

中兴通讯隐私保护 白皮书

法律遵从 | 信任共建 | 道德履行


2022

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：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通信信息解决方案提供商，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，开展监督，引入工具，嵌入流程等，持续改进隐私保护能力，全面落地数据合规要求。

中兴通讯将隐私保护理念融入产品设计和提供服务过程，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

1 隐私保护政策	1
1.1 合规愿景.....	1
1.2 合规使命.....	1
1.3 合规目标.....	2
1.4 合规保障.....	2
2 隐私保护框架	3
2.1 组织架构.....	3
2.2 规则体系.....	4
2.3 流程机制.....	5
2.4 风险管控.....	5
3 隐私保护共建	7
3.1 内部共建.....	7
3.2 客户共建.....	9
3.3 供应商共建.....	9
3.4 合作伙伴共建.....	9
3.5 行业领域共建.....	10
4 隐私保护实践	10
4.1 法律研究.....	10
4.2 业务实践.....	11
4.3 开放共享.....	18
4.4 核心认证.....	18
5 大事记	19

中兴通讯隐私保护白皮书

(2022)

1 隐私保护政策

随着数字经济的深化演进，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，隐私合规成为产业界的重要议题。作为通信行业跨国企业，中兴通讯确立了合规目标下“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。

1.1 合规愿景

隐私保护合规确保体系科学、规则适用、执行有效。

中兴通讯努力建立隐私保护合规体系并持续改进。体系致力于：既遵从法律规定、满足监管要求，又契合行业特点、符合企业实际，与公司治理体系全面融合；规则致力于：“可查、易查”，“易学、易懂”，宣贯有力、便于遵从，动态优化；执行致力于：合规要求嵌入流程，管控融入场景，易于执行，监督有力。

中兴通讯努力提升隐私保护的效果、效率和效益。效果方面，将复杂要求梳理成通俗语言，提升友好度，促进隐私合规良性运行、持续有效。效率方面，围绕主营业务主流产品，设置关键管控点，开发IT系统，减少人工卡点和线下操作占比，提升效率。效益方面，平衡合规成本和管理投入，理念先进、措施务实，力争中国隐私保护的先行者，全球隐私合规的践行者。

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。

中兴通讯持续推进“合规创造价值”理念并付诸行动。合规工作“始于法律，合于规则，嵌于业务，信于客户，融于品牌”，深入探索内部创新的合规方案，广泛吸纳外部成熟的合规实践，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“正循环”的合规导入获得“正反馈”的合规落地。

中兴通讯持续整合隐私保护的风控、增信和品牌。风控方面，遵从适用法律，履行合规义务，消除潜在风险，降低违规概率，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。

1.3 合规目标

1.3.1 遵从法律要求，防范控制风险

中兴通讯遵守业务开展所在地适用的隐私保护法律法规。持续加强外部隐私保护义务识别及规则转化，完善内部政策、制度、指引、流程，对标业界成熟隐私保护实践案例，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

中兴通讯尊重用户和所有相关方的隐私关切、保障隐私权利。持续推进合规要求在业务活动中的有效执行，探索合规管理与业务实践结合落地方法，通过合理的规则、全面的培训、坚决的执行、有效的稽查，实现内部规则敬畏，外部合规信任。

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，与出口管制、反商业贿赂共同列为公司三大合规领域，确保合规要求到具体业务过程的有效落地。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，形成良性的合规知识、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 业务融合与良好氛围

中兴通讯形成了卓越合规文化下的专业部门合规建设，业务单位合规遵从，全体员工合规

参与的良好氛围。隐私保护专业部门制定隐私保护合规政策、手册、指引，优化管控流程，促进合规与业务的融合发展。业务单位围绕合规要求落实动作、执行措施，充分披露、持续消减、协同处置各类风险；全体员工尊重和敬畏规则，开放意见建议，参与合规建设。

1.4.4 系统改造和工具嵌入

中兴通讯积极采用适用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。通过持续加强IT化建设，引入信息系统、专业工具以及技术方案，与现有隐私保护管理流程和IT环境进行整合，确保全流程数据处理可记录、可查询、可追溯和可核验，逐步实现全流程、一体化、自动化管控。

2 隐私保护框架

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，实施重点业务专项治理与关键国别示范治理，将隐私保护要求融入到产品设计、服务交付和内控管理活动中，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。

中兴通讯探索以风险为导向的隐私保护合规管理体系，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、案例化，推进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。

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、数据保护合规专业部门、业务领域 BU 合规总监/经理/接口人的隐私保护团队，进行合规管理要求制定及推动落实，合规稽查部门负责审计和调查。

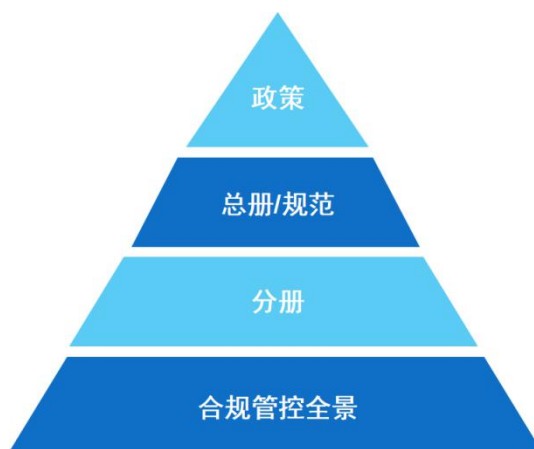
中兴通讯合规管理委员会是负责合规管理体系运作与合规事项决策的最高指导机构，听取数据保护合规重大事项汇报并进行指导。数据保护合规部是进行隐私保护工作的专业部门，负责全球数据保护法律法规、政策标准研究与转化，隐私保护合规策略和合规规则的规划、制定、执行与监督，对具体业务流程的合规风险进行评估和审查。

中兴通讯隐私保护依托合规专业部门、业务领域合规团队、合规稽查部门分工协同机制。

合规专业部门关注法律要求的识别和风险偏好的选择，通过研究外部法律环境，结合内部实际选择风险偏好，制定合规规则；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最优化，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与管理的平衡，建立了多维度举报方式，鼓励员工积极举报违规，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、分册、合规管控全景”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业务所在国家/地区适用的隐私保护法律法规，以及董事会、合规管理委员会对于隐私保护合规给予支持的决心，是中兴通讯开展合规工作的纲领性文件。

2.2.2 总册/规范

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。总册，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，是对总册中有已有管控点的细化，或源于外部法律变化快速遵从而单独制定，识别法律法规规定的关键义务、合规要求制定的专项规范。

2.2.3 分册、合规管控全景

分册，是在总册的基础上，各业务领域结合自身业务特点编制的具体要求。

合规管控全景是基于分册要求引入实际场景进一步细化，形成业务领域隐私保护合规指引集群。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，亦可根据需求更新变化，实现规则的透明、可视，保障规则的及时和可落地。

2.3 流程机制

中兴通讯针对数据泄露响应、数据主体权利响应、数据保护影响评估等关键义务开发IT系统并嵌入业务流程，便于跨部门协同参与，自动保持运行记录，成为合规体系有效的佐证。

2.3.1 个人数据泄露响应

中兴通讯通过完善管理制度、强化教育培训、组织应急演练等确保个人数据处理活动符合法律法规，降低个人数据泄露事件发生概率。当发生切实、疑似或潜在个人数据泄露事件时，依托“个人数据泄露响应系统”，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自动记录，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，使个人数据泄露事件更加科学、妥善地处理。

2.3.2 数据主体权利响应

中兴通讯开发了IT化的、简单便捷且公开的数据主体权利行使申请入口，确保数据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，对数据主体做出专业、客观、妥当回应，自动形成流程跟踪和响应记录，为数据主体提供较好的交互体验，有利于呈现良好行为，提升公众信任。

2.3.3 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、重大产品服务变更等进行线上评估，确保对个人权益有重大影响的个人数据处理活动满足合规要求。研发阶段，评估收集的个人数据类型，分析在权限、日志、加密、匿名等方面采取的隐私保护措施；在处理及传输个人数据前，评估合规要求符合情况，引导产品、服务采取合规措施，降低业务风险。

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 满足数据收集和处理前提的条件

作为直接面向个人用户提供产品/服务的数据控制者时，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。

作为面向客户、合作伙伴提供产品/服务的数据处理者时，主要评估：

- 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。

2.4.2 履行对数据主体应当承担的义务

作为直接面向个人用户提供产品/服务的数据控制者时，主要评估：

- 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。

作为面向客户、合作伙伴提供产品/服务的数据处理者时，主要评估是否能积极协助数据控制者对数据主体的权利请求进行响应。

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/服务的数据控制者时，主要评估：

- 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。

作为面向客户、合作伙伴提供产品/服务的数据处理者时，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。

2.4.4 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/服务的数据控制者时, 主要评估:

- 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。

作为面向客户、合作伙伴提供产品/服务的数据处理者时, 主要评估:

- 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执行。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联系, 使规则与业务发展相匹配。国别方向, 加强重点国家和地区, 针对特殊规定对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, 为更广的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, 与安全部门共建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, 针对个人数据

跨境传输、新技术隐私合规等高风险隐私保护场景，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、工程服务、事件管理和各支撑职能领域，形成了贯穿产品生命周期的产品安全保障体系。《网络安全白皮书——为客户提供安全可信的产品和服务》系统地介绍了中兴通讯如何通过采纳行业标准和最佳实践，将网络安全治理以及隐私保护设计理念贯穿产品全生命周期。

中兴通讯秉承开放透明的原则，在中国、意大利运营网络安全实验室，在比利时和土耳其建有透明中心，使客户、监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。同时设置安全奖励计划，持续欢迎全球安全从业机构和机构反馈产品和服务中存在的安全问题。

产品安全与隐私保护息息相关，海外特别是欧洲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，建立了完整信息安全管理体系、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，以降低个人数据的泄露、滥用风险。项目目标包括：识别包含个人数据的高风险系统，同时将高风险系统的个人数据后台导出纳入信息安全内审；由业务单位将包含个人数据的系统进行识别和上报，确定是否进行后续治理；进行“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，确保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数据，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，另一方面也涉及泄漏后可能对数据主体权益的侵害，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

中兴通讯严格遵守商业准则及客户要求，以实现对个人数据的全面保护为目标，在商务协议中明确各自承担的责任义务，与客户共同维护良好的隐私保护环境。

中兴通讯作为数据处理受托方时，遵循适用的符合国际标准的控制措施。个人数据处理协议中明确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。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，并保留必要的记录，以证明遵守其代表客户处理个人数据的义务。为客户提供履行其面对数据主体所应承担的义务的协助。例如，在指定的记录期限内按照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，并将管理制度提供给客户，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，以保证数据传输到指定接收方，防止数据泄露。

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力作用。

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，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，如数据保护协议或安全协议、合规备案、重点供应商安全审计等，明确约定发生个人数据主体行权和发生个人数据泄露时的协助义务。针对不同业务场景，根据数据处理活动中的角色关系区分“控制者-处理者”和“处理者-子处理者”，履行法律法规规定的合规义务。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，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角色及其职责，各自在数据主体行权以及

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数据时，与合作伙伴构成共同的数据控制者，会协同合作伙伴对数据主体进行恰当的隐私通知设置。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。在将数据共享、转移给合作伙伴的过程中，遵守数据保护合规要求以及协议中规定的义务。

3.5 行业领域共建

中兴通讯以透明、开放、信任、合作理念，通过行业领域交流跟踪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、高等院校等保持互动，就最新立法解读、合规体系建设、数据跨境合规等话题开展沟通，指导实践。2021年3月，中兴通讯举办第二届跨国企业贸易合规论坛，在反贿赂、反洗钱及数据保护分论坛中，与行业专家研讨数据跨境流动的合规治理、公众媒体视角下的数据保护合规等话题，介绍了跨国企业数据保护合规建设要点，分享了中兴通讯数据保护合规建设实践；2021年12月，中兴通讯举办“第二届法律合规学者论坛-数据安全与个人信息保护沙龙”，邀请高校知名教授就中国《数据安全法》《个人信息保护法》最新态势、数据安全与个人信息保护热点问题进行沟通研讨，为企业自身和行业共性合规治理提供参考。

4 隐私保护实践

4.1 法律研究

中兴通讯密切关注全球重点国家和地区的外部规则，研究转化为适用的内部规则。依托欧洲《通用数据保护条例》等全球主流数据和隐私法，中国《网络安全法》、《数据安全法》、《个人信息保护法》及配套文件，结合国际标准组织发布的ISO/IEC 27701《隐私信息管理体系》等国际标准，全国信息安全标准化技术委员会发布的GB/T 35273《信息安全技术 个人信息安全规范》等国家标准，将个人信息在收集、存储、使用、共享、转让、公开披露等环节的要求吸收融入到内部规则中。

中兴通讯建立了隐私保护法律资源空间，包括全球数据保护立法、监管机构清单、欧洲执法案例等栏目，面向业务单位、合规团队开放，便于随时查阅，推动能力内化。将法律研究成果梳理汇总，形成《GDPR执法案例精选白皮书》《GDPR执法案例全景白皮书》，从实际执法

案例中提炼出业务活动场景化红线，便于以风险为导向判断执法重点，远离高危事项。立足年度合规治理项目，将成果沉淀总结形成《5G应用场景与隐私保护前沿报告》《数据跨境合规治理实践白皮书》《隐私保护设计（PbD）研究报告》等专业报告，为自身合规建设提供持续价值和长期指导。

4.2 业务实践

中兴通讯针对隐私保护领域法律法规频繁出台、成熟治理方案相对滞后的专业现状，采取“研究牵引合规转化，探索促进合规理解，实践推动合规落地”的基本策略，鼓励合规要求与业务的灵活结合，在鲜活场景中积累实践经验，解决复杂多变的实操挑战。

中兴通讯将业务部门实施的隐私保护良好实践案例进行收集整理，从组织措施、技术措施、合规管控措施三个方面进行分类汇编，形成内部隐私保护良好实践案例集。通过数据保护合规实践成果呈现，不断促进公司内部各业务领域对合规方法与管控措施的交流与学习，使得数据保护合规措施不断优化与完善。

中兴通讯鼓励业务单位基于自身特点执行数据保护规则，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数据的处理，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数据，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数据的目的是，取得数据主体的同意，并在活动结束后及时删除。

竞标管理业务活动场景中，如处理客户所持有的个人数据，会与客户签署数据处理协议，以获得数据处理的授权。如涉及数据跨境处理，同样会获取数据跨境的客户授权。

因履行合同义务为海外运营商提供技术支持时，如需从客户网络中提取并跨境传输数据，在签约评审阶段识别该需求，对客户进行明示告知，充分披露数据处理的目的是、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，方可执行数据跨境操作。

4.2.2 系统产品

中兴通讯系统产品业务包括无线产品（无线网络、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数据安全，主要关注隐私保护设计、数据主体权利实现、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）嵌入研发设计主流程（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，把个人数据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。

系统产品对已正式发布的产品进行定期评估，例如在HPPD流程中系统方案阶段需要进行DPIA。具体包括：

(1) 风险识别：风险识别的目的是识别潜在的风险，系统产品各部门/项目应基于已识别的个人数据和数据流向，从数据主体权利保障和数据安全两方面，识别并记录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；

(2) 风险分析：使用《研发项目个人数据梳理和数据保护影响评估工具》，从风险发生的可能性和后果两方面进行风险分析；

(3) 风险评价：风险分析阶段确定的风险估值，可确定已识别风险项的风险等级；

(4) 风险处置：确定风险处置策略，制定风险处置方案并组织实施。可选的风险处置策略包括采取控制措施降低风险、调整业务需求规避风险、转移风险和接受风险等多种类型；

(5) 结果审核：根据数据处理现状识别、数据保护合规要求识别、数据保护基本原则确定和数据保护风险评估等各阶段的工作，及时填写《系统产品数据保护影响评估报告模板》，记录每阶段输出的数据保护合规要求、数据处理场景、安全控制措施、风险评估结果、处置方案、处置计划、接受风险和风险备案项、遗留问题清单等，形成数据保护影响评估报告初稿，并提交至产品安全团队审核；

(6) 报告管理：根据系统产品研发隐私保护设计指导书，通过技术评审归档的文档，在技术评审点审核归档。

4.2.3 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。工程服务涉及数据保护合规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数据、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，制定了《中兴通讯数据保护合规手册-工程服务分册》，以风险为导向，制定工程服务业务活动的保护场景化指引，将数据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；工程服务领域通过数据保护培训、宣贯、数据保护一页纸等方式，将相关业务场景和流程的数据保护管控要求传递、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的执行偏差；工程服务领域通过建立适用于工程服务业务特点的数据保护合规关键管控点（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的保护KCP的执行，从而保障业务场景的KCP切实落地。通过对业务活动KCP执行的检查结果分析、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覆盖业务活动主要数据保护风险的前提下，持续提升管控的有效性以及降低规则执行的成本。

技术交付业务活动中，为运营商客户提供比如网络维护、故障处理等技术交付相关的服务时，作为数据处理者不可避免的涉及局方客户网络用户数据的处理，部分网络问题甚至需要国内研发专家提供远端支持。为了满足GDPR关于个人数据跨境的要求，同时结合手册和实际业务活动场景的特点，制定适用于GDPR的场景指引，明确了远程接入业务场景的数据保护管控要求及措施：

(1) 依据GDPR规定与作为数据控制者的客户签署DPA/SCC，并将相关协议的签署状态嵌入技术交付远程接入的业务流程，通过系统IT化实现未签署SCC无法启动远程接入业务的精准管控；

(2) 在业务申请流程中嵌入审批要求，评估每次远程接入必要性；

(3) 采用客户获得认可的网络接入方案、以及搭建专用于数据处理的安全屋，采取保障数据处理安全的组织措施与技术安全措施；

(4) 将数据处理活动全面及时记录的要求融入业务系统申请流程中，让业务人员在完成远程接入业务的申请、执行和流程关闭过程中实现对处理活动的记录；

(5) 定期进行业务活动的保护合规管控动作执行情况的检查和审计，确保相关业务管控要求得到切实落地实施。

4.2.4 终端

中兴通讯终端业务是生产设计终端产品，并进行销售和提供售后服务的端到端系列活动，主要包括产品研发、产品经营、销售、产品供应及客服、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，是终端向用户、

向社会递交的一张可信赖名片。终端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。终端研发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APP隐私合规监管矩阵要求，制定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、BU 合规及COE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；自研隐私合规检测工具——自动化安全漏洞及隐私合规扫描平台 (AppSecScanner)，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。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，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数据保护合规要求。

中国对于APP个人隐私保护的监管日趋严格，终端产品安全团队对APP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“自研隐私合规探测器”。“自研隐私合规探测器”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，有效支撑了中兴终端、数字技术产品部 (DT) 及系统产品等APP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。

4.2.5 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数据的业务活动包含采购、物流管理、逆向等。采购业务涉及个人隐私保护的场景主要有：供应商认证、培训与会议等活动；物流管理业务涉及个人隐私保护的场景主要有：物流运输、成品仓储、海关关务等活动；逆向业务涉及个人隐私保护的场景主要有报废成品的破坏及售卖。

供应链领域采购、物流管理、逆向、返修等业务活动中，会处理客户、供应商提供的业务联系人姓名、电话、邮件地址等信息，以便于货物的接收、交付与维修。在供应商认证场景中，会处理供应商提供的高管、销售、财务等人员的姓名及联系方式，便于认证及后续的商务谈判、招标、付款的顺利进行。我们在以上个人数据处理的场景中，会严格遵守处理个人数据的相关法律法规，有效地保护个人数据。主要管控方式有：

(1) 在透明性告知及个人数据处理合法性基础的要求下，收集供应商提供的个人数据时，会通过适当方式 (隐私声明、邮件等)，向其说明收集和处理个人数据的目的及其他必要内容，

在适用的情况下取得数据主体的同意；

(2) 仅收集与业务相关且必须的最小范围的个人数据；

(3) 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数据时，会对供应商进行个人数据保护履约能力调查、审计及监督，并与其签署适当的数据保护协议（数据保护条款、数据处理协议、数据跨境协议等）；

(4) 保障个人数据主体的权利，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数据时，进行及时、有效的响应；

(5) 对个人数据存储期限进行评估，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数据；并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数据；

(6) 存储、传输供应商提供的个人数据时，IT系统会进行权限管理、安全加密以及记录操作日志；

(7) 对于从客户回收的产品，评估报废品中是否可能包含个人数据，并根据评估结果选择适当的实物处理方式，降低个人数据非法访问的风险。

从客户（运营商）回收的设备，以及维修时替换下来的器件中可能存在客户（运营商）的或最终用户的个人数据，需要防范这些数据的泄露、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擦除或破坏处理。如果需要交由回收商进行实物处理，会通过要求其签署安全协议、提供处理报告等措施减少个人数据泄露风险。

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行政物业管理服务，以及与政府、行业协会组织或机构、高校、科研院所等相关的公共事务。

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数据主体权利；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实现人力资源管理活动的活动。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。人力资源业务的系统（招聘网站、人事在线、时间管理、健康安全事故上报等系统）均实现隐私政策的嵌入，将收集信息的类型、合法性基础、数据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的基线要求。对于线下活动，如涉及员工或员工家属的个人信息收集，通过书面形式发布隐私告知书，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”是公司面向海外员工家属的凝聚力活动，为了让员工家属走进中兴、了解中兴、认识中兴，公司通过此类活动来提升家属对员工的职业认同及工作支持。为了给员工家属提供住行饮食一条龙贴心服务，中兴通讯会收集员工家属的身份信息、饮食习惯等信息，在确保家属体验的前提下遵循最小化收集原则，并在隐私告知书中明确告知公司所收集员工家属信息的类型与目的。使用公司内部的加密文档库存储信息，仅限活动组织方人员有权限查看。活动组织方人员也按照职责进行信息隔离。比如接送机组同事有权限查阅员工家属姓名、电话、航班号，而无法获取身份证号和饮食习惯等与行程无关的信息。为了便捷高效向员工家属提供服务，引入了商旅供应商，并通过服务协议中的数据保护条款来约束供应商的行为以保护员工家属的个人信息不被泄露及滥用。活动结束后，会及时删除电子版的个人数据，打印的纸质信息会直接销毁，严格遵守业务经营所在国法律法规和政策要求确保对员工及家属的个人信息进行合规处理。

4.2.8 财务

中兴通讯财务业务承担公司整体财务管理工作，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、证券事务等一系列活动。财务领域业务活动主要面向公司内部员工和外部合作方，处理的个人数据敏感度较高，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数据进行全方位的保护以维护员工和外部合作方的个人权益和隐私。

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。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，对个人数据的传输和存储进行严格管理，并对系统进行信息安全加固。除费用报销外的其他场景，如个税申报、证券事务信息披露等，也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数据保护合规要求，保护内部员工和外部合作方的个人权益和隐私。

为了满足员工的差旅资金需求，减少员工因商务差旅垫资或借款的压力，公司为员工开通商务卡办理渠道，员工可以基于自愿进行办理。商务卡持卡员工由于公司商务活动所产生的消费可使用该商务卡支付，在业务报销时提供商务卡的消费记录。为了便于员工报销和追溯员工商务消费，公司建立了商务卡消费信息与中兴财务在线系统的银企直连，持卡员工使用银行商务卡进行消费，消费记录会同步到公司财务在线系统中，并通过邮件将消费明细发送到员工的工作邮箱。在员工申请商务卡时，在商务卡办理申请书（包含商务卡领用合约）中嵌入相关隐私条款，对员工进行充分告知并获取同意。实际上除了商务消费外，部分员工还将商务卡用于个人消费并自行还款，记录员工因私消费信息缺乏稳固的处理合法性基础。公司掌握这一情况后，及时采取相应管控措施，将员工持商务卡进行个人消费的记录屏蔽于公司的财务在线系统外，在满足公司商务卡报销管理业务的需求基础上，实现对个人隐私的保护与尊重。

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和收购、实体新设、撤资/股权出售、实体解散、实体转型、对外合作、展会活动等系列活动。战略及投资业务领域涉及处理个人数据的场景集中在展会业务中，举行或参加各类展会、论坛活动，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数据处理活动，展会场景下的数据合规工作是中兴通讯隐私保护的重要一环。

为了保证各类展会场景下个人信息处理活动合法合规，制定了《展会数据保护合规指引》，以展前、展中、展后作为时间节点划分管控措施。其中，展前阶段关注客户邀请、线上活动准备，展中阶段关注会场布置、嘉宾演讲等环节，展后阶段关注客户回访、客户数据删除等环节，在各环节设置隐私保护关键控制点。在展会开展过程中，除业务人员外，业务线合规经理以及数据保护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。

以通信领域内的国际盛会巴塞展为例，中兴通讯在展前、展中、展后全阶段实现巴塞展全

流程的数据合规管控，保护客户的个人数据安全。

(1) 展前阶段：中兴通讯在向客户发送《邀请函》的同时发送《隐私通知书》，明确告知收集个人数据的种类、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。在为客户预定机票/酒店/车辆时，中兴通讯在与供应商签订的合同中嵌入“数据保护条款”，明确供应商应承担的隐私保护责任；中兴通讯在巴塞展轻网站上线隐私政策，告知用户收集的 personal 数据的范围、目的，存储地点、期限等内容，体现了个人数据保护的透明性原则。

(2) 展中阶段：在展会摄像头下方、场地入口、专门拍照区域或其他具有采集肖像、语音等个人数据的功能的设备前，中兴通讯会设置提示标语，提醒用户其肖像、语音可能被采集。

(3) 展后阶段：如在展后进行客户调查问卷回访，中兴通讯严格限制调查问卷收集客户的信息范围，将客户名称、联系方式、电子邮箱等非必要个人信息设置为非必填项；在展会结束后，中兴通讯及时删除展会中收集的客户个人数据。

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，针对隐私保护相关问题开设了“数保前线”栏目，致力于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，分享最实用企业隐私保护合规实践。“数保前线”栏目发布的《数据跨境合规治理实践白皮书》《隐私保护设计 (PbD) 研究报告》《欧洲经济区监管执法监测》《疫情期间的隐私保护合规问题》等系列文章，在隐私保护合规领域建立了名片。

4.4 核心认证

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、管理和技术、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。

中兴通讯持续关注业界权威认证，中国总部及部分子公司已通过 ISO/IEC 27001:2013 信息安全管理体系认证，终端、5G、核心网、数字技术产品线以及人力资源管理已通过 ISO/IEC 27701:2019 隐私信息管理体系认证，5G 产品线已通过全球移动通信系统协会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，一批 5G 产品已通过 NESAS 设备安全评估，5G RAN 解决方案获得系统级解决方案的通用标准 (CC) EAL3+ 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

● 举办第二届法律合规学者论坛-数据安全与个人信息保护热点问题研讨沙龙	2021/12
● 发布《隐私保护设计 (PbD) 研究报告》	2021/12
● 发布《数据跨境合规治理实践白皮书》	2021/12
● 人力资源管理获得 ISO/IEC 27701:2019 隐私信息管理体系国际标准认证	2021/09
● 终端产品获得 ISO/IEC 27701:2019 隐私信息管理体系国际标准认证	2021/09
● iCenter 产品获得 ISO/IEC 27701:2019 隐私信息管理体系国际标准认证	2021/07
● 核心网产品获得 ISO/IEC 27701:2019 隐私信息管理体系国际标准认证	2021/07
● 发布《中兴通讯隐私保护白皮书 (2020) 》	2021/02
● 获得 BSI “隐私战略贡献奖”	2020/12
● 发布《中兴通讯数据保护合规良好实践 (2020) 》	2020/12
● 默认隐私保护设计原则嵌入研发流程	2020/12
● 默认隐私保护设计原则嵌入终端研发基线	2020/10
● 搭建中兴通讯数据保护合规管控全景	2020/07
● 5G 产品获得 ISO/IEC 27701:2019 隐私信息管理体系国际标准认证	2020/05
● 举办 5.25 数据合规年会(2020)	2020/05
● 发布《5G 应用场景与隐私保护研究报告》	2020/05
● 发布《GDPR 执法案例全景白皮书 (2020) 》	2020/05
● 发布《中兴通讯隐私保护白皮书 (内宣版) 》	2020/05
● 发布《全球疫情防控隐私合规政策指南》	2020/05
● 发布《中兴通讯数据保护合规良好实践 (2019) 》	2019/12
● 荣获 “CACC 管理创新优秀法律合规团队奖”	2019/11
● 数据主体权利响应系统 (DSRRS) 上线	2019/11
● 发布《GDPR 执法案例精选白皮书 (2019) 》	2019/10
● 建立数据泄露及应急响应模拟演练机制	2019/07
● 举办 “中国数据合规沙龙·深圳站”	2019/04
● 数据泄露事件管理系统 (DBIMS) 上线	2019/04
● 运营商 GDPR 合规管理系统 (ZXRDC) 嵌入运行	2019/03

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：

高瑞鑫 杨宇鑫 宋伟强 徐敏 黄浩 王志宇 王晨 周宇心 梅傲婷 丁沛 魏安迪 方圆 黄惠娥 蒋璐 杨桂荣 李华烘 池逸飞 赵智海 惠兆帅 陈立生 李琳 龙浩 马华 薛育松 王欢

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