ICS 03.100.01
A 02

团　　体　　标　　准

T/ISC 0050—2024

企业个人信息保护合规管理体系 指南

Guidelines for compliance management system of personal information protection on enterprises

（发布稿）

2024－6－12 发布　　2024－7－12 实施

中　国　互　联　网　协　会　　发布

目　次

前　言 III
引　言 IV
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 原则 2
4.1 有效性原则 2
4.2 全面性原则 2
4.3 独立性原则 2
4.4 动态性原则 2
4.5 可追溯原则 3
5 所处环境 3
5.1 合规管理体系 3
5.2 合规义务识别 3
5.3 合规风险评价 4
6 机构职责 4
6.1 合规方针 4
6.2 领导作用和承诺 4
6.3 组织机构与职责 5
6.4 合规管理沟通与协作 6
7 运行机制 6
7.1 过程和程序 6
7.2 提出疑虑 7
7.3 合规调查 7
7.4 奖惩措施 7
8 保障机制 7
8.1 聘用管理 7
8.2 合规培训 7
8.3 合规文化 8
8.4 合规咨询 8
8.5 合规管理信息化建设 8
8.6 文件化信息 8
9 评价机制 8
9.1 绩效评价 8
9.2 合规审计 8
10 持续改进 8

10.1 改进..... 8
10.2 不合规和纠正措施..... 8
附录 A（规范性附录） 企业个人信息保护合规义务清单 9
附录 B（规范性附录） 企业个人信息保护合规义务履行指引 13

前　言

本标准按照GB/T 1.1-2009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这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：中国信息通信研究院、清华大学智能法治研究院、北京互联网法院、广东小天才科技有限公司、度小满科技（北京）有限公司、小米科技有限责任公司、南京苏宁易付宝网络科技有限公司、新汽有限公司、上海倍孜网络技术有限公司、重庆首讯科技股份有限公司、咪咕文化科技有限公司、中国联合网络通信集团有限公司、国家市场监督管理总局竞争政策与评估中心、金杜律师事务所、北京世辉律师事务所、浙江京衡律师事务所、北京雷腾律师事务所、北京市中闻律师事务所、北京中银（深圳）律师事务所。

本标准主要起草人：李文宇、申卫星、孙铭溪、张夕夜、陈慧、程晓蕾、林中天、刘云、阙梓冰、颜君、毛春联、金诚、张伊岚、李洁婷、邢璟、李鹏、张向拓、黄亚熙、卢启祯、杨慧、张强、米胜荣、姚锦丽、聂子尧、江志鹏、史喆、汪浩、陈星州、王璟婷、王宁、熊尚威、郝梦尧、李辉、胡尚文、宁宣凤、吴涵、方禹、王新锐、毕芸、张豪、张玲玲、王军义、张凤杰、潘良。

引　言

在大数据、云计算、万物互联的时代，基于数据的应用日益广泛，个人信息保护问题日渐凸显。过度收集、非法买卖个人信息等侵犯个人信息权益的乱象时有发生。为了保护个人信息权益，规范个人信息处理活动，同时促进个人信息合理利用，我国先后颁布了《网络安全法》《民法典》《数据安全法》《个人信息保护法》等法律法规，逐步构建起个人信息保护的基础制度体系。

合规管理是企业积极应对不断变化的内、外部环境，传统与非传统风险的有效途径。有效的企业合规管理体系能够表明企业在经营管理过程中遵守相关法律法规、政府监管要求、行业守则、良好的治理标准、社会一般道德和对期望的承诺。为全面遵守个人信息保护法律和政策要求，提升个人信息保护水平，助力企业高质量全面发展，根据《个人信息保护法》《合规管理体系 要求及使用指南》及相关法律法规、标准，制定本文件。

本文件旨在从企业合规管理的角度细化并落实个人信息保护的义务和要求，助力企业开展个人信息保护合规管理工作。

企业个人信息保护合规管理体系 指南

1 范围

本文件规定了企业建立、实施、评估、维护及改进个人信息保护合规管理体系的总体指南。

本文件适用于开展个人信息保护合规管理相关工作的企业。

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 35770-2022/ISO 37301:2021 合规管理体系 要求及使用指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 42574-2023 信息安全技术 个人信息处理中告知和同意的实施指南

T/ISC 0023-2023 信息通信及互联网行业企业合规管理体系 指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

合规 compliance

履行组织的全部合规义务。

[来源：GB/T 35770-2022/ISO 37301:2021, 3.26]

3.2

合规义务 compliance obligations

组织强制性地必须遵守的要求，以及组织自愿选择遵守的要求。

[来源：GB/T 35770-2022/ISO 37301:2021, 3.25]

3.3

合规风险 compliance risk

因未遵守组织合规义务而发生不合规的可能性及其后果。

[来源：GB/T 35770-2022/ISO 37301:2021, 3.24]

3.4

合规管理 compliance management

以有效防控合规风险为目的，开展包括体系构建、制度制定、风险识别、合规审查、风险应对、责任追究、考核评价、合规培训等有组织、有计划的管理活动。

[来源：T/ISC 0023-2023, 3.3]

3.5

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

企业采用访谈、检查、测试等评估方法，按照评估必要性分析、评估准备工作、风险源识别、个人权益影响分析、安全风险综合分析、评估报告、风险处置和持续改进等流程，在处理个人信息前，评估其个人信息的处理目的、处理方式等是否合法、正当、必要，对个人权益的影响及安全风险（如是否会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇等），所采取的保护措施是否合法、有效并与风险程度相适应等内容。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。

3.6

个人信息保护法定特别机构 specialized statutory agencies for protection of personal information

企业处理个人信息在数量、跨境、主体资格等方面符合相关法定情形时，根据法律法规要求建立的相应机构，包括个人信息保护负责人、境内专门机构或者指定代表、由外部成员组成的独立机构等。

4 原则

4.1 有效性原则

企业个人信息保护合规管理制度宜有效嵌入到经营业务的具体环节当中，与法律风险防范、审计监察、内控及风险管理等工作相统筹、相衔接，并建立全员合规责任制，明确管理人员和各岗位员工的合规责任并督促有效落实，确保合规管理闭环。

4.2 全面性原则

企业个人信息保护合规管理的范围包括但不限于来自于用户的个人信息、内部员工的个人信息及企业日常经营过程中来自于外部客户或合作伙伴的个人信息，宜覆盖收集、存储、使用、加工、传输、提供、公开、删除等处理行为；合规工作宜覆盖业务涉及的研发、生产、销售、对外合作、投资推广、招投标及采购等各个环节，贯穿决策、执行、监督全流程，并确保所有与个人信息保护相关的业务、部门和人员均已纳入合规工作体系。

4.3 独立性原则

企业个人信息保护合规职能部门的运行宜不受任何不当的干扰和压力；合规职能部门应严格依照法律法规及企业相关制度等对企业和员工行为进行客观评价和处理；承担合规管理职责的人员应独立履行职责，不受其他部门和人员的干涉。

4.4 动态性原则

企业个人信息保护合规工作宜与企业经营范围、组织结构和业务规模相适应，合规工作宜根据企业内外部环境的变化适时进行调整和完善，企业经营管理中存在的合规风险问题，要能够得到及时反馈、纠正和改进。

4.5 可追溯原则

企业个人信息保护合规工作宜有明确的操作文档作为依据，确保企业合规管理有迹可循、有证可查。

5 所处环境

5.1 合规管理体系

企业个人信息保护合规管理，是企业通过履行个人信息保护合规义务，证明其规范生产经营的一种公司管理能力，是在履行合规义务的框架之下，为实现最佳经营业绩的一种公司治理方式，也是企业实现可持续发展，承担社会责任，开展自我监督的有效方式。企业宜正确认识和理解个人信息保护合规管理体系：

a) 企业个人信息保护合规管理体系是一个框架，该框架是方针、流程和行为的有机结合；
b) 企业个人信息保护合规管理体系无法完全避免不合规的发生，但相应的过程能够确保对不合规做出适当的反应和补救；
c) 企业宜确定个人信息保护合规管理体系的范围，包括地理和/或组织边界；
d) 企业个人信息保护合规管理体系宜结合企业环境，反映企业的价值观、方针和合规风险。

5.2 合规义务识别

5.2.1 合规义务

个人信息保护合规义务是企业建立、开发、实施、评价、维护和改进合规管理体系的基础。通常，个人信息保护合规义务来源于两个方面，必须要遵守的要求和自愿选择遵守的承诺。企业必须要遵守的个人信息保护要求包括：

——法律法规；
——监管机构发布的命令、条例或者指南；
——行政决定；
——法院判决；
——条约、公约和协议。

企业自愿选择遵守的个人信息保护承诺包括：

——与社会团体等非政府组织签订的协议；
——与客户和公共权力机构签订的协议；
——相关产业的标准；
——企业内部制度、公开承诺等。

5.2.2 合规义务分析

企业宜系统梳理来源于其活动、产品和服务的个人信息保护合规义务。

企业宜识别新增及变更的个人信息保护合规义务，确保持续合规。

企业宜评价变更的个人信息保护合规义务对合规管理体系产生的影响，并对个人信息保护合规义务管理实施必要的调整。

企业个人信息保护合规义务清单应符合附录A的规定，企业个人信息保护合规义务履行应符合附录B的规定。

5.3 合规风险评价

5.3.1 合规风险

企业宜通过将其个人信息保护合规义务与活动、产品、服务以及运行的相关方面关联，来分析个人信息保护合规风险。

企业宜对个人信息合规风险进行分级。

企业宜评估与个人信息处理外包和第三方相关的合规风险。

企业宜定期或在企业环境发生重大变化时进行个人信息保护合规风险评估。

5.3.2 合规风险提示

企业在评估个人信息保护合规风险内容的基础上，可根据自身经营规模、组织体系、业务内容以及市场环境，分析和评估个人信息保护合规风险的来源、发生的可能性、后果的严重性等，并对个人信息保护合规风险进行分级。个人信息保护合规管理部门宜根据风险评估结果对不同职级、不同工作范围的管理层与员工进行风险提示，降低管理层和员工的违法犯罪风险。

5.3.3 应急管理

当发生或者可能发生个人信息泄露、篡改、丢失时，企业宜按照应急预案及时采取处置措施，防止危害扩大，消除安全隐患，记录事件内容，保留相关证据，并向有关主管部门报告。安全事件对个人、组织造成实质性危害的，宜及时以电话、短信、邮件等方式向所涉主体告知安全事件情况、危害后果、已采取的补救措施等信息。无法逐一告知的，可采取公告方式告知。

6 机构职责

6.1 合规方针

企业宜确立个人信息保护合规管理方针，该方针可包括：

a) 个人信息保护合规宣言；

b) 个人信息保护总体方针；

c) 个人信息保护合规责任和资源的分配。

6.2 领导作用和承诺

企业管理层的直接领导和积极承诺对顺利开展个人信息保护合规管理至关重要，保障资源可获取、强调沟通的重要性、支持人员做出贡献。领导作用在个人信息保护合规管理体系的作用体现在以下几个方面：

a) 管理者以身作则支持合规；

b） 分配合规职能，提供充分资源；
c） 支持持续改进。

6.3 组织机构与职责

6.3.1 组织体系

企业开展个人信息处理活动宜建立健全个人信息保护合规管理组织机构和常态化沟通协作机制，强化个人信息保护合规意识。企业可以根据业务规模、合规风险等因素组建合规管理队伍，设置由企业的最高管理者、个人信息保护合规管理部门和法定特殊机构组成的个人信息保护合规管理组织体系。

6.3.2 第一责任人

企业主要负责人是个人信息保护合规的第一责任人，宜承担以下职责：

a） 分配足够和适当的资源来建立、发展、实施、评估、维护和改进个人信息保护合规管理体系；
b） 确保建立举报个人信息保护违规的有效机制；
c） 确保战略和运营目标与履行个人信息保护合规义务之间的一致性；
d） 建立和维护问责机制，包括纪律处分和后果；
e） 确保将个人信息保护合规落实情况和效果纳入企业内部人员绩效考核体系；
f） 规划个人信息保护合规管理体系建设工作，研究合规管理重大事项并提出指导意见，批准、签批重大方案；
g） 统筹协调重大个人信息保护合规风险事件的处理。

6.3.3 个人信息保护合规管理部门

企业宜设置专门的个人信息保护合规管理部门，一般由董事会直接设立企业合规部门、下设个人信息保护合规管理部门等各类专业合规部门。主要负责人宜向个人信息保护合规管理部门负责人提供足够的授权、人力、财力来支持个人信息保护合规管理体系的运行。合规管理部门主要负责：

a） 具体起草本企业个人信息保护合规管理计划和管理制度；
b） 组织开展或者参与个人信息保护影响评估、个人信息保护合规审计、检查与考核等相关工作，及时发现薄弱环节，督促违规整改和持续改进；
c） 落实本企业个人信息保护合规宣传计划，定期和不定期组织或协助人事部门、业务部门开展合规培训、宣传等工作；
d） 指导各业务单位做好个人信息保护合规、为各业务单位提供合规咨询和支持；
e） 就个人信息保护合规举报进行登记和受理并对举报进行调查和审核，判断是否存在违规行为，并提出处理建议；
f） 代表企业对接履行个人信息保护职责的部门。

6.3.4 业务部门

业务部门负责本领域的日常个人信息保护合规管理工作。业务部门主要负责：

a） 主动开展并配合个人信息保护合规管理部门开展合规工作，按照合规要求完善业务管理制度和流程；

b） 组织或配合个人信息保护合规管理部门进行合规风险识别和隐患排查，及时向个人信息保护合规管理部门通报风险事项，妥善应对合规风险事件；
c） 组织或配合违规调查及整改工作。

6.3.5 法定特别机构

若企业处理个人信息在数量、跨境等方面符合以下情形，宜建立符合法律特定要求的相应机构：

a） 处理个人信息达到国家网信部门规定数量的企业，宜指定个人信息保护负责人，并公开个人信息保护负责人的联系方式，报送履行个人信息保护职责的部门，个人信息保护负责人可以与个人信息保护合规管理部门负责人是同一人；
b） 境外企业宜在中华人民共和国境内设立专门机构或者指定代表，并报送履行个人信息保护职责的部门；
c） 用户数量巨大、业务类型复杂的企业宜成立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。

6.4 合规管理沟通与协作

个人信息保护合规管理部门宜加强与业务部门的分工协作。相关业务部门宜主动进行日常个人信息保护合规管理工作，识别业务范围内的合规要求，制定并落实业务管理制度和风险防范措施，配合个人信息保护合规管理部门进行合规风险审查、评估和调查、处置、整改工作。

个人信息保护合规管理部门宜与其他具有合规管理职能的职能部门（如法务部门、安全部门、审计部门、监察部门等）建立明确的合作和信息交流机制，加强协调配合。

个人信息保护合规管理部门宜积极与履行个人信息保护职责的部门建立沟通渠道，了解履行个人信息保护职责的部门期望的个人信息保护合规管理体系，并制定符合其要求的个人信息保护合规制度；对于复杂或专业性强且存在重大个人信息保护合规风险的事项，可以向履行个人信息保护职责的部门咨询；面对履行个人信息保护职责的部门的调查，企业宜积极沟通并予以配合。

7 运行机制

7.1 过程和程序

企业宜通过行为准则确立与业务过程有关的运营控制，以在企业活动和运行环境中实现合规义务。如果企业在处理个人信息时使用了第三方或外包过程，企业宜确保第三方或外包得到控制和监视。

控制包括：

——清晰、实用且易于遵守的工作指示；
——岗位和职责；
——年度合规计划；
——信息化工具；
——批准；
——合规审查；
——管理层承诺；

——内外部沟通；
——合规报告。

7.2 提出疑虑

企业宜建立违反企业行为规范的内部举报制度及企业外部人员投诉管理制度，建立畅通有效的举报与投诉渠道及对举报人、投诉人的保护措施。企业宜公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息保护投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。

企业宜建立畅通有效的举报投诉电话、邮箱等举报投诉渠道，保障举报人、投诉人安全畅通地进行举报、投诉。

企业宜对举报人、投诉人的相关信息予以保密，保障举报人和投诉人免遭报复。

7.3 合规调查

企业宜结合举报、投诉线索的真实性、有效性及时启动调查程序，确保调查过程的独立性、公正性，形成调查结果报告并采取相应处理和改进措施，持续完善个人信息保护合规管理制度体系。个人信息保护合规管理部门负责组织职责范围内的违规事件调查，参与由其他具有合规管理职能的监督部门组织展开的调查活动；对于严重违规事件，个人信息保护合规管理部门应主动配合履行个人信息保护职责的部门展开调查。

7.4 奖惩措施

企业宜建立个人信息保护合规考核机制，考核结果作为企业绩效考核的重要依据，与员工的评优评先、职务任免、职务晋升以及薪酬待遇等挂钩。

对于严格遵守个人信息保护合规义务的员工，企业宜制定适当的激励措施使合规管理计划得到一致遵守和执行。

企业宜完善违规惩戒机制，明晰责任范围，细化惩戒标准。对于不严格执行甚至违反合规管理计划的管理层和员工，采取适当的纪律措施进行惩戒，并根据违规程度采取不同的风险处置措施。

8 保障机制

8.1 聘用管理

企业宜将遵守个人信息保护合规要求和履行个人信息保护合规义务作为人员聘用条件，确保相关人员在适当的教育、培训或经验的基础上胜任工作。对个人信息处理关键岗位的员工开展必要的背景调查，了解其犯罪记录、诚信状况等相关信息，并通过签署合规承诺书、保密协议等方式明确其应遵守的个人信息保护合规要求和履行的个人信息保护合规义务。关键岗位员工离岗后，应当按照个人信息保护合规管理要求执行离岗交接、审计、脱密等措施。

8.2 合规培训

个人信息保护合规管理部门应当建立培训机制，定期或者在合规义务发生变化时，为管理层、员工培训个人信息保护相关规定和制定，使其充分了解个人信息保护法律法规、个人信息保护合规管理计划、岗位角色与职责等。宜注重培训实效，可通过不定期抽查或现场考

试等形式加大培训督查力度，并考虑将是否参加过个人信息保护合规培训以及相关抽查、考试成绩纳入员工年度考核内容，保留培训及考核记录。

8.3 合规文化

企业宜将个人信息保护合规文化作为企业文化建设的重要内容，推行个人信息保护的合规理念，践行合规经营的价值观，不断增强员工的个人信息保护合规意识。

8.4 合规咨询

企业宜建立个人信息保护合规咨询机制，管理层和各部门员工在工作中可以向个人信息保护合规管理部门咨询个人信息保护合规问题。个人信息保护合规管理部门应当不断学习、提升合规管理水平，也可以同外部机构开展个人信息保护合规咨询合作。

8.5 合规管理信息化建设

企业宜合理应用数字技术，对个人信息保护管理工具进行测试、优化和不断升级，获取并运用合规管理体系运行数据，持续提升个人信息保护合规管理体系的有效性。

8.6 文件化信息

企业宜以适当的形式和载体记录个人信息保护合规管理体系运行产生的文件化信息，包括合规风险评估、应对措施、调查过程、审核的记录，可作为证据。文件化信息应当以清晰、易读和易检索的方式保存，并采取必要措施防止泄密、不当使用或完整性受损。

9 评价机制

9.1 绩效评价

企业宜对个人信息保护合规管理体系进行监视，评价合规目标的实现情况。企业宜建立获取合规绩效反馈的渠道，开发、实施和维护一套适当的指标。

9.2 合规审计

企业宜在策划的时间间隔内对个人信息保护的合规情况实施审计，策划和实施审计方案，以了解其个人信息保护合规义务得到了实施和维护的情况。

10 持续改进

10.1 改进

企业应持续改进合规管理体系的适宜性、充分性和有效性。

10.2 不合规和纠正措施

发生不符合或不合规时，企业宜对个人信息保护合规管理体系做出反应，采取控制和纠正措施，确定产生不符合、不合规的原因，评审纠正措施的效果。

附 录 A

（规范性附录）

企业个人信息保护合规义务清单

表A.1规定了企业个人信息保护合规义务清单，企业宜根据所处行业、产品及服务类型等识别自身合规义务。

表A.1 企业个人信息保护合规义务清单

序号	合规义务（一级）	合规义务（二级）		是否适用	备注
1	个人信息分类	处理了敏感个人信息			
2		敏感个人信息中存在不满十四周岁未成年的个人信息			
3		处理了私密个人信息			
4		仅处理了非敏感非私密的个人信息			
5	采取安全技术措施	加密			
6		去标识化			
7		其他技术措施			
8	处理敏感个人信息	向个人告知了处理敏感个人信息的必要性以及对个人权益的影响			
9		取得了个人单独同意			
10		进行了个人信息保护影响评估			
11		取得了未满十四周岁未成年人父母或者其他监护人的同意			
12		制定了未满十四周岁未成年人专门的个人信息处理规则			
13		存储时采取了相应的加密、去标识化等技术措施			
14		展示时采取了脱敏等处理措施			
15		开发、测试环境中对敏感个人信息进行了脱敏处理			
16	获取个人信息处理的合法性基础	基于同意处理个人信息			
17		同意的例外	为订立、履行个人作为一方当事人的合同所必需		
18			为实施人力资源管理所必需		
19			为履行法定义务所必需		
20			紧急情况下为保护自然人财产安全所必需		
21			为公共利益实施新闻报道、舆论监督		

22			在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息		
23	个人信息全生命周期管理	收集	不以误导、欺诈、胁迫等方式收集个人信息，不隐瞒产品或服务所具有的收集个人信息的功能，不从非法渠道获取个人信息		
24			收集个人信息的类型与实现产品或服务的业务外功能有直接关联，即没有所收集的个人信息的处理，产品或服务的功能无法实现		
25			自动采集个人信息的频率是实现产品或服务的业务功能所必需的最低频率		
26			基于同意收集个人信息的，提供了撤回其同意的功能和方法，或者为撤回设置了合理的路径和操作步骤		
27		存储	对于从第三方获取的个人信息，获得了提供方获取个人同意或其他合法性基础的保证		
28			存储期限为实现使用目的所必需的最短时间		
29			实施了有效的备份和恢复策略，或者其他必要的措施保障存储的个人信息安全		
30		使用、加工	使用个人信息时，未超出收集个人信息时所声称目的直接相关的范围		
31			对被授权访问个人信息的人员，建立了最小授权的访问控制策略，对批量修改、拷贝、下载个人信息等重要操作，设置了内部审批流程		
32			开发、测试环境与生产环境实现了有效隔离		
33		提供	取得了个人单独同意		

34			进行了个人信息保护影响评估		
35			向个人告知了接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类		
36		传输	采取了相应的管理手段和技术手段，防止个人信息在传输的过程中被篡改、伪造、窃取等安全风险		
37		公开了自身所处理的个人信息	取得了个人单独同意		
38			进行了个人信息保护影响评估		
39		处理了非自身公开的个人信息	在合理的范围内处理已公开的个人信息		
40			处理已公开的个人信息时，个人未明确拒绝		
41			对个人权益有重大影响的，取得了个人同意		
42		删除	符合删除个人信息的情形时，主动、及时删除个人信息		
43			删除个人信息从技术上难以实现的，停止了除存储和必要的安全保护措施之外的其他处理行为		
44	多主体处理个人信息	共同处理			
45		委托处理	进行了个人信息保护影响评估		
46			签订了委托合同并对受托人的个人信息处理活动进行了监督		
47			合同不生效、无效、被撤销或者终止的，要求合作方返还或者删除个人信息		
48		转移个人信息	向个人告了知接收方的名称或者姓名和联系方式		
49	自动化决策	开展了个人信息保护影响评估			
50		提供了便捷的拒绝方式			
51		增强了透明度和结果公平			
52		未实施不合理的差别待遇			

53		进行信息推送、商业营销时，同时提供了不针对个人特征的选项		
54	跨境提供个人信息	向个人告知了境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项		
55		取得了个人单独同意		
56		进行了个人信息保护影响评估		
57		数据出境安全评估		
58		个人信息保护认证		
59		个人信息出境标准合同签订		
60	个人信息请求权	查阅复制		
61		更正补充		
62		删除		
63		可携带		
64		解释说明个人信息处理规则		
65		死者近亲属对死者个人信息的请求		
66	个人信息安全事件应急预案	制定个人信息安全事件应急预案		
67		每年组织内部相关人员开展至少一次应急演练，使其掌握岗位职责和应急处置的策略和规程		
68		发生或者可能发生个人信息保护泄露、篡改、丢失的	立即采取补救措施	
69			上报主管部门	
70			以邮件、信函、电话、推送等方式告知个人；难以逐一告知个人信息主体的，采取合理、有效的方式发布与公众与关的警示信息	
71	配合监管执法	协助、配合履行个人信息保护职责的部门依法行政，不拒绝、阻挠		

附 录 B

（规范性附录）

企业个人信息保护合规义务履行指引

B.1 基于同意处理个人信息

B.1.1 告知

企业宜规范处理个人信息的告知行为，制定必要的告知制度和操作规程。企业可以采用下列显著和清晰易懂的方式履行告知义务：

a） 以加粗、下划线、特殊字体等处理方式明确标识或突出显示个人信息处理规则中的重点条款；

a） 提供简化版的个人信息处理规则，内容宜浓缩与处理活动最相关的关键处理规则，包括个人信息保护政策的章节结构（点击后可直接访问对应内容），当前处理活动所必需的个人信息种类，收集方式、目的，以及处理个人询问、投诉的联系方式等；

b） 以专章或专门规则方式告知个人信息处理规则中的重点条款；

c） 在首屏展示具体场景对应的个人信息处理规则，避免在交互中对个人信息处理规则进行折叠、遮挡或隐藏；

d） 将对个人产生重要影响的、易于引起异议或争端的内容靠前推送；

e） 针对儿童或残障人士等特定群体使用符合其理解水平的个人信息处理规则。

企业不宜以下列方式履行告知义务：

a） 在已经开启个人信息处理权限、已经收集个人信息的同时或之后告知该个人信息的处理事项；

b） 个人信息处理规则未在合理范围或以合理方式公开并提示个人，如通过遮挡弹出窗口、放置边缘位置、选用清晰度不足的字体色号等造成个人阅读困难；

c） 个人信息处理规则对目的、方式、种类的告知不清晰、不准确、不完整，或告知语言晦涩难懂；

d） 告知事项发生变更时，未以适当方式将变更部分告知个人；

e） 获取处理个人敏感信息的同意前，未同步告知处理目的、方式、范围、处理的必要性和对个人权益的影响。

B.1.2 同意

企业宜规范获取个人或者其监护人同意的行为，制定必要的获取同意制度和操作规程。企业不宜以下列方式获取个人或者其监护人的同意：

a） 企业要求个人同意处理其信息才提供产品或者服务，但是处理该信息属于提供产品或者服务所必需的除外；

b) 通过捆绑产品或服务各项业务功能的方式，要求个人一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求；
c) 以默认勾选、提前点亮个人信息处理条款等非自主选择的方式作为个人同意处理其个人信息的授权；
d) 未按照法律、法规的规定对应当取得个人单独同意或书面同意的事项，取得个人的单独同意或书面同意，包括以取得个人对个人信息处理规则的概括性同意替代法律、法规规定事项的单独同意；
e) 个人信息的处理目的、处理方式和处理的个人信息种类发生变更，或者个人信息接收方变更原先的处理目的、处理方式，未重新取得个人同意的；
f) 仅以改善服务质量、提升使用体验、研发新产品、增强安全性等缺乏特定处理目的的理由，强制要求个人同意收集个人信息。

B.1.3 单独同意

企业获取个人或者其监护人的单独同意，可以采用下列方式：
a) 在分项选择同意的交互式界面内，采取单独勾选、单独点击、单独点亮等方式的；
b) 采取自然人主动填写、上传、输入需要取得单独同意的处理活动所需的个人信息等方式的；
c) 在纸质或电子的书面文件中有形地载明需要取得单独同意的处理活动并由自然人单独签名、签章的；
d) 为需要取得单独同意的处理活动制作专门的个人信息处理同意书，在醒目位置张贴或以音频方式播放，自然人通过刷卡、刷指纹、刷脸等动作表示同意的；
e) 通过电子邮件、电话、短信等方式告知需要取得单独同意的处理活动并取得自然人同意的回复的。

B.1.4 个人不同意处理其个人信息或者撤回同意

个人拒绝企业处理其个人信息或者撤回同意后，请求企业继续提供产品或者服务的，企业应当提供产品或者服务的基本业务功能，处理个人信息属于提供基本业务功能所必需的除外。企业可以综合考虑个人使用企业产品或者服务的主要目的、相关法律法规等认定基本业务功能。企业不宜将下列情形认定为产品或者服务的基本业务功能：
a) 仅为实现改善服务质量、提升使用体验、定向推送信息、研发新产品等目的的业务功能；
b) 外部第三方或关联公司提供的业务功能（基本业务功能除外）；
c) 如基本业务功能有多种可选的实现方式，则对个人信息权益负面影响更大的实现方式不宜认定为基本业务功能。

B.2 同意的例外

B.2.1 为订立、履行个人作为一方当事人的合同所必需

以“为订立、履行个人作为一方当事人的合同所必需”为处理个人信息合法性基础的，企业宜综合下列因素评估适用该合法性基础是否准确：

a) 是否存在个人作为一方当事人的合同以及合同是否有效，包括企业向第三人履行的合同；
b) 在“订立个人作为一方当事人的合同”的场景下，个人是否主动要求企业处理个人信息；
c) 个人是否在客观上合理地期待处理行为会因为订立、履行合同而发生，包括该处理行为是否符合所处行业的惯例等；
d) 排除处理行为是否将导致合同无法订立、履行或使企业承担不合理的经济成本；
e) 是否存在对个人信息权益影响更小的处理行为。

B.2.2 为实施人力资源管理所必需

以“为实施人力资源管理所必需”为处理个人信息合法性基础的，企业可以依据自身制定的劳动规章制度和和签订的集体合同未经同意处理个人信息，但有下列情形之一的除外：

a) 劳动规章制度或者集体合同违反法律、法规的规定，包括不符合民主制定程序、劳动者未充分行使参与权等；
b) “实施人力资源管理”的处理目的不明确或不合理，未符合社会惯例和一般公众的预期，或者未履行告知义务保证劳动者知悉处理目的；
c) 处理的个人信息类型与实施人力资源管理无直接关联，处理频率和数量超出实施人力资源管理所必需的最低频率和数量。

B.2.3 为履行法定义务所必需

以“为履行法定义务所必需”为处理个人信息合法性基础的，企业可以根据相关部门履行法定职责的要求，提供用户的姓名、联系方式、所在地址等必要个人信息，但不得违反法律、法规规定的权限、程序或者超出必要范围和限度。

B.2.4 紧急情况下为保护自然人财产安全所必需

以“紧急情况下为保护自然人财产安全所必需”为处理个人信息合法性基础的，电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等企业主体的以下个人信息行为可认为保护自然人财产安全所必需：

a) 电信业务经营者监测并核验涉诈异常电话卡用户；
b) 银行业金融机构、非银行支付机构监测识别涉诈异常账户和可疑交易，并采取必要防范措施；
c) 互联网服务提供者监测识别并重新核验涉诈异常账号。

B.2.5 为公共利益实施新闻报道、舆论监督

以“为公共利益实施新闻报道、舆论监督”为处理个人信息合法性基础的，企业处理的个人信息不应当超过必要限度，或者处理方式不合理侵害个人人格权益，以下因素可作为判断合理使用的参考：

a) 客观行为特征，合理使用对应的行为是新闻报道或舆论监督；
b) 主观目的特征，合理使用对应的主观目的是出于公共利益；
c) 符合比例原则，对个人信息的使用是诚实的、可以接受的、合理的或者公平的，而非恶意的、无法让人接受的、不合理的或者不公平的。

B.2.6 在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息

以“在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息”为处理个人信息合法性基础的，企业宜综合下列因素评估适用该合法性基础是否准确：

a) 是否超出个人信息公开时的特定范围；
b) 是否为用户提供符合其预期的更优质服务；
c) 是否有利于实现个人信息的初始公开目的；
d) 是否采取合理的技术措施和管理措施，使处理行为对个人权益损害最小化，并仍为个人提供拒绝处理的选项。

B.3 个人信息全生命周期管理

B.3.1 提供个人信息

企业向其他个人信息处理者提供其处理的个人信息的，宜履行以下合规义务：

a) 向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人单独同意，符合法律、法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；
b) 与接收方约定处理个人信息的目的、范围、处理方式、个人信息保护措施等，通过合同等形式明确双方的个人信息保护义务，并对接收方的个人信息处理活动进行监督；
c) 留存个人同意记录及提供个人信息的日志记录至少五年；
d) 接受方变更处理目的、处理方式的，监督其是否依照法律、行政法规规定重新取得个人同意；
e) 事前进行个人信息保护影响评估。

B.3.2 公开个人信息

企业公开其处理的个人信息的，宜取得个人单独同意，并在事前进行个人信息保护影响评估。企业不宜向已公开个人信息实施下列违规行为：

a) 向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的信息；
b) 利用已公开的个人信息从事网络暴力活动；
c) 处理个人明确拒绝处理的已公开个人信息；
d) 未取得个人同意处理已公开的个人信息且对个人权益造成重大影响。

B.3.3 删除个人信息

有下列情况之一的，企业宜主动删除个人信息：

a) 处理目的已实现、无法实现或者为实现处理目的不再必要；
b) 停止提供产品或者服务；
c) 处理个人明确拒绝处理的已公开个人信息；
d) 未取得个人同意处理已公开的个人信息且对个人权益造成重大影响。

B.4 多主体处理个人信息

B.4.1 共同处理

企业与他人共同处理个人信息的，宜在事前约定下列事项：

a) 各自的权利义务；
b) 各方采取的个人信息保护措施；
c) 个人信息权益保护机制；
d) 个人信息安全事件报告机制；
e) 侵害个人信息权益造成损害的，各方应当承担的责任。

B.4.2 委托处理

企业委托他人处理个人信息的，宜履行以下合规义务：

a) 在委托处理个人信息前开展个人信息保护影响评估；
b) 在委托合同中约定委托处理的目的、期限、方式及个人信息的种类、受托人应当采取的技术措施和管理措施、双方的权利义务等；
c) 采取定期检查等方式，对受托人的个人信息处理活动进行监督，以确保委托处理个人信息的活动符合法律规定；
d) 监督受托人是否严格按照委托合同的约定处理个人信息，是否存在超出约定的处理目的、处理方式处理个人信息的情况；
e) 当委托合同不生效、无效、被撤销或者终止时，监督受托人将个人信息返还企业或者予以删除；
f) 监督受托人是否存在转委托他人处理个人信息的情况，是否得到企业的同意。

B.4.3 转移个人信息

企业因合并、分立、解散、被宣告破产等原因需要转移个人信息的，宜履行以下合规义务：

a) 向个人告知接收方的名称或者姓名和联系方式；
b) 监督接收方是否继续履行个人信息处理者的义务；
c) 接收方变更原先处理目的、处理方式的，监督其是否依照法律、行政法规有关规定重新取得个人同意。

B.5 自动化决策

B.5.1 提供便捷的拒绝方式

企业宜建立利用个人信息进行自动化决策的管理机制，规范自动化决策行为。企业利用自动化决策方式进行个人信息处理活动，宜在个人第一次使用时提供与作出同意同等便捷的拒绝方式，包括在取得自动化决策的同意时明确告知具体的拒绝路径并设置常驻入口，或者同时提供不针对个人特征的选项。

B.5.2 增强透明度和结果公平

企业利用个人信息进行自动化决策的，宜保证自动化决策的透明度和结果公平、公正，并以适当方式公示其自动化决策的基本原理、目的意图和主要运行机制等信息。企业可以采取以下方式增强自动化决策的透明度和结果公平、公正：

a) 在隐私政策中以明确、易懂和合理的方式披露个性化推荐应用情况，包括具体的业务场景、使用的个人信息、使用方式和目的等，并标注“推荐”，企业也可在网页、移动端内开设阅读端口，用户可通过该端口了解自动化决策对用户的具体影响；
b) 事前对算法模型进行安全评估，并按国家相关规定进行备案，以尽可能减少自动化决策算法模型存在的缺陷，当应用场景和主要功能发生变化时，对算法模型重新进行评估；
c) 事前主动告知个人自动化决策处理个人信息的种类及可能带来的影响；
d) 事前进行个人信息保护影响评估；
e) 向个人提供保障机制，以便个人可以要求企业就应用自动化决策方式作出对用户个人权益有重大影响的决定予以说明；
f) 向个人提供删除或者修改用于自动化决策服务的针对其个人特征的用户标签功能；
g) 对个人信息处理、标签管理、模型训练等自动化决策过程中的人工操作进行记录，防范人为恶意操纵自动化决策信息和结果。

B.5.3 不实施不合理的差别待遇

企业利用自动化决策方式进行个人信息处理活动，不宜实施下列不合理的差别待遇：

a) 对同一产品或者服务，基于个人的支付能力、消费偏好、使用习惯等个人特征，针对个人采取不同的交易价格、交易方式或者其他交易条件；
b) 对在交易安全、交易成本、信用状况、交易环节、交易持续时间等方面不存在实质性差别的个人，采取不同的交易价格、交易方式或其他交易条件；
c) 基于有损人格尊严、人身自由的方式，或者违背诚信、公平原则而实施的交易条件上的差别待遇。

B.6 跨境提供个人信息

B.6.1 数据出境安全评估

企业向境外提供个人信息，有下列情形之一的，宜通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

a) 所提供的个人信息构成重要数据；
b) 关键信息基础设施运营者和处理 100 万人以上个人信息的企业向境外提供个人信息；
c) 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的企业向境外提供个人信息；
d) 国家网信部门规定的其他需要申报数据出境安全评估的情形。

B.6.2 个人信息保护认证

企业选择个人信息保护认证的方式向境外提供个人信息的，宜通过专业机构依据TC260-PG-20222A《个人信息跨境处理活动安全认证规范》、GB/T 35273《信息安全技术个人信息安全规范》所做的认证。

B.6.3 个人信息出境标准合同

企业通过订立标准合同的方式向境外提供个人信息的，宜同时符合下列情形：

a) 非关键信息基础设施运营者；
b) 处理个人信息不满 100 万人的；
c) 自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；
d) 自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

企业不宜采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

B.7 个人信息请求权

B.7.1 保障机制

企业应当保障个人行使个人信息权益，建立个人行使权利的申请受理机制，向个人提供便捷的查阅、复制、转移、更正、补充、删除个人信息的方法，及时响应个人行使权利的申请，及时、完整、准确告知处理意见或者执行结果。

B.7.2 查阅复制权

企业宜建立个人行使查阅或复制其个人信息的相关机制，明确个人有权要求企业提供其收集的个人主动提供的个人信息、因合同履行而被记录的个人信息及个人信息处理的相关情况，包括企业是否处理其个人信息、个人信息的处理目的和方式、处理的个人信息种类和内容以及保存期限、个人信息的其他共同处理者和受托人（如有）、个人信息的提供方和接收方（如有）、处理的合法公开的个人信息及其来源（如有）、个人信息的存储环境和使用情境等。

除存在依法不得查阅复制或权利滥用等情形外，企业不宜设置查阅复制个人信息的前提条件或额外程序，例如存在个人信息泄露风险或申请查阅复制的个人对查阅复制的个人信息具有正当利益等。企业可以提供个人信息查阅复制方法或在技术可行的前提下直接传输，且原则上不应当收取费用，但对一定时期内多次重复的请求，企业可以收取合理的费用。

B.7.3 更正补充权

企业宜建立个人行使更正权或补充权的相关机制，在设置隐私政策中对个人行权方式进行说明。

企业可以在App功能设置中嵌入相关选项，对个人信息进行修改和补充。

企业还可以通过客服、投诉渠道满足个人的更正和补充个人信息的权利，并在个人行权过程中遇到的具体问题接受咨询或提供帮助。

B.7.4 删除权

有下列情形之一的，企业宜主动删除个人信息，并记录删除时间、操作人、数据内容等相关信息。企业未删除的，个人有权请求删除：

a) 处理目的已实现、无法实现或者为实现处理目的不再必要；
b) 企业停止提供产品或者服务，或者保存期限已届满；
c) 个人撤回同意；
d) 企业违反法律、行政法规或者违反约定处理个人信息；
e) 法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，企业宜停止除存储和采取必要的安全保护措施之外的处理。

企业宜建立个人信息删除的操作规程和管理制度，明确删除的对象、权限、流程和技术等要求，并对相关活动进行记录和留存。企业对个人信息存储设备和介质进行报废处理的，宜事先采取格式化、重复删除、介质消磁等方式删除其中存储的个人信息，并采取物理损毁等方式对介质进行彻底销毁。

B.7.5 可携带

个人主张转移个人提供的个人信息，或者因合同履行而被记录的信息，包括用户行为记录、行踪轨迹、网页浏览历史以及搜索记录等与本人相关的个人信息的，企业可予支持。

个人主张携带他人通过计算派生的数据，或者通过分析而产生的数据，例如经由算法预测的个人偏好、使用习惯等，或者匿名化的个人信息，企业可不予支持。

B.7.6 解释说明

企业宜提供便捷的方式和途径，接受、处理个人关于个人信息处理规则解释说明的请求。接到个人的请求后，企业宜在合理的时间内使用通俗易懂的语言对其个人信息处理规则作出解释说明。

B.7.7 死者个人信息

死者的近亲属为保护本人利益请求对死者个人信息行使个人信息处理中的权利的，应证明其利益合法、正当，企业可考虑死者的生前意愿、第三人的合法利益，对近亲属的前述请求是否成立进行判断。

死者生前通过订立遗嘱或与企业订立合同的方式，明确限定了行使个人信息权利的主体，或者明确任何人都不得使用其个人信息的，可以认定为《个人信息保护法》第四十九条规定的“死者生前另有安排”的情形。

B.8 应急预案制定和实施

企业应制定并组织实施个人信息安全事件应急预案，按照危害程度、影响范围等因素对个人信息安全事件进行分级，并结合分级情况确定应急处置的方针策略、人员职责、具体措施、流程规范、物资保障等事项。企业宜每年至少组织一次应急响应培训和应急预案演练，使相关人员掌握熟悉应急处置策略和规程。

B.9 配合监管执法

企业宜建立监管执法配合机制，受到监管部门调查时应立即通知主要负责人、个人信息保护合规管理部门和相关职能部门负责人等人员，启动必要的内部调查程序并明确监管调查对接人员，必要时宜当暂停相应的个人信息处理活动。企业应当对监管部门的监管执法予以协助、配合，不得拒绝、阻挠，不得提供虚假材料、信息或隐匿、销毁、转移证据。企业积极配合监管并主动开展合规整改采取措施有效减轻、消除危害后果的，可以向监管部门申请酌情从轻或减轻行政处罚。

企业宜按照监管部门提出的监管建议及时采取整改措施，优化、更新个人信息保护合规管理制度，建立健全个人信息保护合规长效机制，有效消除安全隐患。