为行业数据安全监管提供制度保障

——《工业和信息化领域数据安全管理办法（试行）》解读

工业和信息化部网络安全管理局

- *对国家数据安全管理制度要求进行细化，明确开展数据分类分级保护等工作的具体要求。*
- *构建工业和信息化领域数据安全监管体系，明确工业和信息化部的职责范围。*
- *指导数据处理者健全数据安全管理和技术保护措施，履行安全保护主体责任。*
- *明确重要数据和核心数据处理者每年至少完成一次数据安全风险评估。*
- *明确“部-省-企业”三级联动协同的数据安全风险监测预警工作机制。*

近日，工业和信息化部印发《工业和信息化领域数据安全管理办法（试行）》（工信部网安〔2022〕166号）（以下简称《管理办法》），并就《管理办法》重点问题进行了解读。

一、《管理办法》出台的背景和目的是什么？

当前，数据已成为数字经济时代最为活跃的新型生产要素。与此同时，数据安全风险日益突出，成为关系个人权益、公共利益和国家安全的重要因素。2021年9月1日，《中华人民共和国数据安全法》（以下简称《数据安全法》）正式实施，为开展数据安全监管和保护工作提供了法律依据和根本遵循，其中明确工业和信息化部承担工业、电信行业数据安全监管职责，并对数据处理者的安全保护义务提出了相关要求。

工业和信息化领域是数字经济发展的主阵地和先导区，是推进数字经济做强做优做大的主力军。为贯彻落实《数据安全法》，加快推动工业和信息化领域数据安全管理工作制度化、规范化，工信部研究起草了《管理办法》，一是在工业和信息化领域对国家数据安全管理制度要求进行细化，明确开展数据分类分级保护、重要数据管理等工作的具体要求，细化数据全生命周期安全义务，为行业数据安全监管提供制度保障。二是构建工业和信息化领域数据安全监管体系，明确工业和信息化部、地方行业监管部门的职责范围，建立权责一致的工作机制。三是根据工业、电信、无线电领域的实际情况，明确数据全生命周期保护要求，指导数据处理者健全数据安全管理和技术保护措施，履行安全保护主体责任。

二、《管理办法》的定位和主要内容是什么？

《管理办法》作为工业和信息化领域数据安全管理顶层制度文件，共八章四十二条，重点解决工业和信息化领域数据安全“谁来管、管什么、怎么管”的问题。主要内容包括七个方面：一是界定工业和信息化领域数据和数据处理者概念，明确监管范围和监管职责。二是确定数据分类分级管理、重要数据识别与备案相关要求。三是针对不同级别的数据，围绕数据收集、存储、加工、传输、提供、公开、销毁、出境、转移、委托处理等环节，提出相应安全管理和保护要求。四是建立数据安全监测预警、风险信息报送和共享、应急处置、投诉举报受理等工作机制。五是明确开展数据安全监测、认证、评估的相关要求。六是规定监督检查等工作要求。七是明确相关违法违规行为的法律责任和惩罚措施。

三、《管理办法》明确的监管范围是什么？

《管理办法》对工业和信息化领域数据处理活动进行安全监管，具体可以从处理对象、处理主体、处理活动三方面进行认识：从处理主体看，工业和信息化领域数据处理者是指能够在工业和信息化领域数据处理活动中自主决定处理目的、处理方式的各类主体，主要包括工业数据处理者、电信数据处理者以及无线电数据处理者。从处理对象看，工业和信息化领域数据主要包括工业数据、电信数据和无线电数据等。从处理活动看，数据收集、存储、使用、加工、传输、提供、公开等活动都属于监管范围。

四、《管理办法》明确了怎样的监管职责分工？

《管理办法》构建了“工业和信息化部、地方行业监管部门”两级监管机制。工业和信息化部统筹工业和电信领域数据安全监管工作，包括组织制定行业数据安全管理政策制度和标准规范，编制行业重要数据和核心数据目录，建立重要数据目录备案、监测预警、风险信息报送和共享、应急处置等工作机制，指导地方行业监管部门开展属地监管，督促全行业数据处理者加强数据安全保护工作。

地方行业监管部门，包括各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局和无线电管理机构，分别负责对本地区工业、电信、无线电领域数据处理者进行监督管理，包括审核重要数据目录备案，编制重要数据和核心数据具体目录，开展监测预警、风险信息报送和共享、应急处置、风险评估、投诉举报受理等工作，并可结合工作实际，建立更加细化完善的工作机制。

五、《管理办法》对数据分级保护的要求是什么？

《管理办法》以数据分级保护为总体原则，要求一般数据加强全生命周期安全管理，重要数据在一般数据保护的基础上进行重点保护，核心数据在重要数据保护的基础上实施更加严格保护。对于不同级别数据同时被处理且难以分别采取保护措施的，采取“就高”原则，按照其中级别最高的要求实施保护。

六、《管理办法》要求重要数据处理者履行哪些数据安全保护义务？

《管理办法》依据国家数据分类分级保护制度要求，规定重要数据处理者在履行一般数据处理者数据安全保护义务的基础上，还应承担以下保护义务：一是开展数据识别备案，按照相关标准规范识别重要数据，形成本单位具体目录并进行备案；二是加强内部管理，建立数据安全工作体系，明确数据安全负责人，加强数据处理关键岗位管理，构建重要数据处理登记审批机制，强化数据全生命周期安全保护措施；三是组织常态化监测预警与应急处置，涉及重要数据和核心数据安全事件的应第一时间进行上报；四是定期实施风险评估，及时发现整改风险问题，并按照要求上报风险评估报告。

七、企业如何按照《管理办法》开展重要数据识别和目录备案工作？

工业和信息化部结合国家数据安全保护要求和行业实际，组织制定工业和信息化领域重要数据和核心数据识别认定标准规范，明确识别规则和方法。数据处理者应当定期梳理本单位数据资源，按照所属行业标准规范识别重要数据后，向本地区行业监管部门备案重要数据目录。当备案内容发生重大变化后，数据处理者应当及时履行备案变更手续，保证目录备案的时效性、准确性与真实性。

八、《管理办法》对保障数据全生命周期提了哪些要求？

《管理办法》围绕数据收集、存储、使用、加工、传输、提供、公开等全生命周期关键环节，分别针对一般数据、重要数据、核心数据细化明确了安全保护要求，主要包括明确细化了协议约束、安全评估、审批等管理要求，以及校验与密码技术使用、数据访问控制等技术保护要求。

九、《管理办法》要求在哪些情形下需要开展数据安全风险评估？

《管理办法》明确重要数据和核心数据处理者每年至少完成一次数据安全风险评估，可以自行或委托第三方评估机构开展，及时整改风险问题，并向本地区行业监管部门报告。评估内容包括合规评估和风险研判：合规评估是指对标对表法律法规和政策文件，评估是否满足相关要求，风险研判是指通过分析数据处理者的安全保障能力、面临的威胁情况和发生安全事件后的影响程度等，评估数据处理活动的安全风险等级。

十、《管理办法》要求如何开展数据出境安全评估？

《管理办法》明确工业和信息化领域数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据，法律、行政法规有境内存储要求的，应当在境内存储，确需向境外提供的，应当依照《数据安全法》《数据出境安全评估办法》等法律法规进行安全评估。

十一、如何按照《管理办法》开展数据安全风险监测预警工作？

监测预警是有效发现和防范数据安全突出风险的重要工作。《管理办法》明确了“部-省-企业”三级联动协同的数据安全风险监测预警工作机制：一是工业和信息化部统筹指导行业数据安全监测预警工作，建设行业数据安全风险监测预警技术手段，统一汇集、研判、通报数据安全风险信息。二是地方行业监管部门负责建立本地区本领域数据安全监测预警机制，组织管辖范围内的数据处理者开展数据安全风险监测和信息报送。三是数据处理者做好本单位数据安全风险监测，按照行业监管部门要求开展风险监测排查，及时防范化解风险隐患。

十二、企业如何按照《管理办法》开展数据安全应急处置工作？

《管理办法》明确建立工业和信息化领域数据安全应急处置工作机制，细化不同主体的责任与义务：一是工业和信息化部统筹行业数据安全应急处置管理工作，制定数据安全事件应急预案，组织协调行业重要数据和核心数据安全事件应急处置工作；二是地方行业监管部门负责组织开展本地区数据安全事件应急处置工作，及时上报涉及重要数据和核心数据的安全事件；三是数据处理者制定本单位数据安全事件应急预案并定期开展应急演练，在发生数据安全事件后及时进行处置，并按要求及时向行业监管部门报告。

十三、《管理办法》对中央企业提出了哪些要求？

中央企业是国民经济的重要支柱和骨干力量，产生、汇聚了大量关系国计民生的重要数据。中央企业所属公司业务既受地方行业监管部门管理，也受集团公司管理。因此，《管理办法》对中央企业提出两项工作要求：一是督促所属公司按照属地行业监管部门要求，履行重要数据目录备案、风险信息上报等要求。二是做好集团本部数据安全保护工作，全面梳理汇总集团本部、所属公司相关情况，及时向工业和信息化部报送。

十四、下一步如何推进相关工作？

《管理办法》发布后，工业和信息化部将从政策宣贯、细则制定、正向引导、监督执法等方面抓好落实：一是加强宣贯培训。对《管理办法》的主要内容进行全面、系统解读，指导行业数据处理者准确理解、全面把握、认真落实相关要求，提升数据安全保护意识和能力。二是制定配套规范标准。重点推进监测预警、应急处置、安全评估等制度机制的实施细则，为企业进一步提供深入细致、操作性强的工作指引。三是加强正向引导。通过行业自律、贯标达标，典型案例遴选等形式，加强示范引领，引导企业自动对标管理要求，自觉提升数据安全保护能力。四是加强监督执法。通过专项行动、监督检查等工作，及时发现违法违规行为，并依法进行处罚。

压实终端生产企业主体责任 强化预置APP全链条管理

——《关于进一步规范移动智能终端应用软件预置行为的通告》解读

工业和信息化部信息通信管理局

- *针对移动智能终端预置APP行为，明确“谁预装、谁负责”和保障用户知情权、选择权等。*
- *明确预置APP的定义，针对移动智能终端预置APP能否卸载作出具体细化规定。*
- *要求生产企业提升终端产品安全性，进一步明确生产企业对预置APP的全链条管理责任。*
- *工业和信息化部会同国家互联网信息办公室加强对预置APP的监督检查和违规处理。*
- *要求生产企业提升终端产品安全性，避免在销售渠道被非法“刷机”、安装APP。*

近日，工业和信息化部、国家互联网信息办公室联合出台《关于进一步规范移动智能终端应用软件预置行为的通告》（以下简称《通告》）。为更好地理解和执行《通告》要求，工业和信息化部信息通信管理局对《通告》有关内容解读如下。

一、《通告》出台的背景和目的是什么？

2016年，工业和信息化部出台《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号），对移动智能终端预置、分发应用软件等行为加强监管，明确了只有预置的“基本功能软件”才可设为不可卸载等管理要求。该文件自2017年7月实施以来取得良好效果，有效规范了终端预置应用软件行为，有力保护了用户合法权益。

近几年，随着应用软件（APP）产业的迅猛发展和不断创新，为广大消费者提供了丰富多彩的互联网应用，便利了人民群众生产生活，但同时也出现了一些新情况、新问题，有必要在现有规定基础上，进一步明确和细化“不可卸载”预置APP的定义和范围，压实终端生产企业主体责任，强化预置APP全链条管理。

因此，为进一步规范移动智能终端APP预置行为，提升移动互联网服务供给水平，构建更加安全、更有活力的产业生态，营造更加放心的信息消费环境，工业和信息化部、国家互联网信息办公室联合发布本《通告》。

二、《通告》制定过程是什么样的？

2021年11月，工业和信息化部会同国家互联网信息办公室成立专项起草组，深入开展调研、座谈和论证工作，梳理工信部信管〔2016〕407号文件等有关规定的执行情况，分析当前移动智能终端预置APP方面存在的主要问题，听取移动互联网领域专家学者的意见建议，形成《通告》征求意见稿。后多次向移动智能终端生产企业、相关行业协会、专业机构征求意见，并于2022年2月中旬至3月上旬面向社会公开征求意见。在充分吸纳各方意见建议基础上，《通告》由工业和信息化部和国家互联网信息办公室联合发布公布实施。

三、《通告》的定位和主要内容是什么？

《通告》是在工信部信管〔2016〕407号文件确立的管理原则和各项要求基础上，对APP预置行为有关事项作出补充细化的具体规定。主要内容包括：

一是针对移动智能终端预置APP行为，提出“依法合规、用户至上、安全便捷、最小必要”的原则要求，明确“谁预装、谁负责”和保障用户知情权、选择权等标准。

二是明确预置APP的定义，针对移动智能终端预置APP能否卸载作出具体细化规定，即不可卸载的APP应限于系统设置、多媒体摄录、接打电话、应用商店等少数基本功能软件。

三是要求生产企业提升终端产品安全性，避免在销售渠道被非法“刷机”、安装APP。进一步明确生产企业对预置APP的登记、审核、监测、留存、下架等全链条管理责任。

四是工业和信息化部会同国家互联网信息办公室加强对预置APP的监督检查和违规处理。

四、《通告》所称“移动智能终端”的范围是什么？

工信部信管〔2016〕407号文件规定，移动智能终端是指接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

根据移动智能终端和预置APP的监管实践和用户实际使用需求，《通告》所称“移动智能终端”范围，主要包括接入公众移动通信网络的智能手机、平板电脑、可穿戴设备等大众消费类通信终端产品，不含工业终端、车载终端等面向特定行业和用途的数据终端，也不含未接入公众移动通信网络的智能终端产品。

五、《通告》限定的基本功能软件范围和主要考虑是什么？

工信部信管〔2016〕407号文件规定，移动智能终端的基本功能软件是指保障移动智能终端硬件和操作系统正常运行的应用软件，主要包括操作系统基本组件、保证智能终端硬件正常运行的应用、基本通信应用、应用软件下载通道等。

《通告》在现有规定基础上，按照“最小必要”原则，进一步明确每一类基本功能软件包含的具体APP类型，既充分保障用户能够正常使用终端产品，又最大限度的压缩不可卸载APP的范围，维护用户知情权和选择权。

六、《通告》对于终端安全管理有哪些要求和考虑？

由于移动智能终端允许用户自行安装和卸载APP，在产品流通过程中就有可能会被非法“刷机”，包括被更换操作系统或安装一些非法的APP。为避免“刷机”带来的安全风险，保护用户权益，《通告》要求生产企业完善移动智能终端权限管理机制，提升操作系统安全性，采取技术和管理措施预防“刷机”行为。

七、下一步如何抓好《通告》贯彻落实？

《通告》发布后，工业和信息化部将从政策宣贯、标准修订、强化监管、促进发展等方面抓好落实。一是加强宣贯落实，做好政策解读，加强移动智能终端预置APP管理相关工作指导，组织生产企业将《通告》各项要求及时落实到位。二是同步修订配套的标准规范。组织修订完善《移动智能终端预置应用软件分类与可卸载实施指南》等配套标准规范，强化标准引领，切实抓好《通告》贯彻落实。三是完善APP全链条监管体系，在APP预置和分发等环节共同发力，加强进网环节对预置APP的安全检测，持续强化APP管理，促进移动互联网和智能终端产业安全、有序、健康发展。