涉及的信息系统组件	收集			存储		使用		对外提供		废弃
			目的	方法	控制措施	存储位置	控制措施	方式	控制措施	对象	控制措施	控制措施

表 B-3 个人信息保护相关方关系表

个人信息类型	个人信息主体涉及的主要群体	涉及的个人信息控制者		涉及的个人信息处理者		需要对外提供的第三方		涉及的其他相关机构（交易平台经营者、外部服务供应商、云服务商等）		涉及的其他情形（如跨境传输等）
		对象	责任部门和人员	对象	约束和监管机制	对象	约束和监管机制	对象	约束和监管机制	保护机制

表 5-4 个人权益影响分析表

个人信息处理活动	是否涉及个人敏感信息	识别脆弱点	情况描述	发现证据	个人信息处理活动存在的问题	对个人权益产生的影响
处理活动 A	敏感/非敏感	个人敏感信息的判定是否准确				
		收集个人信息的目的是否正当、合法				
		从第三方获得的数据是否得到正式的处理授权				
		新设个人信息处理目的是否超出原有目的				
		个人信息受让方采取的个人信息保护措施的有效性				
		公开披露个人信息对个人权益造成的影响				
处理活动 B						

表 B-5 安全事件可能性分析表

个人信息处理活动	涉及的信息系统组件	是否涉及个人敏感信息	对个人权益的影响	已实施的措施	相应证据	可能发生的安全事件	安全事件发生的可能性
处理活动A		敏感/非敏感	影响个人自主决定权				
			引发差别性待遇				
			个人名誉受损或遭受精神压力				
			个人财产受损				
处理活动B							

表 B-6 风险分析过程表

个人信息处理活动	对个人权益的影响	影响程度	安全事件可能性	风险等级	风险处置建议	风险涉及的相关方
处理活动A	影响个人自主决定权					
	引发差别性待遇					

	个人名誉受损或遭受精神压力					
	个人财产受损					
处理活动 B						

表 B-7 合规差距分析表

条款编号	条款内容	分析内容	处理活动 A	处理活动 B	处理活动 C
1.1		个人信息处理活动描述			
		合规性差距分析			
		对个人权益产生的影响			
1.2		个人信息处理活动描述			
		合规性差距分析			
		对个人权益产生的影响			