CAICT 中国信通院

政务数据共享开放安全研究报告

中国信息通信研究院安全研究所

2021 年 1 月

版权声明

本报告版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。

前　言

政务数据是政府部门满足经济社会治理需求，履行职能过程中产生或使用的重要资源，蕴藏着难以估量的经济发展、社会运行以及国家战略价值。近年来，我国政府高度重视政务数据共享开放的促进与发展，在大力推动政务数据共享开放的同时，数据安全作为数据共享与开放的核心基础也倍受关注，相关法律法规逐步完善。

2020 年 4 月，中共中央、国务院发布《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》，提出要推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。《中华人民共和国数据安全法（草案）》于 2020 年 6 月 28 日在第十三届全国人大常委会第二十次会议审议，其中第五章对政务数据安全与开放予以规制。

我国政府逐步从“政府信息公开”向“政府数据开放”探索前进，各地政务数据向社会公众开放的进程逐步加快，随着新兴技术快速发展、应用场景迅速扩展、安全形势不断变化，在数据成为社会发展关建变量的同时，政务数据作为重要的生产要素，也面临着安全挑战。

报告全文从对政务数据共享开放的认识出发，介绍了国际政务数据共享开放形势及安全实践经验，对我国政务数据共享开放的发展现状及存在的问题进行了分析和分享。在此基础上研究分析政务数据共享开放发展面临的挑战因素，以及数据存储加工、数据共享

开放、共享交换平台三个维度潜藏的安全风险。进一步，给出了政务数据共享开放的安全框架。最后，从政策标准、监管机制、技术能力、人才队伍几方面提出相关建议。

本报告的编制过程中，得到了来自全知科技（杭州）有限责任公司、深圳市网安计算机安全检测技术有限公司的技术支持，特此，向支持、参与本报告编制工作的相关人员表示感谢。

CAICT 中国信通院

目 录

一、对政务数据共享开放的认识.....1
（一）政务数据共享开放和数据安全受到高度重视.....1
（二）以“政务数据、公共数据”替代“政务信息资源”的趋势十分明显.2
（三）政务数据共享开放过程中的数据权属变化成为关注要点.....3
二、国际政务数据共享开放形势及安全实践.....4
（一）美国发布联邦数据战略，确立政府范围内数据共享开放和数据安全的框架原则.....5
（二）美国建立受控非密信息安全管理体系，严格管控敏感信息.....6
（三）欧盟致力于在内部建立安全、高效的政务数据共享开放体系.....7
（四）爱尔兰为政务数据共享开放提供战略引导和安全保障.....8
三、我国政务数据共享开放发展现状及存在问题.....9
（一）发展现状.....9
1、政策法规和标准体系建设步伐全面加快.....9
2、政务数据与社会数据对接融合逐步加深.....11
3、全国建设结合地方特点趋向精细化发展.....12
（二）存在的问题.....15
1、数据权责难以界定.....15
2、发展进程存在差异.....15
3、政企数据融合不足.....16
4、安全防护有待加强.....17
5、人才队伍面临缺口.....17
四、 政务数据共享开放发展面临的挑战及安全风险.....18
（一）面临的挑战.....18
1、政务数据大量汇聚，容易成为攻击目标.....18
2、共享开放环节复杂，数据流动潜藏风险.....18
3、新兴技术快速发展，催生多种攻击手段.....19
（二）安全风险.....20

1、数据存储加工风险.....20
2、数据共享开放风险.....20
3、共享交换平台风险.....21
五、政务数据共享开放的安全框架.....21
（一）政务数据共享开放安全原则及发展理念.....21
1、安全原则.....21
2、发展理念.....22
（二）安全框架.....23
1、数据生命周期.....24
2、数据安全技术.....26
3、数据业务活动.....29
4、安全管理体系.....30
5、安全运维体系.....32
六、相关建议.....33
（一）完善法律法规，加快标准研制.....33
（二）健全管理机制，形成监管闭环.....34
（三）聚焦数据核心，提升技术能力.....34
（四）提高思想认识，培养复合人才.....35

图 目 录

图 1　美国联邦数据战略行动计划（2020）.....5
图 2　政务数据共享开放安全发展理念.....22
图 3　政务数据共享开放安全框架.....23
图 4　政务数据生命周期安全要点.....24
图 5　政务数据共享开放业务流程.....29

CAICT 中国信通院

表 目 录

表 1　国家重要文件（部分）相关概念.....3
表 2　政务数据安全主要国家标准及研究项目.....10
表 3　地方大数据管理机构（部分）.....12
表 4　部分省市共享开放平台数据统计.....14

CAICT 中国信通院

一、对政务数据共享开放的认识

（一）政务数据共享开放和数据安全受到高度重视

数据安全是国家最重要的战略安全之一，也是数据共享开放的核心基础。近年来，我国政府高度重视数据安全和政务数据共享开放。早在2015年8月31日，国务院印发的《促进大数据发展行动纲要》中就提出要“加快政府数据开放共享，推动资源整合”，“大力推动政府信息系统和公共数据互联开放共享，加快政府信息平台整合，消除信息孤岛，推进数据资源向社会开放。”2020年，中共中央、国务院先后两次发布重要文件，数据首次被正式纳入生产要素范围。《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》提出，要推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护，并强调引导培育大数据交易市场。《中共中央、国务院关于新时代加快完善社会主义市场经济体制的意见》中提出，要加强数据资源整合和安全保护，制定数据隐私保护制度和安全审查制度，推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。

在大力推动政务数据共享开放的同时，数据安全的重要性愈发突出，数据安全相关法律法规逐步完善。在数据安全方面，《网络安全法》[1]主要在“数据存储与跨境安全”“数据（信息）内容安全”和“数据系统、平台、设施安全”等方面予以规制。《数据安全法（草

[1] 《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，自2017年6月1日起施行。

案）》[2]提出“鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展”，其中第五章对政务数据安全与开放提出了具体要求。2020 年 10 月 21 日，全国人大法工委公开就《中华人民共和国个人信息保护法(草案)》征求意见，《草案》对国家机关处理个人信息作出了特别规定，明确国家机关履行法定职责处理个人信息应当承担的保护义务和责任。另外，《数据安全管理办法》、《个人信息和重要数据出境安全评估办法》等部门规章也在制定中，并已公开征求意见。

（二）以“政务数据、公共数据”替代“政务信息资源”的趋势十分明显

在早期政策文件中，“政务信息资源”[3]概念的使用较为常见，随着时间的推移，特别是近年来数字经济的快速发展，以“数据”（政务数据、公共数据）替代“信息”（政务信息资源、公共信息资源）的趋势已经十分明显。从国家已出台的重要政策文件来看，政务信息资源、公共信息资源、政务数据（资源）、政府数据、公共数据（资源）等概念均在使用，而政务信息资源、公共信息资源使用较少。在具体执行层面，“政务信息”与“政务数据”的定义及内涵基本一致。并且，为了推动社会需求较大的医疗、金融等应用领域的数据开放，部分地区将具有公共服务职能的事业单位数据一并纳入政务数据管理要求。

[2] 《中华人民共和国数据安全法》（草案）6 月 28 日在第十三届全国人大常委会第二十次会议审议。
[3] 政务信息资源，是指政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源。

表 1 国家重要文件（部分）相关概念

序号	发布时间	文件名称	相关概念
1	2015 年 8 月	《国务院关于印发促进大数据发展行动纲要的通知》国发〔2015〕50 号	政府数据、公共数据资源
2	2016 年 9 月	《国务院关于印发政务信息资源共享管理暂行办法的通知》（国发〔2016〕51 号）	政务信息资源
3	2017 年 3 月	中共中央办公厅、国务院办公厅《关于推进公共信息资源开放的若干意见》	公共信息资源
4	2017 年 12 月	习近平总书记主持中共中央政治局第二次集体学习	政务数据资源
5	2020 年 3 月	《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》（中发〔2020〕9 号）	政府数据、公共数据
6	2016 年 12 月	工业和信息化部关于印发《大数据产业发展规划（2016－2020 年）》的通知（工信部规〔2016〕412 号）	公共数据资源、政府数据
7	2019 年 8 月	科技部关于印发《国家新一代人工智能创新发展试验区建设工作指引》的通知（国科发规〔2019〕298 号）	公共数据
8	2019 年 10 月	国家发展改革委 中央网信办关于印发《国家数字经济创新发展试验区实施方案》的通知（发改高技〔2019〕1616 号）	政务数据、公共数据

来源：公开资料整理

（三）政务数据共享开放过程中的数据权属变化成为关注要点

数据作为生产要素转化为新型生产力尚处于初级阶段，数据资源的应用方式、管理模式、组织机制、运营环境等生产关系的调整仍有待探索，政务数据在共享开放过程中的属性变化也是关注重点。导致其属性发生变化的因素主要包括，一是政务数据流动引发的变化，当前涉及政务数据的活动较为普遍，政务数据在多个业务和应用场景下

流动交互；二是安全域的变化，在政务数据共享开放过程中，数据会跨越不同组织、机构、层级的安全域使用；三是政务数据存储的变化，原有场景下政务数据固化在各部门安全域中，存储较为分散，共享开放推动政务数据大量汇聚、集中存储；四是政务数据主体的变化，政务数据多方交互，数据提供者、使用者在交互过程中也发生着主体角色变化；五是政务数据共享开放对象的变化，政务数据随着业务流程、应用场景的变化，共享开放的领域不断扩展，使用、获取政务数据的群体同步扩大。

二、国际政务数据共享开放形势及安全实践

伴随全球政务数字化与电子政务平台建设的深入发展，政务数据安全已成为无法回避的核心议题。联合国经济和社会事务部（UNDESA）出版的《2018 年电子政务调查报告》指出，2014 年以来，联合国 193 个会员国已全部实现某种形式的政务信息数字化。电子政务的普及，在为政企、公众带来便利的同时，其数据流转、处理、应用中的安全压力也与日俱增。针对政务信息系统、政务数据的安全威胁不断升级，威胁态势日益严峻，欧美国家作为电子政务和数据共享开放的先行者，在相关制度设计、管理体系、安全技术等方面遭遇的问题、困难及优秀应对案例，对我国推广政务数据共享开放、保护政务数据安全具有一定借鉴意义。

（一）美国发布联邦数据战略，确立政府范围内数据共享开放和数据安全的框架原则

2019 年 12 月 23 日，美国白宫行政管理和预算办公室(OMB)发布《联邦数据战略与 2020 年行动计划》，描述了美国联邦政府未来十年的数据愿景，并初步确定了各政府机构的关键行动。

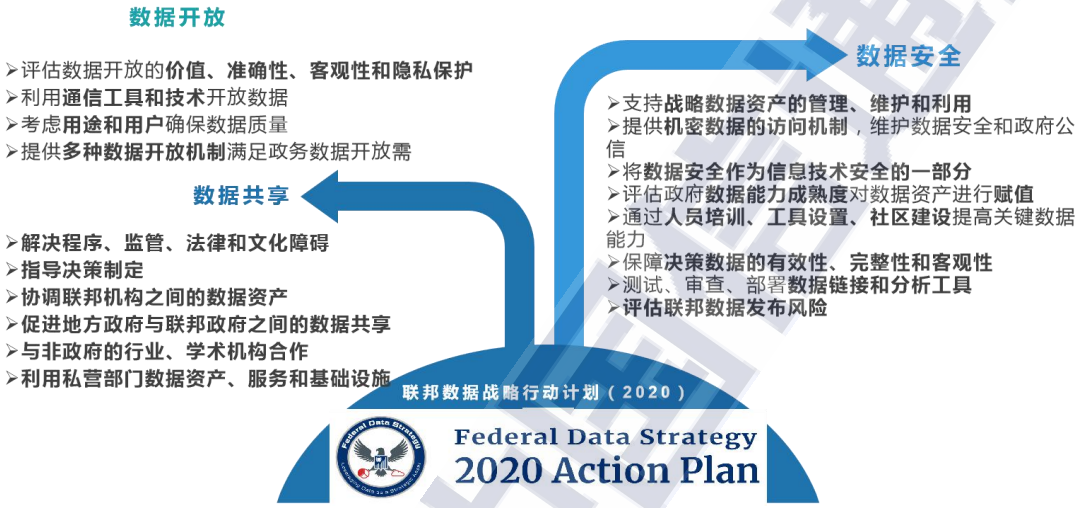


图 1 美国联邦数据战略行动计划（2020）

在政务数据共享方面，该行动计划要求政府消除程序、监管、法律和文化上的障碍，与非政府行业、学术机构合作，提高数据可用性和质量，协调联邦机构之间的数据资产，推进数据在政府机构间以及不同机构间的共享。在此基础上，政府各部门充分利用数据价值，指导决策制定，提高政府机构透明度、公信力。同时，促进地方政府与联邦政府之间的数据共享，并提供相应安全措施保护数据安全，合理利用私营部门数据资产、服务和基础设施，提高政务数据共享开放效率，降低成本。

在政务数据开放方面，该行动计划要求联邦政府定期评估公众对联邦数据开放的价值、准确性、客观性和隐私保护的信心，有效利用

通信工具与技术，在充分考虑数据用途及用户、确保政务数据质量的前提下，广泛开放政务数据。此外，要求政府在满足政务数据开放需求与数据可用性的同时，保护数据的隐私、机密性和各方利益。

在政务数据安全方面，该行动计划要求对国家战略数据资产进行有效的管理、维护和利用。一是将数据安全保障视为政府信息安全的重要组成部分，提供安全的数据访问机制，评估政府机构数据能力成熟度，维护高完整性、高质量的政务数据资产。二是对数据资产进行赋值，优化资源决策，通过人员培训、工具建设等手段提升数据分析、评估等关键数据活动的能力。三是保障重要公共或私营部门决策数据的有效性、完整性和客观性，测试、审查、部署安全可靠的数据传输通道，并评估联邦数据发布风险，降低脱敏数据重新识别等风险，确保政务数据的安全共享开放。

（二）美国建立受控非密信息安全管理体系，严格管控敏感信息

2010 年 11 月，时任美国总统奥巴马签署第 13556 号行政命令，建立和实施受控非密信息登记备案及标识管理制度，对政府数据中非个人数据、非国家秘密信息实施安全管理，并以法律法规形式加以固化，形成美国受控非密信息（Controlled Unclassified Information，CUI）安全管理体系。该体系由信息安全监督办公室及国家档案和记录管理局牵头，在联邦规章中明确给出实施办法，并被纳入美国联邦法规国防事务范畴，包括 8 项核心机制：数据注册、数据类别和子类别分类、安全保障措施、访问和传播控制措施、解除控制规范、数据标记机制、

机构政策适用性限制、机构自查程序。

目前，CUI 安全管理体系主要被用于识别各政府部门中需要保护或进行传播控制的非机密信息，美国政府 CUI 按数据涉及的领域分为 20 类、124 子类，根据其类型、内容、涉及机构等进行标记，分为禁止国外传播、仅联邦雇员、仅联邦雇员及承包商等，满足政务数据的传播管控。此外，美国国家标准与技术研究院（NIST）还制定了非联邦系统和机构 CUI 保护标准，将 CUI 扩大到了非联邦范围，并针对关键程序和高价值的受控非密信息提出安全控制措施，以保护 CUI 的机密性和完整性，通过访问控制、安全培训、审计核查等方式，建立严格的 CUI 数据安全防护体系。

（三）欧盟致力于在内部建立安全、高效的政务数据共享开放体系

近年来，欧盟将数据定位为其数字化转型的核心，以数据驱动改善政府政策制定和公共服务。自 2016 年颁布《通用数据保护条例》（GDPR）以来，各成员国结合 GDPR 要求，逐步加强政务数据、公共数据及个人信息的保护，致力于政务数据的安全开放、共享。

2020 年 2 月，欧盟发布《塑造欧洲的数字未来》《欧洲数据战略》和《人工智能白皮书》三篇通讯，旨在通过完善数据可用性、数据共享、网络基础设施、研究和创新投资等，助力欧盟完成数字单一市场构建。战略关注三大数据共享开放模式，一是政府向企业公开数据（G2B），在公共政策评估框架内开放政府数据供企业、公众使用。二是私营部门间私有数据共享（B2B），通过立法等手段，明确各方

权责，鼓励企业间数据共享。三是企业向政府开放数据（B2G），建立数据共享框架，鼓励企业向政府开放数据，提高政府决策能力。此外，欧盟一方面通过《通用数据保护条例》建立数字信任框架，审核、监督相关框架实施，另一方面依托《网络安全法案》（CSA）和《开放数据指令》等立法，强化数据开放共享安全，致力于在欧盟内部建立安全、高效的政务数据共享开放体系。

（四）爱尔兰为政务数据共享开放提供战略引导和安全保障

作为欧盟成员国的爱尔兰在电子政务建设、公共信息共享开放领域已拥有一定基础。在制度设计上，通过结合欧盟 GDPR 相关要求，爱尔兰颁布《数据保护政策 2020》（Data Protection Policy），对包括政务信息在内的公共数据安全保护提出要求，明确相关责任机构及职责。其中爱尔兰公共支出和改革部负责制定开放数据政策及国家开放数据门户建设，向公众提供政务数据的访问。截止 2020 年 6 月，该门户已涵盖 1 万多个数据集，提供各类已经获得开放许可的政务数据。此外，爱尔兰政府在其《2017-2022 年开放数据战略》中明确提出两大战略：一是增加高价值政府数据的发布。二是促成与相关行业、社区等合作，发挥数据社会和经济价值，推动数据利用。同时，爱尔兰政府主导成立开放数据治理委员会和公共机构咨询小组，指导政务数据共享开放工作。其中开放数据治理委员会根据国际最佳实践对政务数据共享开放建设提供战略引导，监督数据开放战略的实施。公共机构咨询小组则提供相关技术建议，设计技术框架，明确技术要求，

确保已发布的数据集符合标准，保障开放数据的安全性、可访问性和可利用性。

三、我国政务数据共享开放发展现状及存在问题

（一）发展现状

1、政策法规和标准体系建设步伐全面加快

在政策法规方面，自 2015 年 8 月《国务院促进大数据发展行动纲要》出台以来，中央和各部委发布了多份提及政务数据共享开放的重要文件，如《关于推进公共信息资源开放的若干意见》、《数字经济发展战略纲要》、《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》等。特别是《政务信息资源共享管理暂行办法》[4]、《政务信息系统整合共享实施方案》[5]、《政务信息资源目录编制指南（试行）》[6]三份重要文件，不仅明确了政务数据共享的原则，也为信息系统整合实施和标准体系建设提供了引导。

此外，2020 年公布的《数据安全法（草案）》明确提出“提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力”；“建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全”；“国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据”；“制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务

[4] 国务院关于印发政务信息资源共享管理暂行办法的通知（国发〔2016〕51 号）
[5] 国务院办公厅关于印发政务信息系统整合共享实施方案的通知（国办发〔2017〕39 号）
[6] 国家发展改革委 中央网信办关于印发《政务信息资源目录编制指南（试行）》的通知（发改高技〔2017〕1272 号）

数据开放利用”。

在标准规范方面，政务数据相关国家标准和地方性标准规范陆续启动研制工作，并取得一定成效。2020 年 6 月，《国家电子政务标准体系建设指南》正式出台，在政务数据共享开放标准子体系中明确建设重点包括数据安全等政务数据管理标准。部分地区在推动数据共享开放工作中制定相关标准，明确共享开放数据范围，并将落实数据分类分级作为确保数据安全的第一步，为政务数据共享开放和安全防护提供指引。

贵州省率先制定发布了《政府数据 数据分类分级指南》，在全国做到了先试先行,指南为贵州省政府部门在共享和开放政府数据时恰当分类和定级提供参考，是对政府数据实施有效有序管理的大胆尝试。实施数据分类分级有利于按类别正确开发利用政府数据，实现政府数据价值最大化。

表 2 政务数据安全主要国家标准及研究项目

研制方向	标准规范名称	标准号
元数据	电子政务数据元 第 2 部分：公共数据目录	GB/T 19488.2-2008
信息资源目录	政务信息资源目录体系 第 1 部分：总体框架	GB/T 21063.1-2007
	政务信息资源目录体系 第 2 部分：技术要求	GB/T 21063.2-2007
	政务信息资源目录体系 第 3 部分：核心数据	GB/T 21063.3-2007
	政务信息资源目录体系 第 4 部分：政务信息资源分类	GB/T 21063.4-2007
	政务信息资源目录体系 第 5 部分：政务信息资源标识符编码方案	GB/T 21063.5-2007
	政务信息资源目录体系 第 6 部分：技术管理要求	GB/T 21063.6-2007

开放共享	政务信息资源交换体系 第 1 部分: 总体框架	GB/T 21062.1-2007
	政务信息资源交换体系 第 2 部分: 技术要求	GB/T 21062.2-2007
	政务信息资源交换体系 第 3 部分: 数据接口规范	GB/T 21062.3-2007
	政务信息资源交换体系 第 4 部分: 技术管理要求	GB/T 21062.4-2007
	信息技术 大数据政务数据开放共享第 1 部分: 总则	GB/T 38664.1-2020
	信息技术 大数据政务数据开放共享第 1 部分: 基本要求	GB/T 38664.2-2020
	信息技术 大数据政务数据开放共享第 1 部分: 开放程度评价	GB/T 38664.3-2020
	政务信息资源共享评价指标	20190842-T-469
安全管理	信息安全技术 基于互联网电子政务信息安全实施指南 第 1 部分: 总则	GB/Z 24294.1-2018
	信息安全技术 基于互联网电子政务信息安全实施指南 第 2 部分: 接入控制与安全交换	GB/Z 24294.2-2017
	信息安全技术 基于互联网电子政务信息安全实施指南 第 3 部分: 身份认证与授权管理	GB/Z 24294.3-2017
	信息安全技术 基于互联网电子政务信息安全实施指南 第 4 部分: 终端安全防护	GB/Z 24294.4-2017
	基于云计算的电子政务公共平台安全规范 第 2 部分: 信息资源安全	GB/T 34080.2-2017
	政务信息共享 数据安全技术要求	20190907-T-469
	信息技术大数据 数据分类指南	GB/T 38667-2020
	政务信息资源安全分级指南	研究项目

来源: 公开资料整理

2、政务数据与社会数据对接融合逐步加深

随着我国经济形态由工业经济、后工业经济向数字经济迈进，在政务数据共享开放的发展趋势下，政务数据与社会数据对接融合的种类数量、对接程度、应用领域、价值实现不断扩张。进入数字经济时代，多源异构数据呈指数级增长，政府难以独立处理海量政务数据，而企业具有相对丰富的数据处理分析经验。通常先对政务数据进行脱敏，再借助企业技术与能力进一步分析利用，并为政府提供决策支撑。

政企数据对接具有企业深度参与、数据双向融合流动的特点，其对接模式主要包括以行政方式对接、以接口方式融合应用、通过模型算法融合应用、数据以抽象化的特征形式融合应用四种模式。其中，通过模型算法融合应用的模式在政务数据与社会数据对接中具有明显优势，这种模式下共享的既不是原始数据，也不是脱敏数据，而是对数据进行处理的模型算法，不易导致数据或隐私泄漏。

3、全国建设结合地方特点趋向精细化发展

（1）管理机制

2017 年以来，多个省市设立了省级层面和地市级层面的大数据管理机构，机构形式包括大数据管理局、大数据发展管理局、大数据管理中心等，承担起城市数据的收集、汇总和管理工作，通过体制转变实现数据资源的统一管理，归集管理政务民生数据。

表 3 地方大数据管理机构（部分）

序号	单位名称	隶属机构
1	北京市经济和信息化局 （北京市大数据管理局）	北京市人民政府

2	天津市大数据管理中心	中共天津市委网络安全和信息化委员会办公室
3	内蒙古自治区大数据发展管理局	内蒙古自治区人民政府
4	辽宁省信息中心	辽宁省人民政府
5	吉林省政务服务和数字化建设管理局	吉林省人民政府
6	上海市大数据管理中心	上海市人民政府
7	江苏省大数据管理中心	江苏省政务服务管理办公室
8	浙江省大数据发展管理局	浙江省人民政府
9	安徽省数据资源管理局	安徽省人民政府
10	福建省数字福建建设领导小组办公室（省大数据管理局）	福建省人民政府
11	山东省大数据局	山东省人民政府
12	河南省大数据管理局	河南省人民政府
13	湖北省政务管理办公室	湖北省人民政府
14	广东省政务服务数据管理局	广东省人民政府
15	广西壮族自治区大数据发展局	广西壮族自治区政府
16	海南省大数据管理局	海南省人民政府
17	重庆市大数据应用发展管理局	重庆市人民政府
18	四川省大数据中心	四川省政府
19	贵州省大数据发展管理局	贵州省人民政府
20	云南省数字经济局	云南省政府
21	陕西省工业和信息化厅（省政务数据服务局）	陕西省人民政府

来源：公开资料整理

在中央政策的引导下，各地陆续推动地方性政务数据、公共数据共享开放有关政策的研究制定，部分地区启动具有针对性的目标规划，地方性数据共享开放政策整体走向精细化。

2019 年 8 月 16 日，上海出台国内首部公共数据开放管理暂行办法《上海市公共数据开放暂行办法》，促进和规范本市公共数据开放和利用，提升政府治理能力和公共服务水平，推动数字经济发展，《办法》于 10 月 1 日起执行。

2020 年 6 月 17 日，浙江省正式公布《浙江省公共数据开放与安

全管理暂行办法》，规范和促进本省公共数据开放、利用和安全管理，加快政府数字化转型,推动数字经济、数字社会发展。

2020 年 9 月 11 日，重庆市发布《重庆市公共数据开放管理暂行办法》，旨在促进和规范公共数据开放和利用，提升政府治理能力和公共服务水平，推动数字经济高质量发展。

2020 年 9 月 25 日，《贵州省政府数据共享开放条例》经贵州省第十三届人民代表大会常务委员会第十九次会议通过，自 2020 年 12 月 1 日起施行，提出推动政府数据共享开放，加快政府数据汇聚、融通、应用，培育发展数据要素市场，提升政府社会治理能力和公共服务水平，促进经济社会发展。

（2）平台建设

2018 年 1 月，中央网信办、国家发改委、工信部联合印发《公共信息资源开放试点工作方案》，在北京、上海、浙江、福建、贵州五地首先开展公共信息资源开放试点。陆续有多个省市自治区结合当地特色，启动省市平台互通和省直部门接入工作，并实现与国家平台对接，上海、浙江等十余个省级政府数据共享交换、数据开放平台已搭建完成。

表 4 部分省市共享开放平台数据统计[7]

省市	开放部门	资源	数据集	数据项	数据量	API
北京	69	-	4,539	-	16.9 亿	-
上海	98	-	3,639	35,625	97,911,040	1,689
天津	52	-	606	-	-	586
福建	48	705	-	-	61077.98 万	1,331

[7] 表内统计数据截至 2020 年 7 月

四川	47	6,455	-	-	95,911,653	-
浙江	-	-	7,292	33,041	70218.84 万	3,692
深圳	45	-		22,165	274,413,171	2009
哈尔滨	46	-	1,112	-	5,755,091	2,320
佛山	49	-	1,068	-	42,671,557	
珠海	40	430	371	-	-	491
广州	62	-	1,474	-	122,630,383	-

来源：公开资料整理

其中，上海已开放的 3600 余项公共数据集基本覆盖各市级部门的主要业务领域，通过行业数据融合赋能，重点聚焦金融、医疗、旅游、交通、能源、城市管理和开放数据等领域，汇聚产学研用多方主体和数据资源。

（二）存在的问题

1、数据权责难以界定

政务数据整合、共享、交换过程中，存在多部门、多主体（数据提供方、数据共享交换服务方和数据使用方）参与，数据在不同主体之间流动。一方面，在各个应用场景下，数据权益归属存在差异，难以事先抽象约定数据权益归属，从而存在权属关系不明确、职责分工模糊、安全措施不完备的现象；另一方面，共享标准不统一，部分主体共享意愿不强，共享数据的权威性、规范性不足，难免出现源头数据质量不高、责任划分不清、权限难以控制、数据溯源困难等问题。

2、发展进程存在差异

政务数据共享开放起步以来，整体政策制度尚不完善，各地推进

步调不一致，思想认识不统一，各地大数据机构设置多元化，运行机制各有差异。面对政务数据流通规模庞大、应用领域广泛、涉及技术复杂、需要全面监管的特征，管理机制上下不联、横向不通，政务信息系统烟囱林立、条块分割、重复建设等问题还依然存在，跨部门、跨系统、跨区域统筹协调难度依然很大，难以形成整体合力。在政策法规方面，地方涉及政务数据开放的政策以倡导性、计划性居多，部分地区尚未专门针对政务数据共享开放制定政策，未统一标准要求；在平台建设方面，除基础功能外，各地在数据分类维度、数据下载格式、接口服务标准等方面各不相同；在开放内容方面，地方政府提供的数据内容多以本级政府所管辖的政务数据为主。

3、政企数据融合不足

打造数字政府、建设智慧城市和发展数字经济都离不开政务数据和社会数据的开发利用及价值激活。然而，由于两类数据的主体性质不同、利益不同、数据类型不同等因素，部分数据主体共享意愿不强，导致政务数据和社会数据对接机制缺失、对接范围不广、对接数据不足、融合应用不深等问题存在，制约了政务数据与社会数据共享利用。另外，各级政府通过平台共享开放的多为公益类数据，涉及领域较为单一，一些垂直领域数据以及跨部门数据的开放数量和质量不能满足社会需求，企业及社会难以获取真正需要的数据进而有效开发利用。我国政务数据与社会数据共享利用的潜在价值尚未完全激活。

4、安全防护有待加强

政务数据在各单位之间流动、共享和开放，业务数据不仅存在于数据区域、业务区域、终端区域，还进一步流出到外网，数据安全防护需求随之动态变化。同时，政务数据共享交换使得数据资产集中存储和管理，大量分散的、结构化和非结构化的数据汇集到共享交换平台，由于各地、各部门政务数据标准不一致，属性不同，数据分类分级等安全策略有待落实，难以进行有效管控。政务数据共享开放对安全防护技术提出了更高的要求，如果对数据识别不清、安全级别判断不足，易发生数据源伪造、传输数据遭窃听篡改、数据非授权使用、数据共享外发泄露等问题。

5、人才队伍面临缺口

据研究，截至2017年底，我国大数据技术人才缺口超过150万[8]，随着数据海量增长，数据开发利用的广度和深度同步扩展，应用场景愈加广泛，专业人才供不应求，尤其缺乏兼具技术能力与行业经验的复合型人才。目前政务数据应用存在数据与业务“两张皮”、数据开发利用深度不够、开放认识不足等问题，导致在政务数据与社会数据融合过程中，难以有效统筹协调政府与企业、社会的关系，相关政策落实有一定难度。要在实际应用中把握政务数据共享开放尺度、与社会数据的融合模式、数据生命周期的安全保障等要素，不管是在组织管理方面、还是技术层面，亟需既懂政府又懂市场、既懂业务又懂数

[8] 清华经管互联网发展与治理研究中心和LinkedIn(领英)联合发布《中国经济的数字化转型：人才与就业——中国数字人才现状与趋势研究报告》

据的复合型人才。

四、政务数据共享开放发展面临的挑战及安全风险

政务数据是政府部门进行社会治理的重要记录与呈现，蕴藏着难以估量的政治、经济、科学、文化和社会价值，在国民经济建设和国家安全战略体系中的地位日益凸显。在政府职能转变和产业转型发展的背景下，我国政府逐步从“政府信息公开”向“政府数据开放”探索前进，随着各地政府数据向社会公众开放的步子加快，数据作为重要资产，在成为发展新变量的同时，也面临严峻的安全挑战。

（一）面临的挑战

1、政务数据大量汇聚，容易成为攻击目标

在我国数字经济发展和数字政府建设过程中，政务数据进行大规模的整合存储，涉及公民、企业、政府部门、社会组织有关社保、户籍、疾控、政策等领域个人敏感信息和重要数据，甚至涉及国家战略数据。在大量政务数据汇聚发挥数据价值的同时，也更容易成为攻击目标，这些数据一旦泄露，对个人而言可能致使隐私曝光、经济受损，导致企业核心经营数据和商业秘密外泄，更可能对政府调控、决策治理造成严重影响。数据主管部门和数据提供者、使用者承担着更大的安全管理责任，面临着更高的安全风险。

2、共享开放环节复杂，数据流动潜藏风险

政务数据共享开放使得数据流动成为常态，多环节的信息隐性留

存，数据流转环境复杂，数据泄露风险增大。一方面，政务数据在各政府机构、部门之间流动、共享和交换，系统和数据安全的责权边界变得模糊，主体责任划分不清，权限控制不足，发生安全事件难以追踪溯源；另一方面，政务数据对外开放，原本的边界安全机制无法有效保护流转到边界外的数据，基于边界的安全管理和技术措施，已经无法适应当前的安全需要。如何适应不断变化的安全管控需求，防止数据在流动过程中不被非法复制、传播、篡改、甚至泄露，成为一大挑战。

3、新兴技术快速发展，催生多种攻击手段

大数据、人工智能等技术的发展催生出新型攻击手段，攻击范围广、命中率高、潜伏周期长，针对大数据环境下的高级可持续攻击（APT）通常隐蔽性高、感知困难，使得传统的安全检测、防御技术难以应对，无法有效抵御外界的入侵攻击。目前数据平台大多基于Hadoop 框架进行二次开发，安全机制有所缺失，通常借助在网络边界部署防火墙、IPS、IDS 等安全设备，以流量分析和边界防护的方式提供保护。政务网具有网络节点多、业务系统多、数据资源多的特点，各类政务数据安全保护机制不尽相同，系统安全防护水平参差不齐，接入平台后使得整体安全薄弱点增多。出于网络结构日趋复杂、应用系统和安全建设分期投入等现实情况，安全防护能力跟不上政务数据共享开放的发展需求，安全风险持续增加。

（二）安全风险

政务数据面临的安全风险涉及各业务部门、系统中数据流转的全过程，与数据生命周期息息相关。在政务数据共享开放过程中，安全风险因素主要潜藏于数据存储加工、数据共享开放、以及共享交换平台环节。

1、数据存储加工风险

在政务数据跨部门、跨行业融合利用过程中，各个应用场景下需要收集多方的数据，集中存储，进行加工处理后使用，由于各行业标准的不同，在涉及多个领域政务数据时难以统一管控。部分重点领域和行业已经形成个人信息分类分级方法或指引，但符合行业特点的重要数据分类分级标准或指南尚未形成，部分领域未制定数据分类分级安全技术要求。另外，不同行业、不同分类数据的差异化保护要求存在落实困难，难以全面覆盖，使得部分数据缺乏有效的安全防护，容易造成数据的非授权访问等风险发生。

2、数据共享开放风险

数据共享开放扩大了数据访问的范围，政务数据资源跨部门、跨领域共享使用，不免被各方调取、使用、或存储到本地，存在共享管理责任不明确、数据超范围共享、扩大数据暴露面等安全风险和隐患。相关部门可能出现单纯从业务视角出发，未针对应用场景充分识别、评估影响，未对照法律法规和技术标准逐一梳理共享开放要求的情况，任何一个数据使用方未按照要求共享开放数据、未严格控制数据

共享范围、或防护措施不当，都可能导致数据未按照预设规则被访问、使用，进而引发数据泄露或滥用事件，使得个人隐私、企业利益乃至国家安全受到影响。

3、共享交换平台风险

政务数据共享交换平台作为政务数据汇聚的中心，不管是经济还是战略层面都具有极大价值，成为备受关注的攻击目标。共享交换平台通常采用分布式部署，大范围互联互通，涉及的软硬件较多，任何关键节点遭受故障或攻击，都可能导致整体安全出现问题。攻击者可以从防护能力薄弱点着手突破，通过破坏计算节点、篡改传输数据和渗透攻击，最终达到破坏或控制整个系统的目的。用户或管理终端也可能成为攻击共享交换平台的跳板，如果终端身份认证和访问控制系统防护不足，容易被攻击者非法获取共享交换平台以及政务信息系统的高级权限，进行非法数据操作。

五、政务数据共享开放的安全框架

（一）政务数据共享开放安全原则及发展理念

1、安全原则

在政务数据的共享开放中，建议遵循以下安全原则。

以共享为原则，不共享为例外。各政务部门形成的政务数据资源原则上应予以共享，涉及国家秘密和安全的，按相关法律法规执行。

需求导向，明确要求。因履行职责需要共享数据的部门应提出明

确的共享需求和使用目的，共享数据的产生和提供部门应及时研判共享需求的合理性和安全性，并根据政策要求提供服务。

统一标准，统筹建设。按照国家相关标准进行政务数据资源的采集、存储、处理、共享、开放等工作，形成各级政务数据资源目录，统筹建设政务数据共享开放安全保障体系。

建立机制，保障安全。各级政务部门和相关单位应建立政务数据共享开放管理机制和工作评价机制，加强对数据共享开放全过程的安全保障能力建设。

2、发展理念

政务数据的共享开放并非一蹴而就，而是在政务信息化逐步推进和大数据、云计算等新技术的驱动下，为了更有效支撑政府部门间业务流转，满足社会、人民对于政务数据资源和信息公开的需求，从实际出发，将技术和管理有效结合，统筹规划，构建政务数据共享开放安全机制并推向实践。

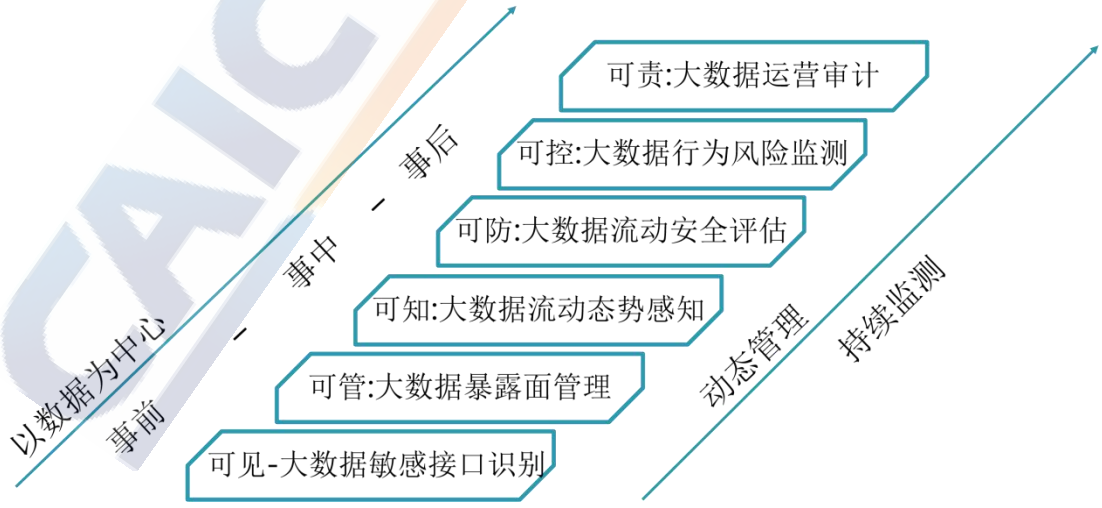


图 2 政务数据共享开放安全发展理念

在数据成为发展新变量的形势下，数据安全经历着从被动安全保护向主动风险控制转变。政务数据共享开放的安全防护应结合实际情况，围绕“数据安全”的愿景，以“数据为中心”进行建设，全面深入地厘清政务数据资产分布，揭示安全风险和防护缺失，分类分级实施保护，落实各级政务部门数据合规要求，实行动态管理和持续监测，满足事前、事中、事后闭环安全，实现政务数据生命周期各环节的可见、可管、可知、可防、可控、可责。

（二）安全框架



图 3 政务数据共享开放安全框架

为应对政务数据在共享开放中可能面临的安全风险，政务数据安全防护能力建设应基于数据共享交换平台、数据开放平台、大数据平台和数据服务总线等基础设施，统一政务数据应用通道，支撑政务业务流转，提供政务数据共享开放能力；在确保平台自身安全和平台级联安全的前提下，明确数据生命周期各环节的安全防护要点；梳理数据安全关键技术，围绕数据共享开放业务场景和活动，分析安全需求并落实具体防护措施；动态调整管理策略，合理调配人员、技术资源，持续开展安全风险监测、评估和审计，及时发现并迅速处置安全隐患；

从数据生命周期、数据安全技术、数据业务活动、安全管理体系、安全运维体系等方面综合构建政务数据共享开放安全框架，提升政务数据的体系化安全保障能力。

1、数据生命周期

政务数据生命周期需要关注的安全要点有所不同，应在各个环节落实有效的安全措施，防范安全风险。



图 4 政务数据生命周期安全要点

（1）数据采集

数据采集安全环节应明确政务数据采集原则、方法和目的，对数据源进行质量监测和有效管理，确保数据采集和汇聚的正当、合法、合规。数据采集过程中，可以通过认证、密码算法、审计等技术保障采集安全。

（2）数据传输

数据传输安全环节要确保政务数据的完整性、机密性，防止数据被篡改、窃取。数据传输中，可采用校验技术或密码技术保证数据在

传输过程中的完整性；采用深度内容检测技术对传输中的敏感内容进行监测，阻断非法传输，防范敏感信息泄露；建立数据传输安全策略和数据传输接口安全管理规范，并构建数据传输通道对源端进行身份鉴别和认证的能力。

（3）数据存储

数据存储安全环节要确保存储数据的机密性、可用性，支撑政务数据存取的安全需求。根据政务数据分类分级实际情况，建立不同等级的数据存储逻辑域对应存储，并进行有效容灾备份。采取数据加密、数据容灾、数据合规性检测等技术，并对数据库、数据共享交换平台、存储文件等实施相应的安全防护，保障政务数据存储安全。

（4）数据处理

数据处理是对数据进行操作、加工、分析的过程，此环节能够最直接、深入的接触数据，也面临较大的安全风险。数据处理环节的安全要点包括权限控制、访问控制、行为审计、事件溯源、流量监控、数据脱敏、数据加密等。

（5）数据交换

政务数据共享开放过程中，数据在不同控制者之间的交换和使用，所有数据活动都是在数据交换中通过相应的数据接口完成，此环节需要重点关注接口安全、权限控制、行为审计、事件溯源等。

（6）数据销毁

数据销毁环节应根据数据资源目录中对各级各类数据共享开放期限的要求，在停止共享开放服务、数据使用以及存储空间释放再分

配等场景下，对数据库、服务器和终端中的剩余数据以及硬件存储介质等，采用数据擦除或者物理销毁的方式确保数据无法复原。在数据销毁过程中，存在因数据未彻底删除而导致的数据泄露风险，应对数据销毁流程进行严格把控和审查，确保数据被有效销毁。

2、数据安全技术

（1）用户管理

政务数据共享开放应对用户进行角色权限设置，设立管理、审计及操作等角色，根据业务需求、管理范围、组织架构等设置访问控制策略，建立完整的用户管理机制，包括用户账号建立、注销、鉴别、鉴权、授权、审计等制度、流程和方法，并实时监测用户行为，对用户操作、权限、岗位职责等进行相关性分析。

（2）授权管理

针对各类访问政务数据的用户或应用，应从用户访问权限、数据操作权限、应用访问数据权限等维度明确授权机制，授权覆盖资源目录、资源文件、接口、共享发布、共享申请、共享期限等，采用共享数据访问授权凭证、安全策略配置等方式，确保授权管理贯通共享平台和信息系统。

（3）身份鉴别

对政务数据交换双方进行用户身份鉴别或设备认证，保障数据交换方身份的真实性，包括采用用户名/口令、一次性口令、数字证书、标识密码、生物特征等技术实现用户身份鉴别；采用复合鉴别技术，确保在交换敏感数据时的安全；采用数字证书、标识密码等方式实现

设备认证，并确定被授权使用方与认证设备间关系的真实性；在多方数据交换时对各接入方进行交叉认证等。

（4）数据脱敏

根据政务数据共享开放相关政策、分类分级标准、开放资源目录等，对于涉及重要数据、个人敏感信息、以及有特定要求的政务数据，在进行共享开放时，应采用数据脱敏策略进行脱敏处理，脱敏后的数据保留规范的数据格式和属性，以便脱敏数据能够适用于共享开放、开发利用。

（5）数据溯源

政务数据共享开放全过程应支持数据溯源，溯源信息包括业务相关人员、处理系统、IP 地址、处理时间、处理方式等，溯源信息应进行有效存储，并采取安全措施，确保事件追溯时的信息可用性。

（6）数据安全区域

政务数据共享开放过程中，要根据业务领域、涉及数据级别等因素设置不同的数据安全区域，根据数据重要性、数据量级、使用频率等因素，将数据分域分级存储或处理，并针对不同的区域实施分域分级安全防护措施。

（7）安全多方计算

政务数据共享开放中及多源数据的汇聚和处理，采取安全多方计算技术，在参与主体互不信任的情况下，可确保参与主体不能得到其他成员的输入信息，从而进一步确保多源政务数据共享的安全可靠。基于安全访问原则，互不信任的参与方进行协同计算时，具有输入的

独立性、计算的正确性、去中心化等特征，且不泄露各输入值给参与计算的其他成员。

（8）联邦学习

依据各地区、部门、业务领域政务数据资源目录，不同来源的政务数据可能存在差异化要求，无法直接汇总合并。联邦学习技术可在不违反数据资源保护要求情况下,建立一个虚拟的共有模型，数据本身不移动，从而使政务数据资源在不出本地的情况下，有效满足共享需求，避免隐私泄露，确保数据安全、合规。

（9）数据加密

根据政务数据分类分级安全要求，采用符合国家相关标准规定的密码技术，针对不同级别数据采取相应强度的加密策略，确保数据库、文件系统和介质存储安全，以及数据传输、交换环节的数据安全。

（10）数据防泄漏

政务数据共享开放中，应按数据分级分类预先对每类数据设置访问策略、共享策略和传播范围等。并通过部署数据防泄漏系统、采取技术手段防止数据在未授权条件下被下载、复制、删除，或通过截屏等方式被输出。

（11）数据流动监测

数据流动监测关注政务数据全生命周期中的安全风险，通过采集数据流量对协议解析还原，梳理敏感数据和访问行为，发现数据流动中潜在的脆弱性和风险，监测相关人员在数据活动中是否存在非法访问和异常操作，并对数据访问行为记录、审计、分析，形成安全风险、

用户行为关联画像，实现风险预警。

（12）接口监控

政务数据共享交换的过程涉及多种接口的数据交互，可通过部署数据接口监控策略，对共享交换平台、政务信息系统接口实施全面监控，实现对不同接口数据交互的全覆盖监测，在业务变化的过程中，实时梳理、发现接口状态，以及政务数据的实际交互情况，及时防范数据安全风险。

3、数据业务活动

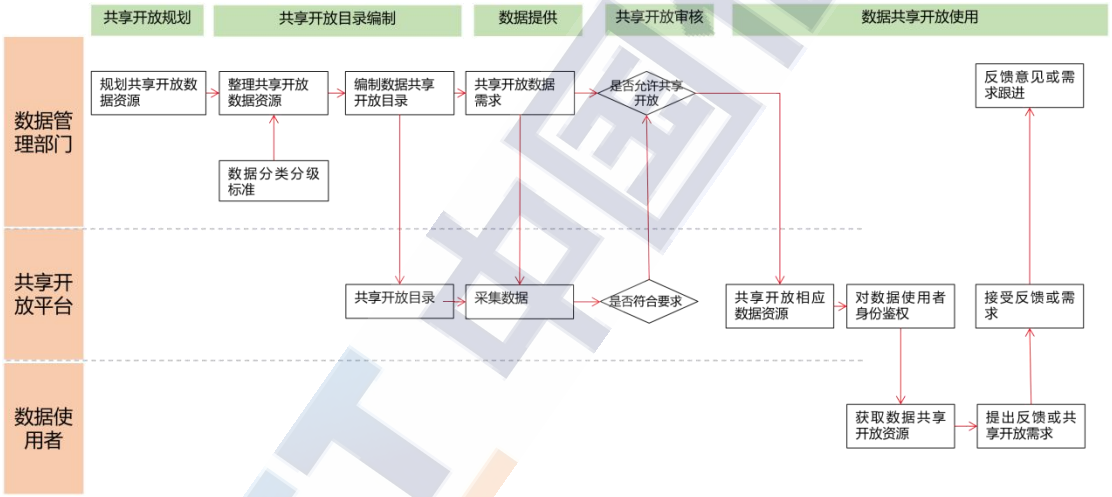


图 5 政务数据共享开放业务流程

（1）数据分类分级

各级政府机构结合业务需求制定政务数据分类分级规则，对不同级别的数据采取差异化安全管控措施。在确保数据合理合规流动的前提下，促进数据安全高效的开发利用和共享。数据共享开放主体应当按照分级分类规则，结合行业、区域特点，制定相应的实施细则，确定数据开放类型、开放条件和监管措施，以匹配后续安全要求和技术落实。

（2）数据目录梳理

对政务数据进行梳理，制定数据共享目录和开放目录编制指南，实行目录管理，定期发布政府数据共享、开放责任清单。政务数据可分为无条件共享、有条件共享、不予共享、是否向社会开放等，需遵循数据采集、入库、开放全流程把控并落实安全要求。

（3）数据审批

政务数据共享开放前，应由政务数据提供方进行审批，确保所提供的数据符合数据共享开放目录的范围及要求。数据共享开放的运维部门在数据共享开放前也应同步进行审核，确保对外共享开放最终数据的有效性。

（4）数据共享开放

政务数据共享开放业务安全重点关注共享开放流程，安全监控、数据合规以及审计跟踪等。对数据共享开放需求进行确认，明确数据内容、数据范围、时间周期、传输方式、安全管控手段、审核流程等要素，对于有条件共享和不共享的数据，需采取脱敏或匿名化技术手段，针对是否越权访问、访问过程是否安全、数据是否合规使用等方面，部署安全策略、技术工具，实时监测监督，确保及时阻断并有效控制安全风险。

4、安全管理体系

（1）组织架构

在组织架构层面将政务数据开放共享的安全管理要求进行统一管理，实现各级管理架构、管理要求的一致性，建立责任明确、程序

清晰的政务数据安全管理组织架构，明确主管部门和相关部门工作职责、工作程序和协调机制，确保政府部门内外部管理的完整性，实现工作高效协调和统筹管理。

（2）管理制度

制定政务数据共享开放安全规划和管理制度，规范共享开放的审批和工作流程，对政务数据安全管理过程进行规范指导。各级政府和部门可将相关制度细化为安全策略落地实施，明确安全方针、安全原则、安全目标，形成政务数据安全管理要求，确保各级数据分类分级和相应防护要求上下一致贯通。相关管理制度包括数据资产管理、数据分类分级、人员管理、风险管理、合规管理等。

（3）人员管理

制定人员管理要求，对政务数据共享开放相关业务的参与人员进行全面管理，包括背景调查、签署保密协议和数据安全岗位责任协议、人员调离岗位时的权限配置调整等，有效识别内外部人员、特定管理岗位、关建技术岗位人员的身份，遵循最小授权原则，确保管理要求落实，确保政务数据访问、使用的安全可控。

（4）合作管理

各级政府机构在实现政务数据共享开放时，与外部合作第三方或相关服务机构存在交互。应明确合作方机构管理制度，对合作方机构进行审查与评估，签署数据合作协议，对第三方人员严格管理，并对机构及人员进行监督，确保不因外部机构合作或第三方的应用接入而危害政务数据安全。

（5）合规管理

合规管理以防范和控制风险为导向，响应国家相关政策法规，针对业务需求，特别针对重要数据和个人信息保护，建立合规风险识别、评估及处置的制度和流程。持续收集与本单位合规风险及合规管理工作相关的内外部初始信息，根据自身风险情况及业务实际，突出重点领域、重点环节和重点人员，对风险发生的可能性、影响程度、潜在后果等进行系统分析，针对发现的风险制定预案，采取有效措施，及时应对处置，切实防范合规风险。

5、安全运维体系

（1）安全监测

基于敏感数据监控、数据安全风险评估、数据溯源追踪、数据安全态势分析等技术手段，对数据安全风险点进行发现、治理，实现数据风险提前预警、事中及时处置、事后准确追溯，保障政务数据安全合规并且支撑政务信息系统安全运行。

（2）安全审计

在政务数据运营过程中，需要对涉密、涉敏数据的共享和开放进行定期审计。审核政务数据共享开放涉及的日志、各级用户和数据管理角色，具体包含政务数据共享开放的时间、用户、IP 地址、操作对象、操作内容、操作行为和操作结果等相关信息，及时发现政务数据共享开放中存在的隐患和风险。

（3）检查评估

政务数据安全运营过程中应定期开展数据安全评估，覆盖合规审

查、风险管理、安全巡检、安全评估等方面，排查信息系统和运行环境存在的数据泄露、数据篡改、数据窃取、数据非法使用等安全隐患。在法律法规有新的要求，或业务模式、信息系统、运行环境发生重大变更时，也应启动数据安全评估，将发现的数据安全风险全部纳入问题管理流程进行跟踪管理，降低安全风险及可能带来的损失。

（4）应急响应

各级政务数据主管部门应建立政务数据共享开放应急管理制度，指导数据主体针对事件场景和影响程度制定有效的应急响应预案，定期组织应急演练，确保公共数据开放工作安全有序。

（5）事件处置

建立多层次的政务数据安全事件响应和处置机制，及时处置安全事件告警，并在重大事件发生时及时启动应急响应，明确事件处置规范和问责机制，及时分析和总结，动态调整数据安全策略。

六、相关建议

（一）完善法律法规，加快标准研制

为政务数据安全“上锁”，首先需要在法规制度方面“划清红线”。目前《中华人民共和国数据安全法》尚未正式发布，我国在数据共享开放、数据交易流通、数据安全层面的立法，以及数据平台建设、数据安全管理等相关制度、标准规范还需要进一步完善。应在国家电子政务标准体系的基础上，完善数据分类分级、安全管控、安全技术等具体研制方向，加快重点标准研制工作，规范政务数据安全体系、政

务数据源头质量和各环节安全技术等具体要求，为实现同一标准采集数据、同一源头提供数据、同一系统共享数据打好基础，确保跨机构、跨领域政务数据共享开放、融合应用的安全可靠。

（二）健全管理机制，形成监管闭环

政务数据共享开放涉及部门多、应用范围广、协调难度大、相关事务杂，在管理机制方面，应进一步明确政务数据提供、使用、管理、监管等各方的职责权限，完善从顶层规划到地方建设的相关制度，解决政务数据与社会数据共享开放“无据可依”的问题。同步围绕政务数据生命周期，制定符合监管要求和标准规范的检查方案。借助例行检查、年度检查、飞行检查以及专项行动等方式，评估安全风险，及时发现安全隐患，建立跟踪管理流程，将各部门政务数据工作成效纳入政府绩效考核体系。加强数据主管部门、责任主体、支撑单位协作互通，建立公共数据安全运营协同机制，形成监督管理闭环。

（三）聚焦数据核心，提升技术能力

新兴技术发展与数据安全保障是一场竞逐，数据安全与技术发展比肩前行。政务数据安全应聚焦“以数据为核心”保障理念，以大数据、人工智能等新技术为驱动，加强数据安全关建技术研究和试点应用，结合大数据综合试验区、电子政务综合试点、公共信息资源开放试点等试点工作，将政务数据安全纳入其中，通过广泛的实践探索积累经验。根据安全需求和监管要求，动态调整安全策略和技术措施，加强风险感知和监测预警能力建设，实施动态管理、持续监测和主动

防控，针对性挖掘和防范数据生命周期各环节安全风险，筑牢政务数据共享开放的安全屏障，全面提升政务数据安防护能力。

（四）提高思想认识，培养复合人才

促进政务数据共享开放，推动政企数据融合对接及开发利用，需要政府、企业及社会各主体协同配合，全面强化各部门对政务数据共享的重视程度，培养复合型管理人才和专业技术人才，化解数据壁垒，促进政务数据共享科学高效地开展。一方面采取理论学习和实践操作相结合的方式，改变数据专享和数据隐藏的固有观念，明确角色定位，积极履行本部门的责任义务，将共享、公开和透明的管理理念渗透到工作过程中。另一方面，与高校、科研机构、高新技术企业联合开展人才培养计划，培育一批懂政府也懂市场化的复合型管理人才，打造一支懂业务、能实操的专业化人才队伍。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

邮箱：wangdanhui@caict.ac.cn

联系电话：010-62308590　010-62308790

传真：010-62300264