（2025 年 8 月）

目录

一、法规速递

《政务数据共享条例》

发文机关：国务院

生效时间：2025.08.01

第一章　总则

第一条　为了推进政务数据安全有序高效共享利用，提升政府数字化治理能力和政务服务效能，全面建设数字政府，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》等法律，制定本条例。

第二条　政府部门和法律、法规授权的具有管理公共事务职能的组织（以下统称政府部门）之间政务数据共享以及相关安全、监督、管理等工作，适用本条例。

第三条　本条例所称政务数据，是指政府部门在依法履行职责过程中收集和产生的各类数据，但不包括属于国家秘密、工作秘密的数据。

本条例所称政务数据共享，是指政府部门因依法履行职责需要，使用其他政府部门的政务数据或者为其他政府部门提供政务数据的行为。

第四条　政务数据共享工作应当坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，遵循统筹协调、标准统一、依法共享、合理使用、安全可控的原则。

第五条 开展政务数据共享工作，应当遵守法律法规，履行政务数据安全保护义务，不得危害国家安全、公共利益，不得损害公民、法人和其他组织的合法权益。

第六条 国家建立政务数据共享标准体系，推进政务数据共享工作标准化、规范化。

第七条 国家鼓励政务数据共享领域的管理创新、机制创新和技术创新，持续提升政务数据共享效率、应用水平和安全保障能力。

第二章 管理体制

第八条 各级人民政府应当加强对政务数据共享工作的组织领导。

国务院政务数据共享主管部门负责统筹推进全国政务数据共享工作。

县级以上地方人民政府政务数据共享主管部门负责统筹推进本行政区域内政务数据共享工作。

国务院各部门负责本部门政务数据共享工作，协调指导本行业、本领域政务数据共享工作。

第九条 政务数据共享主管部门应当会同其他政府部门研究政务数据共享中的重大事项和重要工作，总结、推广政务数据共享的典型案例和经验做法，协调推进跨层级、跨地域、跨系统、跨部门、跨业务政务数据安全有序高效共享利用。

第十条 政府部门应当落实政务数据共享主体责任，建立健全本部门政务数据共享工作制度，组织研究解决政务数据共享工作中的重大问题。

第十一条 政府部门应当明确本部门政务数据共享工作机构。政务数据共享工作机构负责本部门政务数据共享具体工作，履行以下职责：

（一）组织编制、更新和维护本部门政务数据目录；

（二）组织提出本部门政务数据共享申请，组织审核针对本部门政务数据的共享申请，协调并共享本部门政务数据；

（三）确保本部门提供的政务数据符合政务数据共享标准规范；

（四）组织提出或者处理涉及本部门的政务数据校核申请；

（五）建立健全本部门政务数据共享中数据安全和个人信息保护制度，组织开展本部门政务数据共享安全性评估；

（六）本部门其他与政务数据共享相关的工作。

第三章 目录管理

第十二条 政务数据实行统一目录管理。国务院政务数据共享主管部门制定政务数据目录编制标准规范，组织编制国家政务数据目录。县级以上地方人民政府政务数据共享主管部门组织编制本行政区域内的政务数据目录。

政府部门应当依照本部门职责，按照政务数据目录编制标准规范，编制本部门政务数据目录。

第十三条 政府部门编制政务数据目录，应当依法开展保密风险、个人信息保护影响等评估，并经部门负责人审核同意。

政务数据目录应当明确数据目录名称、数据项、提供单位、数据格式、数据更新频率以及共享属性、共享方式、使用条件、数据分类分级等信息。

第十四条 政务数据按照共享属性分为无条件共享、有条件共享和不予共享三类：

（一）可以提供给所有政府部门共享使用的政务数据属于无条件共享类；

（二）可以按照一定条件提供给有关政府部门共享使用的政务数据属于有条件共享类；

（三）法律、行政法规以及国务院决定明确规定不能提供给其他政府部门共享使用的政务数据属于不予共享类。

第十五条 政府部门应当科学合理确定政务数据共享属性，不得通过擅自增设条件等方式阻碍、影响政务数据共享。

对属于有条件共享类的政务数据，政府部门应当在政务数据目录中列明共享范围、使用用途等共享使用条件。对属于不予共享类的政务数据，政府部门应当在政务数据目录中列明理由，并明确相应的法律、行政法规以及国务院决定依据。

第十六条 政府部门应当将编制的政务数据目录报送同级政务数据共享主管部门审核。政务数据共享主管部门审核通过后统一向政府部门通告。

政府部门应当对照统一发布的政务数据目录，丰富政务数据资源，保障政务数据质

量，依法共享政务数据。

第十七条 政务数据目录实行动态更新。

因法律、行政法规、国务院决定调整或者政府部门职责变化导致政务数据目录需要相应更新的，政府部门应当自调整、变化发生之日起 10 个工作日内对政务数据目录完成更新，并报送同级政务数据共享主管部门审核。因特殊原因需要延长更新期限的，经同级政务数据共享主管部门同意，可以延长 5 个工作日。

政务数据共享主管部门应当自收到更新后的政务数据目录之日起 2 个工作日内完成审核并发布。

第四章 共享使用

第十八条 政府部门应当建立健全政务数据全过程质量管理体系，提高政务数据质量管理能力，加强政务数据收集、存储、加工、传输、共享、使用、销毁等标准化管理。

第十九条 政府部门应当按照法定的职权、程序和标准规范收集政务数据。通过共享获取政务数据能够满足履行职责需要的，政府部门不得向公民、法人和其他组织重复收集。

政务数据收集工作涉及多个政府部门的，政务数据共享主管部门应当明确牵头收集的政府部门并将其作为数源部门。数源部门应当加强与其他有关政府部门的协同配合、信息沟通，及时完善更新政务数据，保障政务数据的完整性、准确性和可用性，并统一提供政务数据共享服务。

第二十条 政务数据共享主管部门应当建立政务数据共享供需对接机制，明确工

作流程。

政务数据需求部门应当根据履行职责需要，按照统一发布的政务数据目录，经本部门政务数据共享工作机构负责人同意后，依法提出政务数据共享申请，明确使用依据、使用场景、使用范围、共享方式、使用时限等，并保证政务数据共享申请的真实性、合法性和必要性。

政务数据提供部门应当按照本条例第二十一条规定的期限对政务数据需求部门提出的政务数据共享申请进行审核，经本部门政务数据共享工作机构负责人同意后作出答复。

第二十一条 政务数据需求部门申请共享的政务数据属于无条件共享类的，政务数据提供部门应当自收到政务数据共享申请之日起 1 个工作日内作出答复；属于有条件共享类的，应当自收到政务数据共享申请之日起 10 个工作日内作出是否同意共享的答复。因特殊原因需要延长答复期限的，政务数据提供部门应当报经同级政务数据共享主管部门同意，并告知政务数据需求部门，延长的期限最长不得超过 10 个工作日。

政务数据需求部门提交的申请材料不全的，政务数据提供部门应当一次性告知其需要补充的材料，不得直接予以拒绝。政务数据提供部门不同意共享的，应当说明理由。

第二十二条 政务数据提供部门应当自作出同意共享的答复之日起 20 个工作日内共享政务数据。

政务数据提供部门可以通过服务接口、批量交换、文件下载等方式向政务数据需求部门共享政务数据。

第二十三条 国家鼓励各级政府部门优化政务数据共享审核流程，缩短审核和提

供共享政务数据的时间。

第二十四条 上级政府部门应当根据下级政府部门履行职责的需要，在确保政务数据安全的前提下，及时、完整回流业务信息系统收集和产生的下级政府行政区域内的政务数据，并做好系统对接和业务协同，不得设置额外的限制条件。

下级政府部门获得回流的政务数据后，应当按照履行职责的需要共享、使用，并保障相关政务数据安全。

第二十五条 政府部门通过共享获得政务数据的，不得擅自扩大使用范围以及用于或者变相用于其他目的，不得擅自将获得的政务数据提供给第三方。确需扩大使用范围、用于其他目的或者提供给第三方的，应当经政务数据提供部门同意。

政务数据共享主管部门以及其他政府部门应当采取措施防范政务数据汇聚、关联引发的泄密风险。

第二十六条 国务院政务数据共享主管部门应当统筹建立政务数据校核纠错制度。

政府部门应当依照本部门职责，建立政务数据校核纠错规则，提供纠错渠道。政务数据需求部门应当记录政务数据使用状态，发现政务数据不准确或者不完整的，应当及时向政务数据提供部门提出政务数据校核申请。政务数据提供部门应当自收到政务数据校核申请之日起 10 个工作日内予以核实、更正并反馈校核处理结果。

第二十七条 政务数据需求部门通过共享获取的政务数据，共享目的已实现、无法实现或者为实现共享目的不再必要的，应当按照政务数据提供部门的要求妥善处置。

政务数据需求部门存在擅自超出使用范围、共享目的使用政务数据，或者擅自将政

务数据提供给第三方的，政务数据共享主管部门或者政务数据提供部门应当暂停其政务数据共享权限，并督促限期整改，对拒不整改或者整改不到位的，可以终止共享。

政务数据提供部门无正当理由，不得终止或者变更已提供的政务数据共享服务。确需终止或者变更服务的，政务数据提供部门应当与政务数据需求部门协商，并报同级政务数据共享主管部门备案。

第二十八条 政务数据共享主管部门应当建立健全政务数据共享争议解决处理机制。

同级政务数据需求部门、政务数据提供部门发生政务数据共享争议的，应当协商解决；协商不成的，应当按照程序向同级政务数据共享主管部门申请协调处理。跨层级、跨地域的政务数据共享发生争议的，由共同的上级政务数据共享主管部门协调处理。经政务数据共享主管部门协调处理仍未达成一致意见的，报政务数据共享主管部门的本级人民政府决定。

第二十九条 政务数据共享主管部门应当对政务数据共享情况进行监督检查，并可以对违反本条例规定的行为予以通报。

政务数据需求部门应当对共享政务数据的使用场景、使用过程、应用成效、存储情况、销毁情况等进行记录，有关记录保存期限不少于 3 年。政务数据共享主管部门和政务数据提供部门可以查阅政务数据需求部门有关记录。法律、行政法规另有规定的，从其规定。

第五章 平台支撑

第三十条 国家统筹数据基础设施建设，提高政务数据安全防护能力，整合构建标

准统一、布局合理、管理协同、安全可靠的全国一体化政务大数据体系。

国务院政务数据共享主管部门统筹全国一体化政务大数据体系的建设和管理工作，负责整合构建国家政务大数据平台，实现与国务院有关部门政务数据平台、各地区政务数据平台互联互通，为政务数据共享提供平台支撑。

县级以上地方人民政府政务数据共享主管部门负责本行政区域政务数据平台建设和管理工作，按需向乡镇（街道）、村（社区）共享政务数据。

国务院有关部门负责建设、优化本部门政务数据平台，可以支撑本行业、本领域的政务数据共享工作。未建设政务数据平台的，可以通过国家政务大数据平台开展本部门政务数据共享工作。

第三十一条 政府部门已建设的政务数据平台应当纳入全国一体化政务大数据体系。除法律、行政法规另有规定外，原则上不得通过新建政务数据共享交换系统开展跨层级、跨地域、跨系统、跨部门、跨业务的政务数据共享工作。

第三十二条 政府部门应当通过全国一体化政务大数据体系开展政务数据共享相关工作。

第三十三条 国家鼓励和支持大数据、云计算、人工智能、区块链等新技术在政务数据共享中的应用。

第六章 保障措施

第三十四条 政务数据共享主管部门应当会同同级网信、公安、国家安全、保密行政管理、密码管理等部门，根据数据分类分级保护制度，推进政务数据共享安全管理制

度建设，按照谁管理谁负责、谁使用谁负责的原则，明确政务数据共享各环节安全责任主体，督促落实政务数据共享安全管理责任。

政务数据需求部门在使用依法共享的政务数据过程中发生政务数据篡改、破坏、泄露或者非法利用等情形的，应当承担安全管理责任。

第三十五条 政府部门应当建立健全政务数据共享安全管理制度，落实政务数据共享安全管理主体责任和政务数据分类分级管理要求，保障政务数据共享安全。

政府部门应当采取技术措施和其他必要措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用。

政府部门应当加强政务数据安全风险监测，发生政务数据安全事件时，立即启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。

第三十六条 政府部门委托他人参与建设、运行、维护政府信息化项目，存储、加工政务数据，应当按照国家有关规定履行批准程序，明确工作规范和标准，并采取必要技术措施，监督受托方履行相应的政务数据安全保护义务。受托方应当依照法律、行政法规的规定和合同约定履行政务数据安全保护义务，不得擅自访问、获取、留存、使用、泄露或者向他人提供政务数据。

政务数据平台建设管理单位应当依照法律、行政法规的规定和国家标准的强制性要求，保障平台安全、稳定运行，维护政务数据安全。

第三十七条 政府部门及其工作人员在开展涉及个人信息的政务数据共享活动时，应当遵守《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行

政法规的规定。

公民、法人和其他组织有权对政务数据共享过程中侵犯其合法权益的行为进行投诉、举报，接到投诉、举报的政府部门应当按照规定及时处理。

第三十八条 县级以上人民政府应当将政务数据共享工作所需经费列入本级预算。县级以上人民政府及其有关部门应当对政务数据共享相关经费实施全过程预算绩效管理。政务数据共享情况应当作为确定政府信息化项目建设投资、运行维护经费和项目后评价结果的重要依据。

政务数据共享主管部门应当加强对本行政区域内政务数据提供部门数据共享及时性和数据质量情况、政务数据需求部门数据应用情况和安全保障措施等的监督，并向本级人民政府报告。

第七章 法律责任

第三十九条 政务数据提供部门违反本条例规定，有下列情形之一的，由同级政务数据共享主管部门责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分：

（一）未按照要求编制或者更新政务数据目录；

（二）通过擅自增设条件等方式阻碍、影响政务数据共享；

（三）未配合数源部门及时完善更新政务数据；

（四）未按时答复政务数据共享申请或者未按时共享政务数据，且无正当理由；

（五）未按照规定将业务信息系统收集和产生的下级政府行政区域内的政务数据回流至下级政府部门；

（六）收到政务数据校核申请后，未按时核实、更正；

（七）擅自终止或者变更已提供的政务数据共享服务；

（八）未按照规定将已建设的政务数据平台纳入全国一体化政务大数据体系；

（九）违反本条例规定的其他情形。

第四十条 政务数据需求部门违反本条例规定，有下列情形之一的，由同级政务数据共享主管部门责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分：

（一）重复收集可以通过共享获取的政务数据；

（二）擅自超出使用范围、共享目的使用通过共享获取的政务数据；

（三）擅自将通过共享获取的政务数据提供给第三方；

（四）共享目的已实现、无法实现或者为实现共享目的不再必要，未按照要求妥善处置通过共享获取的政务数据；

（五）未按照规定保存通过共享获取的政务数据有关记录；

（六）未对通过共享获取的政务数据履行安全管理责任；

（七）违反本条例规定的其他情形。

第四十一条 政务数据共享主管部门违反本条例规定，有下列情形之一的，由本级人民政府或者上级主管部门责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分：

（一）未按照规定明确数源部门；

（二）未按照规定对政务数据共享争议进行协调处理；

（三）违反本条例规定的其他情形。

第四十二条 政府部门及其工作人员泄露、出售或者非法向他人提供政务数据共享工作过程中知悉的个人隐私、个人信息、商业秘密、保密商务信息的，或者在政务数据共享工作中玩忽职守、滥用职权、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第八章 附则

第四十三条 国家推动政府部门与其他国家机关参照本条例规定根据各自履行职责需要开展数据共享。

第四十四条 本条例自 2025 年 8 月 1 日起施行。

《关键信息基础设施商用密码使用管理规定》

发文机关：国家密码管理局,国家互联网信息办公室,公安部

生效时间：2025.08.01

第一条　为规范关键信息基础设施商用密码使用，保护关键信息基础设施安全，根据《中华人民共和国密码法》、《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》、《商用密码管理条例》和《关键信息基础设施安全保护条例》、《网络数据安全管理条例》等有关法律、行政法规，制定本规定。

第二条　依据《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律、行政法规和国家有关规定认定的关键信息基础设施的商用密码使用管理，适用本规定。

第三条　国家密码管理部门会同国家网信部门、国务院公安部门负责规划、指导和监督全国的关键信息基础设施商用密码使用管理工作，建立关键信息基础设施商用密码使用管理信息共享机制。

县级以上地方各级密码管理部门会同网信部门、公安机关负责指导和监督本行政区域的关键信息基础设施商用密码使用管理工作。

第四条　关键信息基础设施保护工作部门（以下简称保护工作部门）在职责范围内负责监督管理本行业、本领域关键信息基础设施商用密码使用工作，单独编制本行业、本领域商用密码使用规划或者纳入本行业、本领域的关键信息基础设施安全规划并组织实施，指导本行业、本领域关键信息基础设施运营者（以下简称运营者）开展商用密码相关制度、人员、经费等保障工作。

保护工作部门应当于每年 3 月 31 日前向国家密码管理部门、国家网信部门、国务院公安部门报告上一年度本行业、本领域关键信息基础设施商用密码使用管理情况。

关键信息基础设施发生涉及商用密码的重大网络安全事件或者发现涉及商用密码的重大网络安全威胁时，保护工作部门应当及时向国家密码管理部门、国家网信部门、国务院公安部门报告，指导运营者开展应急处置，必要时开展商用密码应用安全性评估。

第五条　运营者应当按照相关法律、行政法规和国家有关规定，遵循国家商用密码管理、网络安全等级保护、关键信息基础设施安全保护等制度要求，使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

运营者应当于每年 1 月 31 日前向所属的保护工作部门报告上一年度关键信息基础设施商用密码使用以及商用密码应用安全性评估开展情况。

第六条　运营者应当加强关键信息基础设施商用密码使用制度保障，建立商用密码使用、应急处置、重大事件报告等关键信息基础设施商用密码使用管理制度。

运营者的主要负责人对关键信息基础设施商用密码使用管理负总责，负责关键信息基础设施商用密码使用和涉及商用密码的重大网络安全事件处置工作。

第七条　运营者应当加强关键信息基础设施商用密码使用人员保障，配备取得密码相关专业学历或者密码相关国家职业技能等级认定证书的专业人员分别承担密钥管理员、密码操作员等职责，配备具有安全审计专业能力的人员承担密码安全审计员职责。

运营者应当对密码相关专业人员进行安全背景审查，并定期组织其参加密码相关业

务技能培训，提高密码相关专业人员的商用密码使用能力。

第八条　运营者应当加强关键信息基础设施商用密码使用和应用安全性评估经费保障，将商用密码使用和应用安全性评估经费纳入网络安全和信息化经费安排。

第九条　关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

运营者采购涉及商用密码的网络产品和服务，影响或者可能影响国家安全的，应当按照《网络安全审查办法》进行网络安全审查。

第十条　关键信息基础设施应当按照国家数据安全保护、个人信息保护有关要求，使用商用密码对其存储、使用、传输的核心数据、重要数据和个人信息进行保护。

第十一条　关键信息基础设施规划阶段，其运营者应当依照相关法律、行政法规和标准规范，根据商用密码应用需求，制定商用密码应用方案，规划商用密码保障系统并纳入关键信息基础设施安全规划统筹部署。

运营者应当自行或者委托商用密码检测机构对商用密码应用方案进行商用密码应用安全性评估。商用密码应用方案未通过商用密码应用安全性评估的，不得作为商用密码保障系统的建设依据。

第十二条　关键信息基础设施建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。建设过程中需要调整商用密码应用方案的，应当重新开展商用密码应用安全性评估，评估通过后方可按照调整后的商用密码应用方案继续建设。

关键信息基础设施运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

第十三条　关键信息基础设施建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保关键信息基础设施商用密码的正确使用和商用密码保障系统的有效运行。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，并在改造期间采取必要措施保证关键信息基础设施运行安全。

第十四条　本规定施行前正在建设的关键信息基础设施，其运营者应当加强商用密码应用方案编制论证，建设完善商用密码保障系统，并按照本规定第十二条开展商用密码应用安全性评估。

本规定施行前已经投入运行的关键信息基础设施，其运营者应当按照本规定第十三条开展商用密码应用安全性评估。

第十五条　开展关键信息基础设施商用密码应用安全性评估，应当符合《商用密码应用安全性评估管理办法》有关规定。

关键信息基础设施商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评加强衔接，避免重复评估、测评。

第十六条　国家密码管理部门负责建设和管理国家关键信息基础设施商用密码运行安全管理基础设施，统筹保护工作部门建设本行业、本领域关键信息基础设施商用密码运行安全管理基础设施，会同国家网信部门、国务院公安部门分析研判关键信息基础

设施商用密码运行安全态势，协同应对处置重大商用密码运行安全威胁。

第十七条　密码管理部门应当定期组织开展关键信息基础设施商用密码使用情况监督检查。保护工作部门应当定期对本行业、本领域关键信息基础设施商用密码使用情况进行检查并提出改进措施，必要时可以自行或者委托商用密码检测机构等专业机构进行商用密码应用安全性评估。

运营者对密码管理部门和保护工作部门开展的关键信息基础设施商用密码使用情况监督检查应当予以配合，根据监督检查意见及时进行整改并向保护工作部门报告整改情况，保护工作部门应当将整改情况向国家密码管理部门报告。

开展关键信息基础设施商用密码使用情况监督检查应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。监督检查不得收取费用，不得要求被监督检查单位购买、使用指定单位或者指定品牌的商用密码产品、服务。

第十八条　密码管理部门、有关部门、商用密码检测机构及其工作人员对其在履行职责中知悉的国家秘密、商业秘密和个人隐私承担保密义务，不得泄露或者非法向他人提供。

第十九条　运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法 》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定有关条款，有下列情形之一的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款：

（一）未按照要求使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统的；

（二）关键信息基础设施使用的商用密码产品、服务未经检测认证合格的；

（三）关键信息基础设施使用的密码算法、密码协议、密钥管理机制等商用密码技术未通过国家密码管理部门审查鉴定的；

（四）关键信息基础设施规划阶段，未制定商用密码应用方案，或者未对商用密码应用方案进行商用密码应用安全性评估的；

（五）关键信息基础设施建设阶段，未按照通过商用密码应用安全性评估的商用密码应用方案建设商用密码保障系统的；

（六）关键信息基础设施运行前，未开展商用密码应用安全性评估，或者未通过商用密码应用安全性评估且未进行改造的；

（七）关键信息基础设施建成运行后，未定期开展商用密码应用安全性评估，或者未通过定期开展的商用密码应用安全性评估且未进行改造的。

第二十条　运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第九条，使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额 1 倍以上 10 倍以下罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第二十一条　运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法 》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第十七条，无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的，由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 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 1 万元以上 10 万元以下罚款；情节特别严重的，责令停业整顿。

第二十二条　运营者违反本规定，有下列情形之一的，由密码管理部门、有关部门依据职责责令改正：

（一）未按照要求报告上一年度关键信息基础设施商用密码使用以及商用密码应用安全性评估开展情况的；

（二）未建立关键信息基础设施商用密码使用管理制度的；

（三）未按照要求配备密钥管理员、密码操作员、密码安全审计员的；

（四）未保障关键信息基础设施商用密码使用和应用安全性评估经费的。

第二十三条　从事关键信息基础设施商用密码使用监督管理工作的人员滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的，依法给予处分。

第二十四条　属于国家政务信息系统的关键信息基础设施的商用密码使用管理，除应当遵守本规定以外，还应当按照《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）等有关规定要求执行。

第二十五条　本规定自 2025 年 8 月 1 日起施行。

二、热点案例

中央网信办部署网上涉退役军人不当行为和有害信息内容专项整治

发布机关：国家互联网信息办公室

发布时间：2025.08.29

近期，部分网络账号以“退役军人”名义直播带货售卖假冒伪劣商品，开展低俗表演，消费军旅情怀，损害退役军人形象。针对上述问题，按照有关工作部署，决定自即日起至2025 年 9 月底，开展网上涉退役军人不当行为和有害信息内容专项整治。

一、工作目标

通过开展专项整治，督促网站平台落实主体责任，深入排查清理网上涉退役军人不当行为和有害信息，维护网上退役军人形象，为纪念中国人民抗日战争暨世界反法西斯战争胜利 80 周年营造良好网络环境。

二、整治重点

专项整治重点清理处置以下 10 类涉退役军人不当行为和有害信息内容及相关网络账号：

1.通过穿着军服及其仿制品、佩戴军功章、摆放军用物品、设置背景环境场景等方式，营造虚假退役军人人设。

2.借“退役军人”、“退伍老兵”等身份进行制假售假、违规引流等违法违规营销牟利行为。

3.以“退役军人”名义，使用“军需”、“军品”等用语销售假冒仿制的军服、军用装备等物品。

4.在直播过程中自称“退役军人”，穿着我国武装力量现行或者曾经装备的制式服装及其

仿制品，在团播、连线 PK、人气比拼等过程，以低俗形式吸引用户打赏。

5.打着“退役军人”、“退役专家”等旗号，发布所谓“解析装备细节”、“分析战术战法”、“解读军事行动”等谣言信息，或以传播经验、分享故事等名义，发布“在 XX 地服役有什么危害”等误导性内容。

6.以“丑化”、“恶搞”等形式戏谑调侃退役生活，损害退役军人形象，或通过“街头采访”、虚假摆拍等方式，编造发布涉退役军人及其家属待遇保障等相关话题，进行引流炒作。

7.使用人工智能、深度合成等技术，制作发布穿着军装的虚假退役军人图片、视频。

8.以提供“转业安置咨询”等为噱头，进行收费服务或卖课牟利，歪曲解读军队抚恤优待、退役安置等政策制度。

9.虚构捏造“退役军人”身份，利用人民群众拥军情怀，实施网络诈骗、感情欺骗等违法犯罪活动。

10.其他影响退役军人形象的网上不当行为和有害信息。

退役军人是党和国家的宝贵财富，是推进中国式现代化的重要力量，各地网信部门要提高政治站位，按照职责深入开展专项整治工作，督促属地网站平台严格落实履行主体责任，加强涉退役军人信息内容管理，持续做好违规内容发现处置，切实维护网上退役军人形象。

违法违规涉军自媒体账号典型案例

发布机关：国家互联网信息办公室

发布时间：2025.08.14

近期，一些自媒体账号违反《互联网军事信息传播管理办法》，违规发布涉军信息，误导公众认知，损害军队形象，社会影响恶劣。军地职能部门依法依规处置了一批网上违法违规信息及自媒体账号，现遴选通报有关典型案例。

一、冒充官方账号。

网络账号“南部卫士”、“联参智库服务”、“联勤保障”等与军队单位开办的网络账号雷同，以高仿账号冒充官方账号，发布内容多为涉军信息，蹭炒军事热点吸粉牟利。

二、编撰军事谣言。

网络账号“乖乖兔军情”利用 AI 编造“中国四大镇魂武器”等谣言信息，误导认知。网络账号“军事课代表”发布所谓“解析装备细节”、“分析战术战法”、“解读军事行动”等内容，部分文章需付费购买浏览，借军事话题违规牟利。

三、歪曲解读军史。

网络账号“红小岩的自留地”、“红小岩谈古论今”、“红小岩的后花园”等，称抗美援朝志愿军飞行员、空军一级战斗英雄张积慧“战绩有水分”，质疑污蔑英烈功绩，借党史军史严肃话题引流牟利。

四、抹黑军队形象。

网络账号“军创怡姐”、“苏州怡姐”利用所谓“答疑视频”，发布“在 XX 地服役有什么危害”等误导性内容，抹黑军队形象。

五、消费拥军情怀。

网络账号“秦淮河畔”自称退役军人，长期发布身穿各式军服或军服仿制品的短视频，为个人账号违规引流。

六、暴露部队营区。

网络账号“杨阳阳”自称 90 后留守军嫂，发布多篇“部队家属院”短视频，内容含各类训练设备，并标注定位，暴露军队敏感信息。

军地相关部门负责人表示，将持续贯彻落实《互联网军事信息传播管理办法》，坚决依法依规打击自媒体涉军违法违规行为，从严查处发布和炒作不实信息账号主体，曝光典型案例。同时欢迎有关部门和网民积极参与举报，共同打造良好涉军网络环境。

三、实务解读

1. 后数字资产时代的 NFT 营销模式

供稿人：潘永建（上海市通力律师事务所）、邓梓珊（上海市通力律师事务所）、嵇若琳（上海市通力律师事务所）

2021 年，艺术家 Beeple 创作的 NFT（Non-Fungible Token，非同质化代币）《Everydays: The First 5000 Days》拍出天价，NFT 在全球范围内迅速走红。然而，与海外市场中高度金融化的运作模式不同，国内 NFT 在二级市场的交易受到严格的规制。为弱化 NFT 的金融属性、引导其向文化与消费领域合规发展，中国内地主流语境下的 NFT 更多地以“数字藏品”这一称谓出现。

近年来，随着 NFT 市场逐步规范，主流平台（如鲸探、上海数交所等）正在审慎探索 NFT 的交易模式，NFT 正逐步从静态的“收藏品”向动态的“可流转资产”过渡。相应地，“数字资产”这一术语逐渐兴起。在这一背景下，市场探索出一种全新的 NFT 玩法，将其打造为链接品牌与消费者的一种新型营销工具：通过发行附带特定权益的 NFT，实现用户拉新、会员管理和私域流量运营。

本文将系统梳理 NFT 的当前实践现状与监管环境，并分析面临的法律风险与合规要点，以期为相关企业提供参考。为行文方便，本文将统一使用“NFT”指代包括数字藏品在内的各种数字资产。

2. NFT 的政策环境与实践观察

2.1 国家层面：审慎监管

从国家层面来看，目前尚未发布专门针对 NFT 的法律法规，对于 NFT 及相关业务的审慎监管基调并未发生改变，其焦点始终是防范系统性金融风险。

2022 年 4 月，中国互联网金融协会、中国银行业协会、中国证券业协会联合发布《关于防范 NFT 相关金融风险的倡议》（“《倡议》”），是迄今为止最具影响力的行业指引文件。《倡议》明确划定了 NFT 不得与加密货币挂钩、不得违规设立交易场所、不得变相发行交易金融产品等红线。

此外，中国人民银行等部门发布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》等文件，明确了任何形式的虚拟货币相关业务活动均属于非法金融活动。尽管 NFT 基于“非同质化”的核心特征，在理论上与比特币、以太坊等“同质化”的虚拟货币存在本质区别，不直接具备货币的价值尺度和支付流通功能，但如果 NFT 发行、交易模式呈现出高度的金融属性，极有可能被“穿透式监管”认定为变相从事虚拟货币相关非法金融活动。

2.2 地方层面：积极探索

以上海为代表的地方政府，在国家战略指导下，正积极拥抱数字经济，对数字资产等相关产业表现出积极的探索姿态。《上海市“十四五”数字经济发展规划》明确提出“支持龙头企业探索 NFT（非同质化代币）交易平台建设，研究推动 NFT 等资产数字化、数字 IP 全球化流通、数字确权保护等相关业态在上海先行先试”。《上海市培育“元宇宙”新赛道行动方案（2022-2025 年）》中，进一步提出“在上海数据交易所试点开设数字资产交易板块，培育健全数字资产要素市场……逐步完善数字资产、数字艺术品、数字影视版权等合规交易机制”。

相关政策文件表明，地方政府已经认识到 NFT 等数字资产在赋能实体经济方面的重要潜力，希望将数字资产纳入一个可管、可控的要素市场体系。需要注意的是，地方的“积极探索”与中央的“审慎监管”并不矛盾，所有地方层面的探索，都必须在中央划定的“防范金融风险”这一红线之内进行。

2.3 现状观察：以上海数交所为例

目前，市场最关心的问题是：对 NFT 的监管“松绑”了吗，是否可以自由交易？事实上，NFT 的交易并非无限制“松绑”，而是通过设立规范的平台探索交易模式。以上海数交所为例，2022 年 8 月 24 日，上海数据交易所在全国率先设立数字资产交易板块。根据公开信息，其交易规则具有以下特点：

- **资产定性**：上海数交所将 NFT 定义为“数字资产”，并将其界定为“有创作投入、有价值、可交换的数字化商品，具备加密性、唯一性和可追溯性的特征”。实践中，在上海数交所挂牌的 NFT 通常绑定特定实体权益，例如会员资格、产品/服务兑换权或消费折扣券等，具有较强的消费营销属性。
- **准入管理**：根据《上海数据交易所数字资产交易管理规范（试行）》，数字资产交易参与主体需经上海数据交易所认证。不仅发行方需通过资质审核，购买方也需完成实名认证与风险认知测试。此外，NFT 的发行和交易必须分别履行发行登记与挂牌登记程序。
- **场内交易**：NFT 的交易依托上海数交所提供的数字资产交易基础链进行。上海数交所为交易提供统一登记、统一结算、统一清分和统一存证服务，保障数字资产的安全有序流转。

3.作为新型营销工具的 NFT

3.1 从艺术收藏到“数实融合”

在当前监管环境下，市场的主流应用正在转向 NFT 与实体权益深度结合的“数实融合”模式。品牌方通过发行附带特定实体权益的 NFT，将其打造为一种集用户引流、会员管理与私域运营于一体的多功能营销载体。在此模式下，NFT 传统的艺术

收藏属性被一定程度削弱，而身份属性与消费属性则得到增强。

- **身份属性**：拥有某品牌的特定 NFT，成为一种可验证的数字身份，其功能类似于数字化的会员卡或粉丝徽章。例如，宝马为纪念 M 品牌 50 周年在中国发行的限量数字藏品，就成为车主和粉丝圈层的一种独特身份标识。
- **消费属性**：这是新型 NFT 营销模式最核心的价值所在，即 NFT 成为一种可流转的消费权益凭证。例如，在上海数交所发行的“全国首款大健康系列之光明舒睡款”，其持有者可以享受包括光明随心订的牛奶定期配送服务、各类产品折扣券等在内的一系列实体权益。

据此，NFT 的增值逻辑是多元的，其价值的组成可能来源于：

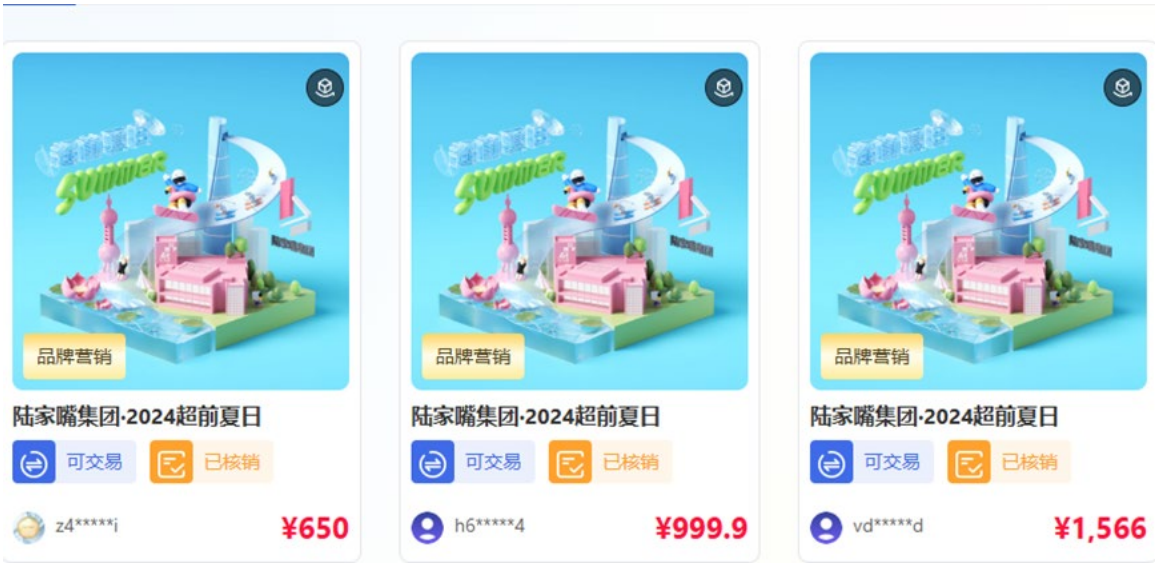
- **内在效用价值**：即 NFT 所绑定的实体权益的公允市场价值。
- **情绪与社交价值**：作为品牌会员或核心粉丝的身份，带来的社群归属感、社交资本等。
- **市场价值**：在合规流转平台内，基于市场供需关系和投机情绪而产生的价格波动。

3.2 概念辨析

- **数字藏品 vs. 数字资产**：如前所述，“数字藏品”是在中国特定监管环境下，行业为主动去金融化、强调文化消费属性而采取的术语。而“数字资产”，如上海数交所的定义，是更广义、更中性的词汇，意在将 NFT 纳入更宏大的“数据要素”框架。当前的市场趋势正是推动“数字藏品”向更广义的“数字资产”演进。
- **“一图多发”vs. FNFT** ：一些品牌在进行 NFT 营销时，会采用“一图多发”的模式，即基于同一个图片发行成百上千个独立的 NFT。此模式下，虽然图片相同，但每一个 NFT 在区块链上都拥有一个独一无二、不可分割的链上标识（Token ID）。每一个 NFT 的所有权是独立的，交易时的定价也是独立的（如下图所示）。

FNFT（Fractional NFT，碎片化 NFT）是指将一个单一的 NFT 的所有权通过技术手

段分割成许多份可互换的 FNFT，以供多人按份持有。此种模式因将单一资产所有权进行份额化拆分，具有典型的“资产证券化”特征，在我国是被明确禁止的。



4、合规要点

4.1 防范金融化、证券化

- 我国对于 NFT 的金融化证券化倾向一直保持高度警惕，我们在为企业评估 NFT 业务模式合规性时，一定会按照《关于防范 NFT 相关金融风险的倡议》逐项审查，确保：
- 不在 NFT 底层商品中包含证券、保险、信贷、贵金属等金融资产，变相发行交易金融产品；
- 不通过分割所有权或者批量创设等方式削弱 NFT 非同质化特征，变相开展代币发行融资(ICO)；
- 不为 NFT 交易提供集中交易(集中竞价、电子撮合、匿名交易、做市商等)、持续挂牌交易、标准化合约交易等服务，变相违规设立交易场所；
- 不以比特币、以太币、泰达币等虚拟货币作为 NFT 发行交易的计价和结算工具；
- 不直接或间接投资 NFT，不为投资 NFT 提供融资支持。

4.2 个人信息合规

当 NFT 从静态的“收藏”走向动态的“交易”，个人信息处理的环节也随之增加，我们提示企业重点注意以下合规要点：

- **知情同意**

- 平台与品牌方在收集和处理用户个人信息时，在平台注册、实名认证（KYC）等不同环节，应当针对不同处理目的，分别进行告知并获取用户同意。
- 对于向他人提供个人信息（如为实现权益兑付，需将用户身份信息同步给品牌方的小程序或线下门店）、处理敏感个人信息（如身份证号码用于实名认证）、公开个人信息（如展示 NFT 持有者身份）等情况，必须依法获取用户的“单独同意”。

- **个人信息权利保护**

区块链的“不可篡改”特性与个人信息保护法中的修改权、删除权存在天然的矛盾。对此，可以考虑采取“链上标识，链下映射”的技术架构，即区块链上仅记录用户标识（如 Token ID），而将用户的姓名、手机号等个人信息存储在平台方的中心化数据库中，并与链上的标识建立映射关系。当用户依法行使其修改或删除个人信息的权利时，平台仅需对链下数据库中的信息进行操作。

4.3 非法集资风险

若对 NFT 的价值预期引导不当，极易触碰非法集资的刑事红线。为有效隔离此风险，我们通常都会特别提示企业，务必加强对于宣传营销和社群运营的合规管理：

- 在宣传文案、社群运营、直播等公开渠道，不得向用户暗示或明示购买 NFT 能够“稳定升值”、“价格翻倍”，或承诺未来会以更高的价格“回购”。
- 对员工及合作的 KOL 的言论进行严格约束与审查。对于社群内用户的自发讨论，平台应尽到合理的管理和风险提示义务，通过置顶公告、人工即时介入等方式，

及时对投机炒作言论进行干预和澄清。

4.4 消费者权益保护

当 NFT 与具体的实体商品或服务权益深度绑定，即采用“数实融合”模式时，潜在的消费纠纷风险也随之急剧增加。建议企业：

- 对 NFT 绑定的权益内容、使用期限等信息的宣传必须真实、准确，并对限制性条件（例如地域限制等）进行显著提示，充分保障消费者的知情权。
- 若 NFT 允许流转，必须清晰说明其所附带的权益是否随之一同转移，以及受让方是否需要满足特定条件方可继受该等权益、以及权益在流转后内容是否会发生任何变更等。
- 确保所绑定的实体商品符合质量标准，所提供的服务达到承诺水平。
- 建立清晰、有效的客户服务和投诉处理机制，及时响应用户关于 NFT 权益兑现、使用问题等方面的咨询和投诉。

5、结语

从宏观上看，我国对于 NFT 的监管思路日渐清晰：即严防金融风险，积极探索合规服务实体经济的新模式。在后数字资产时代，企业应深刻理解并遵循监管规则，将合规体系内置于 NFT 业务模式的设计之中，如此方能享受数字资产带来的技术红利，行稳致远。