贵州省人民代表大会常务委员会公告

（2019 第 9 号）

《贵州省大数据安全保障条例》已于 2019 年 8 月 1 日经贵州省第十三届人民代表大会常务委员会第十一次会议通过，现予公布，自 2019 年 10 月 1 日起施行。

贵州省人民代表大会常务委员会

2019 年 8 月 1 日

贵州省大数据安全保障条例

（2019 年 8 月 1 日贵州省第十三届人民代表大会常务委员会第十一次会议通过）

目　录

第一章　总　则

第一条　为了保障大数据安全和个人信息安全，明确大数据安全责任，促进大数据发展应用，根据《中华人民共和国网络安全法》和有关法律、法规的规定，结合本省实际，制定本条例。

第二条　本省行政区域内大数据安全保障及相关活动，应当遵守本条例。

涉及国家秘密的大数据安全保障，还应当遵守《中华人民共和国保守国家秘密法》等法律、法规的规定。

第三条　本条例所称大数据安全保障，是指采取预防、管理、处置等策略和措施，防范大数据被攻击、侵入、干扰、破坏、窃取、篡改、删除和非法使用以及意外事故，保障大数据的真实性、完整

性、有效性、保密性、可控性并处于安全状态的活动。

本条例所称大数据是指以容量大、类型多、存取速度快、应用价值高为主要特征的数据集合，是对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。

本条例所称大数据安全责任人，是指在大数据全生命周期过程中对大数据安全产生或者可能产生影响的单位和个人，包括大数据所有人、持有人、管理人、使用人以及其他从事大数据采集、存储、清洗、开发、应用、交易、服务等的单位和个人。

第四条 大数据安全保障工作坚持总体国家安全观，树立正确的网络安全观，按照政府主导、责任人主体，统筹规划、突出重点，预防为主、综合治理，包容审慎、支持创新，安全与发展、监管与利用并重的原则，维护大数据总体和动态安全。

第五条 大数据安全保障工作应当围绕国家大数据战略和省大数据战略行动实施，建立健全大数据安全管理制度，建设大数据安全地方标准体系、大数据安全测评体系、大数据安全保障体系等，采取大数据安全攻防演练等安全保障措施，推动大数据安全技术、制度、管理创新和发展。

第六条 省人民政府负责全省大数据安全保障工作，市、州和县级人民政府负责本行政区域内大数据安全保障工作。

开发区、新区管理机构根据设立开发区、新区的人民政府的授权，负责本辖区大数据安全保障的具体工作。

第七条 县级以上有关部门按照下列规定，履行大数据安全保障职责：

（一）网信部门负责统筹协调、检查指导和相关监督管理等工作；

（二）公安机关负责安全保护和管理、风险评估、监测预警、应急处置和违法行为查处等监督管理工作；

（三）大数据发展管理部门负责与大数据安全相关的数据管理、产业发展、技术应用等工作；

（四）通信管理部门负责电信网、公共互联网运行安全监督管理等工作；

（五）保密行政管理部门负责保密监督管理等工作；

（六）密码管理部门负责密码监督管理等工作；

（七）其他部门按照有关法律、法规的规定和各自职责做好大数据安全保障工作。

第八条 省人民政府应当根据大数据发展应用总体规划，编制大数据安全保障规划；网信、公安、大数据发展管理等部门应当根据大数据安全保障规划，编制本部门、本行业大数据安全保障专项规划。

第九条 县级以上人民政府应当建立大数据安全保障工作领导协调机制和责任机制，协调和指导本行政区域内大数据安全保障有关事项。

公安机关应当按照网络安全等级保护

要求，会同有关部门制定大数据风险测评、应急防范等安全制度，加强对大数据安全技术、设备和服务提供商的风险评估和安全管理。

第十条 任何单位和个人都有维护大数据安全的义务，不得从事危害大数据安全的活动，不得利用大数据从事危害国家安全以及损害国家利益、社会公共利益和他人合法权益的活动。

对危害大数据安全或者利用大数据从事违法犯罪活动的行为，任何单位和个人都有权劝阻、制止、投诉、举报。收到投诉举报的部门应当依法及时查处，保护举报人的合法权益；不属于本部门职责的，应当及时移送有权处理的部门。

第十一条 鼓励开展大数据安全知识宣传普及、教育培训，增强全社会大数据安全意识，提高大数据安全风险防范能力。

第十二条 鼓励、支持成立大数据安全联盟、行业协会等社会组织，开展行业自律、交流合作和安全技术研究等大数据安全工作。

第二章 安全责任

第十三条 实行大数据安全责任制，保障大数据全生命周期安全。

大数据安全责任，按照谁所有谁负责、谁持有谁负责、谁管理谁负责、谁使用谁负责以及谁采集谁负责的原则确定。

大数据基于复制、流通、交换等同时存在的多个安全责任人，分别承担各自安全责任。

第十四条 大数据安全责任人是单位的（以下简称单位大数据安全责任人），应当履行下列职责：

（一）依法成立安全管理机构或者明确安全管理负责人，定期对从业人员进行安全教育、技术培训和技能考核；

（二）制定安全管理制度、操作规程、应急预案，明确不同岗位安全管理责任；

（三）加强数据采集、使用、处理权限管理，对批量导出、复制、脱敏、销毁数据等实行审查批准；

（四）加强网络运行、访问监测管理，定期开展数据安全检查；

（五）采取数据分类、备份和加密等安全措施；

（六）按照规定期限留存相关的网络日志；

（七）发生数据安全事件时，立即采取措施，保存证据，并及时向行业主管部门和公安机关报告；

（八）发现违法发布或者传输信息的，立即停止发布、传输或者采取阻断、拦截等措施，保留有关记录，并及时向行业主管部门和公安机关报告；

（九）法律、法规规定的其他职责。

大数据安全责任人是个人的（以下简称个人大数据安全责任人），应当依法采取安全管理措施，妥善存储、保管，合理使用，保障大数据安全。

第十五条 单位大数据安全责任人采集、存储、传输、处理、交换、应用、销毁大数据等，应当根据网络安全等级保护要求，建立大数据安全防护管理制度、大数据安全审计制度，制定大数据安全应急预案，落实安全管理责任，并定期开展安全评测、风险评估和应急演练；采取安全保护技术措施，防止数据丢失、毁损、泄露和篡改。

前款规定活动涉及个人信息的，还应当遵守法律、法规关于个人信息保护的规定。

第十六条 采集数据应当具有合法目的和用途，遵循最小且必要和正当原则，禁止过度采集；科学确定采集对象、范围、内容、方式，依法进行采集，并保证数据的真实性、完整性、保密性。

国家机关采集数据应当经被采集人同意，法律、法规另有规定的除外。

采集数据不得侵犯国家秘密、商业秘密和个人信息，不得损害被采集人和他人合法权益。

除法律、法规另有规定外，向不特定公众提供普遍信息、接入、浏览、访问、营销、推广等网络服务的经营者，不得采集与其提供服务无关的数据，不得以使用人拒绝提供相关信息而限制或者拒绝其享受普遍服务。

第十七条 除法律、法规另有规定外，任何单位和个人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，并报当地公安机关备案。留存的数据应当用于合法目的，不得非法向他人提供、查阅、复制和传播。

第十八条 存储数据应当根据数据类型、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系统、介质、设施设备，采取技术和管理措施，保障存储系统和数据安全。

公共数据平台、企业数据中心等集中式大数据存储中心，应当根据国家相关技术标准、规范要求和保障数据安全需要，科学选址，规范建设，建立容灾备份、安全评价、日常巡查管理、防火防盗等安全管理制度，加强存储环境、供电、通信和存储系统、介质、设施设备安全审查。

第十九条 传输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、篡改。

第二十条 处理数据应当保护原始数据，不得随意更改、伪造，不得通过恶意处理导致数据毁灭性更改和永久性丢失。

第二十一条 交换数据应当维护数据的完整性、可用性。交换数据应当合法进行，交换双方不得假冒他人或者以其他方式骗取数据交换。

第二十二条 使用数据不得用于非法目的和用途。明知是通过攻击、窃取、恶意访问等非法方式获取的数据，不得使用。

使用数据开展广告宣传、营销推广等活动，不得干扰被采集人正常生产生活，

不得损害被采集人及他人合法权益。

第二十三条 销毁数据应当根据大数据安全保护管理需要，合理确定销毁方式和销毁要求。销毁公共数据、涉及商业秘密和个人信息等重要数据的，应当进行安全风险评估。

第二十四条 单位大数据安全责任人应当加强数据内容管理，定期清理、审查数据内容，发现其持有、管理、发布的数据含有违法内容的，应当及时予以处理，并采取相关补救措施；超出自身处理权限的，应当立即停止使用，告知数据提供人并向公安机关报告。

第二十五条 为他人提供基础网络、互联网数据中心或者系统服务的网络运营者，应当建立安全监测预警平台，加强对服务对象的数据安全管理，督促其建立安全管理制度，落实安全监测保护技术措施。

开展互联网平台和数据空间等租赁业务的，出租人应当将租赁信息依法报通信管理部门备案，通信管理部门应当将备案信息与公安机关共享。未经出租人同意，承租人不得擅自转租。涉及互联网数据中心业务和互联网接入服务业务的，应当遵守有关法律、法规的规定。

第二十六条 各级人民政府及有关部门和公共机构、公共服务企业因信息公开、数据开放以及公示、公告等需要公布企业、个人数据的，应当采取脱密、脱敏等措施，防止泄露国家秘密、商业秘密和个人信息。

第二十七条 银行、保险、房地产、航空、铁路、公路、供电、供水、供气、邮政、通信、快递、电子商务、旅游服务等经营者和学校、医疗机构、社保、户籍管理、车辆登记、公积金、社会信用管理等单位，应当加强内部管理，建立数据接触、访问审查等制度，明确数据提供、调用、分析、处理等权限。

前款规定单位在经营、服务活动中获取的用户数据，除依法共享开放外，单位及其工作人员不得泄露，不得出售或者非法向他人提供。

第二十八条 禁止发布、传播下列信息：

（一）危害国家主权、安全和发展利益；

（二）损害社会公共利益和他人合法权益；

（三）煽动民族仇恨、民族歧视；

（四）黄、赌、毒等违法犯罪信息；

（五）法律、法规禁止的其他信息。

第二十九条 禁止非法采集、窃取、存储、传输、使用、买卖个人信息。

第三十条 采集、存储、使用、处理人脸、指纹、基因、疾病等生物特征数据，应当遵守法律、法规的规定，不得危害国家安全、公共安全，不得侵犯个人合法权益。

第三十一条 单位大数据安全责任人因公共数据共享开放提供数据，基于提供

时的合理预见无安全风险的，提供人不承担相关责任。

通过大数据分析、挖掘、整合等取得的数据或者得出的结论，可能危害国家安全、损害国家利益、社会公共利益的，不得使用、传播，并应当立即停止相关活动，报公安机关依法予以处理。

第三章　监督管理

第三十二条　省人民政府应当建立统一的大数据安全监管平台，负责大数据安全信息收集、分析评估和通报，监测大数据安全状况，发布大数据安全监测预警信息，统筹协调大数据安全事件处置。

行业主管部门负责监测本行业、本领域大数据安全状况，发布相关信息，督促、指导本行业、本领域的大数据监测预警处置工作。

关键信息基础设施运营者、公共数据平台、企业数据中心等集中式大数据存储中心以及其他重要大数据安全责任单位，应当建立大数据安全监测预警平台，负责监测本单位大数据安全状况，发布相关信息。

第三十三条　县级以上公安机关应当加强大数据安全风险分析、预测、评估，收集相关信息；发现可能导致较大范围黑客攻击、病毒蔓延等大数据安全事件的，应当及时发布预警信息，提出防范应对措施，指导、监督大数据安全责任人做好安全防范工作。

第三十四条　行业主管部门、关键信息基础设施和重要信息系统运营单位发现本行业、本单位大数据安全事件发生的风险增大时，应当加强监测，及时收集相关信息，开展安全风险分析评估，发布风险预警，并采取避免、减轻危害的措施。

第三十五条　单位大数据安全责任人的应急预案应当包括大数据安全事件应急处置的组织机构及其职责、安全事件分级、应急响应程序、处置措施等内容，并定期组织演练。

关键信息基础设施运营者、公共数据平台、企业数据中心等集中式大数据存储中心以及其他重要单位大数据安全责任人的应急预案，应当报行业主管部门和县级以上公安机关备案。

第三十六条　发生大数据安全事件时，安全责任人应当及时启动应急预案，采取相应处置措施，防止危害扩大，告知可能受到影响的用户，并向行业主管部门和县级以上公安机关报告。行业主管部门和县级以上公安机关应当根据事件的性质和特点，及时予以处置并依法发布相关信息。

处置大数据安全事件时应当保护现场，记录并留存相关数据信息。

第三十七条　县级以上公安机关应当建立大数据安全日常监测制度，加强对大数据安全责任人履行安全职责情况的巡查、检查，指导、监督安全责任人建立安

全管理制度，加强安全风险防范，落实安全保障责任。

县级以上公安机关发现有关单位和个人安全管理责任落实不到位，存在较大安全风险或者可能发生安全事件的，应当及时提出整改意见并督促落实。

第三十八条 建立大数据安全情况报告制度。关键信息基础设施经营者、公共数据平台、企业数据中心等集中式大数据存储中心以及其他重要单位大数据安全责任人，应当定期向行业主管部门和县级以上公安机关报告大数据安全情况。

第三十九条 有关部门因履行职责需要，按照有关法律、法规的规定要求提供掌握的宏观经济、社会管理、网络安全等数据的，有关单位和个人应当及时提供。

除依法共享开放外，有关部门不得将前款规定的数据用于与履行职责无关的用途。

第四十条 大数据安全责任人应当协助公安机关、国家安全机关依法查处危害国家安全、公共安全及其他犯罪行为，为预防、侦查危害国家安全、公共安全及其他犯罪活动提供相关资料、数据和技术接口等支持。

大数据安全责任人按照前款规定或者公安机关、国家安全机关的要求采集的数据，未经公安机关、国家安全机关同意，不得自行处理、使用或者向他人提供。

第四十一条 县级以上社会信用管理部门应当建立大数据安全诚信档案，记录大数据安全责任人数据采集、管理、使用等信用信息，并按照有关规定纳入社会信用体系。

第四章 支持与保障

第四十二条 省人民政府应当支持大数据安全技术创新，推进大数据安全产业基地、园区和大数据安全城市建设，推动形成大数据安全产品研发、生产、应用的大数据安全产业链。

市、州和县级人民政府应当采取相应措施，引导、扶持、推动大数据安全相关产业、技术、产品发展应用。

鼓励高等院校、科研机构和企业事业单位加大大数据安全技术研发投入，开展大数据安全技术创新研究和大数据安全关键技术攻关，形成自主知识产权，推动科技成果转化。

第四十三条 省人民政府标准化部门应当会同有关部门制定并适时修订有关大数据安全以及大数据产品、服务和运行安全的地方标准，建立和完善大数据安全地方标准体系。

鼓励和支持企业、科研机构、高等院校和相关行业组织开展大数据安全相关标准的研究、制定和协同攻关，推动形成国家、行业和地方标准。

第四十四条 县级以上人民政府设立的大数据发展应用专项资金、大数据发展基金、科技成果转化资金等，对大数据安

全技术研发及成果转化应用、安全规范和安全标准制定、安全监测预警平台建设、安全保障体系建设、容灾备份体系建设、安全意识培训等，应当给予支持。

符合国家税收优惠政策规定的大数据安全企业，依法享受税收优惠。

鼓励金融机构创新金融产品，完善金融服务，支持大数据安全相关产业、技术、产品发展应用。

第四十五条 县级以上人民政府应当加强大数据安全监督管理人才队伍建设，鼓励和支持大数据安全及相关领域专业人才的培养、引进。

支持高等院校、科研机构大数据安全学科、专业等建设，开设大数据安全相关课程；创新教育培养模式，开展校企合作办学，实行订单式培养，为大数据安全提供人才支撑。

第四十六条 县级以上人民政府应当加强实体经济企业大数据安全体系建设引导，支持实体经济企业与大数据深度融合，加强实体经济企业信息化、大数据应用系统的安全保障能力和安全防护意识。

第四十七条 县级以上人民政府推进大数据安全社会化服务体系建设，鼓励和支持企业开展安全测评、电子认证、数据加密、容灾备份等数据安全服务。

第四十八条 鼓励企业事业单位使用符合大数据安全要求的产品、技术、服务，并依法享受优惠政策。

第四十九条 鼓励和支持建立大数据安全实验室、大数据安全靶场、技术验证基地等，开展大数据及网络安全攻防演练，对大数据安全新技术、新应用、新产品进行测试、检验。

第五章 法律责任

第五十条 违反本条例第十四条第一款、第十五条第一款、第二十四条、第二十七条第一款、第三十一条第二款的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正或者导致危害大数据安全等后果的，处以1万元以上10万元以下罚款，对直接负责的主管人员处以5000元以上5万元以下罚款。

第五十一条 违反本条例第十六条第一款、第二款规定，过度采集数据或者采集数据未经被采集人同意的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正的，处以5000元以上5万元以下罚款，对直接负责的主管人员处以1000元以上1万元以下罚款；造成损失的，依法予以赔偿。

违反本条例第十六条第三款规定的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正的，处以1万元以上10万元以下罚款，对直接负责的主管人员处以5000元以上5万元以下罚款。

第五十二条 违反本条例第十七条规定的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正，或者擅

自向他人提供、查阅、复制、传播留存的数据且情节严重的，可处以5000元以上5万元以下罚款，对直接负责的主管人员处以1000元以上1万元以下罚款。

第五十三条 违反本条例第十八条、第十九条、第二十条、第二十一条规定的，由有关部门或者县级以上公安机关责令改正，给予警告。

违反本条例第十八条第二款规定，拒不改正或者导致危害大数据安全等后果的，由有关部门或者县级以上公安机关处以10万元以上100万元以下罚款，对直接负责的主管人员处以1万元以上10万元以下罚款。

第五十四条 违反本条例第二十二条规定的，由有关部门或者县级以上公安机关责令改正，给予警告，没收违法所得，可处以违法所得1倍以上5倍以下罚款；没有违法所得的，处以5万元以上50万元以下罚款。

第五十五条 违反本条例第二十三条规定，销毁数据未进行安全风险评估的，由有关部门或者县级以上公安机关责令改正，给予警告，可处以5000元以上5万元以下罚款。

第五十六条 违反本条例第二十五条第二款规定未备案或者擅自转租的，由通信管理部门责令改正，给予警告；拒不改正的，可处以5000元以上5万元以下罚款。

第五十七条 违反本条例第二十七条第二款、第二十九条规定的，由有关部门或者县级以上公安机关责令改正，给予警告，没收违法所得，并可处以违法所得1倍以上10倍以下罚款；没有违法所得的，处以100万元以下罚款，对直接负责的主管人员和其他直接责任人员处以1万元以上10万元以下罚款；情节严重的，责令暂停相关业务、停业整顿，或者吊销相关业务许可证、营业执照。

第五十八条 违反本条例第四十条规定的，由县级以上公安机关责令改正；拒不改正或者情节严重的，处以5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员，处以1万元以上10万元以下罚款。

第五十九条 国家机关及其工作人员违反本条例规定，或者玩忽职守、滥用职权、徇私舞弊，妨碍大数据安全保障工作，尚不构成犯罪的，由其上级主管部门或者监察机关对直接负责的主管人员和其他直接责任人员依法予以处分。

第六十条 违反本条例规定的其他行为，法律、法规有处罚规定的，从其规定。

第六章 附 则

第六十一条 本条例自2019年10月1日起施行。