宁波市公共数据安全管理暂行规定

(2020年9月25日宁波市人民政府令第254号公布 自2020年12月1日起施行)

第一条 为了保障公共数据安全，促进和规范公共数据使用，根据《中华人民共和国网络安全法》《浙江省公共数据和电子政务管理办法》《浙江省公共数据开放与安全管理暂行办法》等规定，结合本市实际，制定本规定。

第二条 本市行政区域内公共数据的安全管理活动，适用本规定。法律、法规和浙江省人民政府规章另有规定的，从其规定。

本规定所称的公共数据，是指行政机关以及履行公共管理和服务职能的事业单位（以下统称公共管理和服务机构）在依法履行职责过程中获得的各类数据资源。

第三条 公共数据安全管理应当坚持政府主导、综合防范、保护隐私、兼顾发展的原则。

公共数据安全管理应当贯穿于公共数据的采集、归集、清洗、共享、开放、使用、传输和销毁等 生命周期全过程。

第四条 市大数据发展管理部门是本市公共数据安全管理工作的主管部门，负责本市公共数据安全的组织协调、统筹规划和监督管理工作。区县（市）人民政府确定的大数据发展管理部门是本行政区域内公共数据安全管理工作的主管部门，负责公共数据安全的相关监督管理工作。

市、区县（市）网信、公安、通信、保密、密码管理等部门按照各自职责做好公共数据安全的监督管理工作。

第五条 公共管理和服务机构对职责范围内的公共数据安全管理承担主体责任，履行下列职责：

（一）明确本机构安全管理责任组织和人员，负责公共数据安全管理工作；

（二）编制本机构公共数据目录，明确数据共享和开放属性，落实分类分级管理制度；

（三）制定本机构公共数据安全管理制度和操作规程，落实网络安全等级保护制度；

（四）采取防范计算机病毒和危害网络安全行为、日志记录和监测、数据备份和加密等技术措施，定期开展公共数据安全风险评估；

（五）制定公共数据安全应急处置预案，定期组织应急演练；

（六）发生数据安全事件时，立即采取处置措施，并及时向公安机关等部门报告；

（七）对本机构公共数据服务外包活动开展安全审查；

（八）定期开展公共数据安全教育和技术培训；

（九）其他公共数据安全管理工作。

第六条 公共管理和服务机构应当遵循合法、必要、正当的原则采集各类数据；无法律、法规依据，不得采集公民、法人和其他组织的相关数据；采集公共数据应当限定在必要范围内，不得超出公共管理和服务需要采集数据，可以通过共享方式获得的数据不得重复采集。

公共管理和服务机构应当对数据采集的环境、设施、网络、系统等采取必要的安全防护措施，不得利用私人设备采集公共数据。

第七条 除法律、法规另有规定外，公共管理和服务机构采集公共数据时涉及个人信息的，应当告知其采集的目的、方式和范围。

除法律、法规另有规定外，公共管理和服务机构在公共场所设置数据采集设施、设备采集信息的，应当设置明显标识。

个人可以向公共管理和服务机构查阅或者复制涉及本人信息的数据，发现存在错误的，有权提出异议并要求公共管理和服务机构及时采取更正等必要措施。

第八条 公共管理和服务机构在公共数据处理过程中应当遵守下列规定：

（一）未经数据提供单位或者被采集人同意，不得改变原始数据值；

（二）在公共数据汇聚、挖掘等处理过程中获得的数据或者得出的结论，可能涉密、涉敏或者危害国家安全、损害国家利益、公共利益的，应当进行安全风险评估。

公共管理和服务机构不得对外使用、传播前款第二项获得的数据或者得出的结论。

第九条 公共管理和服务机构应当按照公共数据的共享属性将其分为无条件共享类、受限共享类、非共享类，并实行分级管理。其中，对非共享类公共数据实行负面清单管理制度，具体由市大数据发展管理部门会同有关部门另行制定。

第十条 公共管理和服务机构应当按照公共数据的开放属性将其分为无条件开放类、受限开放类和禁止开放类，并实行分级管理。

公共管理和服务机构拟将公共数据对外开放的，应当按照规定进行安全风险评估。

公民、法人和其他组织认为开放的公共数据侵犯其商业秘密、个人隐私等合法权益的，有权要求提供公共数据开放服务的公共管理和服务机构按照规定中止、撤回开放的数据。

第十一条 公共管理和服务机构通过共享获得的公共数据，除用于本机构履行职责外，不得用于其他用途。

公共管理和服务机构应当采取必要的电子签名、权限控制、访问控制、日志审计等技术管 控措施确保公共数据在使用中安全可控、可溯源。

鼓励高等院校、科研机构和市场主体开展数据安全与隐私保护等技术研究，提高公共数据使用安全管理水平。

第十二条 传输公共数据应当合理选择传输渠道，采取必要的安全措施防止数据被窃取、泄露或者篡改。

第十三条 公共管理和服务机构应当根据公共数据类型、规模、用途、安全等级、重要程度等因素选择相应安全性能和防护级别的网络、系统、介质、设施设备。其中，涉及个人信息等事项的重要数据应当采取加密存储、身份鉴别和访问控制等措施，保障存储系统和数据安全。

第十四条 行政机关应当依托省、市政务网络、政务云、大数据中心和重大基础性数据资源、应用支撑平台等公共技术平台开展公共数据活动。

公共技术平台的管理维护单位应当根据相关技术标准、规范的要求，建立安全管理制度，加强安全风险评测，保障公共数据安全。

第十五条 公共管理和服务机构对于不需要继续使用、保存的公共数据，或者损害国家利益、公共利益以及公民、法人和其他组织合法权益的公共数据，应当将其从应用系统或者平台中销毁；其中涉及存储介质销毁的，应当交由保密部门指定的机构处置。

公民、法人和其他组织发现公共管理和服务机构因未履行数据销毁职责而损害其合法权益的，可以要求公共管理和服务机构删除相关数据，公共管理和服务机构应当在收到申请后3个工作日内予以答复或者处理。

第十六条 公共管理和服务机构按照应对突发事件有关法律、法规规定，可以要求相关单位提供具有公共属性的数据，并向个人采集应对突发事件相关的数据。

突发事件应对结束后，公共管理和服务机构应当对从相关单位和个人获得的公共数据进行分类评估，将其中涉及国家秘密、商业秘密和个人隐私的公共数据进行封存或者销毁等安全处理，并关停相关数据应用。

第十七条 任何单位和个人不得泄露、篡改、毁损、出售或者非法向他人提供涉及个人信息的公共数据。

第十八条 公共管理和服务机构依法通过服务外包方式开展数据活动的，应当对服务提供方进行审查，与其签订安全保护及保密协议。公共数据服务外包协议示范文本由市大数据发展管理部门会同有关部门制定。

服务提供方应当按照服务外包协议的要求开展相关数据活动，不得违反规定将公共数据扩散或者传播；服务结束后，应当立即清除公共管理和服务机构提供的账号、密码及数据。

第十九条 市、区县（市）大数据发展管理部门应当会同网信、公安等部门建立健全数据安全监督检查工作机制，明确监督检查的内容、目标、方式和标准，对监督检查中发现的安全隐患和问题，及时提出整改意见并予以督促落实。

市、区县（市）网信部门、公安机关、大数据发展管理部门应当定期通报监督检查过程中发现的安全隐患及安全事件查处等情况，提高公共数据安全的协同防护能力和预警能力。

第二十条 公共管理和服务机构及其工作人员未按照规定履行公共数据安全监督管理职责的，由同级人民政府或者上级主管部门责令整改；情节严重的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

第二十一条 公共管理和服务机构及其工作人员按照有关法律、法规、规章和本规定进行公共数据安全管理，并履行了监督管理职责和合理注意义务，由于难以预见或者难以避免的因素导致公共数据使用主体或者其他第三方损失的，对有关单位和个人不作负面评价，依法不承担或者免予承担相关责任。

第二十二条 水务、电力、燃气、通信、公共交通、民航、铁路等公用事业运营单位涉及公共属性数据的安全管理，参照适用本规定。

第二十三条 本规定自 2020 年 12 月 1 日起施行。