

江苏宁沪高速公路股份有限公司

隐私与数据保护政策

第一章 总则

第一条 为保护自然人个人信息权益，规范公司个人信息处理活动，依据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等法律法规及江苏交通控股有限公司相关制度要求，结合江苏宁沪高速公路股份有限公司（以下简称“公司”）业务实际，制定本政策。

第二条 本政策适用于公司本部、全资及控股子公司（以下统称“各单位”）在开展业务、管理、服务过程中，处理消费者、客户、供应商、合作伙伴、员工及其他相关主体个人信息的全部活动。供应商、承包商等受托处理方通过合同约定适用本政策要求。本政策经批准后可在公司官网公开。

第三条 本政策所称个人信息，是指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；敏感个人信息是指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。

第二章 基本原则

第四条 合法、正当、透明原则。处理个人信息应当严格遵守法律法规，遵循正当业务目的，以清晰、易懂的方式向个人信息主体告知处理规则，充分保障知情权。

第五条 目的限制原则。个人信息处理应当基于具体、明确、合法的业务目的，不得超出约定目的范围对个人信息进行二次处理，不向任何第三方出售客户个人信息，确有业务需要的，须重新告知并取得客户单独同意。

第六条 数据最小化原则。个人信息处理范围与处理程度应当与实现处理目的直接相关、确有必要，不得收集与业务目的无关的个人信息。

第七条 准确性原则。各单位应当采取合理措施保障个人信息的准确性、完整性，及时更新个人信息，发现信息有误的及时更正。

第八条 存储期限最小化原则。个人信息存储期限不得超过实现处理目的所必要的期限，期限届满后及时删除或匿名化处理；法律法规另有规定留存期限的，从其规定。

第九条 完整性与保密性原则。采取与个人信息风险等级相匹配的技术与管理措施，保障个人信息安全，防止信息泄露、篡改、丢失或被非法访问。

第十条 可归责原则。各单位对本领域个人信息处理活动负责，确保个人信息处理活动符合法律法规与本政策要求，并承担相应法律与管理责任。

第三章 个人信息处理全流程管理

第十一条 告知与同意管理

（一）处理个人信息前，应当以显著方式、清晰易懂的语言告知个人信息主体所处理信息的类型、处理目的、处理方式、存储期限以及个人信息主体享有的法定权利；

（二）处理个人信息应当取得个人信息主体明确、自愿的同意，同意应当针对特定处理场景作出；法律法规另有规定无需取得同意的，从其规定；

（三）个人信息主体有权撤回同意，各单位应当提供便捷的撤回渠道，撤回同意不影响撤回前已开展的个人信息处理活动的效力。

第十二条 个人信息采集管理

（一）个人信息采集遵循“一数一源、一源多用”原则，能够通过内部数据共享获取的信息，不得重复采集；

（二）采集个人信息应当具有明确合理的业务目的，采用合法、正当的方式，不得通过误导、欺诈、胁迫等方式采集；

（三）涉及个人信息采集的新建信息系统，上线前须将个人信息采集情况表报运营管理中心备案；

（四）不得强制个人信息主体提供与服务场景无关的个人信息，不得因个人拒绝提供非必要信息而拒绝提供服务。

第十三条 个人信息使用与留存

（一）个人信息的使用应当与告知的目的、授权范围保持一致，不得擅自扩大使用范围或变更使用目的；

（二）基于统计分析、业务优化等目的使用个人信息的，应当优先使用匿名化或去标识化处理后的数据；

（三）按照法定或约定的期限留存个人信息，期限届满后及时删除或进行不可逆匿名化处理。

第十四条 个人信息安全防护

（一）对个人信息实施分级分类管理，针对敏感个人信息采取强化加密、访问控制、脱敏等技术防护措施；

（二）承载个人信息的信息系统采取身份认证、最小权限管控、操作日志审计等安全机制，确保个人信息处理操作全程可追溯；

（三）定期开展个人信息安全风险评估，排查安全隐患，及时采取补救措施；

（四）存储个人信息的系统与设备按照公司数据备份管理要求落实备份策略，保障数据可恢复。

第十五条 访问权限管控

个人信息访问实行最小必要授权原则，根据岗位与业务需求严格配置访问权限，仅授权相关岗位人员访问职责范围内的个人信息；权限变更履行内部审批流程，定期开展权限合规审计。

第十六条 向第三方提供个人信息管理

（一）向第三方提供个人信息的，应当事前评估对方的数据保护能力，通过合同明确双方权利义务与数据保护要求，确保对方提供不低于本政策要求的保护水平；

（二）向第三方提供个人信息须履行公司内部审批流程，涉及个人信息出境的，严格遵守国家相关法律法规要求；

（三）供应商、合作伙伴仅可基于合同约定目的处理个人信息，不得用于其他目的，不得擅自向第三方转提供。

第十七条 个人信息主体权利保障

各单位应当建立个人信息主体权利响应机制，依法受理并处理个人信息主体提出的访问、更正、删除、转移个人信息等请求，在法定期限内予以答复并提供相应便利。

第四章 数据泄露事件处置

第十八条 各单位应当制定个人信息泄露事件专项应急预案，明确事件分级、处置流程、责任分工与通知机制。

第十九条 发生个人信息泄露、篡改、丢失等安全事件时，责任单位应当立即采取补救措施，控制事态影响，第一时间向运营管理中心与企管法务部报告；按照法律法规要求，及时告知受影响的个人信息主体，并向有关监管部门报告。

第二十条 第二十条 事件处置完成后，责任单位应当开展全面复盘，分析事件原因、排查管理漏洞、完善防控措施，对相关责任人依规追责，第三方违约的追究合同责任、纳入不良记录并终止合作。

第五章 职责与分工

第二十一条 运营管理中心是公司隐私与数据保护工作的统筹管理部门，主要职责包括：

- （一）牵头制定公司隐私与数据保护管理制度、标准与规范；
- （二）推动个人信息保护要求融入业务流程与信息系统建设，监督检查各单位制度落实情况；
- （三）统筹个人信息安全风险评估、数据安全事件处置与合规审计工作；
- （四）负责个人信息采集、内部共享、对外提供的备案与审批管理。
- （五）将隐私与数据保护纳入公司全面风险与合规管理体系，定期向经营层及董事会报告；董事会承担最高监督责任。

第二十二条 企管法务部是公司隐私与数据保护工作的法律合规支持部门，主要职责包括：

- （一）负责合同中个人信息保护相关条款的合规审核；
- （二）为个人信息处理活动提供法律支持，参与重大数据安全事件的处置与风险评估；
- （三）对接外部监管机构的合规检查与调查。

第二十三条 人力资源部主要职责包括：

- （一）负责员工个人信息的全生命周期保护，确保员工个人信息处理符合法律法规与本政策要求；

（二）组织开展全员隐私与数据保护意识培训，提升员工合规意识与操作能力。

第二十四条 各业务部门及所属单位是本业务领域、本单位个人信息保护的责任主体，主要职责包括：

（一）落实本领域个人信息保护的各项要求，将保护要求嵌入业务全流程；

（二）配合开展个人信息安全检查、风险评估与事件处置；

（三）面向本部门员工开展日常隐私保护宣贯。

第六章 附则

第二十五条 本政策自发布之日起生效；公司至少每三年或者在相关法律法规、监管要求发生重大变化时对本政策进行评估并适时修订。本政策通过公司官方网站公开。