# 东莞市公共数据安全管理规定

（征求意见稿）

# 第一章 总则

第一条（目的依据） 为贯彻落实党中央、国务院有关加强公共数据安全管理的要求，规范公共数据处理活动，保障公共数据安全，促进数据资源有序开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《广东省公共数据安全管理规定》《东莞市公共数据管理办法》等法律法规规章及有关文件规定，结合本市实际，制定本规定。

第二条（适用范围） 本市行政区域内行政机关以及具有公共事务管理和公共服务职能的组织（以下统称“公共管理和服务机构”）开展公共数据处理活动及其安全监管，适用本规定。

公共数据，是指公共管理和服务机构依法履行职责、提供公共服务过程中制作或者获取的，以电子或者非电子形式对信息的记录。

公共数据安全，是指通过采取必要措施，确保公共数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

涉及国家秘密、商业秘密、个人信息的，按照相关法律、法规、规章的规定执行。

第三条（基本原则） 公共数据安全管理应当坚持安全与发展并重，遵循统筹规划、权责明确、综合防范的原则，保障公共数据依法开放、共享和开发利用。

第四条（人民政府职责） 市人民政府负责组织领导本行政区域内公共数据安全管理工作，协调解决与公共数据安全管理相关的重大问题。

第五条（主管部门职责） 政务服务数据管理部门作为公共数据主管部门，负责统筹本行政区域内公共数据安全管理工作，健全公共数据安全工作机制，建立公共数据处理平台登记、分类分级、风险管理等机制，指导监督公共管理和服务机构落实相关工作要求，承担政务服务领域公共数据安全监管职责。

网信部门负责统筹协调网络数据安全和相关监督管理工作。

公安、国家安全机关负责数据安全保护监督检查和违法行为查处等监督管理工作。

保密行政管理部门负责指导和监督公共管理和服务机构开展保密宣传教育、保密检查、保密技术防护和泄密案件查处等保密工作。

密码管理部门负责密码保障体系规划和管理、密码失泄密事件和违法行为查处等密码监督管理工作。

教育、工业和信息化、自然资源、交通、卫生健康、金融等主管部门承担本行业、本领域公共数据安全监管职责。

第六条（公共管理和服务机构职责） 公共管理和服务机构是本机构公共数据安全管理的责任主体，负责下列工作：

(一)明确公共数据安全管理的目标、制度、责任人和具体负责部门；

(二) 编制本机构的公共数据资源目录；

(三) 保障本机构公共数据安全；

(四) 法律、法规、规章规定的其他公共数据安全管理职责。

第七条（镇街（园区）职责） 镇人民政府、街道办事处、管委会统称为镇街（园区），应当明确本单位的公共数据管理机构，以行政区划或者工作区域作为一级公共管理和服务机构，参照第六条履行职责。

# 第二章 数据安全机制

第八条（数据平台登记制度） 公共数据主管部门应当建立公共数据处理系统登记制度。公共管理和服务机构应当对本机构的公共数据资产进行梳理，形成公共数据资产清单，并将公共数据处理系统涉及管理机构、数据资源、数据安全负责人、数据安全保障措施、数据安全评估结果、数据安全审计结论、网络安全等级保护、密码应用情况等基本信息报送公共数据主管部门登记。

公共管理和服务机构应当定期对本机构的数据资产清单进行更新，因承载公共数据处理活动的系统关闭或发生变更，可能影响公共数据安全保护的，公共管理和服务机构应当自变化之日起15个工作日内向公共数据主管部门申请撤销或变更登记。

第九条（数据分类分级规则） 公共数据主管部门应当根据国家、省公共数据分类分级相关规定，完善公共数据分类分级管理制度。

行业主管部门应当根据上级主管部门和市公共数据主管部门对公共数据分类分级的相关规定，开展本行业公共数据分类分级工作，对本行业公共数据实施分类分级管理。

第十条（数据分级安全防护） 公共管理和服务机构应当落实国家网络安全等级保护制度、商用密码应用要求，并根据分类分级管理要求，采取数据脱敏、加密保护、安全认证、安全审计等安全保护措施，保障公共数据安全；重点保护重要数据，对国家核心数据在重要数据保护基础上实施更加严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中最高级别要求实施保护。

第十一条（纠错机制） 公共管理和服务机构应当保证采集公共数据的完整性、准确性、一致性和时效性。数据使用机构或个人发现公共数据存在问题时，要及时向公共管理和服务机构反映，公共管理和服务机构须在收到问题反映后的15个工作日内予以核实，并及时更正、补充。

第十二条（删除机制） 有下列情形之一的，数据使用机构应当主动删除公共数据：

（一）超范围收集公共数据；

（二）公共数据的存储、加工使用环境不满足安全要求；

（三）超范围使用公共数据；

（四）未按规定流程申请、使用公共数据；

（五）公共数据处理目的已实现、无法实现或者不再必要；

（六）数据使用机构停止履行相关职能或者提供服务；

（七）公共数据保存期限已到期；

（八）数据使用机构违反法律、法规、规章及相关规定处理公共数据；

（九）法律、法规、规章规定的其他情形。

数据使用机构未删除的，提供数据的公共管理和服务机构有权要求其删除；对从技术上难以删除的公共数据，公共管理和服务机构应当督促数据使用机构停止除安全保护措施之外的处理。

# 第三章 数据处理活动安全管理

第十三条（数据收集安全） 收集公共数据，应当明确收集的目的、范围、用途、渠道等，采取访问控制、分类分级标识等必要的安全管控措施，并基于安全可控的环境、设施、人员等条件开展操作。

第十四条（数据存储安全） 存储公共数据，应当根据需要推进数据存储场所物理安全建设，采取脱敏、加密、备份等措施保障存储安全。针对重要数据和国家核心数据，应当建立数据容灾备份及恢复机制，销毁时应采用不可逆方式。

第十五条（数据使用加工安全） 加工使用公共数据，应当采取访问控制、数据防泄漏、操作审计等管控措施确保过程安全、合规、可控、可溯源。数据生产环境与测试环境应隔离，测试数据须经脱敏后使用，并定期清理。

加工使用重要数据或国家核心数据，还应当实施严格的访问控制，建立数据可用不可见、日志留存审计、风险监测评估、实时监控、应急处置、数据溯源等相关技术和管理机制。

利用数据进行自动化决策，应当保证决策的透明度和结果公平合理。

加工使用公共数据不得超出合理范围，不得侵犯公共利益或者他人合法权益。

第十六条（数据传输安全） 传输公共数据，应当根据传输的数据类型、级别和应用场景，制定安全技术规则，并采取身份认证、校验技术密码技术、安全传输通道等保护措施。公共管理和服务机构原则上通过数据资源“一网共享”平台传输公共数据，保障公共数据传输过程可信、可控。

第十七条（数据提供安全） 公共管理和服务机构依法向数据资源“一网共享”平台和公民、法人及其他组织提供公共数据，数据资源“一网共享”平台向数据使用机构提供公共数据时，应当明确提供的内容、条件、程序、渠道、时效等。

数据使用机构和公民、法人及其他组织申请使用公共数据应当明确告知申请受理方数据的使用范围、方式、时限、目的作用以及相应安全保护措施、违约责任等，并与申请受理方签订安全协议；申请受理方有权核实申请方的数据安全保护能力。

# 第四章 数据安全管理措施

第十八条（数据处理环境安全） 公共管理和服务机构应当保障公共数据处理环境安全，处理公共数据的系统应用部署在政务云（行业云）上，不得在公有云等不可信的云系统部署，处理公共数据应当依托政务云（行业云）、已备案的可信交互终端开展。

第十九条（数据处理终端安全） 公共管理和服务机构应当加强数据处理终端安全管理，采取集中管控、用户识别、访问控制、安全审计、病毒防御、补丁修复等技术防护措施对公共数据处理终端进行安全防护。

第二十条（委托安全） 公共管理和服务机构应当加强公共数据供应链安全管理，委托第三方机构建设、维护信息系统或者开展数据处理活动，应当核实第三方机构的数据安全保护能力、资质，确保符合国家、行业主管部门的相关要求，相关安全责任不随委托关系转移。

公共管理和服务机构应当建立公共数据外包或者委托服务安全常态化监督管理机制，确定数据处理操作权限，加强对云服务、终端的常态化安全管理，监督并定期检查第三方机构依照法律、法规、规章的规定和合同约定履行数据安全保护义务情况确保第三方机构不擅自留存、使用、泄露、销毁或者向他人提供公共数据。

第二十一条（人员账号权限管理） 公共管理和服务机构应当加强对数据处理活动相关人员和账号权限管理。明确在人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的管理规定并严格落实。配置账号权限时，应当根据人员岗位职责和业务需求，按照最小授权原则配置。当人员岗位职责或业务需求发生变更时，公共管理和服务机构应该及时调整相关账号权限。

委托开展公共数据处理活动的，应当加强对第三方机构的监督管理，要求第三方机构与相关人员签订保密协议，对关键岗位人员进行安全背景审查，严格实施权限管理，定期进行人员活动审查。

第二十二条（安全培训） 公共管理和服务机构应当加强管理人员和操作人员的安全培训，建立公共数据安全培训制度，定期开展公共数据安全专项培训。培训内容应具有针对性，应当实现分阶段的对不同岗位的人员进行必要的数据安全管理、数据安全意识和数据安全技能等方面的培训。

第二十三条（个人信息安全） 公共管理和服务机构应当加强对个人信息的保护，梳理本机构的个人信息清单，明确已收集个人信息的数据量、涉及人数等信息。

当个人信息数据量超过100万人或者个人敏感信息超过10万人时，应当明确个人信息保护负责人和个人信息保护工作部门，负责全面统筹实施机构内部的个人信息安全工作。

# 第五章 数据安全支撑保障

第二十四条（财政预算保障） 公共管理和服务机构应当建立公共数据安全经费保障制度,将公共数据安全经费纳入本机构年度财务预算。

第二十五条（风险管理机制） 公共数据主管部门根据有关工作要求，指导监督公共管理和服务机构开展公共数据安全风险评估、报告、信息共享、监测工作，加强对公共数据安全风险信息的获取、分析、研判、预警。

第二十六条（风险监测及评估） 公共管理和服务机构应当加强风险监测，全面排查安全隐患，及时整改数据安全评估发现问题，建立常态化风险防范机制。

第二十七条（应急处置） 公共数据主管部门应当协同网信、公安、国家安全、通信管理、保密、密码管理等有关部门和各行业主管部门建立应急预警、响应、支援处理和灾难恢复机制，并加强与公共管理和服务机构间的应急联合演练工作，提升突发事件应急处置能力。

公共管理和服务机构应当制定本单位公共数据安全事件应急预案，定期开展应急演练。发生公共数据安全事件时，公共管理和服务机构须按照应急预案立即开展应急处置，处置完成后及时形成总结报告，报送相关行业、领域主管部门；涉及重要数据和国家核心数据的数据安全事件，还应当及时向公共数据主管部门和相关主管部门报告应急处置进展情况。

第二十八条（安全审计） 公共管理和服务机构在公共数据处理过程中应当记录数据处理、权限管理、配置管理等日志，并对异常操作行为进行告警，保障重要操作行为可溯源。日志应当依照法定形式和期限存留，并定期进行安全审计，形成审计报告。

公共管理和服务机构配合相关主管部门组织的数据安全审计活动，其中涉及委托他人建设、维护信息系统或者开展数据处理活动的，应当加强对第三方机构的安全审计。

# 第六章 监督管理

第二十九条（通报与监督检查） 公共数据主管部门应当协同网信部门、公安机关、国家安全机关、通信管理部门、保密行政管理部门、密码管理部门和各行业主管部门建立健全数据安全监督机制，开展公共数据安全检查，向相关主管部门通报数据安全监测预警、数据安全事件、数据安全漏洞等信息。

第三十条（投诉举报） 自然人、法人和非法人组织有权对违反本规定的行为向相关主管部门投诉、举报。

收到投诉、举报的部门应当及时依法处理，并对投诉、举报人的个人信息予以保密，保护投诉、举报人的合法权益。

# 第七章 附则

第三十一条（实施时间） 本规定自印发之日起实施。本规定由东莞市政务服务数据管理局负责解释。