ICS 35.020
CCS L 70

团　　体　　标　　准

T/GDCSA 021-2024

个人信息保护合规管理实施指南

Personal information protection compliance management implementation guide

2024-12-20 发布　　2025-01-20 实施

广东省网络空间安全协会　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》的规定起草。

本文件由北京神州绿盟科技有限公司提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：北京神州绿盟科技有限公司、深圳大学、广州市数字政府运营中心、广东电网有限责任公司电力科学研究院、网安联认证中心有限公司、广州华南检验检测中心有限公司、绿盟科技集团股份有限公司、广东新兴国家网络安全与信息化发展研究院、北京网络空间安全协会、广东关键信息基础设施保护中心、国源天顺科技产业集团有限公司、广东中证声像资料司法鉴定所、广州绿盟网络安全技术有限公司、广州网络空间安全协会、揭阳网络空间安全协会。

本文件主要起草人：胡斌、曾令平、江魁、赵宇丹、冷令、方程、戴少锋、郝瑞、石晓君、黄劲、刘磊、彭小辉、王伟彬、林实、刘国栋、过晓冰、黄缙华、梁世伟、郭涛、成珍苑、黎韵婷、黄珊珊、覃丽娟、刘悦、刘雪敏、刘常乐、尹文娟、尹亮。

个人信息保护合规管理实施指南

1 范围

本文件规定了个人信息保护合规管理实施的原则、基本要求以及进阶提升等内容。

本文件适用于开展个人信息保护合规管理工作的企事业单位、社会团体、政府部门以及其他各类组织机构（以下统称为组织），也可为监管、检查、评估等活动提供参考。

2 规范性引用文件

下列文件中的内容通过文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，仅该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。

GB/T 25069-2022 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 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 41817-2022 信息安全技术 个人信息安全工程指南

GB/T 43697-2024 数据安全技术 数据分类分级规则

3 术语和定义

下列术语和定义适用于本文件。

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，不包括匿名化处理后的信息。

[来源：GB/T 35273-2020,3.1，有修改]

3.2

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：GB/T 35273-2020,3.2，有修改]

3.3

个人信息处理者 personal information processor

在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

[来源：GB/T 35273-2020,3.4，有修改]

3.4

个人信息主体 personal information subject

个人信息已识别或者可识别的自然人。

[来源：GB/T 35273-2020,3.3，有修改]

3.5

个人信息处理活动 personal information processing activities

个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.6

个人信息保护合规管理 personal information protection compliance management

组织以有效防控个人信息保护合规风险为目的，以提升依法个人信息保护合规经营管理水平为导向，以组织个人信息保护经营管理行为和员工履职行为为对象，开展的包括建立个人信息保护管理制度和操作规程、完善个人信息保护运行机制、培育个人信息保护合规文化、强化个人信息保护监督问责等有组织、有计划的管理活动。

3.7

个人信息保护合规风险 personal information protection compliance risk

因未遵守个人信息保护合规管理而需要承担民事法律责任、行政法律责任或者刑事法律责任的可能性及其后果。

3.8

大型互联网平台运营者 large internet platform operators

注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，具有强大社会动员能力和市场支配地位，数据处理活动对国家安全、经济运行、国计民生等具有重要影响的互联网平台运营者。

注：互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

3.9

重要数据处理者 key data processor

在重要数据处理活动中自主决定处理目的、处理方式的组织。

[来源：GB/T 43697-2024,3.11，有修改]

注：个人一般不作为重要数据处理者。

4 缩略语

下列缩略语适用于本文件。

APP：移动互联网应用程序（Mobile Internet Application）

API：应用程序接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

SSD：固态硬盘（Solid State Drive）

VPN：虚拟专用网络（Virtual Private Network）

5 原则

5.1 个人信息保护基本原则

参考国家法律法规及 GB/T 35273-2020 第 4 章相关内容，个人信息保护应遵循以下基本原则：

a) 合法处理基础：应当坚持个人信息处理的合法性基础，个人信息处理者不得超出处理个人信息的法定情形。

b) 合规基本原则：应当坚持合法、正当、必要、诚信原则，个人信息处理者不得从事与服务目的无关的个人信息处理活动。

c) 总体保护原则：遵循“整体一致、合法正当、目的明确、告知同意、最小必要、公开透明、确保安全、主体参与”的总体原则，设计并实施覆盖个人信息处理活动的安全保护策略。

5.2 个人信息保护合规管理框架

从个人信息保护合规管理基本原则、个人信息保护合规管理基本要求和个人信息保护合规管理进阶提升三个方面提出了总体要求。个人信息保护合规管理框架，见图 1 所示：

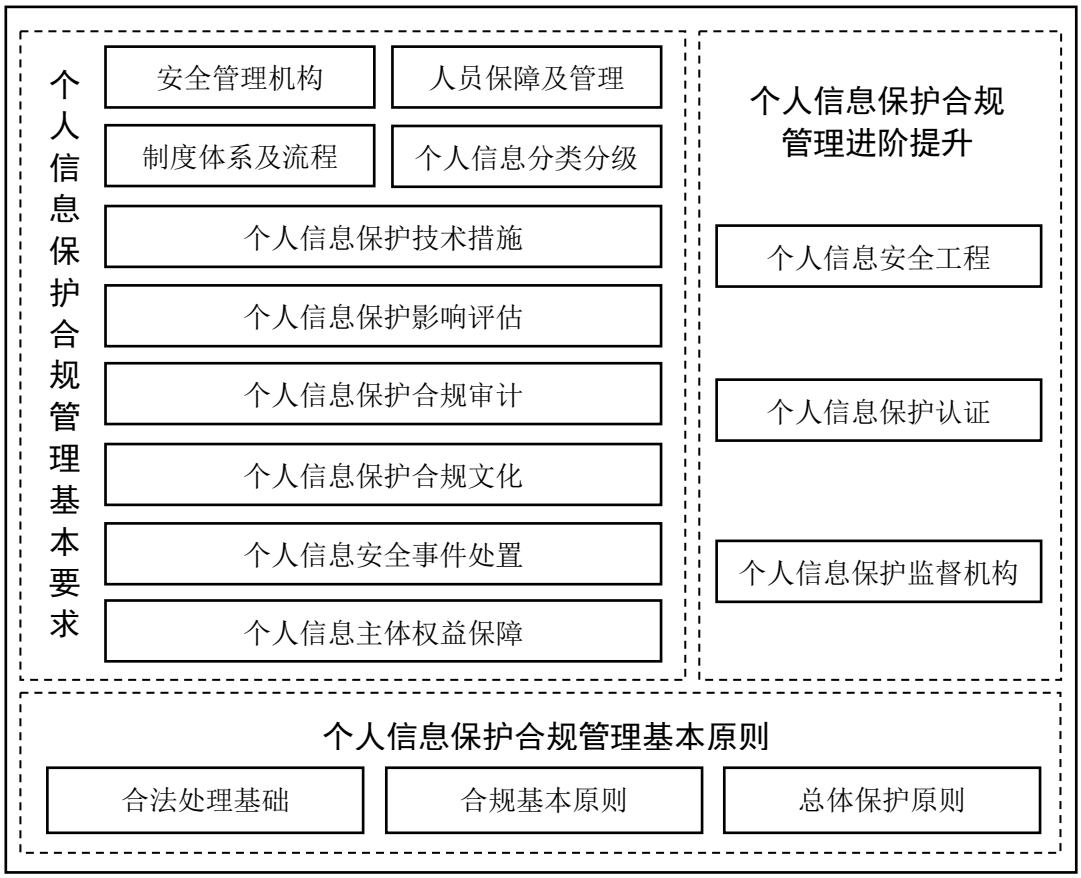

图1 个人信息保护合规管理框架

6 基本要求

6.1 安全管理组织

个人信息保护管理组织应由最高管理者（如法定代表人）、个人信息保护负责人、各部门个人信息

保护负责人、人力资源管理部门负责人、个人信息处理相关责任人等组成。应根据组织具体情况设立专门的个人信息保护管理部门，负责组织的个人信息保护合规管理工作；或在既有的部门机构中增加对个人信息保护的描述，例如数据安全管理部门、人力资源管理部门等，该部门接受个人信息保护官或其他角色的领导。组织应发布机构设置及责任人任命，确定其职能职责，包括但不限于：

a) 依法制定并实施个人信息保护合规管理计划；
b) 制定个人信息保护合规管理制度和操作规程；
c) 监督本组织按照约定的个人信息处理规则处理个人信息，保护个人信息主体权益；
d) 采取有效措施保证按照约定的处理目的、范围、方式处理个人信息，履行个人信息保护义务，保障个人信息安全；
e) 组织开展个人信息保护影响评估；
f) 定期对本组织处理个人信息遵守中华人民共和国法律、行政法规的情况进行合规审计；
g) 组织开展个人信息安全教育和培训；
h) 接受和处理个人信息主体的请求和投诉；
i) 接受个人信息保护职责的部门对个人信息处理活动的监督，包括答复询问、配合检查等。

6.2 人员保障及管理

6.2.1 个人信息保护负责人配备条件

根据《中华人民共和国个人信息保护法》等法律法规要求，以下几类个人信息处理者应指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督，并公开个人信息保护负责人的联系方式，将个人信息保护负责人的姓名、联系方式等报送所在行业监管部门。负责人发生变更的，宜在 7 个工作日内重新报送并公告。

a) 主要业务涉及个人信息处理，且从业人员规模大于 200 人；
b) 重要数据处理者、关键信息基础设施运营者、大型互联网平台运营者等涉及个人信息处理的；
c) 处理 100 万人以上个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；
d) 处理超过 10 万人的敏感个人信息。

个人信息处理者应设立专职或兼职的个人信息安全管理岗位，加强个人信息安全相关管理，明确定义岗位职责。

6.2.2 个人信息保护负责人具体要求

6.2.2.1 个人信息保护负责人应当具备个人信息保护专业知识和相关管理工作经历，由个人信息处理者管理层成员担任，参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作。具体应满足以下要求：

a) 应具备与履行职责相适应的专业水平和相关管理工作经历。
——熟悉个人信息保护、数据安全等相关法律法规、政策、标准。
——为个人信息保护、数据安全等相关领域的合规或技术专家，或者在个人信息保护、数据安全等相关领域具有五年以上合规、测评等工作经验的资深从业人员。
b) 应具备与履行职责相适应的职业道德水平。
——政治可靠，具有较高的政治素质。
——遵纪守法，能够客观独立、公平公正、廉洁地履行职责。
——未曾因犯罪受过刑事处罚的、未曾被开除公职或者受到监管部门惩戒和处罚的。
c) 应了解组织业务的整体状况，熟悉业务流程，具备个人信息保护合规管理的能力。
d) 重要数据处理者、关键信息基础设施运营者、大型互联网平台运营者的个人信息保护负责人应接受安全背景审查。

6.2.2.2 个人信息保护负责人应承担下列职责：

a) 明确个人信息保护合规管理工作的主要目标、基本要求、工作任务、保护措施。
b) 对本组织个人信息保护合规管理负全面领导责任，提供人力、财力、物力保障，确保所需资源可用。
c) 指导、支持相关人员开展本组织的个人信息保护合规管理工作，确保个人信息保护合规管理工作达到预期目标。
d) 向本组织的主要负责人汇报个人信息保护合规管理工作情况，推动个人信息保护合规管理工作持续改进。
e) 其他职责可参考GB/T 35273-2020第11章相关内容。

6.2.3 个人信息保护管理岗位人员

个人信息安全管理岗位人员应具备个人信息保护和数据安全基本知识，熟悉本部门业务、个人信息处理流程、信息系统及相关设备设施、内部和外部环境等。具体应满足以下要求：

a) 明确内部涉及个人信息处理的岗位人员的安全职责，确定相应的权限，建立相应的内部制度。
b) 个人信息安全管理岗位人员签署个人信息保护协议。
c) 对营业场所、处理场所负责人以及具备大量访问、导出、删除生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息权限的岗位人员进行安全背景审查。
d) 定期（至少每年一次）和在个人信息保护政策发生重大变化时，对相关人员开展个人信息安全专业化培训和考核。

6.3 制度体系及流程

组织应制定、签发、实施、定期更新内部个人信息保护合规管理制度和操作规程，保障个人信息处理合规与安全。包括但不限于：

a) 应制定个人信息保护合规管理的总体方针和安全策略等纲领性制度文件，包括本组织的个人信息保护合规管理工作的目标、范围、原则和安全框架等相关说明。
b) 应建立个人信息保护合规管理制度体系，其中包括安全策略、管理制度、操作规程和记录表单。
c) 应建立个人信息分类分级管理要求，针对个人信息处理活动提出具体保护要求，实施相应的安全策略和保障措施，其中包括合理确定个人信息处理的操作权限，采取相应的加密、去标识化等安全技术措施。
d) 涉及处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。
e) 应建立个人信息保护影响评估制度，定期（至少每年一次）开展影响评估工作并处置个人信息处理活动存在的安全风险。
f) 应将个人信息泄露等相关个人信息安全事件处理纳入组织信息安全或数据安全事件应急处置工作机制，制定专门的流程和预案。定期评估应急处理流程和预案，及时保障、有效应对个人信息安全事件，降低安全事件造成的损失及不利影响。
g) 应建立个人信息保护合规审计制度要求，其中包括审计策略、审计对象、审计依据、审计周期、审计内容和审计报告。
h) 应建立个人信息投诉与申诉处理程序，明确投诉、举报与申诉受理部门、处理程序，对个人信息主体要求更正或删除组织收集其个人信息的情况予以受理、核实，并依据国家与行业主管部门要求予以处理和反馈。
i) 应建立针对个人信息处理相关人员的个人信息违规处置或者违规行为责任制度，并有效实施。

6.4 个人信息分类分级

6.4.1 概述

组织应遵循国家关于数据分类分级制度要求，对个人信息实行分类分级管理。参考 GB/T 35273-2020 及相关标准，根据个人信息的种类、来源、敏感程度、用途等，对个人信息进行分类分级，或在原有数据分类分级的基础上增加个人信息分类及确立对应级别。

6.4.2 个人信息分类

个人信息按照业务属性和安全属性分类的思路进行分类。安全属性以个人信息是否涉及个人隐私为标准，个人信息可以分为一般个人信息和敏感个人信息两个一级类别，业务属性则可采取“业务条线——关键业务——业务属性分类”的方式逐层分类，共同形成二层或三层子类框架。详见附录 A。

a) 根据个人信息的业务属性，组织对个人信息进行细化分类。常见业务属性包括但不限于：
   ——业务领域：按照业务范围或业务种类进行细化分类；
   ——责任部门：按照个人信息管理部门或职责分工进行细化分类；
   ——上下游环节：按照业务运营活动的上下游环节进行细化分类；
   ——主题：按照个人信息的内容主题进行细化分类；
   ——用途：按照个人信息使用目的进行细化分类；
   ——处理：按照个人信息处理者类型或个人信息处理活动进行细化分类；
   ——来源：按照个人信息来源进行细化分类。
b) 采用线分类法，按照业务属性（或特征），将个人信息分为若干大类，然后按照大类内部的个人信息隶属逻辑关系，将每个大类的个人信息分为若干层级，每个层级分为若干子类，同一分支的同层级子类之间构成并列关系，不同层级子类之间构成隶属关系。最小个人信息类是指属性（或特征）相同或相似的一组个人信息。

6.4.3 个人信息分级

个人信息分级，根据个人信息重要程度分为 2-4 个级别。具体如下：

a) 数据分级为 4 个级别框架下，如划分为极敏感级、敏感级、较敏感级、低敏感级。敏感个人信息不低于 4 级，个人信息不低于 2 级，组织内部员工个人信息不低于 2 级，去标识化的个人信息不低于 2 级，匿名化个人信息不低于 1 级。
b) 数据分级为 3 个级别框架下，如划分为敏感级或重要敏感级、较敏感级或一般敏感级、低敏感级或非敏感级，敏感个人信息不低于 3 级。个人信息不低于 2 级，组织内部员工个人信息不低于 2 级，去标识化的个人信息不低于 2 级，匿名化个人信息不低于 1 级。
c) 数据分级为 2 个级别框架下，如划分为敏感级和非敏感级，敏感个人信息不低于 2 级。

注 1：没有特别说明的情况下，数据分类分级框架是针对一般数据而言。

注 2：重要数据和核心数据的分级遵循国家及行业主管部门有关规定。

6.5 个人信息保护控制措施

6.5.1 账号权限

综合考虑主体角色、信用等级、业务需要、时效性等因素，依据权限最小化原则分配账号权限，通过技术手段（如统一门户、堡垒机等）统一实现账号认证和权限分配；对个人信息操作设置不同的使用权限，不同用户只能访问与自己职责对应的个人信息。

a) 对敏感个人信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。
b) 特权账号需明确安全责任人，如 root、adminstrator 或其他特权账号的安全责任人指定到系统管理员，同时严格限定特权账号的使用地点，并配套多因素认证措施对使用者进行实名认证。

c） 制定特权账号的使用场景和使用规则，并配套建立审批授权机制，应通过堡垒机进行操作。

6.5.2 日志管理

个人信息处理活动应留存详细的操作日志，操作日志至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等，留存时间不少于 6 个月。

6.5.3 收集

组织收集个人信息应在满足 GB/T 35273-2020 中第 5 章要求基础上符合以下管理要求：

a） 个人信息收集前，需向客户告知收集、使用的目的、方式和范围等规则，同时征得明示同意（征得同意前不得收集个人信息或通过 Cookies 等同类技术或通过调用权限、接口等方式收集个人信息），并告知不同意的后果；同时将客户主动点击、勾选、填写等作为功能开启的条件，确保功能开启后才可收集个人信息。

b） 通过 APP 收集必要个人信息还应符合 GB/T 41391-2022 附录 A 中规定的收集范围。

c） 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

d） 针对线下通过纸质表单办理业务时的个人信息收集，同样需通过合同协议条款（需明确采集规则等内容）、授权同意书等形式获得客户的签字同意。

e） 从外部数据提供方采集个人信息的，具体应满足以下要求：

——负责外部数据采购的牵头部门要求外部数据提供方说明其个人信息来源、采集范围和频度，并事前开展个人信息保护影响评估，以确认其合法性；必要时提供相关主体的授权，以了解外部数据提供方已获得的授权同意的范围、目的、方式，是否允许转让、共享、公开披露、删除等。

——通过合同协议等方式，明确个人信息采集范围、内容、类型、频率、用途、存储期限以及数据供应方提供不合法个人或者不真实个人信息时双方个人信息保护责任及义务。

——通过外部数据提供方等其他途径获得的个人信息，与直接收集的个人信息负有同等的保护责任和义务。

——应当制定外部个人信息采购、合作引入的集中审批管理机制，审查评估外部数据供应方相关个人信息采集合同协议内容和相关个人信息主体的授权信息，对个人信息来源的真实性、合法性进行安全审查，评估外部数据供应方的安全保障能力及其个人信息安全风险。

——记录个人信息收集行为的审批情况、对应合同协议内容。

f） 组织因业务确需，通过采取自动化手段从网站或公开数据库间接收集个人信息的，应符合国家有关要求，该行为等同于从外部数据供应方收集个人信息，除无需签署合同协议之外，应考虑其个人信息处理能力和网络承载能力，不得影响其正常运行，并遵循个人信息收集控制措施。

g） 停止提供其产品或者服务、响应个人信息主体合法权益要求或者合同协议履约终止时，应当立即停止个人信息收集活动，国家及行业主管部门另有规定的按照相关规定执行。

组织收集个人信息应在满足 GB/T 35273-2020 中第 5 章要求基础上符合以下技术要求：

a） 收集个人信息的系统、采集设备应符合国家要求，并对其进行鉴别，采用数据源鉴别技术防止数据源伪冒。

b） 对个人信息收集行为进行日志记录和安全审计，并采取技术措施确保信息来源的可追溯性，对超规模、超范围收集等异常行为进行告警。

c） 通过系统、采集设备批量收集的个人信息需采用摘要、消息认证码、数字签名等密码技术确保采集过程个人信息的完整性。

d） 对人工批量收集个人信息的环境进行安全管控，并通过人员权限管控、信息碎片化等方式，防

止采集过程出现个人信息泄露。

e) 在纸质表单电子化的过程中，采取技术措施对电子化过程中的数据完整性、保密性进行控制。

f) 采用个人信息主体直接录入方式收集敏感个人信息的，应当采取有效技术措施核验个人信息主体身份。

g) 采用信息系统间交互方式收集敏感个人信息的，应当采取有效技术措施核验双方设备或者信息系统的真实性和采集个人信息的完整性。

h) 应结合口令密码、设备指纹、设备物理位置、网络接入方式、设备风险情况等多种因素对采集设备或系统的真实性进行增强验证。

i) APP、WEB 等客户端相关业务完成后不留存敏感个人信息，限制采集过程中使用的临时存储文件，将缓存区域纳入统一安全管控范畴并及时进行清理，不得任意修改存储区域地址，对存储区域的方案实施最小权限原则，只允许采集、上传应用程序使用临时存储区域。

j) 对敏感个人信息收集全过程进行持续动态认证，确保采集设备或系统的真实性，必要时可实施阻断、二次认证等操作。

k) 对采集的敏感个人信息进行数据加密，优先使用 SM 系列等国家商用密码算法。

l) 因履行无障碍义务或者客观条件限制，采用纸质文件、影像或者代为录入等方式采集个人信息时，应当采取自动识别与人工核验等措施，确保个人信息录入及时性和准确性，并按照档案管理要求妥善留存原始个人信息收集凭证。

6.5.4 存储

组织进行个人信息存储时，应在满足 GB/T 35273-2020 中第 6 章要求基础上符合以下管理要求：

a) 在中华人民共和国境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定。

b) 依据最小够用原则存储个人信息，不以任何形式存储非业务必需的个人信息，存储时间为业务必需的最短时间，国家及行业主管部门另有规定的除外。

c) 敏感个人信息原则上不得在终端设备和移动介质中存储。组织应当统一明确敏感个人信息可在终端设备和移动介质中存储的特定场景，并按照规程履行审批手续后，在授权的终端设备和移动介质中存储，存储期限不得超过审批允许的期限。

d) 保存个人信息的主要设备，应对个人信息提供备份和恢复功能，确保个人信息备份的频率和时间间隔，并使用不少于以下一种备份手段：

——具有本地个人信息备份功能；

——将备份介质进行场外存放；

——具有异地个人信息备份功能，敏感个人信息应采取异地容灾。

e) 做好个人信息容灾应急预案，定期开展灾难恢复演练，对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。

f) 定期对备份人信息的有效性和可用性进行检查，定期对主要备份敏感个人信息进行恢复验证，并留存记录，根据介质使用期限及时转储个人信息，确保个人信息可用性。

组织进行个人信息存储时，应在满足 GB/T 35273-2020 中第 6 章要求基础上符合以下技术要求：

a) 采取一定技术措施确保个人信息存储的完整性，存储敏感个人信息时，应采用密码技术、权限控制等技术措施保证数据完整性。

b) 采取一定技术措施保证个人信息存储的保密性，必要时可采取多因素认证、固定处理终端、固定处理程序或工具、双人双岗控制等安全策略。

c) 收集的个人信息应根据不同级别采取相应的安全加密存储等安全措施进行处理，加密算法建议使用国家密码管理局推荐使用的加密算法，加密技术可采用专用加密芯片和设备的硬加密方式，也可采用 SM 系列算法等软加密技术。所有保存的个人信息宜为非明文方式。

d) 文件系统、存储介质、终端设备等存放个人信息时，应采用整个文件加密存储方式进行保护。

6.5.5 使用

组织进行个人信息使用时，应在满足 GB/T 35273-2020 中第 7 章要求基础上符合以下要求：

a) 因数据访问、数据分析、系统运维等工作需要，涉及敏感个人信息使用时，操作前使用多因素认证或二次授权机制，并通过访问控制组件或访问控制代理技术对访问的终端设备、系统进行控制，将操作执行的网络地址限制在有限的范围内。
b) 进行个人信息批量修改、拷贝、下载等重要操作前，需建立访问权限申请和审核批准机制，访问结束后及时对实际操作和申请操作进行验证，保证操作的一致性。涉及导出时还应使用加密、脱敏等技术手段防止数据泄露，国家及行业主管部门另有规定的除外。
c) 通过访问控制等措施限制人员频繁查询个人信息的访问频率，确需批量查询的应通过相应审批并留存相关记录，并提供访问控制组件与审批结果的自动联动能力。
d) 业务系统对敏感个人信息明文查询实现逐条授权、逐条查询，或具备对查询相关授权、次数、频率、总量等指标的实时监测预警功能，并留存相关查询日志。
e) 对应用系统桌面、移动运维终端、柜面受理设备等界面展示增加水印，水印内容应最少包括访问主体、访问时间。
f) 禁用展示界面复制、打印等可将展示数据导出的功能。
g) 涉及通过界面展示个人信息的（如显示屏幕、纸面），宜对需展示的个人信息采取屏蔽等技术措施防止信息泄露，国家及行业主管部门另有规定的除外。
h) 个人信息原则上应当脱敏处理后才能用于开发测试使用，经按照规程履行审批手续后，确需未经脱敏处理的个人信息用于开发测试时应按照规程履行审批手续，同时测试环境应当采取与生产环境一致的管理和技术措施，确保开发测试的个人信息安全。国家及行业主管部门另有规定的除外。
i) 个人信息汇聚融合前根据汇聚融合后可能产生的信息内容、所用于的目的、范围等开展个人信息保护影响评估，并采取适当的技术保护措施。
j) 涉及第三方机构合作的，以合同协议等方式明确用于汇聚融合的个人信息内容和范围、结果用途和知悉范围、各合作方个人信息保护责任和义务，以及个人信息保护要求等，并采用技术手段如多方安全计算、联邦学习、数据加密等技术降低个人信息泄露、窃取等风险。
k) 应对脱敏后的信息或其他数据集汇聚后重新识别出个人信息主体的风险进行识别和评价，并对数据集采取相应的保护措施。

6.5.6 加工

对个人信息进行统计、分析、整合、挖掘、标记、数字画像等二次加工，应符合在收集时已告知个人信息主体的目的。个人信息加工应符合以下要求：

a) 明确原始个人信息加工过程中的个人信息获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容。
b) 敏感个人信息加工之前应进行个人信息保护影响评估，并采用加密、脱敏等技术措施，保证敏感个人信息加工过程的安全性。
c) 所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围和满足对应的管控措施。
d) 对个人信息加工过程进行必要的监督和检查，确保加工过程的安全性。

6.5.7 传输

组织进行个人信息传输时，应在满足 GB/T 35273-2020 中第 6 章要求基础上符合以下管理要求：

a) 应建立对内外部环境间个人信息传输管控机制，对涉及跨安全域的个人信息传输活动实行差异化保护。
b) 敏感个人信息原则上不应对外传输，若因业务需要确需传输的，应经过事先审批授权，明确当前授权的范围、频次、有效期等，避免出现一次性授权、打包授权等情况，并采取数据加密、安全传输通道或安全传输协议等安全措施确保敏感个人信息保密性。
c) 定期检查或评估个人信息传输的安全性和可靠性。
d) 向国家机关、行业主管和监管单位传输个人信息，按照国家及行业相关管理要求进行传输。

组织进行个人信息传输时，应在满足 GB/T 35273-2020 中第 6 章要求基础上符合以下技术要求：

a) 个人信息传输前对接入的设备进行身份鉴别与认证，确保传输双方是可信任的。
b) 传输终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权传输终端接入内部网络。
c) 通过 API 传输个人信息时，应至少使用白名单（IP、域名等）方式进行控制，同时宜使用数字签名等方式保证安全性。
d) 传输过程应采用数字签名、时间戳等方式，确保个人信息传输的抗抵赖性；应采用密码技术或非密码技术等方式，确保数据的完整性。
e) 敏感个人信息传输时应采取数据加密、安全传输通道（如专线、VPN 等）或安全传输协议等安全措施，保证敏感个人信息传输的保密性。禁用 MD5、DES-CBC、SHA1 等不安全的算法。
f) 应在个人信息传输不完整时清除传输缓存数据，在个人信息传输完成后立即清除传输历史缓存数据。
g) 通过物理介质批量传递个人信息时需对其进行加密或脱敏，并由专人负责收发、登记、编号、传递、保管和销毁等，传递过程中可采用密封、双人押送、视频监控等确保物理介质安全到位，传递过程中物理介质不应离开相关责任人、监控设备等的监视及控制范围，且不得在无人监管情况下通过第三方进行传递，国家及行业主管部门另有规定的除外。

6.5.8 提供

个人信息提供主要包括委托处理、共享、转让等几种常见形式。

个人信息委托处理应满足 GB/T 35273-2020 中 9.1 要求基础上符合以下要求：

a) 受委托的第三方机构需满足国家及行业主管部门的相关要求，组织需对第三方机构开展事前尽职调查，调查内容包括但不限于调查其是否具有境外机构投资及股权背景，调查第三方机构安全资质及运营资质，确保第三方机构是合格授权者，能切实保障个人信息安全。重点评估委托处理场景及方案是否满足个人信息保护需求，并特别关注其方案中是否存在供应链引入的安全风险。
b) 委托行为不得超出事前已获得授权及合同协议约定的个人信息使用范围。
c) 根据委托处理的个人信息内容、范围、目的等，对个人信息委托处理行为进行个人信息保护影响评估，并采取相应的有效保护措施。
d) 对被委托方个人信息保护能力进行安全评估，并确保被委托方具备足够的个人信息保护能力，提供了足够的安全保护措施。
e) 个人信息事先采用数据脱敏等技术防止个人信息泄露。因业务确需无法对个人信息进行脱敏或加密处理的，需明确相应授权审批机制，事前对委托处理的内容通过专项审批，并采取技术措施防止数据被泄露、误用和滥用。以及国家及行业主管部门另有规定的除外。
f) 被委托方对委托处理的相关个人信息进行处理完成之后，需对存储的个人信息进行删除，并留存有关记录。
g) 个人信息通过信息系统与委托方进行传递时，则需在相应的控制节点设置安全审计功能，对个人信息的外发与回传进行审计，其中信息系统包括 API、摆渡服务器，控制节点包括信息系统

业务功能、API、服务器用户。

h) 个人信息以纸质介质或磁盘等存储介质与委托方进行传递时，需执行相应的内部授权审批程序，对传递数据的内容、用途、量级，数据接收方情况、使用时长、个人信息是否收回或由对方进行销毁等情况进行说明与审批，有关记录留档备查，其中数据接收方细化至法人机构个人信息保护负责人。

i) 保存委托处理过程记录与有关个人信息的处理情况，以留档备查。

个人信息共享、转让应满足 GB/T 35273-2020 中 9.2、9.3、9.5、9.8 要求基础上符合以下要求：

a) 个人信息共享和转让前应事前进行个人信息保护影响评估，对共享的个人信息内容、范围、时间周期、传输方式、用途、安全管控手段等要素进行评估，并评估接收方个人信息保护能力，并根据评估结果采取有效保护措施。

b) 其他单位或部门申请时，须提交书面函件，经负责法务法规部门评估后，由个人信息业务部门审批是否业务开展所必须的个人信息属性、标签属性及规模，减少其它无关数据、标签、属性的共享，降低多余个人信息外泄风险，并报分管领导同意后方可共享，同时控制共享流转范围，规范交接手续。

c) 敏感个人信息共享和转让前，组织应向个人信息主体等告知数据接收方的名称或者姓名、联系方式、处理目的、处理方式和敏感个人信息类型以及个人信息存储、使用等情况，并事先取得个人的单独同意。数据接收方应当在上述处理目的、处理方式和敏感个人信息类型等范围内处理个人信息；数据接收方变更原先的处理目的、处理方式的，需重新取得个人信息主体同意。

d) 数据接收方通过合同协议等方式，明确双方在个人信息保护方面的责任及义务，并约定共享和转让敏感个人信息的内容和用途、使用范围等。

e) 利用自动化工具如代码、脚本、接口、算法模型、SDK 等进行个人信息共享时，需通过身份认证、数据加密、反爬虫机制、攻击防护和流量监控等手段，有效防范网络监听、接口滥用等网络攻击，并定期检查和评估自动化工具安全性和可靠性。

f) 如因业务需要向境外提供个人信息，应遵守国家相关法律法规和标准的要求。

g) 在组织出现收购、兼并、重组等情形时，依照国家及行业有关规定履行义务。

h) 组织将其提供的产品或服务移交至其他组织时，需通过逐一传达或公告的方式向个人信息主体等履行告知义务。

i) 承接其产品或服务的组织，对其承接运营的产品或服务继续履行个人信息保护责任；如变更其在收购、兼并、重组过程中获取的个人信息使用目的，必须重新获得个人信息主体的明示同意或授权。

j) 对于组织破产且无承接方的情况，组织需将其情况及时报送行业主管部门，将个人信息移交至行业主管部门指定的机构进行继续保存，或依据行业主管部门的要求，对个人信息进行删除处理，并将处理结果通过逐一传达或公告的方式向个人信息主体履行告知义务。

6.5.9 公开

个人信息原则上不应公开披露。个人信息处理者经法律授权或具备合理事由确需公开披露时，在满足 GB/T 35273-2020 中 9.4-9.5 要求基础上符合以下要求：

a) 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。

b) 向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意。

c) 依据国家有关规定与行业主管部门规章，在组织官方渠道（如官方网站、专业客户端、公众号等）披露数据。

d) 个人信息保护管理机构会同有关业务部门，对拟披露个人信息的合规性、业务需求、数据脱敏方案进行审核。

e) 有关业务部门对披露渠道、披露时间、拟公开个人信息的真实性，以及数据脱敏效果进行确认，

披露时间指永久或固定时间段。

f) 依据组织有关程序执行个人信息公开披露审批程序，其审批过程和记录留档。

g) 通过组织官方网站披露个人信息时，采取包括网页防篡改等技术措施，防范披露个人信息篡改风险。

h) 尽可能对个人信息进行加密、匿名、假名等去标识化处理，防止泄露，造成危害。

i) 敏感个人信息（如：个人生物识别信息，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）原则上不得公开披露，国家及行业主管部门另有规定的除外。

j) 准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等。

6.5.10 跨境

个人信息应满足《促进和规范数据跨境流动规定》《数据出境安全评估申报指南（第二版）》《个人信息出境标准合同备案指南（第二版）》等有关要求的基础上，还应对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估，并形成个人信息保护影响评估报告，评估报告至少保存 3 年。评估报告应至少包括下列事项：

a) 个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性。

b) 跨境处理个人信息的规模、范围、类型、敏感程度、频率，个人信息跨境处理可能对个人信息权益带来的风险。

c) 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障跨境处理个人信息的安全。

d) 个人信息跨境处理存在的泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等。

e) 境外接收方所在国家或者地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响，包括但不限于：

   1） 境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生数据安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况；

   2） 该国家或地区现行的个人信息保护法律法规、普遍适用的标准情况，及与我国个人信息保护相关法律法规、标准情况的差异；

   3） 该国家或地区加入的区域或全球性的个人信息保护方面的组织，以及所做出的具有约束力的国际承诺；

   4） 该国家或地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

f) 其他可能影响个人信息跨境处理安全的事项。

6.5.11 删除

个人信息删除应满足 GB/T 35273-2020 中 8.3 要求基础上符合以下要求：

a) 依据国家及行业主管部门有关规定及与个人信息主体约定的时限等，针对不同类型的个人信息设定其保存期，对于多个不同保存期的个人信息集合，保存期限选择最长时限为该个人信息集合的保存期。

b) 对超过保留期限、停止提供其产品或者服务、响应个人信息主体合法权益要求或者合同协议履约终止以及处理目的已实现、无法实现或者为实现处理目的不再必要等情形的，组织应对涉及的个人信息及时进行删除或匿名化处理。法律、行政法规规定的保存期限未届满或有明确规定的，或者删除个人信息从技术上难以实现的，组织应停止除存储和采取必要的安全保护措施之外的处理措施。

c） 开发测试、数据分析等组织内部个人信息使用需求执行完毕后，由数据需求方依据组织个人信息删除有关规定，对其使用的有关个人信息进行删除，记录处理过程，并将处理结果及时反馈至数据提供方，由其进行数据删除情况确认，并及时报备个人信息保护管理机构。

d） 采取技术手段，在产品和服务所涉及的系统中去除待删除的数据。

e） 3 级及以上数据建立数据删除的有效性复核机制，定期检查能否通过业务前台与管理后台访问已被删除数据。

f） 在停止其提供的金融产品或服务时，或者保存期限已届满，对其在提供该金融产品或服务过程中所收集的个人信息进行删除或匿名化处理，与个人信息主体另有约定的除外，国家及行业主管部门另有规定的按照相关规定执行。

g） 存储个人信息的介质不再使用的，应采用不可恢复的方式如消磁、焚烧、粉碎等对介质进行销毁处理。对销毁后的物理存储介质进行登记、审批、交接。严禁非法挪用存储介质，避免个人信息被违规留存或还原。

h） 存储个人信息的介质还需继续使用的，应为不同个人信息的存储方式制定相异的逻辑销毁方法，并确保个人信息的多个副本被同时删除。除了采用删除索引、删除文件系统的方式进行个人信息删除外，还必需通过多次覆写等方式安全地擦除数据，确保介质中的个人信息不可再被恢复或者以其他形式被利用，具体措施包括但不限于：

——采用数据擦除方式销毁个人信息时，明确定义数据填充方式与擦除次数如全零、全一以及随机零一最少填写 7 次，并保证个人信息擦除所填充的字符完全覆盖存储数据区域。

——对于 SSD 固态硬盘的，宜使用 SSD 制造商提供的安全擦除工具或管理软件进行有效的数据擦除。

——通过数据恢复工具或数据发现工具进行个人信息的尝试恢复及检查，验证个人信息销毁结果。

——针对数据擦除后擦除失败的存储介质，进一步采用物理方式进行销毁。

i） 采取双人制实施个人信息删除，分别作为执行人和复核人，并对个人信息删除全过程进行记录，定期对个人信息销毁记录进行检查和审计。

j） 应明确个人信息删除效果评估机制。定期对个人信息删除效果进行抽样认定，通过数据恢复工具或数据发现工具进行个人信息的尝试恢复及检查，验证个人信息删除结果。

k） 删除个人信息可能影响执法机构调查取证时，应采取适当的隔离和屏蔽措施。

6.6 个人信息保护影响评估

6.6.1 评估情形

有下列情形之一的，组织应进行事前的个人信息保护影响评估，并对处理情况进行记录：

a） 处理敏感个人信息的；

b） 利用个人信息进行自动化决策的；

c） 委托第三方或者其他个人信息处理者对个人信息进行处理的；

d） 向信息汇聚平台等其他个人信息处理者提供个人信息的；

e） 公开个人信息的；

f） 向境外提供个人信息的；

g） 其他对个人权益有重大影响的用户个人信息处理活动。

6.6.2 评估内容

组织应参考 GB/T 39335-2020 及相关标准，梳理个人信息处理活动的主要场景并在事前进行个人信息保护影响评估，评估内容应包括：

a) 个人信息的处理目的、处理方式等是否合法、正当、必要；
b) 对个人权益的影响及安全风险；
c) 所采取的保护措施是否合法、有效并与风险程度相适应。

6.6.3 评估流程

根据不同的评估场景，由个人信息保护影响评估工作的发起方组织或邀请第三方参照个人信息保护影响评估方案开展个人信息保护影响评估。业务部门梳理出待评估的个人信息处理活动，技术部门配合完成个人信息保护影响评估工作，并完成相应的风险处置。发起方对风险处置情况进行跟踪，出具个人信息保护影响评估报告并保留相关记录。

6.6.4 评估方案

组织应根据实际情况梳理评估场景，制定个人信息保护影响评估方案，以评估个人信息处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响。可包括以下六个步骤。

a) 评估工作准备：评估工作准备主要围绕评估范围编制个人信息保护影响评估实施方案并获得发起方的支持、认可。实施方案是评估工作实施活动总体计划，是评估准备阶段应输出的最终成果文件，可用于管理评估工作的开展，使评估各阶段工作可控。
b) 必要信息采集：评估团队将针对评估对象进行必要信息采集，所采及信息包括以下三个部分：商业流程、系统信息、个人信息处理流程。
c) 数据流转梳理：数据流梳理的主要工作为数据映射分析，评估团队将会根据数据映射分析的结果对目标系统的个人信息以及个人信息处理活动进行分类工作。
d) 风险综合分析：评估团队将针对已分类的个人信息处理活动进行风险分析，风险分析将从风险所能够造成的个人权益影响与该风险导致安全事件发生的可能性两个方面入手，综合考虑风险的威胁等级，并生成个人信息风险表（根据风险在影响级别和可能性级别两个维度的得分，将其定位在相应的位置）。综合考虑可能性和影响级别能够有效提升资源分配的合理性。
e) 出具评估报告：评估团队在完成检查工作后将根据记录了评估项证明依据以及符合状态的评估表综合分析整理评估对象的合规状况以及所面临的个人信息保护安全风险。综合分析现存个人信息保护风险的危害性以及可能性，生成个人信息安全风险矩阵。针对评估对象所存在的安全问题，选取合适的控制措施遵循合理的优先级提出安全整改建议。
f) 风险处置跟踪：评估团队将对风险处置的结果进行跟踪，并根据风险处置的结果分析剩余风险是否符合风险准则所定义的风险接受标准。在完成处置结果评估之后，评估团队将出具独立的处置结果评估报告。

6.6.5 评估工具

组织在进行个人信息保护影响评估时，应充分参考 GB/T 39335-2020 附录 C 的基础上，选取符合组织实际情况的评估工具进行影响评估，实现组织个人信息保护影响评估工作的 IT 化、自动化和便捷化。其中评估工具宜覆盖以下要求：

a) 具备评估模版配置的功能；
b) 具备个人信息保护合规问卷引擎的功能；
c) 具备个人信息映射的功能；
d) 具备个人信息处理活动清单展示的功能；
e) 具备个人信息安全风险展示功能；
f) 具备告知同意管理的功能；
g) 具备第三方合规管理的功能；

h） 具备个人信息保护合规知识库的功能等。

6.6.6 评估报告

组织应编制个人信息保护影响评估报告，对处理情况进行记录，个人信息保护影响评估报告和处理情况记录至少保存三年。评估报告的内容通常包括：

a） 个人信息保护专员的审批页面；
b） 评估报告适用范围；
c） 实施评估及撰写报告的人员信息；
d） 参考的法律、法规和标准；
e） 个人信息影响评估对象（明确涉及的敏感个人信息），如处理个人信息的规模、范围、类型、敏感程度；
f） 处理个人信息的目的、范围、方式等的合法性、正当性、必要性；
g） 评估内容；
h） 涉及的相关方；
i） 个人权益影响分析结果；
j） 安全保护措施分析结果；
k） 安全事件发生的可能性分析结果；
l） 风险判定的准则；
m） 合规性分析结果；
n） 风险分析过程及结果；
o） 风险处置建议等。

6.7 个人信息保护合规审计

6.7.1 定期审计

由本组织内部机构或者委托专业机构开展定期审计。具体要求如下：

a） 以下个人信息处理者应当每年至少开展一次个人信息保护合规审计。
——重要数据处理者、关键信息基础设施运营者、大型互联网平台运营者等涉及个人信息处理的；
——超过 100 万人个人信息的个人信息处理者；
——处理超过 10 万人的敏感个人信息的个人信息处理者。
b） 其他个人信息处理者应当每二年至少开展一次个人信息保护合规审计。

6.7.2 合规审计

内容包括：

a） 组织在收到个人信息保护职责的部门要求开展个人信息保护合规审计时，应优先选择国家网信部门、公安机关等国务院有关部门确立的推荐目录中的专业机构开展个人信息保护合规审计活动。
b） 原则上应当在 90 个工作日内完成，并按照专业机构给出的整改建议进行整改，并将合规审计报告、专业机构复核后的整改情况报送履行个人信息职责的部门。

6.8 个人信息保护合规文化

6.8.1 宣传

宣传部门负责对内、对外的宣传工作，包括：

a) 应向组织全体员工及其他相关人员宣传《中华人民共和国个人信息保护法》，宣传个人信息保护的重要性和个人信息保护合规管理方针、管理制度，要求其遵照执行。
b) 应向社会公开宣传组织的隐私政策和个人信息保护工作。对外开展涉及个人信息的相关业务时，应公开隐私政策、个人信息处理规则等，并主动宣传组织保护措施、保密承诺及社会责任。
c) 应在宣传资料、网络媒介及其他面向社会的各类文件中包含个人信息保护的相关内容。

6.8.2 培训

组织应将个人信息保护相关培训纳入年度培训计划，并对培训结果进行专项评价。个人信息处理相关岗位人员每年教育培训时间宜大于二十小时。具体如下：

a) 建立新员工个人信息保护培训机制，确保新员工上岗前掌握个人信息保护基础知识和制度要求；不同岗位新员工依据培训体系还可进一步接受针对性培训，确保新员工掌握其岗位应知的安全制度和必备的安全技能。
b) 按照培训计划定期开展全员个人信息保护意识教育与培训，制作个人信息保护技能培训课件、警示教育微课件、个人信息保护微视频，采用线上线下模式、网络学习平台、移动设备新媒体应用等多种渠道开展形式多样的培训方式，培训内容包括但不限于国家有关法律法规、行业规章制度、技术标准、个人信息保护意识及技能培养，以及组织内部个人信息保护有关制度与管理规程等内容，并对培训结果进行评价、记录和归档。
c) 制定个人信息处理相关岗位人员的安全专项培训计划，规定不同岗位员工的必修及选修培训课程。其中不同岗位员工包括个人信息保护安全管理岗位、审计岗位、业务操作与信息技术操作特权账户所有者、个人信息各级权限审批岗位、重要数据处理岗位、信息系统开发及测试岗位人员、外部数据采购岗位及其他个人信息处理关键岗位。
d) 对密切接触敏感个人信息的人员定期开展个人信息保护意识教育和培训，培养办公过程中涉及的个人信息定期删除意识，并定期开展个人信息删除自查工作。
e) 至少每年 1 次或在隐私政策发生重大变化时，对个人信息处理相关岗位人员进行专业化培训和考核，确保人员熟练掌握隐私政策和相关规程。

6.9 个人信息安全事件处置

6.9.1 个人信息安全事件应急处置和报告

组织应对个人信息安全事件时，应满足以下要求：

a) 应制定个人信息安全事件应急预案。
b) 应定期（至少每年一次）组织内部相关人员进行个人信息安全应急响应培训和应急演练，使其掌握应急处置策略和规程，提高对个人信息安全事件的预防和应对能力。
c) 发生个人信息安全事件后，应根据应急预案进行以下处置：
——记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及数量，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；
——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；
——按照《国家网络安全事件应急预案》等有关规定，及时报告所属行业监管部门，报告内容包括但不限于：发生或者可能发生个人信息泄露、篡改、丢失的个人信息类型、数量、内容、性质等总体情况，事件发生的原因和可能造成的危害，已采取或将要采取的处置措施和个人信息主体可以采取的减轻危害的措施，事件处置相关人员的联系方式；
——采取措施能够有效避免个人信息泄露、篡改、丢失造成危害的，组织可以不通知个人信息主体，所属行业监管部门认为可能造成危害的或组织认为个人信息泄露事件可能会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，组织应及时告知个人信息

主体。

d) 根据相关法律法规变化情况以及事件处置情况，及时更新应急预案。

6.9.2 个人信息安全事件告知

组织进行个人信息安全事件告知时，应满足以下要求：

a) 应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

b) 告知内容应包括但不限于：

——安全事件的内容和影响；

——已采取或将要采取的处置措施；

——个人信息主体自主防范和降低风险的建议；

——针对个人信息主体提供的补救措施；

——个人信息保护工作机构和负责人的联系方式。

6.10 个人信息主体权益保障

组织在保障个人信息主体基本权益时，应满足以下要求：

a) 应建立投诉机制和投诉跟踪流程，在验证用户身份后，并且在法律法规或承诺的时限内响应个人信息主体对其个人信息提出的请求，响应时间宜在十五个工作日内，并应当留存处置记录。

b) 通过网站、App、客户端软件等提供服务的，应设置便捷的交互式页面提供功能或选项（例如用户页面展示），便于个人信息主体行使权利。

c) 接口部门确保个人信息主体可以及时受理用户的申请，并进行相关的处置，并留存相应的处置及解释说明记录。

d) 告知的渠道和方式可参照 GB/T 35273-2020 附录 C 执行。

7 进阶提升

7.1 个人信息安全工程

组织在个人信息安全工程设计要点时，应充分参考 GB/T 41817-2022 标准内容的基础上，宜重点对以下内容进行实现：

a) 产品隐私政策设计（如隐私政策弹窗逻辑与页面设计）；

b) 产品权限管理设计（如权限申请弹窗）；

c) 第三方插件/SDK（第三方接入）；

d) 用户告知及授权交互操作设计；

e) 定向推送设计；

f) 用户查询、删除、更正、账号注销、撤回同意等权益功能及机制的设计；

g) 用户信息保存期限的设计；

h) 身份认证和访问控制机制的设计（防止个人信息未经授权的访问及不正当的使用）；

i) 端到端的个人信息技术防护；

j) 隐私功能保护设计（如个人信息去标识化）；

k) 个人信息加密设计及密钥管理设计等。

7.2 个人信息保护认证

国家鼓励个人信息处理者通过认证提升个人信息保护能力，组织在满足个人信息保护合规管理基

础内容的基础上，宜考虑向有关部门提交个人信息保护认证申请。如涉及个人信息保护认证跨境路径，可根据实际情况申请跨境个人信息保护认证方向。具体如下：

a) 个人信息保护认证主要目的是证明个人信息处理者的个人信息处理活动合规合法，帮助建立个人信息主体对个人信息处理者的信任。
b) 跨境个人信息保护认证侧重于以个人信息处理者、境外接收方双方主体为对象，对双方组织层面个人信息保护能力、合规水平的认证，通常适用于合规建设较为完善、境内外主体间长期稳定合作的情形。可参考《TC260-PG-20222A 网络安全标准实践指南—个人信息跨境处理活动安全认证规范 v2.0》相关内容。

7.3 个人信息保护监督机构

7.3.1 大型互联网平台运营者涉及个人信息处理的，在六个月内成立主要由外部成员组成的个人信息保护监督机构，对本组织人信息保护合法合规情况、履行个人信息保护社会责任情况等进行独立监督。

7.3.2 个人信息保护监督机构主要职责建议包括：

a) 要求个人信息保护负责人或其指定的其他个人信息保护相关负责人员对个人信息保护合规管理相关事项作出说明和解释。
b) 对个人信息保护合规管理制度体系、平台规则、隐私政策等进行监督，发表监督意见。
c) 对个人信息保护影响评估事项进行监督，发表监督意见。
d) 对其处理个人信息遵守法律、行政法规的情况开展合规审计进行监督，发表监督意见。
e) 对其定期发布的个人信息保护社会责任报告进行监督，发表监督意见。
f) 对个人信息保护应急预案的制定及实施进行监督，发表监督意见。
g) 对发生或可能发生个人信息泄露、篡改、丢失情形时，对安全处置相关内容进行监督，发表监督意见。
h) 对个人信息跨境提供进行监督，发表监督意见。

附 录 A
（资料性）
个人信息分类示例

表 A 给出了个人信息的一级类别、二级类别、三级类别和相关个人信息典型示例。

表A 个人信息分类参考示例

一级类别	二级类别	三级类别	典型示例和说明
一般个人信息	个人自然信息	个人基本资料	自然人基本情况信息，如个人姓名、生日、年龄、性别、民族、国籍、籍贯、婚姻状况、家庭关系、住址、个人电话号码、电子邮件地址、兴趣爱好等
	网络身份标识信息	网络身份标识信息	可直接标识网络或通信用户身份的信息及账户相关资料信息（金融账户除外），如用户账号、用户 ID、即时通信账号、网络社交用户账号、用户头像、昵称、个性签名、IP 地址、账户开立时间等
	个人健康生理信息	健康状况信息	个人身体健康状况相关的一般信息，如体重、身高、体温、肺活量、血压、血型等
	个人教育工作信息	个人教育信息	个人受教育和培训情况相关信息，如学历、学位、教育经历（如入学日期、毕业日期、学校、院系、专业等）、成绩单、资质证书、培训记录、奖惩信息、受资助信息等
		个人工作信息	个人求职和工作情况相关信息，如个人职业、职位、职称、工作单位、工作地点、工作经历、工资、工作表现、简历等
	个人通信信息	个人通信信息	描述个人通信的元数据（如通话时长）等
	个人上网记录	个人操作记录	个人在业务服务过程中的操作记录和行为数据，包括软件使用记录、点击记录、Cookie、发布的社交信息、收藏列表、服务使用时间、下载记录、访问时间（含登录时间、退出时间）等
		业务行为数据	用户使用某业务的行为记录（如游戏业务：用户游戏登录时间、最近充值时间、累计充值额度、用户通关记录）等
	个人设备信息	可变更的唯一设备识别码	Android ID、IDFA、IDFV、OAID 等
		不可变更的唯一设备识别码	IMEI、IMSI、MEID、设备 MAC 地址、硬件序列号、ICCID 等
		应用软件列表	终端上安装的应用程序列表，如每款应用软件的名称、版本等
	个人位置信息	粗略位置信息	仅能定位到行政区、县级等的位置信息，如地区代码、城市代码等
	个人标签信息	个人标签信息	基于个人上网记录等各类个人信息加工产生的用于对个人用户分类分析的描述信息，如 App 偏好、关系标签、终端偏好、内容偏好等标签信息
	个人运动信息	个人运动信息	步数、步频、运动时长、运动距离、运动方式、运动心率等
敏感个人信息	个人身份信息	个人身份信息	可直接标识自然人身份的信息，如身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证、港澳台通行证等证件号码、证件有效期、证件照片或影印件等
		特定身份信息	自然人基于生物或社会在特殊场景下构建而产生的某种身份信息，如残障人士身份信息、种族、犯罪分子身份、不适宜公开的职业身份信息等个人信息

	个人生物识别信息	个人生物识别信息	生物识别原始信息（如样本、图像等）和比对信息（如特征值、模板等），如个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、人脸图像、人脸面部识别特征、步态等
	个人健康生理信息	个人医疗信息	与个人的身体或心理的伤害、疾病、残疾、疾病风险或隐私有关的健康状况信息，如病症、既往病史、家族病史、传染病史、体检报告、生育信息等
			在疾病预防、诊断、治疗、护理、康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录（如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录、用药记录）、检验检查数据（如检验报告、检查报告）等
	个人财产信息	金融账户信息	金融账户及账户相关信息，如银行卡号、支付账号、银行卡磁道数据（或芯片等效信息）、银行卡有效期、证券账户、基金账户、保险账户、公积金账户、公积金联名账号、账户开立时间、开户机构、账户余额、支付标记信息等
		个人交易信息	交易过程中产生的交易信息和消费记录，如交易订单、交易金额、支付记录、透支记录、交易状态、交易日志、交易凭证、账单，证券委托、成交、持仓信息，保单信息、理赔信息等
		个人资产信息	个人实体和虚拟财产信息，如个人收入状况、房产信息、存款信息、车辆信息、纳税额、公积金缴存明细（含余额、基数、缴纳公司、公积金中心、状态等）、银行流水、虚拟财产（虚拟货币、虚拟交易、游戏类兑换码等）、个人社保与医保存缴金额等
		个人借贷信息	个人在借贷过程中产生的信息，如个人借款信息、还款信息、欠款信息、信贷记录、征信信息、担保情况等
	身份鉴别信息	身份鉴别信息	用于个人身份鉴别的数据，如账户登录密码、银行卡密码、支付密码、账户查询密码、交易密码、银行卡有效期、银行卡片验证码（CVN 和 CVN2）、USBKEY、动态口令、U 盾（网银、手机银行密保工具信息）、短信验证码、密码提示问题、手机客服密码、个人数字证书、随机令牌等
	个人通信信息	个人通信信息	通信记录和内容，如短信、彩信、话音、电子邮件、即时通信等通信内容（如文字、图片、音频、视频、文件等）
	联系人信息	联系人信息	描述个人与关联方关系的信息，如通讯录、好友列表、群列表、电子邮件地址列表等
	个人上网记录	个人操作记录	个人在业务服务过程中的操作记录和行为数据，包括网页浏览记录、搜索记录、下载记录等
	个人位置信息	精准位置信息	能具体定位到个人的地理位置数据，包括经纬度、住宿信息、小区代码、基站号、基站经纬度坐标等
		行踪轨迹信息	与个人所处地理位置、活动地点和活动轨迹等相关的信息，如连续精准定位轨迹信息、车辆行驶轨迹信息、人员活动轨迹信息等个人信息
		住宿出行信息	个人住宿信息，及乘坐飞机、火车、汽车、轮船等交通出行信息等
	未成年人个人信息	未成年人个人信息	14 岁以下（含）未成年人的个人信息
	宗教信仰信息	宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动、特殊宗教习俗等个人信息

	其他信息	其他敏感个人信息	性取向、性生活、婚史、政见或政治观点、未公开的违法犯罪记、展示个人身体私密部位的照片或视频信息等个人信息

参 考 文 献

[1] GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[2] GB/T 35273-2020 信息安全技术 个人信息安全规范
[3] GB/T 37964-2019 信息安全技术 个人信息去标识化指南
[4] GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
[5] GB/T 41391-2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求
[6] GB/T 41817-2022 信息安全技术 个人信息安全工程指南
[7] GB/T 42460-2023 信息安全技术 个人信息去标识化效果评估指南
[8] GB/T 43697-2024 数据安全技术 数据分类分级规则
[9] T/GDNS 007-2023 医疗健康个人信息保护规范
[10] T/SIA 001-2022 企业个人信息安全管理规范
[11] TC260-PG-20222A 网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0
[12] 中华人民共和国网络安全法，2016
[13] 中华人民共和国数据安全法，2021年
[14] 中华人民共和国个人信息保护法，2021年
[15] 网络安全标准实践指南——网络数据分类分级指引（2021年12月31日全国信息安全标准化技术委员会秘书处发布）
[16] 网络与信息安全管理员（数据安全管理员）国家职业标准（2024年版）
[17] 个人信息保护合规审计管理办法（征求意见稿）(2023年8月3日国家互联网信息办公室发布)