中兴通讯隐私保护

白皮书

法律遵从 | 信任共建 | 道德履行

2025

ZTE中兴

声明

内容声明：本文档作为相关方了解中兴通讯股份有限公司隐私保护的参考性资料。除非另有约定，本文档中的所有陈述、信息和建议不构成任何明示或暗示的保证。因产品或服务升级、调整、合规体系的不断优化完善或其他原因，我们有权对本文档内容进行增加、修改、删减、废止，或进行不定期更新。如发现本文档存在任何错误或对本文档内容存在任何疑问，请通过Privacy@zte.com.cn电子邮箱与我们联系。

版权声明：中兴通讯股份有限公司保留一切著作权权利。非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，或实施其他涉嫌侵犯中兴通讯股份有限公司著作权的行为。

商标声明：ZTE中兴和其他中兴通讯商标均为中兴通讯股份有限公司享有的注册商标。本文档提及的其他商标，由各自商标权人拥有。

前言

中兴通讯作为全球领先的综合信息与通信技术解决方案提供商，为全球电信运营商、政企客户和消费者提供创新的技术与产品解决方案。

中兴通讯致力于成为“数字经济筑路者”，助力全行业加速数字化转型，面向广大合作伙伴开放合作，筑路数字经济，共赢数字时代。

中兴通讯高度重视**隐私保护**[1]，遵守业务所在国家和地区适用的隐私保护法律法规，将隐私保护作为“法律遵从、信任共建、道德履行”的重要基线。

中兴通讯聚焦场景，通过建立体系、推进实施、引入工具、嵌入流程、开展监督等，持续改进隐私保护能力，全面落地隐私保护合规要求。

中兴通讯将隐私保护理念融入产品设计和服务提供过程，作为竞争力、价值观的重要内涵，与相关方一起践行合规前提下的可持续发展。

中兴通讯积极参与业界交流，通过举办论坛、发布成果、贡献建议、参编标准等，为推动数字经济时代下的隐私保护进步贡献自身力量。

[1] 隐私保护，也称“数据保护”，本文档中与“个人隐私保护”、“个人数据保护”、“个人信息保护”等做一致性指代。

目录

中兴通讯隐私保护白皮书

(2025)

1 隐私保护政策

随着数字经济的深化演进，新技术的兴起对数据的需求增加，隐私保护成为消费者、社会公众、立法部门、监管机构等多方的关注热点，隐私合规愈加成为产业界的重要议题。作为全球领先的综合信息与通信技术解决方案提供商，中兴通讯始终高度重视隐私保护，确立了“满足法律要求，防控业务风险，赢得市场信任，共建良好生态”的隐私保护政策，构建了端到端、闭环型、流程化的隐私保护合规体系。

1.1 合规愿景

隐私保护合规致力于隐私安全、体系稳健、用户可信、商业自由。

中兴通讯努力建立独立、有效、高效的隐私保护合规体系并持续改进。体系致力于：采用先进的技术和管理措施，确保个人信息全生命周期处理安全可靠；灵活适应不断变化的法律法规与技术进步，确保隐私保护实践可持续发展；通过透明度承诺和负责任的行动，赢得客户与用户信任；隐私保护合规护航业务稳健发展，形成合规创造价值的良性循环。

中兴通讯努力提升隐私保护的效果、效率和效益，力争做全球隐私保护的先行者和践行者。

1.2 合规使命

隐私保护合规支撑业务风控、市场增信、品牌塑造、价值转化。

中兴通讯持续整合隐私保护的风控、增信和品牌，使得合规工作“始于法律，合于规则，嵌于业务，信于客户，融于品牌”。风控方面，遵从适用法律，履行合规义务，聚焦潜在风险，敏捷响应、科学应对和专业处置风险事件。增信方面，主动引入国际认证，积极开展客户交流，在产品研发、项目竞标、服务保障等方面展现合规能力，支撑市场竞争，赢得多方信任。品牌方面，尊重数字伦理和隐私道德，将对用户、客户、员工等相关方隐私关切融入企业价值观，提升隐私感知，丰富品牌内涵。

中兴通讯始终秉持“合规创造价值”理念，将合规能力转化为价值创造能力：深入探索内部创新合规方案，广泛吸纳外部成熟合规实践，在全球风险管控基础上，努力将业务单位的合规投入成本，转换为产品服务的市场信任价值，以合规建设“正循环”获得市场价值“正反馈”。

1.3 合规目标

1.3.1 遵从法律要求，防范控制风险

中兴通讯持续加强以风险为导向的隐私保护义务识别及规则转化。既遵从法律规定，又契合行业特点与企业实际，与公司治理体系全面融合；对标业界成熟实践案例，确保隐私保护风险可视、可防、可控，夯实合规建设基础。

1.3.2 促进业务落地，共建合规信任

中兴通讯积极回应用户和所有相关方的隐私关切，持续推进合规要求在业务活动中的有效执行。通过合规管控点嵌入业务流程，全员通识培训与差异化精准培训，执行坚决，稽查有力，实现内部规则敬畏、外部合规信任，促进隐私合规良性运行、持续有效。

1.3.3 护航商业持续，履行数字道德

中兴通讯坚守合规前提下的商业可持续、履行数字世界隐私道德。持续优化管理成本和合规效率，以强烈的社会责任感和卓越隐私保护合规能力守护用户、客户、合作伙伴、供应商、股东、员工等相关方利益，与各方一起维护产业链上下游的隐私保护良好生态。

1.4 合规保障

1.4.1 高层重视与资源投入

中兴通讯管理层高度重视隐私保护合规工作，将隐私保护与企业合规战略相匹配，将数据合规与出口管制合规、反商业贿赂合规共同列为公司三大合规领域，确保合规要求在具体业务流程的有效落地。高层重视下，中兴通讯在制度、流程、机制、管理、技术、工具上持续投入资源，结合引入外部律所、咨询机构的服务，积攒了丰富的的合规知识、经验和能力沉淀。

1.4.2 成熟组织与能力内化

中兴通讯建立了合规管理委员会领导下的合规管理组织机制，形成纵向贯穿、横向协同的合规运行架构，有利于将合规理念和政策传递到一线。隐私保护遵循公司统一合规组织架构，通过持续的合规培训和能力内化提升，促进各相关方准确理解合规要求，严格执行制度流程，实现合规要求有指引、合规咨询有回应、合规措施有执行的建设目标。

1.4.3 文化融合与良好氛围

中兴通讯形成了卓越合规文化下各方参与的良好氛围。数据合规部门在“专业为本、成就公司、勇担挑战、求真务实”的合规专业文化指引下，不断优化管控流程，与业务融合发展、良性互动。全体员工认同“合规创造价值”理念，围绕合规要求充分披露、持续消减、协同处置各类风险，积极反馈合理化建议，参与合规建设。

1.4.4 系统改造和工具嵌入

中兴通讯积极采用先进的隐私保护技术措施，通过信息系统改造和专业工具嵌入，促进合规管理的数字化转型。围绕主营业务和产品研发流程关键管控点，持续加强IT化建设，引入信息系统、专业工具以及技术方案，确保全流程数据处理可记录、可查询、可追溯和可核验，实现更加系统化、数据化、智能化的隐私合规评审与风险改进跟踪。

2 隐私保护框架

中兴通讯建立了以风险为导向的隐私保护合规管理体系，以风险识别为起点，以合规管理为工具，在自上而下合规体系建设基础上，推动自下而上规则的场景化，确保合规规则与具体业务融合，形成契合业务实际的合规管理体系。

中兴通讯管理层高度重视隐私保护工作，形成合规工作与企业发展相匹配的战略设计，明确了隐私保护合规建设目标、长期规划，通过研究业界成熟模型、吸收业内成功经验，实现在防范风险基础上满足相关方隐私保护期待与要求。

中兴通讯搭建了符合中国《个人信息保护法》、欧洲《通用数据保护条例》以及全球适用的隐私保护法律法规要求的公司级合规规则，实施重点业务示范治理与关键国别专项治理，将隐私保护要求融入到产品设计、服务交付和运营管理活动中，推动业务活动与合规管理结合，支持产品创新与合规遵从的平衡落地。

2.1 组织架构

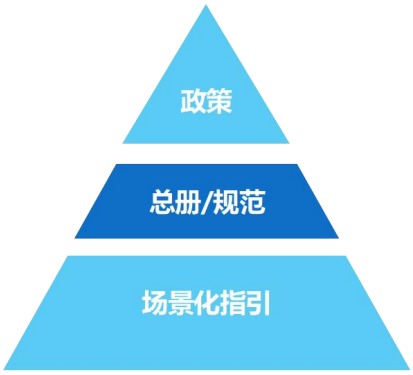
中兴通讯建立了隐私保护合规协同工作机制，在合规管理委员会下，设有数据保护官、数据合规专业部门、业务领域合规团队进行合规管理要求制定并推动落实，合规稽查部门负责审计和调查。

中兴通讯合规管理委员会是负责合规管理体系运作与合规事项决策的最高指导机构，听取数据合规重大事项汇报并进行指导。数据合规部关注法律要求的识别，负责全球数据保护法律法规、政策标准研究与规则转化，隐私保护合规策略和合规规则的规划、制定、执行与监督，对具体业务流程的合规风险进行评估和审查。业务领域合规团队关注合规规则的可落地性以及

管理成本的优化，推动合规规则落地，评估规则的必要性和合理性。合规稽查部门关注规则盲点和风控管理的平衡，建立了多维度举报途径，鼓励员工积极举报违规行为，并进行审计调查和处置处罚。

2.2 规则体系

中兴通讯建立了“政策、总册/规范、场景化指引”的规则体系。



2.2.1 政策

合规政策是根据中兴通讯整体经营策略所制定的政策性文件，明确了在经营活动中需要遵循的红线，表达了中兴通讯遵守其业务所在国家/地区适用的隐私保护法律法规的决心，体现了董事会、合规管理委员会对于隐私保护合规给予的支持，是中兴通讯开展合规工作的纲领性文件。

2.2.2 总册/规范

数据合规总册是基于外部法律法规要求，结合合规政策确定的总体指导文件，是公司层面开展各项隐私保护合规工作的指导文件，涵盖通用合规要求、关键管控点。规范，是对总册中已有管控点的细化，或基于外部法律法规快速变动而单独制定，从而将法律法规规定的关键义务转化为合规要求的专项规范。

2.2.3 场景化指引

场景化指引是基于总册/规范要求，引入实际场景进一步细化而形成的业务领域隐私保护合规指引集群。场景化指引按照业务架构进行排列，依托于数据化协作共享平台，方便员工查询使用，亦可根据需求更新变化，实现规则的透明、可视，保障规则的易学、易懂和可落地。

2.3 流程机制

中兴通讯针对个人信息处理关键义务环节开发IT系统并嵌入业务流程，便于跨部门协同参

与，自动保存完整记录，作为合规管理体系的有效佐证。

2.3.1 默认隐私保护设计

中兴通讯根据系统功能和产品个人信息保护需求，制定合适的隐私保护设计策略。隐私保护设计要求涵盖个人信息收集、传输、存储、使用、共享、销毁的数据全生命周期。产品隐私保护设计要求涵盖产品需求分析、产品设计、产品开发、测试审核、发布部署、运维管理等产品全生命周期。

2.3.2 数据保护影响评估

中兴通讯使用“数据保护影响评估系统”，对新产品、新技术、重大产品服务变更、敏感数据处理活动等进行线上评估，确保对个人权益有重大影响的个人信息处理活动满足合规要求。例如，在研发流程产品需求分析、产品设计环节，评估收集个人信息的必要性，分析在权限、日志、加密、匿名等方面采取的隐私保护措施；在处理及传输个人信息前，评估安全合规要求符合情况，引导产品、服务采取合规措施，降低业务合规风险。

2.3.3 数据提取合规管控

中兴通讯建立后台数据提取管控机制，基于合理必要的业务需求提取系统后台数据前，对拟提取的个人信息进行筛查，对高风险数据采取脱敏或屏蔽措施，可有效降低数据脱离信息系统后的安全风险。

2.3.4 数据跨境传输合规管控

中兴通讯开展涉及个人信息跨境传输的业务活动时，采取充分、适当的数据跨境传输保障机制，例如满足数据出口国的数据跨境监管审批/备案机制，签署个人信息跨境传输相关协议、获得个人信息主体同意、开展跨境影响评估等。

中兴通讯积极响应法规要求，首批申报数据出境安全评估并通过申报，并建立了个人信息跨境筛查机制，根据法律法规采取必要的合法性加固措施。

2.3.5 委托处理数据管控

中兴通讯与第三方开展个人信息处理相关合作之前，针对业务类型及合作场景开展风险评估，并根据风险等级采取不同管控措施。

在业务过程中委托第三方开展个人信息处理活动的，事先签署个人信息处理协议，明确约定委托处理的目的、期限、处理方式、数据种类、保护措施以及双方的权利和义务，由负责与第三方对接的部门履行监督义务。

2.3.6 个人信息主体权利响应

中兴通讯开发了IT化的、简单便捷且公开的个人信息主体权利行使申请入口，确保个人信息主体权利请求得到及时受理、全面管理。依托该系统，隐私合规专家、数据保护官、业务负

责人、技术工程师等能够协同参与响应流程，对个人信息主体权利诉求做出专业、客观、妥当回应，自动形成流程跟踪和响应记录，为个人信息主体提供便捷的交互体验，有利于呈现良好的责任承担意识，提升公众信任。

2.3.7 个人信息泄露响应

中兴通讯通过完善管理制度、组织应急演练、强化合规培训等确保个人信息处理活动符合法律法规，降低个人信息泄露事件发生概率。当发生切实、疑似或潜在个人信息泄露事件时，依托“个人信息泄露响应系统”，线上实施包括上报、判断、分析、处置、修复、通知、复盘与改进等事件响应全流程并完整记录，满足事件多方协同处置、内部文件调阅、外部证据呈送等需求，使个人信息泄露事件响应更加科学、及时、专业、有效。

2.4 风险管控

中兴通讯建立了以风险为导向的隐私保护合规管理体系，通过风险评估与持续改进，更好地适应不断变化的内外部环境。

2.4.1 数据收集和处理的前提条件

作为直接面向个人用户提供产品/服务的数据处理者时，主要评估：

①是否已核对并记录数据处理活动的目的；

②数据处理活动是否具备适当的合法性基础；

③需要获得个人信息主体同意的，是否已获得其同意并允许其撤回，是否对同意的获取情况进行记录；

④需进行数据保护影响评估的，是否进行评估；

⑤涉及到数据处理受托方或共同数据处理者时，是否与其签署适当的协议；

⑥是否对各项数据处理活动进行全面及时的记录。

作为面向客户、合作伙伴提供产品/服务的数据处理受托方时，主要评估：

①是否与数据处理者签订适当的协议对相关内容进行明确；

②是否严格按照数据处理者的书面指示开展个人信息处理活动；

③将从数据处理者处获取的个人信息用于营销和广告前，是否征得个人信息主体同意；

④当数据处理者的数据处理指示违反相关法律法规规定时，是否会及时通知数据处理者；

⑤是否会采取适当的措施以协助数据处理者实现合规要求；

⑥是否会对各项数据处理活动进行全面及时的记录。

2.4.2 履行对个人信息主体应当承担的义务

作为直接面向个人用户提供产品/服务的数据处理者时，主要评估：

①是否明确应当对个人信息主体所承担的义务并记录；

②是否向个人信息主体提供隐私告知；

③是否具备相应的机制以响应个人信息主体的权利请求；

④涉及自动化处理时，是否赋予个人信息主体拒绝的权利；

⑤当收到个人信息主体权利请求时，是否及时通知数据共享或受托处理的第三方；

⑥是否在规定时间内响应个人信息主体的权利请求；

⑦是否对个人信息主体行权响应进行完整记录。

作为面向客户、合作伙伴提供产品/服务的数据处理受托方时，主要评估是否能积极协助数据处理者响应个人信息主体权利请求。

2.4.3 具备设计和默认的隐私保护要求

作为直接面向个人用户提供产品/服务的数据处理者时，主要评估：

①是否仅在目的范围内收集和处理个人信息；

②是否可以保证各项数据的质量和准确性；

③是否明确数据最小化的目标，或是否会采取相关措施以实现数据最小化的要求；

④数据处理目的达成后是否会及时删除数据或进行匿名化处理；或对处理过程中创建的临时文件进行及时删除或销毁；

⑤是否设置明确的个人信息存储期限；

⑥是否会采取适当的措施以保证数据存储和传输安全、准确。

作为面向客户、合作伙伴提供产品/服务的数据处理受托方时，主要评估：

①是否会对处理过程中创建的临时文件进行及时删除或销毁；

②处理活动结束后，是否会按照协议要求及时返还、传输或处置个人信息，或应数据处理者要求提供相应的证明；

③是否会采取适当的措施以保证数据存储和传输安全以及到达指定接收处。

2.4.4 确保数据共享披露与传输合规性

作为直接面向个人用户提供产品/服务的数据处理者时，主要评估：

①是否明确数据共享、披露与传输双方的基本信息，特别是双方所在法域；

②是否明确进行数据共享、披露与传输的合法依据，特别是涉及跨境传输的情形；

③是否会对数据共享、披露与传输进行全面及时的记录。

作为面向客户、合作伙伴提供产品/服务的数据处理受托方时，主要评估：

①是否明确数据披露或传输双方的基本信息，特别是双方所在法域；

②是否明确数据披露或传输的合法依据，特别是涉及跨境传输的情形；

③是否会及时向数据处理者通知数据披露请求；

④是否会提前告知委托方任用、变更其他第三方处理个人信息等相关信息。

中兴通讯结合风险评估方法，针对合规管控点，通过自查、检查、审计、调查等不同方式验证和监督数据处理活动，确保合规治理要求及合规管控点的切实履行。通过动态的业务再评估和风险再发现，反哺和优化合规规则，调整和改善管控措施，提高整体隐私保护合规水平。

中兴通讯聚焦业务、国别两个方向提高合规能力。业务方向，加强规则与业务活动流程之间的衔接，使规则与业务发展相匹配。国别方向，加强重点国家和地区动态跟踪，针对特殊规定基于全球规则作出适用性解释，对本地化规则进行灵活适配。

3 隐私保护共建

中兴通讯积极推动隐私保护的产业链整体合规共建，将隐私保护作为相关方合作的共识和纽带之一，以自身及产品的合规建设为起点，在确保自身产品及服务合规的同时，与产业链内外各方协同共建，共同创建行业良好合规氛围，为隐私保护生态圈建设贡献力量。

3.1 内部共建

中兴通讯隐私保护体系来源于公司内部各部门之间的协同合作与共同建设，除合规部门外，与安全部门协作成为内部共建的重要一环。中兴通讯建立了数据安全合规联席工作机制，集合安全、技术、合规、管理等多领域专家，围绕隐私安全合规治理开展联合行动，针对个人信息跨境传输、新技术开发等高风险业务场景，加固隐私安全、提升合规信任。

3.1.1 产品安全共建

中兴通讯将网络安全作为产品研发和交付的最高优先级，实施自上而下、基于风险的网络安全治理，覆盖供应链、研发、交付和各支撑职能领域，形成了贯穿产品生命周期的产品安全保障体系。2023 年 12 月发布的网络安全白皮书《治理、遵从、开放、透明——中兴通讯网络安全保障实践》[2]系统地介绍了中兴通讯安全治理架构和安全保障体系，着重强调了行之有效的治理方法和实践，即在产品全生命周期安全管控基础上，聚焦于纵深改进，包括设计安全和默认安全、第三方组件管理、事件响应和漏洞管理等。这些安全管理贯穿供应链、研发和交付业务流，并通过数字化支撑系统的不断完善实现有效落地和持续改进。

中兴通讯秉承开放透明的原则，在中国、意大利、德国运营网络安全实验室，使客户、监

[2] 欢迎从“中兴通讯官网——关于我们——信任中心——网络安全”获取《中兴通讯网络安全白皮书（2023）》。

管以及利益相关方能够便捷、透明地验证中兴通讯的产品安全性。公司重视内外部发现的漏洞，结合客户及相关方的意见和要求进行负责任的披露，提供规避措施及解决方案，实现漏洞闭环管理。同时设置漏洞奖励计划，欢迎全球安全从业人员/机构向我们反馈产品和服务的安全问题。

产品安全与隐私保护息息相关，全球市场对网络安全和隐私保护的监管要求不断加强，客户要求不断提升。在产品交付全流程，为保护客户数据，中兴通讯创建了体系化的管理和技术规范，确保公司提供的产品和服务满足法律法规、业界标准、客户标书的安全合规要求。在海外安全合规增信项目中，产品安全与隐私保护保持协同开拓，积极推动与监管/客户沟通、参与行业会议论坛、宣传公司安全合规举措和成果，以开放透明的态度获取市场信任。

3.1.2 信息管理共建

中兴通讯实施信息全生命周期管控，保护信息机密性、完整性、可用性，建立了完善的信息安全管理体系、档案及文档管理体系，定期开展信息安全生命周期稽查工作，发现和调查相关违法违规行为，提升全员信息管理意识。

中兴通讯开展了关于加强个人信息安全治理的项目，以降低个人信息的泄露、滥用风险。项目目标包括：识别包含个人信息的高风险系统，同时将高风险系统后台的个人信息纳入信息安全内审；由业务单位将包含个人信息的系统进行识别和上报，确定是否进行后续治理；将“显示、导出、交换”的安全治理要求嵌入流程，确保系统功能“不达标，不上线”。项目实现了高风险系统的 100%去标识化治理，在满足法律法规要求的前提下，保护了公司员工、客户、上下游合作伙伴等重要主体的个人信息，践行了隐私保护安全与合规理念，获得了内外部信任，以主动合规实现信息管理与隐私保护的深度融合。

信息管理与隐私保护有机结合，建立了嵌入信息安全管理流程的隐私保护机制，信息管理是隐私保护的安全前提，隐私保护是信息管理的重要目标。如发生数据泄露事件，一方面涉及信息系统的机密性缺陷，另一方面泄漏后可能对个人信息主体权益造成侵害，隐私保护与信息管理通力合作，共同解决和处理风险事件。

3.2 客户共建

中兴通讯严格遵守全球通行隐私保护法规、商业准则及客户要求，以实现对个人信息全生命周期的保护为目标，在商务协议中嵌入隐私保护语言，明晰各自数据处理角色并积极承担对应责任义务，与客户共建良好的隐私保护环境，践行企业社会责任。

中兴通讯作为数据处理受托方时，代表客户处理的个人信息不会被用于任何客户书面指示之外的目的；积极协助客户履行其面对个人信息主体所应承担的义务；例如，在指定的记录期

限内按照程序删除因个人信息处理而产生的临时文件，以尽可能安全的方式及时对相关数据进行返还、传输与处置，确保个人信息传输在配备适当控制措施的数据传输网络中进行，以保证数据安全地传输到指定接收方，防止数据泄露。

中兴通讯积极主动向客户提供国际一流隐私安全合规外部认证证书、个人信息处理记录、合规审计报告等合规材料，以证明遵守数据处理受托方的法定及约定义务，亦可满足客户证明其自身合规的需求。中兴通讯也积极协助客户响应外部监管要求，站在客户角度充分研判法律风险，深入一线支持客户的合规诉求，想其所想、解其之难，以协同双赢、合规共建为目标为客户提供可落地的综合解决方案。

3.3 供应商共建

中兴通讯立足供应商管理制度，通过嵌入隐私保护要求促进与供应商的合规共建，对供应链上下游隐私保护合规生态建设发挥推动作用。

中兴通讯通过供应商协议签署、数据跨境转移审批等关键控制点实施合规管控。在供应商准入认证环节，实施分级分类管理，审核供应商的隐私保护能力，根据供应商提供的产品或服务起草恰当的协议或条款，如数据处理协议或安全协议、合规备案、重点供应商安全审计等，明确各方权利义务。针对不同业务场景，根据数据处理活动中的角色关系区分“数据处理者、“数据处理受托方”、“共同数据处理者”，履行法律法规规定的合规义务。针对高风险场景，如AI大模型训练数据采购，中兴通讯设立单独评审流程，对模型训练数据采购需求、供应商资质及采购标的进行合规评估，并要求签署数据交易协议，确保模型数据来源合法合规。如果与供应商之间存在个人信息共享、委托处理及转移情形，依据具体情况进行数据保护影响评估，根据评估结果采取相应管控措施。

3.4 合作伙伴共建

中兴通讯在与隐私保护强相关的业务合作中，对合作伙伴数据保护合规能力进行评估，确保合作过程中进行的个人信息处理活动合法合规。

中兴通讯与合作伙伴在数据处理协议中明确各自角色及其职责、各自在个人信息主体行权以及发生数据泄露时需履行的义务。基于与合作伙伴的共同目的处理个人信息时，与合作伙伴构成共同数据处理者，协同合作伙伴对个人信息主体进行恰当的隐私通知设置。与合作伙伴进行的个人信息处理活动是基于各自的目的时，各自构成独立的数据处理者，分别对个人信息主体进行恰当的隐私通知设置。在将个人信息共享、转移给合作伙伴的过程中，严格遵守数据保

护的法定及约定要求。

3.5 行业领域共建

中兴通讯以透明、开放、信任、合作为理念，通过行业领域交流和吸收前沿隐私保护技术和方法，提升产品和服务隐私保护能力，满足新技术、新应用、新模式下的合规需求。

中兴通讯与监管部门、行业组织、技术机构、高等院校、其他企业等保持互动，就最新立法解读、合规体系建设、新技术驱动的隐私保护等话题开展沟通交流，指导实践。2022 年 9 月 9 日，中兴通讯参与中央网信办、中央文明办主办的“中国网络文明大会个人信息保护论坛”，分享了隐私保护设计（PbD）流程嵌入、自研隐私合规评审系统、自研 App 隐私合规扫描工具以及产品隐私及用户隐私“双中心”建设等创新实践，中兴通讯终端隐私保护及安全合规竞争力建设入选“个人信息保护创新实践案例”；2023 年 11 月 16 日，中兴通讯举办第四届跨国企业贸易合规论坛，在新技术合规管理分论坛中，与行业专家研讨新技术驱动的合规挑战与机遇、人工智能科技伦理、数智时代下的数据安全合规等话题，介绍了生成式人工智能的隐私保护合规要点，分享了中兴通讯隐私保护建设实践。此外，中兴通讯举办了多届数据安全与个人信息保护学者论坛，邀请学界、业界深入探讨数据合规前沿热点与企业实践。

4 隐私保护实践

4.1 法律研究

为顺应全球数据法变动频繁的特性，中兴通讯制定了外部规则动态跟踪识别及分级响应标准化流程，以风险为导向，对业务所在国家和地区的外部法规、监管案例、行业动态等进行常态化识别和响应，为隐私保护风险排查、规则转化提供支撑。对于与公司业务强相关的重要外规动态，逐条进行合规义务识别、业务合规管控成熟度分析与风险评估，根据评估结果，设置关键控制点，嵌入业务流程，将个人信息全生命周期管理的法律要求吸收融入到内部规则中，并向隐私保护合规义务遵从相关方宣贯推送、推动落地。

中兴通讯建立了包括中国数据合规立法、境外数据保护立法、行业前沿、专题研究等栏目在内的隐私保护法律资源空间，面向业务单位、合规团队开放，便于随时查阅，推动能力内化。中兴通讯隐私保护团队还依托“全球法律政策研究院”平台，将前沿法律研究成果、业务实践经验累积沉淀，形成了《个人数据概念疏证》《跨国企业数据保护官设置研究》《合规体系建设关键要素研究》《基于ISO27701 的个人信息管理体系（PIMS）的分析与应用》《合规领域

企业及高管法律责任研究》《中国APP隐私保护法律与隐私设计相关性研究》《隐私合规IT化实证研究》《中国智能网联汽车出海合规挑战》《数据资源采购合规实务》《中兴通讯中国数据出境合规遵从管控方案》等专项研究成果，基于业务实际提供前瞻性分析及对策建议，为自身合规建设提供持续价值和长期指导。

4.2 业务实践

针对隐私保护领域法律法规频繁出台、合规治理方案需因时制宜的专业现状，中兴通讯制定了数据合规风险评估标准化流程，自上而下将外规要求快速转化为与业务灵活结合的合规要求，自下而上在鲜活的业务反馈中查漏补缺，落实专项管控策略，解决复杂多变的实操挑战。

此外，中兴通讯鼓励业务单位基于自身特点执行隐私保护规则，催生大量个人信息保护良好实践，形成一批实际落地经验，扩展合规在业务中的执行基础，提升企业整体隐私保护能力和水平。

4.2.1 营销

中兴通讯营销业务包括市场营销、客户关系管理、商机管理、竞标管理等活动。在客户引入与客户关系维护、客户来访及接待、商务展会中涉及对客户联系人个人信息的处理，在方案制作及投标、合同谈判及签约、合同签约评审中涉及与客户明确数据处理权责的协议签署。

客户关系管理业务活动场景中，主要处理客户提供的业务联系人姓名、电话、邮件地址等信息，便于维持日常商务往来沟通，通过信息系统进行隐私保护管控，保障个人信息收集、储存、使用等符合最小化原则；特殊情况下，当邀请客户来访或参加展会，需要为客户预定机票/酒店时，如需获取护照/证件号码等敏感个人信息，会通过适当方式（如发送隐私通知书）向其说明收集和处理个人信息的目的，取得个人信息主体的同意，并在活动结束后及时删除。

竞标管理业务活动场景中，积极配合客户签署相关协议并履行相关义务，充分披露数据处理的目的、数据流转路径、数据类型、为保障数据安全所采取的技术及组织措施等要素，在获得客户授权同意并通过内部审批后，方可进行数据处理。

4.2.2 系统产品

中兴通讯系统产品业务包括无线及算力产品（无线网络、智算、核心网、服务器等）、有线产品（承载网、固网、多媒体等）、数字能源产品（通信能源等）及产品相关的解决方案。系统产品设备本身的网络安全、数据安全设置将直接影响用户的个人信息安全，主要关注隐私保护设计、个人信息主体权利实现、产品安全加固、权限管理等方面。

系统产品研发将隐私保护设计（PbD）嵌入高效产品开发流程（HPPD），通过规则嵌入

和运行实践，经历了风险识别、嵌入方案设计、项目试点、规范修订发布等步骤，把个人信息全生命周期风险管控以默认隐私设计的要求嵌入到研发需求管理、系统设计、开发验证、发布阶段。在项目技术评审和版本发布等里程碑节点对研发项目的执行进行检查验收。

在HPPD流程的系统方案阶段进行数据保护影响评估，基于已识别的个人信息和数据流向，从个人信息主体权利保障和数据安全两方面，识别数据处理全生命周期中潜在的威胁和产品可能存在的漏洞，评估风险等级，确定风险处置策略，制定风险处置方案并组织实施。

4.2.3 终端产品

中兴通讯终端产品业务是包含研发设计、供应交付、销售及售后服务等并形成经营收入的端到端系列活动，主要包括产品研发、产品经营、产品供应、产品销售及客服、产品品牌管理和质量管理等业务。

守护终端产品隐私合规基线，捍卫公司合规形象，创造终端合规品牌价值，是终端事业部向用户、向社会递交的一张可信赖名片。终端事业部始终致力于提升用户对中兴通讯品牌隐私保护水平的感知，持续为用户打造更安全、安心的产品和服务。终端产品始终坚持将默认隐私保护设计（PbD）理念融入产品研发全生命周期，通过完善的隐私保护组织、流程、技术管理体系，确保全面守护和合规处理所收集的个人信息。

为符合隐私合规监管矩阵要求，终端BU合规团队与业务单位制定了对外发布及预置应用合规评审流程，终端产品及其搭载的应用上线前必须通过严格的隐私合规审核，完成评审问题整改工作，通过业务侧、业务领域BU合规经理及合规专家三级审批进行合规风险识别与管控；技术层面通过数据加密、防泄漏、数据库审计等实现对消费者隐私的守护。产品研发外的其他场景，如电商、供应链、客服、售后、调研、众测等，均设计了完善的流程管理制度，确保业务执行的各个环节满足隐私保护要求。

个人隐私保护的监管日趋严格，终端产品安全团队对产品隐私安全进行深入研究，自主开发及应用终端隐私安全合规检测平台“隐私合规探测器”，通过静态动态扫描实现从评审流程到技术监管的完整闭环。“隐私合规探测器”的研发和上线，突破了人工检测大量代码的不可能性，节省了人工检测的人力及购买第三方检测工具的费用支出，有效支撑了产品开发单位的移动应用检测需求。此检测平台的推出也让中兴终端在合规上的积累与建设有了具象的依托，是合规规则沉淀、合规产品化、合规创造价值的体现。

4.2.4 供应链

中兴通讯供应链业务是通过对物流、信息流和资金流进行设计、规划、控制与优化，整合企业上中下游，最大程度减少内耗与浪费，实现企业整体效率的最优化，保证供应链中的成员取得相应的绩效和利益，快速满足客户需要的整个管理过程。供应链涉及处理个人信息的业务

活动主要包含采购业务、物流业务等。

供应链业务活动主要涉及处理客户、供应商提供的业务联系人姓名、电话、邮件地址等信息，以便于商务谈判、招标、货物的接收、交付、付款能够顺利进行。收集供应商提供的个人信息时，通过适当方式（隐私声明、邮件等）向其说明收集和处理个人信息的目的及其他必要内容，在适用的情况下取得个人信息主体的同意；仅收集与业务相关且必须的最小范围的个人信息；保障个人信息主体的权利，如供应商或个人要求访问、删除、更改由中兴通讯供应链所处理的个人信息时，进行及时、有效的响应；对个人信息存储期限进行评估，在与供应商合作关系终止后，在满足外部法律和内部流程前提下，删除与其相关的个人信息；存储、传输供应商提供的个人信息时，IT系统会进行权限管理、安全加密以及记录操作日志。

当采购合同的主要标的是由供应商处理中兴通讯的、客户的或其他供应商所提供的个人信息时，对供应商进行个人信息保护履约能力调查、审计及监督，并与其签署适当的数据合规协议；要求和督促供应商按照法律法规及合同约定的要求删除个人信息；从客户处回收的设备，以及维修时替换下来的器件中可能存在客户的或最终用户的个人信息，为了防范潜在的数据泄露、不当处理的风险，供应链会对维修中替换下来的存储器件进行数据脱敏或破坏处理。如果需要交由回收商进行实物处理，会要求其签署数据合规协议、提供处理报告，以减少个人信息泄露风险。

4.2.5 工程服务

中兴通讯工程服务业务是将销售合同通过工程交付、技术交付与服务交付的实施转化为交付成果，并实现营业收入的一系列活动。工程服务涉及隐私保护的业务活动主要包括技术交付业务、客户支持业务和工程外包管理业务等，主要涉及的数据类型包括运营商客户的网络用户数据，以及第三方合作伙伴的人员信息等。

工程服务领域契合业务活动的特点，制定工程服务业务活动的数据合规场景化指引，将隐私保护规则要求嵌入具体的业务活动场景和业务流程，实现规则管控场景化、流程化，让规则真正可落地、能实施；工程服务领域通过合规培训、宣贯等方式，将相关业务场景和流程的隐私保护管控要求传递、同步给员工，让员工更好地理解相关管控设置的必要性，清楚具体的管控措施，从而减少因认知不同步带来的管控规则执行偏差；工程服务领域通过建立适用于工程服务业务特点的隐私保护关键管控点（KCP）的检查机制，聚焦高风险业务活动场景和流程，检查和评估业务员工对相关业务活动KCP的执行，从而保障业务活动KCP的切实落地。通过对检查结果的分析、对业务人员关于KCP执行建议的收集与反馈、外部机构的审计建议等途径和方式，评估和审视KCP设置的合理性，并对于KCP的设置和实现方式进行及时的调整和优化，在确保KCP覆盖业务活动主要隐私保护合规风险的前提下，持续提升管控的有效性以及降低规

则执行的成本。

4.2.6 总部职能

中兴通讯总部职能业务包括集团的运营管理，支撑核心业务生产力的的行政物业管理服务。

总部职能领域业务类型广泛，涉及活动众多，主要采用场景化的指引对涉及个人信息收集处理的场景加以管理，对风险场景逐个进行突破。总部职能领域隐私保护管理逻辑是：合法性基础评估、获取同意方式评估、收集信息字段必要性评估、目的与授权范围最小化评估、第三方供应商安全性评估、保存期限合理性评估、系统安全性评估。基于上述因素考量，对风险场景出具具体的管控建议。

以国际第三方客户满意度调查的实践为例，其目的是通过问卷根据客户反馈改善服务和产品，提升用户满意度。为确保目的限制，调查时对客户信息的使用目的、使用时效进行说明；为确保授权范围最小化，被调研人员信息的获取范围，存储和传递需限制在最小范围内；为确保透明性，调查时告知客户传递的个人信息字段、处理原则及客户享有的个人信息主体权利；为确保保密性，调查过程中对客户个人可标识信息严格保密，不传递给第三方。

4.2.7 人力资源

中兴通讯人力资源业务活动包括人力规划、招聘调配、任职管理、干部管理、绩效管理、企业文化、薪酬管理、员工关系、学习与能力发展、健康安全等一系列企业活动。人力资源管理活动需要处理大量员工个人信息，中兴通讯高度尊重员工个人权益、保护员工隐私，一方面将外部法律内化为企业治理规范，另一方面将国内国际标准转化为可落地的管理举措，确保员工信息处理安全可信、过程管理合法合规。凝聚雇主品牌，共建信任力量，塑造“员工隐私捍卫者”形象。

人力资源将隐私保护管控融入业务实施全过程，通过人力资源隐私保护组织建设、规则制定、流程嵌入、信息技术措施等确保收集、处理员工及相关方个人信息的安全合规。人力资源业务系统均实现隐私政策的嵌入，将收集信息的类型、合法性基础、个人信息主体的权利及行权途径明确写入隐私政策。同时，这些系统在需求、开发、测试、发版上线等各阶段均符合中兴通讯的产品安全和信息安全基线要求。对于线下活动，如涉及员工或员工家属的个人信息收集，会发布隐私告知，确保员工及其家属能够充分地理解数据收集和使用的目的。

“爱在中兴”是公司面向员工及家属的凝聚力活动，通过家属认识中兴、走进中兴、了解中兴，来提升员工的职业认同。为了给员工家属提供住行饮食一条龙贴心服务，中兴通讯会在确保家属体验的前提下遵循最小化收集原则，收集员工家属的证件号码、饮食习惯等信息，并在隐私告知中明确公司所收集员工家属信息的类型与目的。所有信息使用公司内部的加密文档库存储，仅限活动组织方人员有权限查看。活动结束后，中兴通讯会及时删除电子版的个人信

息，打印的纸质信息会直接销毁，确保对员工及家属的个人信息处理符合业务经营所在国法律法规和政策要求。

4.2.8 财务

中兴通讯财务业务活动包括财务核算、财资管理、税务管理、预算管理、成本管理、财务绩效管理、应收管理、财务监控、销售融资、对外担保、证券事务等。财务业务活动主要面向公司内部员工和外部合作方，处理的个人信息涉及资金信息、身份信息、税务事宜，敏感度较高，在费用报销、个税申报、证券事务信息披露等场景中需要对个人信息进行全方位的保护以维护员工和外部合作方的个人信息权益。

守护财务活动隐私合规基线，既是保护员工和外部合作方的个人隐私，也是在捍卫公司合规形象。财务始终致力于提升内外部用户对隐私保护水平的感知，持续为用户打造更安全、安心的产品和服务。财务始终坚持将隐私保护理念融入提供财务服务的全过程，通过完善的隐私保护组织、架构、制度流程、技术措施，确保合规处理所收集的个人信息。

以费用报销为例，中兴通讯使用财务在线系统进行费用报销，为符合隐私合规管理的要求，制定了中兴财务在线系统隐私政策评审及上线机制，在中兴财务在线系统中进行权限隔离管控，对个人信息的传输和存储进行严格管理，并对系统进行信息安全加固。基于境外子公司日常经营管理需求，依托IT系统与公司总部进行个人信息跨境传输的情况，通过签署全球母子公司数据跨境协议，确保个人信息跨境传输合规。

4.2.9 战略投资

中兴通讯战略及投资业务承担公司整体战略规划及投资管理工作，具体业务活动包括兼并收购、实体新设、撤资/股权出售、实体解散、实体转型、对外合作、展会活动等一系列活动。战略及投资业务领域涉及处理个人信息的场景主要集中在展会活动、兼并收购、股权出售、实体解散业务中。

中兴通讯举行或参加各类展会活动，涉及到邀请客户代表、参展人员行程、住宿安排及接待事宜，期间涉及到大量的个人信息处理活动，展会场景下的隐私保护工作是中兴通讯隐私保护的重要一环。以通信领域内的国际盛会巴塞展为例，中兴通讯在展会全阶段实现隐私保护合规管控，保护客户的个人信息安全。在展前向客户发送邀请函的同时发送隐私通知书，明确告知收集个人信息的种类、目的，采取的保护措施，客户享有的权利以及行权途径等内容。在展会开展过程中，除业务人员外，业务领域BU合规经理以及数据合规专家顾问会实时为展会提供隐私保护及数据合规方面的支撑，为参展人员提供全方位的个人信息保护。

企业拥有的数据可能创造多种价值与用途，但也因为企业对数据的收集、使用、共享行为而可能为企业带来不同程度的风险。基于国内隐私保护法律对合并、分立、解散、破产等情况

的管控要求，中兴通讯梳理了投融资业务的隐私保护风险管控规则，结合实际业务流程制定了《投资并购数据合规指引》、《子公司出售数据合规指引》及《子公司清算注销数据合规指引》，并在投融资项目中落实，有效管控公司在投融资活动中的隐私保护合规风险。

4.3 开放共享

中兴通讯致力于开放成果共享，促进交流合作。通过论坛、沙龙、出版物、自媒体等形式跟进立法前沿，向企业行业、专业机构、高校院所等社会各界积极分享隐私保护实践场景和合规治理经验，与业内专业人士深度交流，互相促进，共同成长，共同建设可信合规环境。

中兴通讯建立了“合规小叨客”微信公众号，致力于呈现最前沿数据合规动态，打造最扁平国别法律研习纽带，直击行业最鲜活合规治理痛点，分享最实用企业隐私保护合规实践。“合规小叨客”发布的《数据跨境合规治理实践白皮书》《5G应用场景与隐私保护前沿报告》《员工隐私保护实务系列》《欧盟推出全球首部AI监管全面法案》《ChatGPT潜在数据保护风险分析及建议》《AIGC研发及应用数据隐私合规义务识别——以意大利监管ChatGPT为切入点》《一次性说清GDPR管辖权》《个人信息保护法下企业内部调查的合规路径》《白话数据合规》等系列文章取得积极反响，在隐私保护合规领域建立了名片。

中兴通讯定期汇编内部法律研究成果并对外共享，已面向公众发布《数据跨境合规治理实践白皮书》《5G 应用场景与隐私保护前沿报告》《隐私保护设计（pbD）研究报告》《全球数据保护监管机构口袋书》《GDPR 执法案例全景白皮书》等兼具前沿性与实务性的隐私保护研究专业报告，致力于维护开放共享的隐私保护共建文化。

4.4 核心认证

能力是隐私安全的保障。中兴通讯将隐私保护作为产品与服务的重要基线，不断加强物理、管理、技术和组织方面的安全措施，提升数据安全保障能力，打造可持续、透明、开放、可信的隐私保护环境。

中兴通讯持续维持业界权威认证，终端、5G 、核心网、数字技术产品以及人力资源管理等业务线已通过 ISO/IEC 27701:2019 隐私信息管理体系认证，终端业务通过欧洲权威隐私认证机构 ePrivacy GmbH 颁发的 ePrivacyseal Global，为全球用户提供更加规范、成熟、全面的隐私安全保障。

中兴通讯 5G 产品线已多次通过持续迭代的全球移动通信系统协会（GSMA）网络设备安

全保障计划（NESAS）的开发和产品生命周期流程审计，5G RAN 和 5GC 产品通过 NESAS 设备安全评估，5G NR gNodeB 产品获得由德国联邦信息安全办公室（BSI）颁发的“网络设备安全保障方案网络安全认证计划-德国实施”（NESAS CCS-GI）认证证书，5G RAN 解决方案、OTN 全系列产品、数通系列产品先后获得系统级解决方案的通用标准（CC）EAL3+认证，5G 基站软件获得 CC EAL4+认证，为全球客户提供更加安全、可靠、合规的通信产品及解决方案。

5 大事记

权威认证/评估	
通过中国国家数据管理能力成熟度（DCMM）认证（获评最高等级 5 级）	2024/10
通过欧洲隐私权威认证 ePrivacyseal Global 认证	2024/06
通过国际标准 ISO/IEC 27701:2019 隐私信息管理体系认证	2024/05
通过中国国家网信办数据出境安全评估	2024/01
通过美国隐私权威认证 TRUSTe Enterprise Privacy 认证	2022/08
奖项荣誉	
《中兴通讯：提升企业韧性，一流合规体系的建设之道》荣获 2024 拉姆·查兰管理实践奖——杰出奖	2024/10
英国标准协会（BSI）2022 年度“安全隐私合规先锋奖”	2022/12
2022 年中国网络文明大会“个人信息保护创新实践案例”	2022/09
全国首届数字化审计论坛“个人信息保护合规审计先锋实践案例”	2022/07
英国标准协会（BSI）第三届万物互联•智慧高峰经济论坛“隐私战略贡献奖”	2021/01
隐私保护品牌	
努比亚旗舰机 Z50 发布，隐私保护纳入产品亮点	2022/12
Axon40 Ultra 航天版旗舰发布，隐私保护纳入产品亮点	2022/11
中兴隐私中心上线中兴官网	2022/11
中兴终端产品隐私保护 Slogan“隐私安全，用兴守护”和 Logo 发布	2022/07
合规管理平台	
自研数据智检系统（IDS）内部上线	2024/07
自研数据合规系统（DCS）内部上线	2023/12
自研隐私合规评审系统（PCRS）内部上线	2022/10
自研 App 隐私合规扫描工具内部上线	2022/10

感谢

本白皮书由中兴通讯各领域专家共同完成。**在此，感谢对本文做出重要贡献的人：**

黄智敏 杨宇鑫 徐敏 梅傲婷 方圆 梁楚君 张丹妍 郭漂洋 梁彦珊 蒋璐 李华烘 李遨天 曲绅维 陈立生 李琳 文华龙 雷素君 池逸飞 张沁玮 薛育松 周淑瑶 鲁可兴 岳艳红 王宗平 胡志强 陈正伟 张亮 邓园园 陈威特 任紫倩 张骥 唐丹丹 黄智郁 夏萌 伍婵媛 郭倩 李楠

同时，对出版本白皮书的每位贡献者，感谢你们支持！

中兴通讯隐私保护白皮书

法律遵从 | 信任共建 | 道德履行

ZTE中兴