中兴通讯隐私保护

白皮书

法律遵从 | 信任共建 | 道德履行

2020

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担保。因产品或服务升级、调整或其他原因，本文档内容有可能变更。由于合规体系不断优化完善，我们有权对本文档内容进行增加、修改、删减、废止，并进行不定期更新。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，请通过数据保护合规部Privacy@zte.com.cn电子邮箱与我们联系。

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的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

前言

作为全球领先的综合通信信息解决方案提供商，中兴通讯拥有通信业界完整的端到端产品线和融合解决方案，通过全系列的无线、有线、业务、终端产品和专业通信服务，灵活满足全球不同运营商和政企客户的差异化需求以及快速创新的追求。目前，中兴通讯为全球 160 多个国家和地区的电信运营商和政企客户提供创新技术与产品解决方案，为全世界用户提供语音、数据、多媒体、无线宽带等服务。

中兴通讯高度重视**隐私保护**[1]，遵守《中华人民共和国网络安全法》、欧盟《通用数据保护条例》（GDPR）以及全球其他各国和地区适用的隐私保护法律法规，建立了完整的合规体系，实施了系统的风险控制。对于中兴通讯来说，隐私保护不仅仅是法律遵从，更是信任共建和道德履行的重要基线。

中兴通讯聚焦核心场景，通过隐私保护合规架构高效运行，构建端到端、流程化、闭环化的隐私保护合规体系，全面保护个人隐私、全力保障个人数据安全。

中兴通讯将隐私保护理念融入产品设计和服务提供过程，把隐私保护作为企业核心竞争力的重要内涵，与客户、供应商及合作伙伴一起，携手实现合规前提下的卓越、可持续发展。

中兴通讯还积极参与业界互动和交流，定期组织隐私保护合规论坛、发布研究成果、积极参与隐私保护相关标准规范的制定等，为推动隐私保护合规的发展贡献自己的力量。

[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

(2020)

1 隐私保护合规战略

随着全球隐私保护立法和执法不断深入，通信行业因其广泛覆盖新型基础设施建设，涉及庞大个人用户群体，逐渐成为隐私保护关注重点，隐私保护合规建设已成为行业内的重要议题。为有力推进隐私保护合规工作，中兴通讯确立了“满足合规要求，充分防控风险，促进业务落地，建立合规信任，保证商业可持续发展，共建合规良好生态”的隐私保护合规战略。

1.1 合规愿景

建立适用、有效、领先的隐私保护合规体系。

契合通信行业特点，匹配内部风险偏好和外部监管环境，致力于规则合理、宣贯有力、落地坚决、稽查独立，合规要求嵌入业务流程且运行良好、风险可控。力争在隐私保护专业领域，成为中国企业合规的引领者和标杆，成为全球企业合规的先行者和典范。

遵从适用法规，履行合规义务，消除潜在风险，防控监管处罚和司法诉讼，有效响应、应对和处置风险事件。积极开展外部认证，在产品认可、项目投标、客户审计、合规应询等方面展现合规能力，支撑市场竞争，赢得客户信任。主动遵从数字经济时代的隐私道德，将对客户、用户、员工等相关方的数据保护融入默认价值观，成为道德履行的重要基线。

1.2 合规使命

隐私保护合规管控，市场增信，品牌塑造。

做到风险可视、可控和可承受，促进隐私保护始于法律，合于规则，嵌于业务，信于客户，融于品牌。全面统筹、主动规划、直面挑战、管控风险，探索合规方案和业务实践，以正循环的合规导入获得正反馈的合规落地。

规则方面，聚焦重点业务和核心场景，通过关键岗位指引，将复杂的规则梳理成通俗的语言，以易获取、易学习、易复制的模式，使规则在一线单位切实落地，进而确保规则体系得以运行、持续有效。

支撑方面，从业务单位角度思考，平衡合规落地管理成本和管理效率，避免过度投入重复工作，通过逐层赋能使规则下沉，业务单位能独立判断风险，执行合规要求。

管理方面，用矩阵思维规划、执行、检验风控体系，力求风险管控流程简单，将管控点IT化，减少手动和线下操作，降低重复性管控。

隐私保护守护价值，通过业务风险防控和风险点消减，为市场竞争提供稳固环境，隐私保护创造价值，通过产品默认隐私设计和安全加固，为客户信任创造优势条件。

1.3 合规目标

1.3.1 满足法规要求，充分防控风险

恪守商业道德、遵守业务开展所在地法律法规。在全球隐私保护合规立法和执法日趋严格的背景下，遵守业务开展所在地隐私保护法律法规要求，充分应对客户隐私保护审计，有效响应全球数据监管审查，实现隐私保护风险可防可控，夯实隐私保护合规建设基础。

1.3.2 促进业务落地，建立合规信任

尊重用户隐私、保障隐私相关权利。持续推进合规要求在业务活动中的有效执行，不断探索合规管理与业务实践相结合的工作方法，通过合理的规则、全面的培训、坚决的执行和有效稽查，实现隐私保护合规要求的全面落地。

1.3.3 保证商业持续，共建良好生态

保障商业可持续发展。在安全经营前提下实现管理成本最低和效率最高，以卓越隐私保护合规能力守护客户、合作伙伴、股东、员工及利益相关方的利益，携手共建在整个产业链中的隐私保护合规良好生态。

1.3.4 树立合规标杆，创建合规品牌

树立合规标杆，创建合规品牌。与行业专业群体协同发展，开放合作，深度融入隐私保护合规专业圈，挺进业界第一梯队、输出通用成果和标准范例，使隐私保护合规成为竞争优势，为产品服务持续增信贡献力量。

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，将隐私保护合规与企业发展战略相匹配，把

数据保护合规与出口管制合规、反商业贿赂合规并列为中兴通讯三大重点合规领域。高层重视下，持续加大资金投入，加强与外部律所及咨询机构顾问合作，优化组织机构，补强人力资源，补充专家力量，成为确保隐私保护战略实现的重要支撑。

1.4.2 成熟组织与能力提升

中兴通讯建立了合规管理委员会领导下的穿透式合规管理制度，强化合规专业部门COE（Center of Expertise，专家中心）专业化建设，扩充业务单位专职BU（Business Unit，业务单位）合规团队建设，设置业务部门POC（Point of Contact，联系人）等方式，实现穿透式合规管理，将合规理念和政策传递到一线。隐私保护领域遵循统一合规组织架构，联合各业务领域建立起分层管理、多点控制、协同工作的专业保障团队执行合规治理，通过持续的合规培训和能力内化，实现合规要求落地有指引、合规问题咨询有回应、合规措施执行有效果的目标。

1.4.3 业务融入与良好氛围

中兴通讯形成了业务单位积极配合、全员合规意识自驱和整体合规文化融入的建设局面。在推进隐私保护合规工作过程中，业务单位细致梳理业务中涉及的数据处理活动，配合隐私保护合规部门进行风险评估；积极落实各项隐私保护要求，制定业务领域隐私保护合规手册，融合合规要求优化业务流程，大力促进合规与业务的双循环发展。全体员工尊重和敬畏规则，保持开放心态，执行合规要求。

2 隐私保护合规框架

中兴通讯将隐私保护要求融入到产品设计、服务交付和管理内控活动中，搭建了符合欧盟《通用数据保护条例》(General Data Protection Regulation, GDPR)要求的公司级合规规则体系，实施重点业务专项治理与关键国别示范治理，推动业务与合规的高度结合与创新落地。

中兴通讯隐私保护确立了“遵循适用法规，多维穿透治理”原则，将数据主体、数据控制者、数据处理者的权利义务贯穿到产品设计、管理内控、服务交付的运行执行中，实现数据保护的场景穿透和实质运用，促进合规在企业治理体系中的深度吸纳、轮转和融合。

中兴通讯建立了“专业团队支撑、合规防线管控、多主体内外协同运作”的组织模式。设置专职数据保护官，并在总部、各业务领域及各子公司配置了合规总监/产品安全总监，形成纵向贯穿、协同完备的风险防控运行架构。

中兴通讯建立了“高层重视、治理架构、政策规则、风险评估、流程管控、监督检查、合规培训及记录保存”的合规管理要素架构进行多维穿透，保障数据保护合规工作能够有效运行

落地及持续改进。

中兴通讯建立了“政策、手册、原则性规范、场景化指引”的规则架构，引导各部门结合场景去识别、应对业务活动中的数据保护风险。通过体系化的规则建设，提供全面的合规指引和标准规范，确保各业务单位、岗位员工易于理解并执行数据保护要求。

中兴通讯建立了“个人数据泄露响应、数据主体权利响应、数据保护影响评估”等响应机制，有效应对内外部合规诉求响应和合规风险应对，将合规义务嵌入到流程及系统中，确保合规义务的切实履行。

中兴通讯建立了“课程开发、培训实施、效果验证”的一体化培训闭环机制，多维度促进员工合规意识和能力提升。课程开发端，通过全员课程、关键领域课程、基础宣贯、专题宣贯相搭配；培训实施端，采用通识+业务分层次培训模式，发挥各单位专职合规总监中继作用，实现全域、全员覆盖；效果验证端，建立了以考促学机制，重要培训辅以考试评测，保证培训效果。

2.1 组织架构

中兴通讯建立了系统性的隐私保护合规组织架构，形成了以合规专业部门、业务单位合规团队和合规稽查部为核心的合规风险控制的“三道防线”。

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，听取隐私保护合规重大事项汇报并进行指导。中兴通讯数据保护合规部是进行隐私保护工作的专业部门，负责全球数据保护法律法规、政策标准研究与转化，数据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。

隐私保护各团队发挥优势、各司其职、相互配合，兼顾法律法规风控要求和政策可落地性，形成管理合力。合规专业部门关注法律法规的要求和风险偏好的选择，通过理解外部法律环境，结合实际情况选择风险偏好，制定合规红线和规则。业务单位BU合规团队关注合规规则的可落地性以及管理成本的最优化，推动合规规则落地，并评估合规规则的合理性。合规稽查部门关注规则盲点和风控与管理的平衡问题，考察合规风险是否得到有效治理，验证合规体系的有效性。

2.2 管理要素

中兴通讯围绕合规体系建设八要素，将PDCA（Plan-Do-Check-Act计划-执行-核查-处理）引入到合规业务工作中，采取业务与管理的双循环模式，构成合规管理体系核心要素，即合理的规则、全面的培训、坚决的执行、有效的稽查。探索以风险为导向的合规管理体系，以风险

识别为导向，以合规管理为工具，在自上而下的合规体系建设的基础上，推动自下而上规则的场景化、判例化，推进合规规则与具体业务的深度融合，形成契合业务实际的合规管理体系。

中兴通讯参照BS 10012: 2017 并结合业务实际，初步构建了隐私保护管理体系八要素：

2.2.1 高层重视

中兴通讯高度重视数据保护合规工作，管理层已达成数据保护合规与企业发展战略相匹配的战略共识。在高层领导下，数据保护合规工作明确了基本目标、短期及长期规划，推动数据保护合规工作与业界成熟模型对标，满足全球客户数据保护审计要求及全球监管机构审查标准，防范数据保护合规风险。

2.2.2 治理架构

中兴通讯具备多层级、专业化的数据保护合规协同工作机制，已建立起包含数据保护官、数据保护合规专业部门、业务单位BU合规总监/经理/合规接口人的数据保护专业化团队，进行数据保护合规管理要求制定及推动落实，合规稽查部门负责对数据保护合规工作进行审计监督。

2.2.3 政策规则

中兴通讯建立了“政策、手册、原则性规范、场景化指引”的规则体系，并持续推动规则体系的场景化、判例化，促进合规规则与具体业务的深度融合，引导各部门结合场景去识别、应对业务活动中的数据保护风险。通过体系化的规则建设，提供全面的合规指引和标准规范，确保各业务单位、岗位员工易于理解并执行数据保护合规的要求。

2.2.4 风险评估

中兴通讯提炼数据保护合规风险评估四维度，聚焦关键控制点进行风险评估。四维度包括：①满足数据收集和处理的前提条件；②履行应对数据主体承担的义务；③具备设计隐私的基本要求；④确保数据共享、披露与传输合规。所有涉及个人数据处理的业务场景均需满足数据保护合规风险评估四维度的要求，根据不同的个人数据处理角色、处理过程中可能存在的不同风险制定规范，指导业务单位采取适当的措施进行应对。

2.2.5 流程管控

中兴通讯将数据保护合规要求嵌入到的各项业务流程中，从机制上保障合规管控，将默认隐私保护设计嵌入到产品研发端到端流程中，确保产品满足国际通行数据保护合规要求，将数据泄露响应流程及数据主体权利响应流程搭载在 IT 系统中，为合规管理流程的建立和实施提供支持与保障，实现合规流程自动化、可视化。

2.2.6 监督检查

中兴通讯建立了业务单位自查、合规专业团队检查、合规稽查团队稽查的三层检查改进机制，审查不合规事项并明确合规风险，采取适当的措施预防潜在的不合规事项并建立相应的处

理机制，确保合规要求切实落地，并能够根据业务场景的变化进行修正优化。

中兴通讯员工有义务防止、阻止以及举报所有违规行为。当发现潜在的违反数据保护合规要求的行为时，所有中兴通讯员工都有权利和责任暂停相关的业务活动，并可以通过实名或匿名的方式举报相关信息。中兴通讯建立了包括向上级领导举报、向合规稽查部举报、向外部独立第三方举报、通过邮箱/电话/网站举报，以及热线举报等多维度举报方式，鼓励员工举报违规行为。合规稽查部门发起内审，主动调查违规行为，依照明确的合规稽查管理规定进行处罚。

2.2.7 合规培训

合规培训是公司合规意识提升、合规文化建设重要组成部分。中兴通讯持续进行数据保护合规培训，在各项业务活动中传递明确的价值导向，通过培训来提高和增强员工的数据保护意识和能力，在全员中形成合规创造价值、合规是企业赖以生存根基的共识。

2.2.8 记录保存

中兴通讯建立并保持完善的合规记录，以提供符合要求和数据保护合规体系有效运行的证据。除根据明确的个人数据记录规范要求进行数据处理活动记录外，还包括各项数据保护规范宣贯、实施的执行记录，对数据保护合规相关活动进行系统性记录。

2.3 规则体系

中兴通讯建立了包括政策、手册、原则性规范及场景化指引的四层数据保护合规规则体系。

2.3.1 政策

数据保护合规政策是根据中兴通讯整体经营政策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开展业务所在国家/地区适用的数据保护法律/法规，以及董事会、合规管理委员会对于数据保护合规给予全力支持的决心，是中兴通讯开展数据保护合规工作的纲领性文件。

2.3.2 手册

数据保护合规手册是基于对外部法律法规遵从的要求，结合合规政策确定的总体指导文件，中兴通讯数据保护合规手册分为总册及业务领域分册，为整体层面及具体业务领域进行的各类数据处理活动提供基本指引，是开展各项数据保护合规工作的指导文件。具体包括：

总册：陈述了通用数据保护合规政策和整体要求。

业务领域类分册：在总册的基础上，引入业务场景后进一步细化，是业务领域数据保护合规全景图。

2.3.3 原则性规范

数据保护合规原则性规范是中兴通讯开展数据保护合规工作的具体依据及基础支撑。规范内容以全球范围内主流的数据保护法律法规为基础，对各项活动提出基于合规基本要求，同时保留依据具体业务开展国家/地区特殊法律规定进行调整性适用的解释空间，具有拓展性。包括：

管理体系类，即针对数据保护合规管理体系建设规范文件。如《数据保护合规管理规范》。

客体界定类，即界定数据保护合规管理客体的规范文件。如《个人数据识别规范》。

通用要求类，即明确数据保护合规领域一般性要求的规范文件。如《合法性基础判断规范》、《隐私通知及设置规范》、《个人数据留存及销毁管理规范》以及《个人数据处理记录规范》。

专项治理类，即针对某些特殊情形的数据保护合规规范文件。如《数据保护影响评估规范》、《数据主体权利响应规范》以及《个人数据泄露响应规范》。

相关方管理类，即对数据处理活动中涉及的相关方（客户、合作伙伴、供应商等）进行数据保护合规管理的规范文件。如《客户及合作伙伴数据保护合规管理规范》、《供应商数据保护合规管理规范》。

数据安全类，即在信息安全相关要求基础上补充个人数据安全保障要求的规范文件。如《数据安全规范》。

合规审计类，即对合规实施效果进行评估与审计所依据的规范文件。如《合规稽查管理准则》。

2.3.4 场景化指引

场景化指引是业务单位遵照合规指引开展业务活动的直接依据，是在原则性规范结合业务实际场景而形成的具体指导书，明确单个业务活动中整个数据生命周期的流转和具体的风险及管控点，使得一线员工能够清晰了解合规要求和具体的合规动作，能够在遇到具体的合规问题时有据可依。场景化指引打通合规管控全景，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，亦可根据需求实时变化，实现规则的透明化、可视化，保障规则的及时性和可落地性。

2.4 响应机制

2.4.1 个人数据泄露响应

中兴通讯建立了以多方快速协同为核心的个人数据泄露响应机制， 明确了工作流程，并依托专业化通过“个人数据泄露响应系统”管控，对整个应急响应过程进行跟踪和记录，满足内外部潜在文件调阅和证据呈送需求。不定期组织数据泄露应急演练，强化日常岗位责任和应急响应机制的可验证性，充分防范数据泄露发生，科学实施数据泄露处置。

为确保个人数据泄露各项政策措施的落地执行，建立数据保护稽查机制和违规举报渠道，通过专职合规稽查队伍，将自检审计纳入内控保障体系，促进文化建设、资源投入、流程再造、能力提升的正循环。

2.4.2 数据主体权利响应

中兴通讯建立了以多方快速协同为核心的数据主体权利响应机制，明确了工作流程，搭建了上报申请入口，在数据主体行使权利时能够进行有效响应。具体地，通过IT化的工具支撑，搭建了专业化的内部流程响应系统，使合规专家和数据保护官参与到流程中，满足快速对数据主体做出专业回应的要求，并对响应过程进行跟踪记录，一并满足内外部潜在文件调阅和证据呈送需求。

数据主体可以通过“数据主体权利响应系统”系统直接与数据保护合规部联系，便于数据主体简单快捷地提交权利诉求，确保行权过程中的个人数据安全。中兴通讯立足IT化的数据主体权利响应系统，为数据主体提供优质的交互体验，展示良好的合规遵从，提升社会信任度。

2.4.3 数据保护影响评估

中兴通讯采用数据保护影响评估方法，对新产品、新技术、重大产品服务变更等，通过“数据保护影响评估系统”线上评估工具进行，确保个人数据处理过程满足通行数据保护合规要求。

具体实践中，采用“数据保护影响评估”流程，在研发、销售和运维等主要业务流程中推广风险分析动作，采取风险管控措施。研发阶段，评估产品收集的个人数据，分析在权限、日志、加密、匿名等方面采取多项保护措施保障个人数据的安全；在处理及传输数据之前，评估相关国家法律及可适用的国际规则中的要求符合情况，引导产品、服务按照法律规定和规范要求采取措施，降低风险。

2.5 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，以更好地适应不断变化的内外部环境，并将风险评估作为风险管理的重要一环和关键起点。根据 GDPR 的要求及 ISO/IEC 27701:2019 的规定，数据保护合规风险评估涵盖四个维度的专业性评估要点：

2.5.1 满足数据收集和处理前提条件

作为直接面向个人用户提供产品/服务的数据控制者时，第一维度风险评估内容包括：

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需要获得数据主体同意的，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涉及到数据处理者或共同数据控制者时，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。

作为面向局方客户提供产品/服务的数据处理者时，第一维度风险评估内容包括：

①是否与数据控制者签订适当的协议对相关内容进行明确；

②是否严格按照数据控制者的书面指示进行个人数据处理活动；

③是否会在非经个人数据主体同意时将从数据控制者处获取的相关数据用于营销和广告；

④当控制者的数据处理指示违反相关法律法规规定时，是否会及时通知控制者；

⑤是否会采取适当的措施以协助数据控制者实现合规要求；

⑥是否会对各项数据处理活动进行全面及时的记录。

2.5.2 履行应对数据主体承担的义务

作为直接面向个人用户提供产品/服务的数据控制者时，第二维度风险评估内容包括：

①是否明确应当对数据主体所承担的义务并记录；

②是否向个人数据主体提供隐私通知；

③是否具备相应的机制以实现数据主体所行使的权利；

④是否具备相应的机制以响应数据主体的权利请求；

⑤涉及自动化处理时，是否赋予数据主体相应的权利；

⑥当发生个人数据主体权利请求时，是否及时向共享了个人数据的数据处理者或共同数据控制者进行通知；

⑦是否在规定时间内对数据主体的权利请求进行响应。

作为面向局方客户提供产品/服务的数据处理者时，第二维度风险评估的内容则主要是指是否能积极协助数据控制者（即局方客户）对数据主体的权利请求进行响应。

2.5.3 具备设计和默认隐私保护要求

作为直接面向个人用户提供产品/服务的数据控制者时，第三维度风险评估内容包括：

①是否会仅在目的范围内收集和处理个人数据；

②是否可以保证各项数据的质量和准确性；

③是否明确并记录数据最小化的目标，或是否会采取相关措施以实现数据最小化的要求；

④数据处理活动后是否会及时删除数据或进行去标识化处理；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数据存储期限；

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。

作为面向局方客户提供产品/服务的数据处理者时，第三维度风险评估内容包括：

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、传输或处置个人数据，或向控制者提供相应的证明；

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。

2.5.4 确保数据共享披露与传输合规

作为直接面向个人用户提供产品/服务的数据控制者时，第四维度风险评估内容包括：

①是否能明确数据共享、披露或传输双方的基本信息，特别是双方所在法域；

②是否能明确进行数据共享、披露或传输的合法依据，特别是涉及跨境传输的情形；

③是否会对数据共享、披露与传输进行全面及时的记录。

作为面向局方客户提供产品/服务的数据处理者时，第四维度风险评估的内容包括：

①是否能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是否能明确进行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是否会及时向数据控制者通知数据披露请求；

④是否会提前告知客户个人数据子处理者的任用、变更等相关信息。

中兴通讯将各级合规管控点形成检查清单，通过开展业务单位自检、BU合规抽检、合规稽查评估等不同维度的查漏补缺、效果验证等活动，保证合规治理要求及合规管控点的切实执行。通过循环的业务风险再评估和再发现，不断完善优化合规规则及具体措施，持续强化合规建设。

针对业务领域，持续关注业务发展规划及数据相关法律法规的变化，不断优化数据保护合规规则体系及各项规范内容，加强与业务活动流程之间的联系，使规则更加适用于业务的发展。同时推进相关合规系统的IT化建设，使合规要求真正自动嵌入业务流程。

针对不同国别，持续加强对全球数据合规义务的识别与转化，不断完善合规能力，助力业务发展。根据业务开展所面向的重点国家或地区，针对当地特殊规定对中兴通讯数据保护合规规则体系中各项规范作出适用性解释，此外，将开展欧盟/欧洲经济区当地子公司/代表处等的合规治理，结合实际情况对数据保护合规规则进行本地化适用的优化更新。

2.6 培训提升

中兴通讯不断进行各类隐私保护培训及宣贯活动，内化合规能力，整体提升全员的数据保

护合规意识。采用标准化的“1+N”培训模式，1 个岗位培训和N个场景化培训，同时利用外部微信公众号、视频课程等各种新媒体资源进行差异化培训，确保合规专业团队提升自身理论知识水平及工作能力，业务单位合规团队关注项目进展、提高合规能力，员工树立数据保护合规基本意识，关键岗位人员清楚自身职责并推动落实，为具体场景问题提供操作指南。

3 隐私保护合规共建

中兴通讯始终追求与客户、供应商和合作伙伴一起共同实现商业可持续发展，确保产业链的整体安全合规。隐私保护合规共建作为促进相关方合作的基调之一，以自身及产品的隐私保护合规建设为起点，在确保自身产品及服务合规的同时，与产业链中各类合作伙伴协同合规，共同创建通信行业良好合规氛围，为更广的隐私保护生态圈建设贡献力量。

中兴通讯通过将默认和设计的隐私保护理念嵌入到产品研发端到端流程中，向客户提供符合隐私保护合规的产品，为日益关注隐私保护合规的市场做好准备。集中推动具有法律约束力的协议签署，与各相关方广泛签署数据处理协议、标准协议条款、通知函、授权函等，有效控制个人数据处理的潜在风险。关键管控嵌入商事活动流程，针对重要展会、论坛、产品发布会制定了隐私保护合规指引套件，实现活动前、活动中活动后全流程隐私保护管控。

3.1 合规共建价值

3.1.1 企业责任自驱追求

中兴通讯坚持全面加强和供应链的协作，面对客户或个人用户提供合规产品及服务，面对供应商或合作伙伴充分审查其合规能力，从合作源头控制风险，力争成为隐私保护合规共建的引领者和标杆，展示企业责任与担当。

3.1.2 合规信任客观要求

中兴通讯秉承合规创造价值理念，敬畏规则、开放心态，确立隐私保护合规有利于赢得市场竞争，取得客户信赖，获得社会赞誉。通过产业链中各环节深化隐私保护合规共建，支撑合规品牌具有牢固基础。

3.1.3 产品服务协同诉求

中兴通讯导入产品默认隐私保护设计，推进产品源头的隐私保护实现，确保自身产品及服务的合规。持续引导相关方将设计和默认的隐私保护作为产品研发的基础要素，推动业内实践更新变革，推进设计和默认的隐私保护理论和实践在合规共建中落地和深化。

3.1.4 产业行业多方需求

中兴通讯制定客户及合作伙伴、供应商数据保护合规管理规范，在与客户合作之初及引入供应商时即对其能力进行充分评估，通过合规审查、协议签署等方式保障其数据保护合规能力，宣传数据保护合规价值，从合作源头控制风险，与各方共建数据保护合规生态圈。

3.2 客户合规共建

中兴通讯在一切产品和服务中都崇尚客户至上的原则，严格遵守商业准则及客户要求。 根据中兴通讯的数据保护合规政策，不擅自处理为客户提供的产品和服务中所涉及的个人数据，并且客户可以通过中兴通讯产品的各项隐私保护设计匹配各类合规要求和用户需求。

良好的隐私保护合规环境需要我们和客户的共同努力，为了避免因涉及多方主体而产生合规真空区，需要明确在合作过程中所面临的个人数据和我们各自对数据主体所承担的责任义务，由此形成完整的合规链条和风险全覆盖，实现对个人数据的全方位保护。

当中兴通讯作为数据处理者时，遵循适用于处理者的满足国际标准的控制措施。个人数据处理协议中强调其为客户实现其义务提供协助的基本角色，代表客户处理的个人数据不会出于任何客户书面指示之外的目的进行处理。非经个人数据主体同意，中兴通讯不会将受托处理的个人数据用于市场推广和广告用途。中兴通讯向客户提供适当信息以供客户满足证明其自身合规的要求，并保持必要的记录，以证明遵守其代表客户处理个人数据的义务。如果中兴通讯认为处理的指示违反适用法律或法规，将通知客户。

中兴通讯为客户提供履行其面对数据主体所应承担的义务的协助。指定的记录期限内按照记载的程序删除因个人数据处理而产生的临时文件，以安全的方式及时对相关数据进行返还、传输与处置，并将相应制度提供给客户，确保个人数据传输在具有适当控制措施的数据传输网络中进行传输，以保证数据传输到指定接收方，防止泄露。

中兴通讯告知客户有关的个人数据传输，包括传输到供应商、其他主体、其他国家或国际组织的情况；此外，及时通知客户个人数据共享、传输和披露的基础以及任何相关的意图变更，以便客户可反对此类变更或终止协议；明确并记录可能向其传输个人数据的国家或国际组织，并向客户提供上述国家或国家组织以及使用子处理者时可能涉及的国家清单；记录向第三方披露个人数据的相关信息，包括披露的个人数据类型、接收方以及披露时间；个人数据的披露既包括在正常操作过程中的披露，也包括应对合法调查或外部审计而产生的任何其他披露，除非法律另有规定，否则若基于法定要求进行披露时，及时通知客户，并拒绝任何非法定的披露要求；在进行任何披露或接受任何合同约定的、客户授权的披露请求之前，均先咨询客户；引入子处理者之前，向客户披露所有子处理者，对子处理者的使用严格遵循与客户签订的协议要求，

在获得一般书面授权的前提下，通知客户有关增加或更换子处理者的任何变更意图，从而使客户有机会反对这些变更。

3.3 供应商合规共建

中兴通讯作为全球知名的跨国通信产品提供商，拥有庞大的供应商队伍，其中不乏涉及大量个人数据处理的云平台类供应商，也包含各类服务供应商。推行供应商合规共建是保障中兴通讯数据保护合规的重要手段，对隐私保护合规生态圈的建设具有重要意义。

中兴通讯搭建了基于适用法律法规的隐私保护合规框架，实现了数据保护合规培训、制度、流程在供应链领域的优先覆盖，针对供应商侧通过协议签署、数据跨境转移审批等关键点实施管控，平稳度过了风险混沌期，保持了零执法、零诉讼和零舆情事件。

中兴通讯特别关注在供应商引入环节就嵌入数据保护合规要求，于供应商认证或采购环节嵌入了数据保护合规管控措施，包括数据保护协议或安全协议的签署、合规备案、重点供应商安全审计等，期待与全球供应商和合作伙伴共建一个符合数据保护合规要求，安全、可持续的商业网络。

中兴通讯对供应商数据保护合规整体要求包括：

（1）严格遵守所适用的数据保护法律法规，杜绝任何形式的个人数据违法违规处理；

（2）了解并遵守中兴通讯数据保护合规政策，遵守与中兴通讯签订的合同中的数据保护合规条款及其他相关协议要求；

（3）支持中兴通讯对数据保护合规风险的管控，全力配合中兴通讯履行数据保护合规义务；

（4）积极参与中兴通讯组织的供应商数据保护合规培训与演练，并与中兴通讯建立有效的数据保护合规沟通机制；

（5）积极建立完善、有效的数据保护合规体系，按照约定配合中兴通讯发起的供应商数据保护合规检查或审计；

（6）积极采取技术措施和其他必要措施，确保数据安全，防止数据泄露、毁损、丢失；

（7）主动积极向中兴通讯披露或者举报发现的数据保护违法、违规行为。

为确保涉及个人数据处理的各类供应商具备适当的数据保护能力和数据处理能力，并在与业务相关的活动中合法地处理个人数据，供应商数据保护合规要求落地措施包括：

(1) 中兴通讯在供应商准入认证环节就设置管控措施，审核供应商数据保护合规能力，根据供应商提供的产品或服务起草恰当的协议或条款，其中明确说明了发生个人数据主体行权和发生个人数据泄露时供应商的协助义务。

(2) 根据业务场景的多样性，中兴通讯和其供应商在数据处理活动中的角色也不尽相同，通常情况下，供应商会作为处理者或者子处理者参与到数据处理活动中。中兴通讯作为数据控制者，供应商作为数据处理者的情况下，供应商应当严格按照中兴通讯的指示进行数据处理活动。中兴通讯作为数据处理者，供应商作为子处理者的情况下，客户作为数据控制者。中兴通讯作为数据处理者一方面需要满足客户方的相关合规要求，另一方面需要管理作为子处理者的供应商履行法律法规规定的合规义务及控制者的合规要求。如果与供应商之间存在个人数据共享、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（DPIA），根据评估结果采取相应管控措施。

3.4 合作伙伴合规共建

中兴通讯根据具体的合作业务场景，在各项业务活动中与合作伙伴进行合作时对其数据保护合规能力进行持续评估和协作，确保合作过程中进行的个人数据处理活动合法合规。

中兴通讯与合作伙伴在数据处理协议中明确各自数据保护的角色及其职责，各自配合数据主体行权以及发生数据泄露时需履行的义务。中兴通讯基于与合作伙伴的共同目的处理个人数据时，与合作伙伴构成共同的数据控制者，为确保数据处理场景的透明性，会与合作伙伴协同对数据主体进行恰当的隐私通知设置。中兴通讯与合作伙伴进行的个人数据处理活动是基于各自的目的时，与合作伙伴构成单独的数据控制者，分别对数据主体进行恰当的隐私通知设置。

与合作伙伴之间进行数据共享与转移，首先进行数据保护影响评估，并在必要时开展数据保护合规治理工作并积极推动数据处理协议的签署工作。在将数据共享、转移给合作伙伴的过程中，中兴通讯严格遵守数据保护合规要求以及签署协议中规定的义务，并做好相关记录。在数据保护合规治理方面，积极改善数据管理，降低合规风险，维护与商业合作伙伴之间的良好信任关系。在数据处理透明度方面，探索如何在个人权利保障与商业运营之间达成良性平衡关系，尽可能满足数据主体的权利请求。

3.5 行业领域合规共建

中兴通讯持续进行隐私保护技术和方法的研究，通过自主更新和引入先进隐私保护理念和方法，全面提升产品和服务隐私保护能力，以满足新技术、新应用、新模式下的隐私保护需求。

以透明、开放、信任、合作的理念，与客户、合作伙伴、政府、供应商、标准组织开展更为紧密的合作，推动端到端的隐私保护实践，持续提供安全可信的隐私保护环境。

中兴通讯积极参与各类专业会议，传递数据保护合规理念和实践经验。政府方面，与工信部、商务部、财政部、国家发展和改革委员会、国家互联网信息办公室、中国国际贸易促进委员会、中国国际经济贸易仲裁委员会、中国出入境检验检疫协会、深圳市公平贸易促进署等保持密切沟通，参与法律法规解读、标准规范编写、专业知识授课；行业方面，与中国移动研究院、广东移动、江西移动等保持互动交流，就企业常见数据保护相关合规问题进行探讨，如数据保护合规体系建设及数据跨境，《网络安全审查办法》的解读以及合规探讨等，分享中兴通讯合规实践；机构方面，与英国标准协会 BSI、数据法盟、蓝海法律查明和商事调解中心、上海社会科学院、上海技术产业研究院、上海交通大学、华南理工大学、中央财经大学、中南财经政法大学、华东政法大学等单位的合规专家进行专业交流和研讨，就立法执法的动态、企业视角的数据保护合规、跨境数据流动等合规难点进行充分沟通，互通有无，为数据保护合规专业领域提供专业的注解和探索。

中兴通讯联合数据法盟举办“5.25 数据合规年会”，邀请企业、律所、机构、高校专家就数据保护合规态势及实践进行沟通共享，同时发布年度《GDPR 执法案例全景白皮书（2020）》，为行业合规治理提供风向标。数据保护合规团队荣获中国第一法务协会颁发的“CACC 管理创新优秀法律合规团队奖”、英国标准协会 BSI 颁发的“隐私战略贡献奖”，以开放共享、包容兼并的合规探索态度保持与各行业领域密切交互，共同为建设隐私保护生态圈努力。

4 隐私保护合规实践

4.1 标准研究应用

中兴通讯高度重视标准的研究与应用工作，积极参与各类行业协会和标准组织，跟踪政策标准，参与标准研究制定，获取资质认证，持续进行标准的研究与探索。中兴通讯以数据保护合规战略为指引，聚焦业务发展和生态共建，通过适用性评估和持续改进等手段推进标准应用，完善数据保护合规体系建设，为企业发展保驾护航。

中兴通讯加入全国信息安全标准化技术委员会、中国通信标准化协会、中国电子工业标准化技术协会信息技术服务分会等标准化协会，以及 IAPP 国际隐私专业协会、ISC 个人信息保护委员会、中国移动应用安全委员会等行业协会，积极参与标准编写修订工作。

4.2 聚焦法律前沿

国际方面，中兴通讯密切关注欧盟国家法律法规，欧洲数据保护委员会（EDPB）和各成员

国数据保护机构发布的指引，重点评估其中涉及GDPR适用地域、第 42 和 43 条下的认证及其标准、行为准则及其监督、履行合同所必需的数据处理以及数据跨境的例外情形对业务开展的影响程度。此外中兴通讯关注国际执法案例的和动态，对于被执法的案件进行动态跟踪和分析，提炼了被执法依据和处罚金额，形成年度《GDPR执法案例精选白皮书（2019）》、《GDPR执法案例全景白皮书（2020）》，并基于案例输出场景化红线，清晰判断执法重点，选择风险偏好。

国内方面，中兴通讯立足《中华人民共和国网络安全法》，研究网络运营者在网络运行安全、网络信息安全的若干制度性管理要求。跟踪全国信息安全标准化技术委员会制定并公开的国家标准，结合GB/T 35273《信息安全技术 个人信息安全规范》，吸纳规范个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节的相关行为，将其解读并融入到内部管理规范中，并保持对该立法调研的动态跟踪中。2020 年 10 月，我国《个人信息保护法（草案）》全文正式公布，中兴通讯积极响应国家立法机关号召，就草案规则进行呈报提议，本次提议结合了公司近年来在国际国内多标准合规要求下的不同场景适配实践，从个人信息的处理原则、跨境提供、法律责任等方面为国内个人信息保护立法提供智力支持。

中兴通讯将国内外立法执法态势集结整合，形成内部的法律研究资源库，包括全球数据保护立法概览、全球数据保护监管机构清单、执法案例跟踪、全球个人数据保护态势跟踪等模块，将重点热度的国内外执法案例向面向业务单位、员工进行传递和解读，提升合规意识和能力。

4.3 隐私保护设计

中兴通讯将默认隐私设计纳入产品和服务方案中，基于设计和默认的隐私保护理念，制定隐私保护设计规范，明确产品研发流程和业务活动中的隐私保护设计原则、策略和基本要求。在产品研发流程中，实施全流程的隐私保护设计管控。

需求分析阶段：识别产品可能涉及的个人数据，评估个人数据保护需求，依据确定的个人数据保护需求和保护原则，立足风险对产品与个人数据处理有关的功能进行必要性分析；对于确认保留的功能项，应考虑个人数据保护需求关键点，识别潜在风险并初步阐述保护策略。

产品设计阶段：针对已识别的个人数据保护需求，设计合理的安全架构和技术措施。对产品设计方案进行评审，输出数据保护影响评估，针对分析出的风险，进行需求调整或针对性配置组织和技术措施。应在产品设计方案中纳入个人数据保护内容，保留与隐私保护设计相关的文档，为产品改进、评估、管理、维护等提供文件依据。

产品开发阶段：落实个人数据保护需求和设计。在功能实现过程中充分考虑个人数据的收

集、使用、传输、存储、删除等环节是否符合设计要求。

测试验证阶段：对个人数据保护举措进行核实验证，在产品测试方案中纳入个人数据保护内容，并进行符合性测试。

发布阶段：在发布前进行数据保护影响评估或关键控制点复核，并组织评审。评审通过后，方可进行发布或部署。

运营维护阶段：确保产品运行、使用、维护、管理过程符合个人数据保护管控要求。

4.4 催生良好实践

中兴通讯针对外部数据保护法律法规较新，业内成熟方案及治理案例缺乏的现状，制定了“立足研究加快合规转化，基于探索促进合规理解，通过实践推动合规落地”的策略，通过合规与业务的深度结合，在鲜活的场景中深化意识积累经验，协同解决风险评估和治理实操的挑战。

中兴通讯通过对各业务部门实施的数据保护良好实践案例的收集整理，从组织措施、技术措施、合规管控措施进行分类汇编，形成数据保护良好实践案例集。通过数据保护合规实践成果呈现，促进各业务领域合规方法与措施交流学习，更深入理解数据保护规则和原则。

中兴通讯通过践行数据保护规则，催生大量个人信息保护良好实践，极大丰富和弥补了规则的抽象与疏离，贡献了新的观察视角和落地经验，提升企业数据保护能力和水平建设，为进一步的扩展和深入铸造扎实基础和圆满起点。

4.5 开放成果共享

中兴通讯致力于开放成果共享，体系共建，紧密合作，交换理解和履行义务所需的资源，促进交流合作。通过论坛和沙龙等形式，跟进立法脉搏，分享实践场景和合规经验，互相促进，共同成长，携手打造合规品牌，增强国际竞争力。主动分享各项治理经验和成果，关注最新立法态势，通过自媒体和各类专业机构、高校、企业行业合规论坛和沙龙研讨，与业内专业人士深度交流，以吸纳经验更灵活应对合规难点，适应监管环境，共同建设可信合规环境。

中兴通讯建立了“合规小叨客”公众号，针对隐私保护相关问题开设了“数保前线”栏目，呈现最前沿数据保护合规动态，打造最扁平国别法律研习纽带，直击最鲜活行业合规治理痛点，分享最干货企业数据保护合规实践。发布了生物识别的合规遵从、疫情期间的隐私保护合规问题、欧洲经济区的监管执法监测系列文章，在隐私保护合规文化圈建立了响亮名片。

4.6 核心产品认证

中兴通讯将安全作为产品研发和服务交付活动中的最高优先级，致力于提供可信赖的、端到端的、全生命周期的安全保障。2005 年起，中兴通讯已通过 ISO/IEC 27001 信息安全管理体系认证，每年持续更新，认证范围覆盖中兴通讯所有业务。

2020 年，中兴通讯对标国际权威标准 ISO/IEC 27701:2019 隐私信息管理体系和业界最佳实践，在核心产品线导入并建立隐私保护管理体系 PIMS，结合业务实际进行持续改进。目前，选取 5G 核心产品已完成认证深化，通过 ISO/IEC 27701 认证审核并取得认证证书。持续关注业界权威隐私认证机制，持续完善隐私保护体系，持续打造可持续发展的、透明、开放、可信的隐私保护环境。

5 大事记

- 获得 BSI“隐私战略贡献奖” 2020 年 12 月
- 发布《中兴通讯数据保护合规良好实践（2020）》 2020 年 12 月
- 默认隐私保护设计原则嵌入研发流程 2020 年 12 月
- 默认隐私保护设计原则嵌入终端研发基线 2020 年 10 月
- 搭建中兴通讯数据保护合规管控全景 2020 年 7 月
- 获得 ISO/IEC 27701:2019 隐私信息管理体系国际标准认证 2020 年 5 月
- 举办 5.25 数据合规年会(2020)活动 2020 年 5 月
- 发布《5G 应用场景与隐私保护研究报告》 2020 年 5 月
- 发布《GDPR 执法案例全景白皮书（2020）》 2020 年 5 月
- 发布《中兴通讯隐私保护白皮书（内宣版）》 2020 年 5 月
- 发布《全球疫情防控隐私合规政策指南》 2020 年 5 月
- 发布《中兴通讯数据保护合规良好实践（2019）》 2019 年 12 月
- 荣获“CACC 管理创新优秀法律合规团队奖” 2019 年 11 月
- 数据主体权利响应系统（DSRRS）上线 2019 年 11 月
- 发布《GDPR 执法案例精选白皮书（2019）》 2019 年 10 月
- 建立数据泄露及应急响应模拟演练机制 2019 年 7 月
- 举办“中国数据合规沙龙•深圳站” 2019 年 4 月
- 数据泄露事件管理系统（DBIMS）上线 2019 年 4 月
- 运营商 GDPR 合规管理系统（ZXRDC）嵌入运行 2019 年 3 月

结语

合规助力经营，合规创造价值，中兴通讯始终将合规视为公司战略的基石和经营的前提及底线。在整体合规价值观的指导下，中兴通讯通过开展隐私保护合规建设，加强全球数据保护合规义务识别及转化，进一步完善数据保护政策、制度、指引、流程，与业界成熟模型对标，实现满足全球客户数据保护审计要求、符合全球监管机构审查标准、防范全球系统性数据保护合规风险的根本目的。

中兴通讯建立了完整的合规体系，实施了系统的风险控制。对于中兴通讯来说，数据保护不仅仅是法律遵从，更是信任共建和道德履行的重要基线。合规经营不是一项口号，而是企业的一项社会责任，也是每一个中兴人的职责。中兴通讯所有员工不忘初心，合规经营，一起守护价值，创造价值，发扬拼搏创新、锐意进取精神，保障稳健发展，建立合规名片，共创优势价值，共享美好未来！

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

杨宇鑫 陈飘飘 宋伟强 毛安娜 彭唤华 王志宇 高瑞鑫 张涵