数据出境安全法律法规汇编手册

深圳（前海）数据跨境流动综合服务中心

二〇二六年十一月

目　　录

中华人民共和国网络安全法 4
第一章 总 则 4
第二章 网络安全支持与促进 6
第三章 网络运行安全 7
第一节 一般规定 7
第二节 关键信息基础设施的运行安全 8
第四章 网络信息安全 9
第五章 监测预警与应急处置 10
第六章 法律责任 11
第七章 附 则 15
中华人民共和国数据安全法 16
第一章 总则 16
第二章 数据安全与发展 17
第三章 数据安全制度 18
第四章 数据安全保护义务 19
第五章 政务数据安全与开放 20
第六章 法律责任 20
第七章 附则 22
中华人民共和国个人信息保护法 23
第一章 总 则 23
第二章 个人信息处理规则 24
第一节 一般规定 24
第二节 敏感个人信息的处理规则 27
第三节 国家机关处理个人信息的特别规定 27
第三章 个人信息跨境提供的规则 28
第四章 个人在个人信息处理活动中的权利 29
第五章 个人信息处理者的义务 29
第六章 履行个人信息保护职责的部门 31
第七章 法律责任 32
第八章 附 则 33
网络数据安全管理条例 35
第一章 总 则 35
第二章 一般规定 36
第三章 个人信息保护 37
第四章 重要数据安全 39

第五章 网络数据跨境安全管理 41
第六章 网络平台服务提供者义务 41
第七章 监督管理 42
第八章 法律责任 44
第九章 附 则 45
促进和规范数据跨境流动规定 46
数据出境安全评估办法 49
个人信息出境标准合同办法 53
个人信息出境认证办法 55
医疗卫生机构数据安全和个人信息保护管理办法（试行） 58
第一章 总则 58
第二章 数据分类分级保护 59
第三章 数据全生命周期安全管理 59
第四章 数据安全监测预警和应急处置 64
第五章 个人信息保护 65
第六章 监督管理 66
第七章 附则 68
数据出境安全评估申报指南（第三版） 69
一、适用范围 69
二、申报方式及流程 70
三、申请延长评估结果有效期 71
四、咨询、举报联系方式 72
个人信息出境标准合同备案指南（第二版） 85
一、适用范围 85
二、备案方式 86
三、备案流程 86
四、咨询、举报联系方式 87
粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引 113
粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引 116
粤港澳大湾区个人信息跨境流动标准合同备案指南 119
一、适用范围 119
二、备案方式 120
三、备案流程 120
四、咨询方式 121

中华人民共和国主席令

第六十一号

《全国人民代表大会常务委员会关于修改<中华人民共和国网络安全法>的决定》已由中华人民共和国第十四届全国人民代表大会常务委员会第十八次会议于2025年10月28日通过，现予公布，自2026年1月1日起施行。

中华人民共和国主席 习近平

2025年10月28日

中华人民共和国网络安全法

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过　根据2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议《关于修改〈中华人民共和国网络安全法〉的决定》修正）

目 录

第一章 总 则
第二章 网络安全支持与促进
第三章 网络运行安全
第一节 一般规定
第二节 关键信息基础设施的运行安全
第四章 网络信息安全
第五章 监测预警与应急处置
第六章 法律责任
第七章 附 则

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 网络安全工作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，推进网络强国建设。

第四条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第五条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第六条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第七条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第八条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第九条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第十条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十一条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十二条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十三条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖

主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十四条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十五条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十六条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十七条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十八条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十九条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

第二十条 国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

第二十一条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十二条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十三条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改:

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任;

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月;

（四）采取数据分类、重要数据备份和加密等措施;

（五）法律、行政法规规定的其他义务。

第二十四条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十五条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十六条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十七条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事

件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十八条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第三十一条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十二条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十三条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十四条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十五条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十六条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务:

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查;

（二）定期对从业人员进行网络安全教育、技术培训和技能考核;

（三）对重要系统和数据库进行容灾备份;

（四）制定网络安全事件应急预案，并定期进行演练;

（五）法律、行政法规规定的其他义务。

第三十七条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十八条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十九条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第四十条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第四十一条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力;

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享;

第四章 网络信息安全

第四十二条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

第四十三条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十四条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十五条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十六条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十七条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十八条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十九条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第五十条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第五十一条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十二条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十三条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十四条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十五条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十六条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施:

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测;

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度;

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十七条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十八条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十九条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第六十条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第六十一条 网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

第六十二条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款:

（一）设置恶意程序的;

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的;

（三）擅自终止为其产品、服务提供安全维护的。

有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第六十三条 违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。

第六十四条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十五条 违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网

络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十七条 关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十八条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十九条 网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者

应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。

第七十条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款:

（一）拒绝、阻碍有关部门依法实施的监督检查的;

第七十一条 有下列行为之一的，依照有关法律、行政法规的规定处理、处罚:

（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的;

（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的;

（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

第七十二条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十三条 违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。

第七十四条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；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。

第七十五条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，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。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十六条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十七条 境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十八条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十九条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第八十条 军事网络的安全保护，由中央军事委员会另行规定。

第八十一条 本法自 2017 年 6 月 1 日起施行。

中华人民共和国主席令

第八十四号

《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过，现予公布，自2021年9月1日起施行。

中华人民共和国主席　习近平

2021年6月10日

中华人民共和国数据安全法

（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

第一章 总则
第二章 数据安全与发展
第三章 数据安全制度
第四章 数据安全保护义务
第五章 政务数据安全与开放
第六章 法律责任
第七章 附则

第一章 总则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，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。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，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。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，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。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 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。依法不予公开的除外。

第四十二条 国家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，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，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。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自 2021 年 9 月 1 日起施行。

中华人民共和国主席令

第九十一号

《中华人民共和国个人信息保护法》已由中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于2021年8月20日通过，现予公布，自2021年11月1日起施行。

中华人民共和国主席　习近平

2021年8月20日

中华人民共和国个人信息保护法

（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过）

目 录

第一章 总 则
第二章 个人信息处理规则
第一节 一般规定
第二节 敏感个人信息的处理规则
第三节 国家机关处理个人信息的特别规定
第三章 个人信息跨境提供的规则
第四章 个人在个人信息处理活动中的权利
第五章 个人信息处理者的义务
第六章 履行个人信息保护职责的部门
第七章 法律责任
第八章 附 则

第一章 总 则

第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的;

（二）分析、评估境内自然人的行为;

（三）法律、行政法规规定的其他情形。

第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章 个人信息处理规则

第一节 一般规定

第十三条 符合下列情形之一的，个人信息处理者方可处理个人信息:

（一）取得个人的同意;

（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;

（三）为履行法定职责或者法定义务所必需;

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需;

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息;

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项:

（一）个人信息处理者的名称或者姓名和联系方式;

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限;

（三）个人行使本法规定权利的方式和程序;

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图

像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一:

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估;

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证;

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务;

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施

确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失:

（一）制定内部管理制度和操作规程;

（二）对个人信息实行分类管理;

（三）采取相应的加密、去标识化等安全技术措施;

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训;

（五）制定并组织实施个人信息安全事件应急预案;

（六）法律、行政法规规定的其他措施。

第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录:

（一）处理敏感个人信息;

（二）利用个人信息进行自动化决策;

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息;

（四）向境外提供个人信息;

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条 个人信息保护影响评估应当包括下列内容:

（一）个人信息的处理目的、处理方式等是否合法、正当、必要;

（二）对个人权益的影响及安全风险;

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项:

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害;

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施;

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务:

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督;

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务;

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务;

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章 履行个人信息保护职责的部门

第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责:

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作;

（二）接受、处理与个人信息保护有关的投诉、举报;

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果;

（四）调查、处理违法个人信息处理活动;

（五）法律、行政法规规定的其他职责。

第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作:

（一）制定个人信息保护具体规则、标准;

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准;

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设;

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务;

（五）完善个人信息保护投诉、举报工作机制。

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施:

（一）询问有关当事人，调查与个人信息处理活动有关的情况;

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料;

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查;

（四）检查与个人信息处理活动有关的设备、物品;对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警

告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十七条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；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。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章 附 则

第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条 本法下列用语的含义:

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条 本法自 2021 年 11 月 1 日起施行。

中华人民共和国国务院令

第 790 号

《网络数据安全管理条例》已经 2024 年 8 月 30 日国务院第 40 次常务会议通过，现予公布，自 2025 年 1 月 1 日起施行。

总 理 李 强

2024 年 9 月 24 日

网络数据安全管理条例

第一章 总 则

第一条 为了规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益，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 在中华人民共和国境内开展网络数据处理活动及其安全监督管理，适用本条例。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，符合《中华人民共和国个人信息保护法》第三条第二款规定情形的，也适用本条例。

在中华人民共和国境外开展网络数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 网络数据安全管理工作坚持中国共产党的领导，贯彻总体国家安全观，统筹促进网络数据开发利用与保障网络数据安全。

第四条 国家鼓励网络数据在各行业、各领域的创新应用，加强网络数据安全防护能力建设，支持网络数据相关技术、产品、服务创新，开展网络数据安全宣传教育和人才培养，促进网络数据开发利用和产业发展。

第五条 国家根据网络数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对网络数据实行分类分级保护。

第六条 国家积极参与网络数据安全相关国际规则和标准的制定，促进国际交流与合作。

第七条 国家支持相关行业组织按照章程，制定网络数据安全行为规范，加强行业自律，指导会员加强网络数据安全保护，提高网络数据安全保护水平，促进行业健康发展。

第二章 一般规定

第八条 任何个人、组织不得利用网络数据从事非法活动，不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。

第九条 网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。

第十条 网络数据处理者提供的网络产品、服务应当符合相关国家标准的强制性要求；发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告；涉及危害国家安全、公共利益的，网络数据处理者还应当在24小时内向有关主管部门报告。

第十一条 网络数据处理者应当建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。

网络数据安全事件对个人、组织合法权益造成危害的，网络数据处理者应当及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知利害关系人；法律、行政法规规定可以不通知的，从其规定。网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。

第十二条 网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的，应当通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督。向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存3年。

网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

两个以上的网络数据处理者共同决定个人信息和重要数据的处理目的和处理方式的，应当约定各自的权利和义务。

第十三条 网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查。

第十四条 网络数据处理者因合并、分立、解散、破产等原因需要转移网络数据的，网络数据接收方应当继续履行网络数据安全保护义务。

第十五条 国家机关委托他人建设、运行、维护电子政务系统，存储、加工政务数据，应当按照国家有关规定经过严格的批准程序，明确受托方的网络数据处理权限、保护责任等，监督受托方履行网络数据安全保护义务。

第十六条 网络数据处理者为国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的，应当依照法律、法规的规定和合同约定履行网络数据安全保护义务，提供安全、稳定、持续的服务。

前款规定的网络数据处理者未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析。

第十七条 为国家机关提供服务的信息系统应当参照电子政务系统的管理要求加强网络数据安全管理，保障网络数据安全。

第十八条 网络数据处理者使用自动化工具访问、收集网络数据，应当评估对网络服务带来的影响，不得非法侵入他人网络，不得干扰网络服务正常运行。

第十九条 提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。

第二十条 面向社会提供产品、服务的网络数据处理者应当接受社会监督，建立便捷的网络数据安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络数据安全投诉、举报。

第三章 个人信息保护

第二十一条 网络数据处理者在处理个人信息前，通过制定个人信息处理规则的方式依法向个人告知的，个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、清晰易懂，包括但不限于下列内容:

（一）网络数据处理者的名称或者姓名和联系方式;

（二）处理个人信息的目的、方式、种类，处理敏感个人信息的必要性以及对个人权益的影响;

（三）个人信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法;

（四）个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。

网络数据处理者按照前款规定向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形

式予以列明。网络数据处理者处理不满十四周岁未成年人个人信息的，还应当制定专门的个人信息处理规则。

第二十二条 网络数据处理者基于个人同意处理个人信息的，应当遵守下列规定:

（一）收集个人信息为提供产品或者服务所必需，不得超范围收集个人信息，不得通过误导、欺诈、胁迫等方式取得个人同意;

（二）处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，应当取得个人的单独同意;

（三）处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意;

（四）不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息;

（五）不得在个人明确表示不同意处理其个人信息后，频繁征求同意;

（六）个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。

法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第二十三条 个人请求查阅、复制、更正、补充、删除、限制处理其个人信息，或者个人注销账号、撤回同意的，网络数据处理者应当及时受理，并提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。

第二十四条 因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，以及个人注销账号的，网络数据处理者应当删除个人信息或者进行匿名化处理。法律、行政法规规定的保存期限未届满，或者删除、匿名化处理个人信息从技术上难以实现的，网络数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第二十五条 对符合下列条件的个人信息转移请求，网络数据处理者应当为个人指定的其他网络数据处理者访问、获取有关个人信息提供途径:

（一）能够验证请求人的真实身份;

（二）请求转移的是本人同意提供的或者基于合同收集的个人信息;

（三）转移个人信息具备技术可行性;

（四）转移个人信息不损害他人合法权益。

请求转移个人信息次数等明显超出合理范围的，网络数据处理者可以根据转移个人信息的成本收取必要费用。

第二十六条 中华人民共和国境外网络数据处理者处理境内自然人个人信息，依照《中华人民共和国个人信息保护法》第五十三条规定在境内设立专门

机构或者指定代表的，应当将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门；网信部门应当及时通报同级有关主管部门。

第二十七条 网络数据处理者应当定期自行或者委托专业机构对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第二十八条 网络数据处理者处理1000万人以上个人信息的，还应当遵守本条例第三十条、第三十二条对处理重要数据的网络数据处理者（以下简称重要数据的处理者）作出的规定。

第四章 重要数据安全

第二十九条 国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的网络数据进行重点保护。

网络数据处理者应当按照国家有关规定识别、申报重要数据。对确认为重要数据的，相关地区、部门应当及时向网络数据处理者告知或者公开发布。网络数据处理者应当履行网络数据安全保护责任。

国家鼓励网络数据处理者使用数据标签标识等技术和产品，提高重要数据安全管理水平。

第三十条 重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任:

（一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案;

（二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件;

（三）受理并处理网络数据安全投诉、举报。

网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。

掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

第三十一条 重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。

风险评估应当重点评估下列内容:

（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要;

（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险;

（三）网络数据接收方的诚信、守法等情况;

（四）与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务;

（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险;

（六）有关主管部门规定的其他评估内容。

第三十二条 重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。

第三十三条 重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。

风险评估报告应当包括下列内容:

（一）网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等;

（二）处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身;

（三）网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性;

（四）发现的网络数据安全风险，发生的网络数据安全事件及处置情况;

（五）提供、委托处理、共同处理重要数据的风险评估情况;

（六）网络数据出境情况;

（七）有关主管部门规定的其他报告内容。

处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。

重要数据的处理者存在可能危害国家安全的重要数据处理活动的，省级以上有关主管部门应当责令其采取整改或者停止处理重要数据等措施。重要数据的处理者应当按照有关要求立即采取措施。

第五章 网络数据跨境安全管理

第三十四条 国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。

第三十五条 符合下列条件之一的，网络数据处理者可以向境外提供个人信息:

（一）通过国家网信部门组织的数据出境安全评估;

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证;

（三）符合国家网信部门制定的关于个人信息出境标准合同的规定;

（四）为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息;

（五）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息;

（六）为履行法定职责或者法定义务，确需向境外提供个人信息;

（七）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息;

（八）法律、行政法规或者国家网信部门规定的其他条件。

第三十六条 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

第三十七条 网络数据处理者在中华人民共和国境内运营中收集和产生的重要数据确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。网络数据处理者按照国家有关规定识别、申报重要数据，但未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。

第三十八条 通过数据出境安全评估后，网络数据处理者向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。

第六章 网络平台服务提供者义务

第四十条 网络平台服务提供者应当通过平台规则或者合同等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。

预装应用程序的智能终端等设备生产者，适用前款规定。

第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三

方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。

国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保。

第四十一条 提供应用程序分发服务的网络平台服务提供者，应当建立应用程序核验规则并开展网络数据安全相关核验。发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当采取警示、不予分发、暂停分发或者终止分发等措施。

第四十二条 网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

第四十三条 国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则进行推广应用。

鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息。

第四十四条 大型网络平台服务提供者应当每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。

第四十五条 大型网络平台服务提供者跨境提供网络数据，应当遵守国家数据跨境安全管理要求，健全相关技术和管理措施，防范网络数据跨境安全风险。

第四十六条 大型网络平台服务提供者不得利用网络数据、算法以及平台规则等从事下列活动:

（一）通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据;

（二）无正当理由限制用户访问、使用其在平台上产生的网络数据;

（三）对用户实施不合理的差别待遇，损害用户合法权益;

（四）法律、行政法规禁止的其他活动。

第七章 监督管理

第四十七条 国家网信部门负责统筹协调网络数据安全和相关监督管理工作。

公安机关、国家安全机关依照有关法律、行政法规和本条例的规定，在各自职责范围内承担网络数据安全监督管理职责，依法防范和打击危害网络数据安全的违法犯罪活动。

国家数据管理部门在具体承担数据管理工作中履行相应的网络数据安全职责。

各地区、各部门对本地区、本部门工作中收集和产生的网络数据及网络数据安全负责。

第四十八条 各有关主管部门承担本行业、本领域网络数据安全监督管理职责，应当明确本行业、本领域网络数据安全保护工作机构，统筹制定并组织实施本行业、本领域网络数据安全事件应急预案，定期组织开展本行业、本领域网络数据安全风险评估，对网络数据处理者履行网络数据安全保护义务情况进行监督检查，指导督促网络数据处理者及时对存在的风险隐患进行整改。

第四十九条 国家网信部门统筹协调有关主管部门及时汇总、研判、共享、发布网络数据安全风险相关信息，加强网络数据安全信息共享、网络数据安全风险和威胁监测预警以及网络数据安全事件应急处置工作。

第五十条 有关主管部门可以采取下列措施对网络数据安全进行监督检查:

（一）要求网络数据处理者及其相关人员就监督检查事项作出说明;

（二）查阅、复制与网络数据安全有关的文件、记录;

（三）检查网络数据安全措施运行情况;

（四）检查与网络数据处理活动有关的设备、物品;

（五）法律、行政法规规定的其他必要措施。

网络数据处理者应当对有关主管部门依法开展的网络数据安全监督检查予以配合。

第五十一条 有关主管部门开展网络数据安全监督检查，应当客观公正，不得向被检查单位收取费用。

有关主管部门在网络数据安全监督检查中不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途。

有关主管部门发现网络数据处理者的网络数据处理活动存在较大安全风险的，可以按照规定的权限和程序要求网络数据处理者暂停相关服务、修改平台规则、完善技术措施等，消除网络数据安全隐患。

第五十二条 有关主管部门在开展网络数据安全监督检查时，应当加强协同配合、信息沟通，合理确定检查频次和检查方式，避免不必要的检查和交叉重复检查。

个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等应当加强衔接，避免重复评估、审计。重要数据风险评估和网络安全等级测评的内容重合的，相关结果可以互相采信。

第五十三条 有关主管部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等网络数据应当依法予以保密，不得泄露或者非法向他人提供。

第五十四条 境外的组织、个人从事危害中华人民共和国国家安全、公共利益，或者侵害中华人民共和国公民的个人信息权益的网络数据处理活动的，国家网信部门会同有关主管部门可以依法采取相应的必要措施。

第八章 法律责任

第五十五条 违反本条例第十二条、第十六条至第二十条、第二十二条、第四十条第一款和第二款、第四十一条、第四十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处100万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员可以处1万元以上10万元以下罚款。

第五十六条 违反本条例第十三条规定的，由网信、电信、公安、国家安全等主管部门依据各自职责责令改正，给予警告，可以并处10万元以上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可以处1万元以上10万元以下罚款；拒不改正或者情节严重的，处100万元以上1000万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处10万元以上100万元以下罚款。

第五十七条 违反本条例第二十九条第二款、第三十条第二款和第三款、第三十一条、第三十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，可以并处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可以处1万元以上10万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处50万元以上200万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处5万元以上20万元以下罚款。

第五十八条 违反本条例其他有关规定的，由有关主管部门依照《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》等法律的有关规定追究法律责任。

第五十九条 网络数据处理者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。

第六十条 国家机关不履行本条例规定的网络数据安全保护义务的，由其上级机关或者有关主管部门责令改正；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。

第六十一条 违反本条例规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第九章 附 则

第六十二条 本条例下列用语的含义：

（一）网络数据，是指通过网络处理和产生的各种电子数据。

（二）网络数据处理活动，是指网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

（三）网络数据处理者，是指在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。

（四）重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

（五）委托处理，是指网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动。

（六）共同处理，是指两个以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。

（七）单独同意，是指个人针对其个人信息进行特定处理而专门作出具体、明确的同意。

（八）大型网络平台，是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

第六十三条 开展核心数据的网络数据处理活动，按照国家有关规定执行。

自然人因个人或者家庭事务处理个人信息的，不适用本条例。

开展涉及国家秘密、工作秘密的网络数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第六十四条 本条例自 2025 年 1 月 1 日起施行。

国家互联网信息办公室令

第 16 号

《促进和规范数据跨境流动规定》已经 2023 年 11 月 28 日国家互联网信息办公室 2023 年第 26 次室务会议审议通过，现予公布，自公布之日起施行。

国家互联网信息办公室主任 庄荣文

2024 年 3 月 22 日

促进和规范数据跨境流动规定

第一条 为了保障数据安全，保护个人信息权益，促进数据依法有序自由流动，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》等法律法规，对于数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行，制定本规定。

第二条 数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

第三条 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第四条 数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第五条 数据处理者向境外提供个人信息，符合下列条件之一的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证:

（一）为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的;

（二）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的;

（三）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的;

（四）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息）的。

前款所称向境外提供的个人信息，不包括重要数据。

第六条 自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（以下简称负面清单），经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。

自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第七条 数据处理者向境外提供数据，符合下列条件之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估:

（一）关键信息基础设施运营者向境外提供个人信息或者重要数据;

（二）关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息。

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。

第八条 关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。

第九条 通过数据出境安全评估的结果有效期为3年，自评估结果出具之日起计算。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前60个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期3年。

第十条 数据处理者向境外提供个人信息的，应当按照法律、行政法规的规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。

第十一条 数据处理者向境外提供数据的，应当遵守法律、法规的规定，履行数据安全保护义务，采取技术措施和其他必要措施，保障数据出境安全。发生或者可能发生数据安全事件的，应当采取补救措施，及时向省级以上网信部门和其他有关主管部门报告。

第十二条 各地网信部门应当加强对数据处理者数据出境活动的指导监督，健全完善数据出境安全评估制度，优化评估流程；强化事前事中事后全链条全领域监管，发现数据出境活动存在较大风险或者发生数据安全事件的，要求数据处理者进行整改，消除隐患；对拒不改正或者造成严重后果的，依法追究法律责任。

第十三条 2022年7月7日公布的《数据出境安全评估办法》（国家互联网信息办公室令第11号）、2023年2月22日公布的《个人信息出境标准合同办

法》（国家互联网信息办公室令第 13 号）等相关规定与本规定不一致的，适用本规定。

第十四条 本规定自公布之日起施行。

国家互联网信息办公室令

第 11 号

《数据出境安全评估办法》已经 2022 年 5 月 19 日国家互联网信息办公室 2022 年第 10 次室务会议审议通过，现予公布，自 2022 年 9 月 1 日起施行。

主 任 庄荣文

2022 年 7 月 7 日

数据出境安全评估办法

第一条 为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，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》等法律法规，制定本办法。

第二条 数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的，依照其规定。

第三条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

第四条 数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估:

（一）数据处理者向境外提供重要数据;

（二）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息;

（三）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息;

（四）国家网信部门规定的其他需要申报数据出境安全评估的情形。

第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项:

（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性;

（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险;

（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全;

（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；

（六）其他可能影响数据出境安全的事项。

第六条 申报数据出境安全评估，应当提交以下材料：

（一）申报书；

（二）数据出境风险自评估报告；

（三）数据处理者与境外接收方拟订立的法律文件；

（四）安全评估工作需要的其他材料。

第七条 省级网信部门应当自收到申报材料之日起5个工作日内完成完备性查验。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。

国家网信部门应当自收到申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者。

第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：

（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；

（二）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

（三）出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

（四）数据安全和个人信息权益是否能够得到充分有效保障；

（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；

（六）遵守中国法律、行政法规、部门规章情况；

（七）国家网信部门认为需要评估的其他事项。

第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：

（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第十条 国家网信部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。

第十一条 安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。

数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

第十二条 国家网信部门应当自向数据处理者发出书面受理通知书之日起45个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。

评估结果应当书面通知数据处理者。

第十三条 数据处理者对评估结果有异议的，可以在收到评估结果15个工作日内向国家网信部门申请复评，复评结果为最终结论。

第十四条 通过数据出境安全评估的结果有效期为2年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估:

（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的;

（二）境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的;

（三）出现影响出境数据安全的其他情形。

有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满60个工作日前重新申报评估。

第十五条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十六条 任何组织和个人发现数据处理者违反本办法向境外提供数据的，可以向省级以上网信部门举报。

第十七条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。

第十八条 违反本办法规定的，依据《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》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十九条 本办法所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

第二十条 本办法自 2022 年 9 月 1 日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改。

国家互联网信息办公室令

第 13 号

《个人信息出境标准合同办法》已经 2023 年 2 月 3 日国家互联网信息办公室 2023 年第 2 次室务会议审议通过，现予公布，自 2023 年 6 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

2023 年 2 月 22 日

个人信息出境标准合同办法

第一条 为了保护个人信息权益，规范个人信息出境活动，根据《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第二条 个人信息处理者通过与境外接收方订立个人信息出境标准合同（以下简称标准合同）的方式向中华人民共和国境外提供个人信息，适用本办法。

第三条 通过订立标准合同的方式开展个人信息出境活动，应当坚持自主缔约与备案管理相结合、保护权益与防范风险相结合，保障个人信息跨境安全、自由流动。

第四条 个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形:

（一）非关键信息基础设施运营者;

（二）处理个人信息不满 100 万人的;

（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的;

（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

法律、行政法规或者国家网信部门另有规定的，从其规定。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

第五条 个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容:

（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性;

（二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险;

（三）境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全;

（四）个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等;

（五）境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响;

（六）其他可能影响个人信息出境安全的事项。

第六条 标准合同应当严格按照本办法附件订立。国家网信部门可以根据实际情况对附件进行调整。

个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。

标准合同生效后方可开展个人信息出境活动。

第七条 个人信息处理者应当在标准合同生效之日起10个工作日内向所在地省级网信部门备案。备案应当提交以下材料:

（一）标准合同;

（二）个人信息保护影响评估报告。

个人信息处理者应当对所备案材料的真实性负责。

第八条 在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续:

（一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的;

（二）境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的;

（三）可能影响个人信息权益的其他情形。

第九条 网信部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十条 任何组织和个人发现个人信息处理者违反本办法向境外提供个人信息的，可以向省级以上网信部门举报。

第十一条 省级以上网信部门发现个人信息出境活动存在较大风险或者发生个人信息安全事件的，可以依法对个人信息处理者进行约谈。个人信息处理者应当按照要求整改，消除隐患。

第十二条 违反本办法规定的，依据《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十三条 本办法自2023年6月1日起施行。本办法施行前已经开展的个人信息出境活动，不符合本办法规定的，应当自本办法施行之日起6个月内完成整改。

国家互联网信息办公室

国家市场监督管理总局

第 20 号

《个人信息出境认证办法》已经 2025 年 7 月 21 日国家互联网信息办公室 2025 年第 17 次室务会会议审议通过，并经国家市场监督管理总局同意，现予公布，自 2026 年 1 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

国家市场监督管理总局局长 罗 文

2025 年 10 月 14 日

个人信息出境认证办法

第一条 为了保护个人信息权益，规范个人信息出境认证活动，促进个人信息高效安全跨境流动，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》、《中华人民共和国认证认可条例》等法律法规，制定本办法。

第二条 个人信息处理者通过个人信息保护认证的方式向中华人民共和国境外提供个人信息，适用本办法。

第三条 本办法所称个人信息出境认证，是指按照《中华人民共和国个人信息保护法》第三十八条第一款第二项规定，由依法取得个人信息保护认证资质的专业认证机构，证明个人信息处理者向中华人民共和国境外提供个人信息等个人信息处理活动符合相关法律、行政法规、部门规章、标准、技术规范的合格评定活动。

第四条 国家网信部门会同国家数据管理部门和其他有关部门制定个人信息出境认证相关标准、技术规范。国家市场监督管理部门会同国家网信部门制定个人信息保护认证规则、统一认证证书及标志。

第五条 个人信息处理者通过个人信息出境认证的方式向境外提供个人信息的，应当同时符合下列情形:

（一）非关键信息基础设施运营者;

（二）自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息。

前款所称向境外提供的个人信息，不包括重要数据。

法律、行政法规或者国家网信部门另有规定的，从其规定。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过个人信息出境认证的方式向境外提供。

第六条 个人信息处理者在申请认证向境外提供个人信息前，应当按照法律、行政法规的规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。个人信息保护影响评估重点评估以下内容:

（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性;

（二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对国家安全、公共利益、个人信息权益带来的风险;

（三）境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全;

（四）个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等;

（五）境外接收方所在国家或者地区的个人信息保护政策和法规对出境个人信息安全和个人信息权益的影响;

（六）其他可能影响个人信息出境安全的事项。

第七条 个人信息处理者通过认证方式向境外提供个人信息的，应当向专业认证机构申请个人信息出境认证。

中华人民共和国境外的个人信息处理者申请个人信息出境认证的，应当由其在境内设立的专门机构或者指定代表协助进行申请。

第八条 专业认证机构应当按照认证基本规范、个人信息保护认证规则开展个人信息出境认证活动。符合认证要求的，专业认证机构应当及时出具认证证书。

认证证书的有效期为 3 年。证书到期需继续使用的，个人信息处理者应当在有效期届满前 6 个月提出认证申请。

第九条 专业认证机构应当在出具认证证书或者认证证书状态发生变化后 5 个工作日内，向全国认证认可信息公共服务平台报送个人信息出境认证证书相关信息，包括认证证书编号、获证个人信息处理者名称、认证范围以及证书状态变化信息等。

国家市场监督管理部门与国家网信部门建立认证信息共享机制。

第十条 专业认证机构发现获证个人信息处理者存在个人信息出境情况与认证范围不一致等情形，不再符合认证要求的，应当暂停其使用直至撤销相关认证证书。

国家网信部门和有关部门在个人信息保护监督管理工作中发现获证个人信息处理者存在前款情形的，专业认证机构应当配合暂停其使用直至撤销相关认证证书。

前两款规定的情形，应当通过全国认证认可信息公共服务平台予以公布。

第十一条 专业认证机构在开展认证活动中，发现个人信息出境活动违反法律、行政法规和国家有关规定的，应当及时向国家网信部门和有关部门报告。

第十二条 开展个人信息出境认证的专业认证机构应当自国家市场监督管理部门批准取得个人信息保护认证资质之日起10个工作日内向国家网信部门办理备案手续。办理备案时，应当提交下列材料:

（一）取得的个人信息保护领域的认证资质情况;

（二）近3年从事数据安全、个人信息保护领域专业工作情况;

（三）专业认证机构人员安全背景审查材料;

（四）个人信息保护认证实施细则及工作计划;

（五）个人信息安全风险防范机制;

（六）对获证个人信息处理者进行的个人信息出境活动符合认证标准情况的持续监督机制;

（七）投诉受理和争议解决机制;

（八）其他需要提交的材料。

专业认证机构应当对所备案材料的真实性负责。

国家网信部门收到专业认证机构提交的备案材料后，会同国家数据管理部门对备案材料进行审核。材料齐全的，应当在30个工作日内予以备案并进行公示；材料不齐全的，不予备案，应当在30个工作日内通知专业认证机构并说明理由。

第十三条 国家市场监督管理部门和国家网信部门对个人信息出境认证活动进行监督，开展定期或者不定期的检查，对认证过程和认证结果进行抽查，对专业认证机构进行抽查和评价。

第十四条 国家机关、专业认证机构等从事认证活动的机构及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十五条 任何组织和个人发现获证个人信息处理者违反本办法规定向境外提供个人信息的，可以向专业认证机构、网信部门和有关部门投诉、举报。

第十六条 省级以上网信部门和有关部门发现获证个人信息处理者个人信息出境活动存在较大风险或者发生个人信息安全事件的，可以依法对获证个人信息处理者进行约谈。获证个人信息处理者应当按照要求整改，消除隐患。

第十七条 违反本办法规定的，依据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》、《中华人民共和国认证认可条例》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十八条 本办法施行前制定的关于个人信息出境认证的相关规定与本办法不一致的，按照本办法执行。

第十九条 本办法自2026年1月1日起施行。

国家卫生健康委员会　公安部　国家互联网信息办公室

国家中医药管理局　国家疾病预防控制局

关于印发《医疗卫生机构数据安全和个人信息保护管理办法（试行）》的通知

国卫规划发〔2026〕6号

医疗卫生机构数据安全和个人信息保护管理办法（试行）

第一章 总则

第一条 为了规范医疗卫生机构数据安全和个人信息保护管理，促进医疗卫生机构数据开发和个人信息合理利用，保护个人、组织的合法权益，统筹发展和安全，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》《中华人民共和国基本医疗卫生与健康促进法》《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条 本办法适用于医疗卫生机构的数据安全和个人信息保护管理。

本办法所称的数据，是指任何以电子或者其他方式对信息的记录。

本办法所称的医疗卫生机构数据，是指医疗卫生机构收集和产生的各种数据，包括但不限于各类临床、科研、管理等业务数据与医疗设备产生的数据。

本办法所称的数据处理活动，包括数据的收集、存储、使用、加工、传输、提供、公开等。

个人信息是特别重要的一种数据，当达到一定精度、规模时，个人信息要按照数据分类分级管理要求，纳入国家重要数据目录进行重点保护。

第三条 在国家数据安全工作协调机制的统一部署下，国家卫生健康委、国家中医药局、国家疾控局负责统筹规划、指导、评估、监督医疗卫生机构数据安全和个人信息保护管理工作。县级以上地方卫生健康行政部门（含中医药和疾控部门，下同）负责本行政区域内医疗卫生机构数据安全和个人信息保护管理工作。医疗卫生机构按照属地管理的原则，接受卫生健康行政部门监管。

第四条 医疗卫生机构对本单位医疗卫生机构数据安全和个人信息保护管理负主体责任，县级以上医疗卫生机构应当成立网络安全和信息化工作领导小组，由单位主要负责人担任组长，每年至少召开一次医疗卫生机构数据安全和个人信息保护会议，部署数据安全和个人信息保护工作，研究制定相关制度规范。

医疗卫生机构主要负责人是本单位数据安全和个人信息保护管理第一责任人，分管负责人是直接责任人。按照“管业务必须管安全”“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，明确本单位业务部门与信息化部门的职责，加强医疗卫生机构数据安全和个人信息保护管理。

第二章 数据分类分级保护

第五条 依据有关法律和卫生健康行业数据分类分级有关要求，医疗卫生机构数据分为 核心数据 、重要数据和一般数据 ，落实分类分级保护制度。不同类别、级别数据同时被处理且难以分别采取保护措施的，按照其中级别最高的要求实施保护。

第六条 省级卫生健康行政部门按照卫生健康行业数据分类分级有关要求组织开展省域内医疗卫生机构数据的分类分级工作，提出重要数据具体目录和核心数据目录建议并报国家卫生健康委（中医领域报送国家中医药局、疾控领域报送国家疾控局），目录发生变化的，应当及时更新并上报。各级卫生健康行政部门确认为重要数据的，应当及时告知医疗卫生机构。

医疗卫生机构应当定期梳理医疗卫生机构数据，确定医疗卫生机构数据类别，识别重要数据，并向属地卫生健康行政部门报送，上报内容包括但不限于医疗卫生机构数据来源、类别、级别、规模、处理目的和方式、责任主体、跨境传输、安全保护措施等基本情况，不包括医疗卫生机构数据内容本身。

第七条 医疗卫生机构数据级别确定后，出现下列情形之一的，应对医疗卫生机构数据级别及时变更:

（一）医疗卫生机构数据内容发生较大变化。

（二）医疗卫生机构数据内容未发生变化，但医疗卫生机构数据规模、医疗卫生机构数据时效性、医疗卫生机构数据应用场景、医疗卫生机构数据加工处理方式等发生较大变化。

（三）需要对医疗卫生机构数据级别进行变更的其他情形。

第八条 医疗卫生机构数据经过脱敏、标签、统计、汇聚融合等加工活动而产生的衍生数据，应在原始数据定级的基础上，重新评估确定数据级别。

第三章 数据全生命周期安全管理

第九条 医疗卫生机构开展医疗卫生机构数据和个人信息处理活动，应当遵守法律法规规定，履行相应数据安全保护义务，坚持保障数据安全与发展并重，通过管理和技术手段保障医疗卫生机构数据安全和医疗卫生机构数据应用的有效平衡，通过开展包括但不限于以下工作，确保医疗卫生机构数据持续处于有效保护和合法合规利用的状态，防止未经授权的访问以及个人信息泄露、篡改、丢失:

（一）强化制度保障。建立医疗卫生机构数据安全管理制度、操作规程及技术规范，针对不同类别和级别的医疗卫生机构数据，明确收集、存储、使用、加工、传输、提供、公开等环节的具体保护要求。

（二）强化人员保障。加强医疗卫生机构数据安全管理人员队伍建设，定期开展医疗卫生机构数据安全教育和培训，提高全员数据安全、个人信息保护意识和水平。

（三）强化管理保障。严格医疗卫生机构数据和个人信息处理活动的日常管理，明确处理的操作权限。自行或委托第三方评估机构定期对本单位的医疗卫生机构数据进行安全风险评估，及时掌握数据安全状态，及时整改风险问题，消除隐患，并向属地卫生健康行政部门报送风险评估报告。

（四）强化技术保障。在医疗卫生机构数据的收集、存储、使用、加工、传输、提供、公开、删除等环节，针对不同场景综合运用加密、鉴权、认证、脱敏、去标识化、数字水印、校验、审计等技术手段进行安全保护。

（五）强化应急保障。根据工作实际与应对医疗卫生机构数据安全事件的需要，应制定完善应急预案，并定期开展演练。

（六）法律、行政法规等规定的其他措施。

第十条 处理重要数据的医疗卫生机构，应当明确医疗卫生机构数据安全负责人和管理机构，落实医疗卫生机构数据安全保护责任，每年度对其医疗卫生机构数据处理活动开展风险评估，并向省级及以上卫生健康行政部门报送风险评估报告，卫生健康行政部门应当及时通报同级网信部门、公安机关。医疗卫生机构提供、委托处理、共同处理重要数据前应当进行风险评估，属于履行法定职责或者法定义务的除外。

医疗卫生机构向其他医疗卫生机构数据处理者提供、委托处理重要数据的，应当通过合同等方式与接收方约定处理目的、方式、范围以及安全保护义务等，并对医疗卫生机构数据接收方履行义务的情况进行监督。

第十一条 医疗卫生机构在存储处理重要数据时要落实三级及以上网络安全等级保护要求。存储处理核心数据的，涉及关键信息基础设施的，要在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求，不涉及关键信息基础设施的，应落实四级网络安全等级保护要求。医疗卫生机构数据内容发生较大变化，需要变更医疗卫生机构数据级别的，应根据情况及时进行网络安全等级保护重新定级备案。法律法规和国家有关规定要求使用 商用密码 进行保护的，应当遵守商用密码保护有关规定。

进行核心数据跨不同法人主体提供、转移、共享等活动时，应采取必要的安全保护措施，并告知数据接收方按照对应级别进行分类分级保护。自当年度1月1日起可能累计达到上一年度末该项核心数据静态总量30%及以上的，应

经国家卫生健康委报有关部门组织风险评估。涉及国家机关依法履职、国家机关或企事业单位内部流动的除外。

医疗卫生机构在处理核心数据时，在重要数据保护要求的基础上:

（一）优先使用商用密码进行保护;

（二）优先使用安全可信的产品和服务;

（三）优先使用第三方评估机构开展风险评估;

（四）涉及核心数据安全事件处置、溯源的相关日志留存时间不少于三年;

（五）对相关关键岗位人员、涉核心数据信息系统建设和运维单位等，提交公安机关、国家安全机关进行国家安全背景审查。

第十二条 支持医疗卫生机构在确保医疗卫生机构数据安全的前提下，依法依规加强医疗卫生机构数据共享。医疗卫生机构应当加强对医疗卫生机构数据共享、调用的安全管理，采取技术措施定期监测医疗卫生机构数据共享调用等情况，对医疗卫生机构数据查询、下载、修改、删除等操作日志开展审计分析，及时发现违规或异常行为，采取相应处置措施，并配备认证鉴权、威胁告警等安全保护措施。

第十三条 支持医疗卫生机构在确保医疗卫生机构数据和个人信息安全的前提下，依法依规加强数据要素开发利用工作。

医疗卫生机构应当建立完善医疗卫生机构数据使用申请及批准流程，遵循“谁主管、谁审查”，坚持事前申请批准、事中监管、事后审核的原则，严格执行业务管理部门同意、医疗卫生机构领导核准、信息技术部门支撑执行的工作程序，如涉及对外提供医疗卫生机构数据的，需按相关要求报审，确保医疗卫生机构数据活动流程合法合规。医疗卫生机构应当对医疗卫生机构数据接收方履行安全管理责任进行监督。

鼓励医疗卫生机构通过“原始数据不出域，数据可用不可见，数据可控可计量”等方式，促进医疗卫生机构数据依法合理有效利用。

第十四条 医疗卫生机构依据国家关于公共数据资源开发利用的有关规定，按照公共数据资源授权运营实施规范，探索建立数据分类分级授权运营机制，将授权运营纳入医疗卫生机构领导班子集体决策范围，明确授权条件、运营模式、运营期限、退出机制和安全管理责任，授权符合条件的运营机构开展公共数据资源开发、产品经营和技术服务。

第十五条 卫生健康行政部门等国家机关为履行法定职责需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行。法律、行政法规和国家有关规定明确医疗卫生机构可以拒绝其他行政部门重复采集医疗卫生机构数据的，医疗卫生机构可以拒绝相关组织或个人收集超出履行法定职责所必需的范围和限度的医疗卫生机构数据。

各级卫生健康行政部门应当按照《中华人民共和国数据安全法》等法律、行政法规和国家有关规定，切实履行行业监管职责，加强向医疗卫生机构采集数据的归口管理，建立健全医疗卫生机构数据共享共用机制，加强部门间数据共享，各级全民健康信息平台和各级传染病监测预警与应急指挥平台已经采集的医疗卫生机构数据，原则上应通过跨部门共享交换实现。

医疗卫生机构应当及时将对外提供医疗卫生机构数据的情况报告属地卫生健康行政部门。属地卫生健康行政部门应当依法依规加强医疗卫生机构数据报送管理，重点管理重复采集医疗卫生机构数据、超范围采集医疗卫生机构数据等违反有关规定的情形。

第十六条 医疗卫生机构委托他人处理或与他人共同处理医疗卫生机构数据的，数据安全责任不因委托而改变。医疗卫生机构应当经过严格的审批程序，明确受托方的数据处理权限和保护责任，并监督受托方履行数据安全保护义务。

涉及使用云计算服务处理医疗卫生机构数据的，应当选择通过云计算服务安全评估的云计算服务，并同时遵守本办法有关要求。

卫生健康行政部门原则上不得委托学会、协会面向医疗卫生机构采集数据，确有必要的，应当经过卫生健康行政部门数据管理机构的统筹论证，并报同级卫生健康行政部门网络安全和信息化工作领导小组审核。

第十七条 医疗卫生机构应当与参与其信息化建设运行维护的相关单位及涉及医疗卫生机构数据存储的相关医疗设备生产经营企业书面约定各方义务和责任，落实责任追究制度。

第十八条 医疗卫生机构应当按照业务工作需要和最小授权原则，依据岗位职责设定医疗卫生机构数据处理权限，控制医疗卫生机构数据接触范围，人员变动时应当及时调整权限。

第十九条 重要数据处理活动应当记录维护数据安全所需的日志，涉及安全事件处置、溯源的，相关日志留存时间应当不少于一年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间应当不少于三年。

第二十条 医疗卫生机构在使用人工智能等新技术处理医疗卫生机构数据时，应当评估使用新技术带来的安全风险，采取必要的技术措施，加强医疗卫生机构数据安全防护。

第二十一条 医疗卫生机构因合并、分立、解散、被宣告破产等原因需要转移、销毁医疗卫生机构数据的，应当采取必要的安全保护措施，并事前向属地卫生健康行政部门报告医疗卫生机构数据处置方案。引起医疗卫生机构数据目录发生变化的，应当及时报告属地卫生健康行政部门。

第二十二条 医疗卫生机构应当加强对医疗卫生机构数据全生命周期的管理，医疗卫生机构及其人员不得有以下行为：

（一）不得违法采集医疗卫生机构数据。医疗卫生机构应当加强医疗卫生机构数据收集的合法性管理，明确业务部门和管理部门在医疗卫生机构数据收集合法性中的主体责任，不得超范围采集医疗卫生机构数据，不得窃取或者以其他非法方式采集医疗卫生机构数据。

（二）不得违法存储医疗卫生机构数据。医疗卫生机构在我国境内收集和产生的重要数据，应当在境内存储，并采取备份、加密等措施加强医疗卫生机构数据的存储安全。

（三）不得违法进行医疗卫生机构数据传输。医疗卫生机构应当在数据分类分级的基础上，进一步明确不同安全级别医疗卫生机构数据的加密传输要求，不得通过邮箱、网盘、社交软件等传输核心数据、重要数据和敏感数据。加强传输过程中的接口安全控制，采取数据脱敏、数据加密、链路加密等防控措施，确保在通过接口传输时的安全性，防止医疗卫生机构数据被窃取。

（四）不得违法向境外提供医疗卫生机构数据。医疗卫生机构采集的医疗卫生机构数据确需向境外提供，具有国家互联网信息办公室《促进和规范数据跨境流动规定》第七条规定情形之一的，医疗卫生机构应当先行开展自评估工作，经本单位网络安全和信息化工作领导小组或领导班子同意并报属地卫生健康行政部门审核通过后，由省级网信部门向国家网信部门申报医疗卫生机构数据出境安全评估。医疗卫生机构在学术合作活动中收集和产生的医疗卫生机构数据向境外提供，不包含个人信息、敏感数据或重要数据的，免予申报医疗卫生机构数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

（五）不得越权使用医疗卫生机构数据。医疗卫生机构应当严格规定不同人员的权限，加强医疗卫生机构数据使用过程中的申请及批准流程管理，加强日志留存及管理工作，不得篡改、删除日志，确保医疗卫生机构数据在可控范围内使用，防止医疗卫生机构数据越权使用。医疗卫生机构数据使用部门和医疗卫生机构数据使用者应当严格按照申请所述用途与范围使用医疗卫生机构数据，对医疗卫生机构数据的安全负责。非本医疗卫生机构人员在无监管情况下，不得对信息系统或医疗设备进行远程运维。

（六）不得未经授权处理医疗卫生机构数据。未经医疗卫生机构授权，医疗卫生机构信息系统建设运维人员不得处理医疗卫生机构数据；建设运维期间，收集产生的医疗卫生机构数据未经授权不得用于其他用途，服务完成后按照约定对医疗卫生机构数据予以返还或销毁；信息系统建设运维项目的承担单位，未经批准不得转包、分包。

（七）不得未经批准提供医疗卫生机构数据。未经医疗卫生机构网络安全和信息化工作领导小组或领导班子批准，任何部门和个人不得将未对外公开的

信息和医疗卫生机构数据传递至医疗卫生机构之外，不得以任何方式将其泄露。

（八）不得随意公开医疗卫生机构数据。医疗卫生机构在对医疗卫生机构数据公开前，应当分析研判可能对国家安全、经济社会安全、公共利益、个人信息安全及医疗卫生机构运行产生的影响，存在重大影响的不得公开。

（九）不得未经销毁医疗卫生机构数据报废设备或变更用途。医疗卫生机构在设备报废或变更用途前，应当按照电子产品信息清除技术要求对医疗卫生机构数据进行彻底清除处理，不得未经处置直接报废或转移他用。

（十）不得隐瞒医疗卫生机构数据安全事件。医疗卫生机构发生医疗卫生机构数据安全事件时，应当立即启动应急预案，采取措施防止危害扩大，消除安全隐患，并按照规定向属地卫生健康行政部门等有关主管部门报告。

第四章 数据安全监测预警和应急处置

第二十三条 国家卫生健康委建立健全医疗卫生机构数据安全风险监测预警机制，组织制定医疗卫生机构数据安全监测预警标准规范，统筹运用医疗卫生机构数据安全监测预警技术手段，具备监测、预警、处置、溯源等能力，与相关部门加强信息共享。

地方卫生健康行政部门建立健全本地区医疗卫生机构数据安全风险监测预警机制，组织开展医疗卫生机构数据安全风险监测，按照有关规定及时发布预警信息，指导医疗卫生机构及时采取应对措施。

医疗卫生机构应当建立医疗卫生机构数据安全风险监测预警与应急处置机制，及时通过国家信息安全漏洞共享平台等渠道获取信息系统应用漏洞，通过升级补丁、配置更新、系统加固等技术措施，防范医疗卫生机构数据被篡改、泄露、丢失等安全风险。

第二十四条 国家卫生健康委建立健全医疗卫生机构数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报医疗卫生机构数据安全风险隐患，鼓励行业组织、安全服务机构、科研所等开展医疗卫生机构数据安全险信息上报和共享。

地方卫生健康行政部门及时汇总分析本地区医疗卫生机构数据安全风险隐患，将可能造成重要数据或核心数据安全事件的风险隐患报国家卫健康委（中医领域国家中医药局、疾控领域报送国家疾控局）。

医疗卫生机构应当及时将可能造成重要数据或核心数据安全事件的风险隐患向属地卫生健康行政部门报告。

第二十五条 国家卫生健康委制定卫生健康行业数据安全事件应急预案并开展应急演练，指导涉及重要数据和核心数据的安全事件应急处置工作。

地方卫生健康行政部门分别组织开展本地区医疗卫生机构数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报国家卫生健康委，并及时报告事件发展和处置情况。

医疗卫生机构应当制定医疗卫生机构数据安全事件应急预案，并定期组织演练。发生医疗卫生机构数据安全事件后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，及时向属地卫生健康行政部门报告，安全事件处置完成后应当及时形成总结报告。发生医疗卫生机构数据安全事件时，应当及时告知用户，并采取避免、减轻危害的处置措施，同时向属地卫生健康行政部门报告。

第五章 个人信息保护

第二十六条 医疗卫生机构应当按照《个人信息保护合规审计管理办法》要求，自行或者委托专业机构定期开展个人信息保护合规审计工作。

第二十七条 医疗卫生机构委托处理个人信息时，应当事前进行个人信息保护影响评估并与受托方签订委托协议和保密协议，明确委托处理范围、目的、期限、处理方式、个人信息种类、保护措施以及双方的权利和义务，并监督协议执行情况。受托方应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息。委托合同不生效、无效、被撤销或者终止的，受托方应当将个人信息返还医疗卫生机构或者予以删除，不得保留。未经个人信息处理者同意，受托方不得委托他人处理个人信息。受托方应当对从业人员开展岗前培训和离职审查。

第二十八条 医疗卫生机构在使用人工智能等新技术过程中，涉及患者病历等个人信息的，必须确保个人信息安全。

第二十九条 医疗卫生机构应当加强对个人信息的保护，医疗卫生机构及其人员不得有以下行为:

（一）不得违法处理个人信息。医疗卫生机构及其人员不得违法收集、存储、使用、加工、传输、提供、公开、删除个人信息，不得非法买卖、提供或者公开传播个人信息，不得从事危害国家安全、公共利益的个人信息处理活动。

（二）不得违法收集个人信息。医疗卫生机构收集个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式收集个人信息。

（三）不得超范围收集个人信息。医疗卫生机构收集个人信息应当具有明确、合理的目的，应当限于实现处理目的的最小范围，不得过度收集个人信息。

（四）不得超授权调阅个人信息。医疗卫生机构应当采取有效措施和技术手段，严格身份认证，防范患者个人信息被无关人员违法查询或调取，应当制定授权规则，通过场景管理和人员管理结合的方式，明确医疗、教学、科研和公共卫生紧急情况等合法调阅情形，不得违法调阅，重点加强孕产妇、新生儿、艾滋病人、精神障碍患者、逝者及遗属、公众人物等特殊人群个人信息管理。区分不同岗位和人员，实行动态授权管理，及时回收离职离岗、转岗人员权限。推广使用授权管理、日志存档、数字水印等技术进行调阅权限管理，确保个人信息操作痕迹、标记操作时间和操作人员信息可查询、可追溯。

（五）不得违法提供个人信息。未经本人或者其监护人同意，医疗卫生机构及其人员不得超出工作需要提供个人的姓名、出生日期、身份证号码、生物识别信息、住址、电话号码、行踪轨迹等个人信息，为应对突发公共卫生事件或者紧急情况下为保护自然人的生命健康所必需等法律、行政法规另有规定的除外。因国家机关履行法定职责提供的，不得超出履行法定职责所必需的范围和限度。

（六）不得违法公开个人信息。医疗卫生机构不得在电子屏等公共区域，显示患者的个人姓名、身份证号码、电话号码等个人信息，确因业务需要的，应当脱敏显示。未经本人同意，不得在新闻报道、公开讲座、社交媒体、学术论文、科学研究等场景中公开患者个人信息。不得通过通讯软件、社交媒体等方式传输患者个人信息，不得通过拍照、截图等方式公开患者个人信息。

（七）不得违法向境外提供个人信息。医疗卫生机构因业务等需要，确需向境外提供个人信息的，应当符合《中华人民共和国个人信息保护法》第三十八条规定的条件，并向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使有关权利的方式和程序等事项，取得个人的单独同意。

（八）不得滥用人脸识别信息。应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家 人口基础信息库 、国家网络身份认证公共服务等渠道实施。实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，医疗卫生机构不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，医疗卫生机构应当提供其他合理、便捷的方式。除法律法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。

第六章 监督管理

第三十条 各级卫生健康行政部门发现医疗卫生机构数据处理活动存在较大安全风险或者发生数据安全事件的，应当督促指导医疗卫生机构及时处置并整改。

医疗卫生机构对卫生健康行政部门通报指出的安全漏洞隐患，应当及时开展安全整改加固，堵塞漏洞，消除风险。

医疗卫生机构应当配合网信部门与公安机关开展医疗卫生机构数据安全事件核查调查。

第三十一条 地方各级卫生健康行政部门不履行本办法规定的数据安全和个人信息保护义务的，由其上级机关责令改正；对直接负责的主管人员和其他直接责任人员依法依纪给予处分。

第三十二条 医疗卫生机构违反《中华人民共和国基本医疗卫生与健康促进法》规定，因医疗信息安全制度、保障措施不健全，导致医疗信息泄露的，由县级以上人民政府卫生健康等主管部门责令改正，给予警告，并处以罚款；情节严重的，可以责令停止相应执业活动，对直接负责的主管人员和其他直接责任人员依法追究法律责任。

医疗卫生机构的相关人员泄露公民个人信息的，由县级以上人民政府卫生健康行政主管部门依照有关执业医师、护士管理、个人信息保护等法律、行政法规的规定予以行政处罚，属于政府举办的医疗卫生机构中的人员的，依法给予处分。

非法收集、使用、加工、传输公民个人健康信息，非法买卖、提供或者公开公民个人健康信息等，构成违反治安管理行为的，依法给予治安管理处罚。

第三十三条 违反《中华人民共和国民法典》规定，泄露患者的隐私和个人信息，或者未经患者同意公开其病历资料的，应当承担侵权责任。

第三十四条 根据《中华人民共和国数据安全法》规定，各级卫生健康行政部门在履行医疗卫生机构数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关医疗卫生机构进行约谈，并要求医疗卫生机构采取措施进行整改，消除隐患。

医疗卫生机构违反《中华人民共和国数据安全法》，不履行规定的数据安全保护义务，或者向境外提供重要数据的，按照有关条款予以处理。

第三十五条 根据《中华人民共和国个人信息保护法》规定，各级卫生健康行政部门、网信部门和公安机关在履行职责中，发现医疗卫生机构存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该医疗卫生机构的法定代表人或者主要负责人进行约谈，或者要求医疗卫生机构委托专业机构对其个人信息处理活动进行合规审计。医疗卫生机构应当按照要求采取措施，进行整改，消除隐患。卫生健康等履行个人信息保护职责的部门在履行职责中，发现违反《中华人民共和国个人信息保护法》规定的，按照《中华人民共和国个人信息保护法》相关规定处理，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第三十六条 任何组织、个人有权对违法个人信息处理活动向卫生健康等履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。卫生健康等履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 附则

第三十七条 开展涉及国家秘密、工作秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第三十八条 医疗卫生机构可以根据本办法制定相应的实施细则。

第三十九条 本办法由国家卫生健康委负责解释。

第四十条 本办法自印发之日起施行。

国家卫生健康委员会　公安部　国家互联网信息办公室

国家中医药管理局　国家疾病预防控制局

2026 年 2 月 14 日

国家互联网信息办公室发布《数据出境安全评估申报指南（第三版）》

为了指导和帮助数据处理者规范有序申报数据出境安全评估，国家互联网信息办公室编制了《数据出境安全评估申报指南（第三版）》，对数据处理者申报数据出境安全评估需要提交的相关材料进行了优化简化，明确数据处理者申请延长数据出境安全评估结果有效期的条件、流程、材料等内容。

数据处理者因业务需要向境外提供重要数据和个人信息，符合数据出境安全评估适用情形的，应当根据《数据出境安全评估办法》和《促进和规范数据跨境流动规定》，按照申报指南申报数据出境安全评估。评估结果有效期届满，符合申请延长评估结果有效期条件的，数据处理者可以在有效期届满前60个工作日内提出延长评估结果有效期申请。

数据处理者可以通过线上方式申报。请直接访问“数据出境申报系统”（网址：https://sjcj.cac.gov.cn），也可从中国网信网（https://www.cac.gov.cn）首页“全国网信政务办事大厅”栏目访问“数据出境申报系统”。

国家互联网信息办公室

2025年6月27日

数据出境安全评估申报指南（第三版）

根据《数据出境安全评估办法》、《促进和规范数据跨境流动规定》，为指导和帮助数据处理者规范有序申报数据出境安全评估，特制定本指南。

一、适用范围

（一）数据处理者向境外提供数据，有下列情形之一的，应当申报数据出境安全评估:

1.关键信息基础设施运营者向境外提供个人信息或者重要数据;

2.关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息。

属于《促进和规范数据跨境流动规定》第三条、第四条、第五条、第六条规定情形的，从其规定。

（二）以下情形属于数据出境行为:

1.数据处理者将在境内运营中收集和产生的数据传输至境外;

2.数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出;

3.符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。

二、申报方式及流程

数据处理者申报数据出境安全评估，应当通过线上方式提交申报材料。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的数据处理者，采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估。

（一）系统登录与项目申报

数据出境申报系统网址：https://sjcj.cac.gov.cn。

1.账号注册与登录。对于初次登录申报系统进行申报的数据处理者，点击“注册账户”，填写用户名、密码、手机号码等信息。注册成功后，登录申报系统进行基础信息录入，填写数据处理者单位名称、统一社会信用代码、单位注册所在省份等。

2.项目新建与申报。数据处理者选择“数据出境安全评估”栏目，选择新增申报评估项目，并将准备好的申报材料进行上传。申报材料（材料要求见附件1）包括:

（1）统一社会信用代码证件影印件

（2）法定代表人身份证件影印件

（3）经办人身份证件影印件

（4）经办人授权委托书（模板见附件2）

（5）数据出境安全评估申报表（模板见附件3）

（6）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件

（7）数据出境风险自评估报告（模板见附件4）

（8）其他相关证明材料

数据处理者对所提交材料的真实性负责，提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

（二）完备性查验与项目受理

数据处理者可通过申报系统查看已申报项目的进展情况，具体包括:

1.省级网信办在数据处理者提交申报材料之日起5个工作日内完成申报材料的完备性查验，并同步更新申报系统内的完备性查验结果。未通过完备性查验的，省级网信办向数据处理者告知未通过完备性查验原因。

2.通过完备性查验的，省级网信办将申报材料提请国家网信办受理，国家网信办自收到省级网信办提交的申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者，并同步更新申报系统内的受理结果。

（三）补充更正材料与查询评估进展

国家网信办将在出具评估项目受理通知书后立即组织开展数据出境安全评估，需要补充或者更正申报材料的，数据处理者应当按照告知要求及时通过申报系统补充或者更正材料。无正当理由不补充或者更正申报材料的，国家网信办可以终止安全评估。情况复杂或者需要补充、更正材料的，国家网信办可以适当延长评估时间，并告知数据处理者预计延长的时间。

数据处理者可通过申报系统及时查询了解评估进展。评估完成后，国家网信办向数据处理者出具评估结果通知书。

数据处理者应当按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范相关数据出境活动。数据处理者对评估结果有异议的，可以在收到评估结果通知书15个工作日内向国家网信办申请复评，复评结果为最终结论。

三、申请延长评估结果有效期

（一）适用条件

评估结果准予开展的数据出境活动，同时符合以下条件的，数据处理者可以在评估结果有效期届满前60个工作日内，通过所在地省级网信办向国家网信办申请延长评估结果有效期:

1.数据出境的目的、范围等未发生变化;

2.数据处理者和境外接收方等未发生变化;

3.出境个人信息的，未来三年涉及自然人数量增幅不超过原评估结果准予过去三年出境数量的20%;

4.出境重要数据的，未来三年出境数据规模（MB/GB/TB）增幅不超过原评估结果准予过去三年出境数据规模的20%;

5.与境外接收方订立的法律文件符合《数据出境安全评估办法》第九条规定;

6.过去三年数据出境活动严格按照评估结果通知书合规开展，且未发生重大数据安全事件。

（二）申请延长

数据处理者申请延长评估结果有效期，应当通过申报系统提交申请材料。关键信息基础设施运营者或者其他不适合通过系统申请的数据处理者，采用线下方式提交申请材料。

针对通过线上方式申报项目的评估结果有效期延长申请，数据处理者登录申报系统后，可直接选择申报项目进行申请延长操作，上传申请材料；针对通过线下方式申报项目的评估结果有效期延长申请，数据处理者登录申报系统后，在“延长评估结果有效期”栏目下申请，输入申报项目时的受理编号，上传申请材料。申请材料包括：

1.统一社会信用代码证件影印件（无变化可不重新提供）

2.法定代表人身份证件影印件（无变化可不重新提供）

3.经办人身份证件影印件（无变化可不重新提供）

4.经办人授权委托书（模板见附件 2）

5.延长评估结果有效期申请表（模板见附件 5）

（三）完备性查验

数据处理者可通过申报系统查看已申请延长评估结果有效期项目的完备性查验情况。省级网信办在数据处理者提交申请材料之日起 5 个工作日内完成完备性查验，并同步更新系统内的完备性查验结果。未通过完备性查验的，省级网信办向数据处理者告知未通过完备性查验原因。通过完备性查验的，省级网信办将申请材料提交国家网信办。

（四）延长评估结果有效期审核

国家网信办自收到省级网信办提交的申请材料之日起 20 个工作日内，确定是否准予延长评估结果有效期并书面通知数据处理者。情况复杂或者需要补充、更正材料的，可以适当延长审核时间，并告知数据处理者预计延长的时间。数据处理者可通过申报系统查看延长评估结果有效期审核进展、补充或者更正材料，在收到延长评估结果有效期通知书后，应当按照数据出境安全管理相关法律法规和通知书的有关要求，规范相关数据出境活动。

四、咨询、举报联系方式

数据处理者如在申报过程中遇到任何疑问或需要协助，欢迎与我们联系，联系方式如下：

联系电话：010-55627135

电子邮箱：sjcj@cac.gov.cn

附件：1.数据出境安全评估申报材料要求

2.经办人授权委托书（模板）

3.数据出境安全评估申报表（模板）

4.数据出境风险自评估报告（模板）

5.延长评估结果有效期申请表（模板）

附件 1

数据出境安全评估申报材料要求

序号	材料名称	要求	备注
1	统一社会信用代码证件	影印件加盖公章	
2	法定代表人身份证件	影印件加盖公章	
3	经办人身份证件	影印件加盖公章	
4	经办人授权委托书		
5	数据出境安全评估申报表		使用中文填写
6	与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件		对数据出境相关约定条款作高亮、线框等显著标识。法律文件以中文版本为准，若仅有非中文版本，须同步提交准确的中文译本。
7	数据出境风险自评估报告		使用中文撰写
8	其他相关证明材料		

注：采用线下方式提交申报材料的数据处理者，需同步通过光盘提交相应电子版材料。

附件 2

经办人授权委托书（模板）

本人*姓名（身份证件号码：　）*系*数据处理者名称*的法定代表人，现授权我单位*姓名（身份证件号码：　）*为*数据出境安全评估申报工作/延长评估结果有效期申请工作*经办人。经办人代表我单位进行*数据出境安全评估申报工作/延长评估结果有效期申请工作*过程中的一切行为，包括所签署和上传的资料，我单位均予以承认，并将承担相应的法律责任。

授权委托期限：　年　月　日至　年　月　日

经办人无转委托权。

单位名称（盖章）：

法定代表人（签字）：

经 办 人（签字）：

年　月　日

附件 3

数据出境安全评估申报表（模板）

1 数据处理者情况	单位名称			
	单位性质	☐政府部门 ☐事业单位 ☐企业 ☐社会组织 ☐其他		
	单位类型	☐内资 ☐外资 ☐中外合资 ☐港澳台资 ☐其他		
	单位注册地		办公所在地	
	员工数量		统一社会信用代码	
	是否为关键信息基础设施运营者	☐是 ☐否	处理个人信息规模	*按自然人（去重）统计数量*
2 法定代表人信息	姓名		职务/国籍	
	联系电话		电子邮箱	
	证件类型	☐居民身份证 ☐护照 ☐台湾居民来往大陆通行证 ☐港澳居民来往内地通行证 ☐其他		
	证件号码			
3 数据安全负责人和管理机构信息	姓名		职务/国籍	
	联系电话		电子邮箱	
	证件类型	☐居民身份证 ☐护照 ☐台湾居民来往大陆通行证 ☐港澳居民来往内地通行证 ☐其他		
	证件号码			
	管理机构名称		管理机构人数	
4 经办人信息	姓名		职务/国籍	
	联系电话		电子邮箱	
	证件类型	☐居民身份证 ☐护照 ☐台湾居民来往大陆通行证 ☐港澳居民来往内地通行证 ☐其他		

<table>
<tr><td></td><td>证件号码</td><td colspan="4"></td></tr>
<tr><td>5 数据处理者遵守中国法律、行政法规、部门规章情况</td><td colspan="5">简述近 2 年在业务经营活动中受到行政处罚和有关主管监管部门调查及整改情况，重点说明数据和网络安全方面相关情况</td></tr>
<tr><td rowspan="11">6 数据出境场景 1</td><td>出境场景简述</td><td colspan="4">据实填写此次申报的数据出境场景业务、数据出境目的、数据出境方式等，应与法律文件中涉及业务名称一致，不超过 100 字（数据出境方式参考：公共互联网传输、跨境专线传输、公共互联网远程访问、跨境专线远程访问等）</td></tr>
<tr><td rowspan="4">拟出境数据情况</td><td rowspan="2">数据类型</td><td>☐重要数据</td><td colspan="2">重要数据认定主管部门名称</td></tr>
<tr><td>☐个人信息</td><td>是否包含敏感个人信息</td><td>☐是
☐否</td></tr>
<tr><td>涉及行业/领域</td><td colspan="3">☐工业 ☐电信 ☐交通 ☐金融
☐自然资源 ☐卫生健康 ☐教育
☐科技 ☐能源 ☐国防科工 ☐文旅
☐跨境电商 ☐零售 ☐互联网
☐其他</td></tr>
<tr><td>涉及自然人（去重）数量</td><td>包括当年已出境数量、未来三年出境数量以及两者的关系</td><td>涉及重要数据规模</td><td>MB/GB/TB</td></tr>
<tr><td rowspan="7">境外接收方情况</td><td>境外接收方名称</td><td colspan="3"></td></tr>
<tr><td>所在国家或者地区</td><td colspan="3"></td></tr>
<tr><td>所在地址</td><td colspan="3"></td></tr>
<tr><td>主营业务</td><td colspan="3"></td></tr>
<tr><td>负责人姓名</td><td></td><td>负责人职务</td><td></td></tr>
<tr><td>联系方式</td><td colspan="3">☐电话:
☐邮箱:</td></tr>
<tr><td colspan="4">统计说明: （如需）</td></tr>
</table>

6 数据出境场景 2	……
6 数据出境场景 3	……
本单位承诺: ☐申报材料所有内容真实、完整、准确和有效。为国家网信办组织实施的数据出境安全评估工作提供必要的配合和支持。自评估工作为申报之日前 3 个月内完成，且至申报之日未发生重大变化。若承诺不实或者违背承诺，愿意承担相应法律责任。	

注：1.自评估报告内容应与申报表内容保持一致。

2.申报表第 6 项应按场景分项描述，可根据实际申报的出境场景数量增加申报表第 6 项。

3.境外接收方数量众多、范围不确定、无法逐一列举的，申报表第 6 项境外接收方情况可填写统计数据。

4.申报表严格按照模板填写，必须使用中文填写，字体四号“仿宋”，数字、字母统一使用四号“Times New Roman”字体，行距固定值 16 磅，段落首行缩进 2 字符。页面设置：A4 纸，上下页边距为 2.54cm，左右页边距为 3.18cm。

附件 4

数据出境风险自评估报告（模板）

数据处理者名称:　　（盖章）

年　月　日

说明:

（一）数据处理者申报数据出境安全评估时需提供自评估报告，并对所提交的自评估报告及附件材料真实性负责;

（二）报告所述自评估活动为本次申报前3个月内完成;

（三）如有第三方机构参与自评估，须在自评估报告中说明第三方机构的基本情况及参与评估的情况;

（四）自评估报告严格按照模板撰写。自评估报告必须使用中文撰写，正文字体四号“仿宋”（其中，正文一级标题黑体、二级标题楷体加黑、三级标题仿宋加黑），数字、字母使用四号“Times New Roman”字体，行距固定值26磅，段落首行缩进2字符。页面设置：A4纸，上下页边距为2.54cm，左右页边距为3.18cm。

一、自评估工作情况

简要概述自评估工作开展情况，包括起止时间、组织情况、实施过程、实施方式等内容。

二、出境活动整体情况

简要说明数据处理者基本情况、数据处理者安全保障能力情况、境外接收方情况、法律文件约定情况等，详细说明拟出境数据情况。包括不限于:

（一）数据处理者基本情况

1.基本情况简介，包括股权结构、实际控制人、境内外投资情况等;

2.组织架构和数据安全管理机构信息;

3.整体业务与数据资产情况。

（二）拟出境数据情况

1.数据出境涉及业务、数据资产等情况;

2.数据出境及境外接收方处理数据的目的、范围、方式，及其合法性、正当性、必要性;

3.按照申报业务场景梳理对应的出境数据项情况，以列表形式呈现数据项清单并逐一说明（如下表所示），同一场景下的数据项需去重;

序号	数据项名称	内容描述	出境必要性	示例	备注
1					
2					
.....					

4.拟出境数据在境内存储的系统平台、数据中心（包含云服务）等情况，数据出境链路相关情况（数据处理者、境外接收方的网络系统域名及网络地址，数据出境方式等），计划出境后存储的系统平台、数据中心等;

5.数据出境后向境外其他接收方提供的情况;

6.涉及个人信息的，按照自然人（去重）统计当年的出境数量，预估未来3年的出境数量。

（三）数据处理者数据安全保障能力情况

1.数据安全管理能力，包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况;

（涉及个人信息出境的，需提供履行《个人信息保护法》第三十九条规定的情况说明及佐证材料，包括告知义务和取得个人的单独同意等，若属于《个人信息保护法》第十三条第一款第二项至第七项规定情形的，不需取得个

人同意）

2.数据安全技术能力，包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等;

3.数据安全保障措施有效性证明，例如开展的数据安全风险评估、数据安全认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评等情况;

4.遵守数据和网络安全相关法律法规的情况。

（如涉及受到行政处罚和监管整改的，可以提供证明整改完成的相关佐证材料）

（四）境外接收方情况

1.境外接收方基本情况;

2.境外接收方处理数据的用途、方式等;

3.境外接收方履行责任义务的管理和技术措施、能力等。

（五）法律文件约定数据安全保护责任义务的情况

1.数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等;

2.数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施;

3.对于境外接收方将出境数据再转移给其他组织、个人的约束性要求;

4.境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化，以及发生其他不可抗力情形，导致难以保障数据安全时，应当采取的安全措施;

5.违反法律文件约定的数据安全保护义务的补救措施、

违约责任和争议解决方式;

6.出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

（六）数据处理者认为需要说明的其他情况

三、出境活动的风险自评估情况及结论

对照《数据出境安全评估办法》第五条规定事项，说明数据出境风险自评估情况，重点说明自评估发现的问题和整改情况。

综合风险自评估情况和相应整改情况，对拟申报的数据出境活动作出客观的风险自评估结论，充分说明得出自评估结论的理由。

附件 5

延长评估结果有效期申请表（模板）

1 基本情况	
数据处理者名称	
申请延长评估结果有效期的评估项目受理编号	
与境外接收方订立的法律文件符合《数据出境安全评估办法》第九条规定	□是　□否
2 数据出境场景 1	
数据出境的目的、范围等未发生变化	□是　□否
数据处理者和境外接收方等未发生变化	□是　□否
出境个人信息的，未来三年涉及自然人数量增幅（与原评估结果准予过去三年出境数量相比）	_____%　□不涉及
出境重要数据的，未来三年出境数据规模增幅（与原评估结果准予过去三年出境数据规模相比）	_____%　□不涉及
数据出境链路、存储系统、数据中心未发生变化	□是　□否（如变化请在“3 其他需要说明的情况”描述变化情况）
境外接收方处理数据的用途和方式未发生变化	□是　□否（如变化请在“3 其他需要说明的情况”描述变化情况）
2 数据出境场景 2	
.....	
2 数据出境场景 3	

……
3 其他需要说明的情况
主要说明以下情况，可另附页: *（1）采取保障数据出境安全的措施及相关工作情况;* *（2）境外接收方按照法律文件履行出境数据安全责任义务情况;* *（3）过去三年按照评估结果通知书合规开展数据出境活动的基本情况;* *（4）过去三年发生重大数据安全事件以及在业务经营活动中受到行政处罚和有关主管监管部门调查、整改情况。*
本单位承诺: ☐申请材料所有内容真实、完整、准确和有效。为国家网信办组织实施的延长评估结果有效期审核工作提供必要的配合和支持。若承诺不实或者违背承诺，愿意承担相应法律责任。

注：1.申请表第 2 项应按场景分项描述，可根据实际申请的出境场景

数量增加申请表第 2 项。

2.申请表严格按照模板填写，必须使用中文填写，字体四号“仿宋”，数字、字母统一使用四号“Times New Roman”字体，行距

固定值 16 磅，段落首行缩进 2 字符。页面设置：A4 纸，上下页边距为 2.54cm，左右页边距为 3.18cm。

国家互联网信息办公室发布《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》

为了指导和帮助数据处理者规范有序申报数据出境安全评估、备案个人信息出境标准合同，国家互联网信息办公室编制了《数据出境安全评估申报指南（第二版）》、《个人信息出境标准合同备案指南（第二版）》，对申报数据出境安全评估、备案个人信息出境标准合同的方式、流程和材料等具体要求作出了说明，对数据处理者需要提交的相关材料进行了优化简化。

数据处理者因业务需要向境外提供重要数据和个人信息，应当遵守《数据出境安全评估办法》、《个人信息出境标准合同办法》和《促进和规范数据跨境流动规定》有关规定。符合数据出境安全评估适用情形的，按照申报指南申报数据出境安全评估；通过与境外接收方订立个人信息出境标准合同的方式向境外提供个人信息的，按照备案指南向所在地省级网信部门备案。

国家互联网信息办公室开通了“数据出境申报系统”，网址：https://sjcj.cac.gov.cn。数据处理者可以通过该系统申报数据出境安全评估、备案个人信息出境标准合同，具体使用说明见系统首页《用户手册》。

国家互联网信息办公室

2024年3月22日

个人信息出境标准合同备案指南（第二版）

根据《个人信息出境标准合同办法》、《促进和规范数据跨境流动规定》，为指导和帮助个人信息处理者规范有序备案个人信息出境标准合同（以下简称标准合同），特制定本指南。

一、适用范围

个人信息处理者通过订立标准合同的方式向境外提供个人信息，同时符合下列情形的应当向所在地省级网信部门备案：

（一）关键信息基础设施运营者以外的数据处理者；

（二）自当年1月1日起，累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）的；

（三）自当年1月1日起，累计向境外提供不满1万人敏感个人信息的。

属于《促进和规范数据跨境流动规定》第三条、第四条、第五条、第六条规定情形的，从其规定。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

以下情形属于个人信息出境行为:

（一）个人信息处理者将在境内运营中收集和产生的个人信息传输至境外;

（二）个人信息处理者收集和产生的个人信息存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出;

（三）符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他个人信息处理活动。

二、备案方式

个人信息处理者应当在标准合同生效之日起10个工作日内，通过数据出境申报系统备案，系统网址为 https://sjcj.cac.gov.cn。

三、备案流程

标准合同备案流程包括材料提交、材料查验及反馈备案结果、补充或者重新备案等环节。

（一）材料提交

个人信息处理者备案标准合同，应当提交如下材料（要求见附件1）:

1.统一社会信用代码证件影印件

2.法定代表人身份证件影印件

3.经办人身份证件影印件

4.经办人授权委托书（模板见附件2）

5.承诺书（模板见附件3）

6.标准合同（范本见附件4）

7.《个人信息保护影响评估报告》（模板见附件5）

（二）材料查验及反馈备案结果

省级网信办应当自个人信息处理者提交备案材料之日起15个工作日内完成材料查验，并向符合备案要求的个人信息处理者发放备案编号。需要补充完善材料的，个人信息处理者应当在10个工作日内提交补充完善材料；逾期未补充完善材料的，可以终止本次备案程序。

（三）补充或者重新备案

在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续:

1.向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的;

2.境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的;

3.可能影响个人信息权益的其他情形。

个人信息处理者在标准合同有效期内补充订立标准合同的，应当向所在地省级网信办提交补充材料；重新订立标准合同的，应当重新备案。补充或者重新备案的材料查验时间为 15 个工作日。

个人信息处理者对所提交材料的真实性负责，提交虚假材料的，注销备案编号，并依法追究相应法律责任。

四、咨询、举报联系方式

联系电话：010-55627565

电子邮箱：bzht@cac.gov.cn

附件：1.个人信息出境标准合同备案材料要求

2.经办人授权委托书（模板）

3.承诺书（模板）

4.个人信息出境标准合同（范本）

5.个人信息保护影响评估报告（模板）

附件 1

个人信息出境标准合同备案材料要求

序号	材料名称	要求
1	统一社会信用代码证件	影印件加盖公章
2	法定代表人身份证件	影印件加盖公章
3	经办人身份证件	影印件加盖公章
4	经办人授权委托书	
5	承诺书	
6	个人信息出境标准合同	
7	个人信息保护影响评估报告	使用中文撰写

附件 2

经办人授权委托书（模板）

本人 *姓名（身份证件号码：　）*系 *个人信息处理者名称*的法定代表人，现授权我单位 *姓名（身份证件号码：　）*为个人信息出境标准合同备案经办人。经办人代表我单位进行个人信息出境标准合同备案过程中的一切行为，包括所签署和上传的资料，我单位均予以承认，并将承担相应的法律责任。

授权委托期限：__年__月__日至__年__月__日

经办人无转委托权。

单位名称（盖章）：

法定代表人（签字）：

经 办 人（签字）：

年　月　日

附件 3

承 诺 书（模板）

本单位郑重承诺:

一、出境个人信息的收集、使用符合中华人民共和国有关法律法规规定;

二、备案材料所有内容真实、完整、准确和有效;

三、未采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供;

四、为国家网信办组织实施的个人信息出境标准合同备案工作提供必要的配合和支持;

五、个人信息保护影响评估工作为备案之日前 3 个月内完成，且至备案之日未发生重大变化。

本单位知晓并充分理解上述承诺内容，若承诺不实或者违背承诺，愿意承担相应法律责任。

法定代表人（签字）:

单位（盖章）:

年 月 日

附件 4

个人信息出境标准合同

国家互联网信息办公室 制定

为了确保境外接收方处理个人信息的活动达到中华人民共和国相关法律法规规定的个人信息保护标准，明确个人信息处理者和境外接收方个人信息保护的权利和义务，经双方协商一致，订立本合同。

个人信息处理者：_____

地址：_____

联系方式：_____

联系人：_____职务：_____

境外接收方：_____

地址：_____

联系方式：_____

联系人：_____职务：_____

个人信息处理者与境外接收方依据本合同约定开展个人信息出境活动，与此活动相关的商业行为，双方【已】/【约定】于_年_月_日订立 （商业合同，如有）。

本合同正文根据《个人信息出境标准合同办法》的要求拟定，在不与本合同正文内容相冲突的前提下，双方如有其他约定可在附录二中详述，附录构成本合同的组成部分。

第一条 定义

在本合同中，除上下文另有规定外：

（一）“个人信息处理者”是指在个人信息处理活动中自主决定处理目的、处理方式的，向中华人民共和国境外提供个人信息的组织、个人。

（二）“境外接收方”是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。

（三）个人信息处理者或者境外接收方单称“一方”，合称“双方”。

（四）“个人信息主体”是指个人信息所识别或者关联的自然人。

（五）“个人信息”是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

（六）“敏感个人信息”是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

（七）“监管机构”是指中华人民共和国省级以上网信部门。

（八）“相关法律法规”是指《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》《中华人民共和国民法典》《中华人民共和国民事诉讼法》《个人信息出境标准合同办法》等中华人民共和国法律法规。

（九）本合同其他未定义术语的含义与相关法律法规规定的含义一致。

第二条 个人信息处理者的义务

个人信息处理者应当履行下列义务：

（一）按照相关法律法规规定处理个人信息，向境外提供的个人信息仅限于实现处理目的所需的最小范围。

（二）向个人信息主体告知境外接收方的名称或者姓名、联系方式、附录一“个人信息出境说明”中处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

（三）基于个人同意向境外提供个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

（四）向个人信息主体告知其与境外接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在30日内明确拒绝，则可以依据本合同享有第三方受益人的权利。

（五）尽合理地努力确保境外接收方采取如下技术和管理措施（综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外接收方的保存期限等可能带来的个人信息安全风险），以履行本合同约定的义务：

（如加密、匿名化、去标识化、访问控制等技术和管理措施）

（六）根据境外接收方的要求向境外接收方提供相关法律规定和技术标准的副本。

（七）答复监管机构关于境外接收方的个人信息处理活动的询问。

（八）按照相关法律法规对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。重点评估以下内容：

1.个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性。

2.出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险。

3.境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全。

4.个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等。

5.按照本合同第四条评估当地个人信息保护政策和法规对合同履行的影响。

6.其他可能影响个人信息出境安全的事项。

保存个人信息保护影响评估报告至少 3 年。

（九）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（十）对本合同义务的履行承担举证责任。

（十一）根据相关法律法规要求，向监管机构提供本合同第三条第十一项所述的信息，包括所有合规审计结果。

第三条 境外接收方的义务

境外接收方应当履行下列义务：

（一）按照附录一“个人信息出境说明”所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。

（二）受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。

（三）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（四）采取对个人权益影响最小的方式处理个人信息。

（五）个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

（六）按下列方式保障个人信息处理安全：

1.采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。

2.确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。

（七）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问，应当开展下列工作：

1.及时采取适当补救措施，减轻对个人信息主体造成的不利影响。

2.立即通知个人信息处理者，并根据相关法律法规要求报告监管机构。通知应当包含下列事项：

（1）发生或者可能发生篡改、破坏、泄露、丢失、非法利用、

未经授权提供或者访问的个人信息种类、原因和可能造成的危害。

（2）已采取的补救措施。

（3）个人信息主体可以采取的减轻危害的措施。

（4）负责处理相关情况的负责人或者负责团队的联系方式。

3.相关法律法规要求通知个人信息主体的，通知的内容包含本项第 2 目的事项。受个人信息处理者委托处理个人信息的，由个人信息处理者通知个人信息主体。

4.记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。

（八）同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息：

1.确有业务需要。

2.已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

3.基于个人同意处理个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

4.与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任。

5.根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。

（九）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一“个人信息出境说明”中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。

（十）利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者向个人信息主体提供便捷的拒绝方式。

（十一）承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。

（十二）对开展的个人信息处理活动进行客观记录，保存记录至少 3 年，并按照相关法律法规要求直接或者通过个人信息处理者向监管机构提供相关记录文件。

（十三）同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问、配合监管机构检查、服从监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。

第四条 境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响

（一）双方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。

（二）双方声明，在作出本条第一项的保证时，已经结合下列情形进行评估：

1.出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。

2.境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素：

（1）该国家或者地区现行的个人信息保护法律法规及普遍适用的标准。

（2）该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺。

（3）该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

3.境外接收方安全管理制度和技术手段保障能力。

（三）境外接收方保证，在根据本条第二项进行评估时，已尽最大努力为个人信息处理者提供了必要的相关信息。

（四）双方应当记录根据本条第二项进行评估的过程和结果。

（五）因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。

（六）境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个人信息要求的，应当立即通知个人信息处理者。

第五条 个人信息主体的权利

双方约定个人信息主体作为本合同第三方受益人享有以下权利：

（一）个人信息主体依据相关法律法规，对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理，有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。

（二）当个人信息主体要求对已经出境的个人信息行使上述权利时，个人信息主体可以请求个人信息处理者采取适当措施实现，或者直接向境外接收方提出请求。个人信息处理者无法实现的，应当通知并要求境外接收方协助实现。

（三）境外接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照相关法律法规所享有的权利。

境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。

（四）境外接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机构提出投诉和寻求司法救济的途径。

（五）个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和境外接收方的一方或者双方主张并要求履行本合同项下与个人信息主体权利相关的下列条款：

1.第二条，但第二条第五项、第六项、第七项、第十一项除外。

2.第三条，但第三条第七项第 2 目和第 4 目、第九项、第十一项、第十二项、第十三项除外。

3.第四条，但第四条第五项、第六项除外。

4.第五条。

5.第六条。

6.第八条第二项、第三项。

7.第九条第五项。

上述约定不影响个人信息主体依据《中华人民共和国个人信息保护法》享有的权益。

第六条 救济

（一）境外接收方应当确定一个联系人，授权其答复有关个人信息处理的询问或者投诉，并应当及时处理个人信息主体的询问或者投诉。境外接收方应当将联系人信息告知个人信息处理者，并以简洁易懂的方式，通过单独通知或者在其网站公告，告知个人信息主体该联系人信息，具体为：

联系人及联系方式（办公电话或电子邮箱）

（二）一方因履行本合同与个人信息主体发生争议的，应当通知另一方，双方应当合作解决争议。

（三）争议未能友好解决，个人信息主体根据第五条行使第三方受益人的权利的，境外接收方接受个人信息主体通过下列形式维护权利：

1.向监管机构投诉。

2.向本条第五项约定的法院提起诉讼。

（四）双方同意个人信息主体就本合同争议行使第三方受益人

权利，个人信息主体选择适用中华人民共和国相关法律法规的，从其选择。

（五）双方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》向有管辖权的人民法院提起诉讼。

（六）双方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。

第七条 合同解除

（一）境外接收方违反本合同约定的义务，或者境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，个人信息处理者可以暂停向境外接收方提供个人信息，直到违约行为被改正或者合同被解除。

（二）有下列情形之一的，个人信息处理者有权解除本合同，并在必要时通知监管机构：

1.个人信息处理者根据本条第一项的规定暂停向境外接收方提供个人信息的时间超过 1 个月。

2.境外接收方遵守本合同将违反其所在国家或者地区的法律规定。

3.境外接收方严重或者持续违反本合同约定的义务。

4.根据境外接收方的主管法院或者监管机构作出的终局决定，境外接收方或者个人信息处理者违反了本合同约定的义务。

在本项第 1 目、第 2 目、第 4 目的情况下，境外接收方可以解除本合同。

（三）经双方同意解除本合同的，合同解除不免除其在个人信息处理过程中的个人信息保护义务。

（四）合同解除时，境外接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

第八条 违约责任

（一）双方应就其违反本合同而给对方造成的损失承担责任。

（二）任何一方因违反本合同而侵害个人信息主体享有的权利，应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应当承担的行政、刑事等法律责任。

（三）双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。

第九条 其他

（一）如本合同与双方订立的任何其他法律文件发生冲突，本合同的条款优先适用。

（二）本合同的成立、效力、履行、解释、因本合同引起的双方间的任何争议，适用中华人民共和国相关法律法规。

（三）发出的通知应当以电子邮件、电报、电传、传真（以航

空信件寄送确认副本）或者航空挂号信发往（具体地址）或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的__天应当视为收讫；如以电子邮件、电报、电传或者传真发出，在发出以后的__个工作日应当视为收讫。

（四）双方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，双方应当协商解决；协商解决不成的，任何一方可以采取下列第__种方式加以解决（如选择仲裁，请勾选仲裁机构）：

1.仲裁。将该争议提交

□中国国际经济贸易仲裁委员会

□中国海事仲裁委员会

□北京仲裁委员会（北京国际仲裁中心）

□上海国际仲裁中心

□其他《承认及执行外国仲裁裁决公约》成员的仲裁机构

按其届时有效的仲裁规则在（仲裁地点）进行仲裁；

2.诉讼。依法向中华人民共和国有管辖权的人民法院提起诉讼。

（五）本合同应当按照相关法律法规的规定进行解释，不得以与相关法律法规规定的权利、义务相抵触的方式解释本合同。

（六）本合同正本一式__份，双方各执__份，其法律效力相同。

本合同在（地点）签订

个人信息处理者：_____

____年____月____日

境外接收方：_____

____年____月____日

附录一

个人信息出境说明

根据本合同向境外提供个人信息的详情约定如下：

（一）处理目的：

（二）处理方式：

（三）出境个人信息的规模：

（四）出境个人信息种类（参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：

（五）出境敏感个人信息种类（如适用，参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：

（六）境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）：

（七）传输方式：

（八）出境后保存期限：

（ 年 月 日至 年 月 日）

（九）出境后保存地点：

（十）其他事项（视情况填写）：

附录二

双方约定的其他条款（如需要）

附件 5

个人信息保护影响评估报告（模板）

（出境版）

个人信息处理者名称：__（盖章）__

年 月 日

说明:

（一）个人信息处理者备案个人信息出境标准合同时需提供个人信息保护影响评估报告，并对所提交的评估报告真实性负责;

（二）报告所述评估工作为本次申报前 3 个月内完成;

（三）如有第三方机构参与评估，须在评估报告中说明第三方机构的基本情况及参与评估的情况;

（四）评估报告严格按照模板撰写。评估报告必须使用中文撰写，正文字体四号“仿宋”（其中，正文一级标题黑体、二级标题楷体加黑、三级标题仿宋加黑），数字、字母使用四号“Times New Roman”字体，行距固定值 26 磅，段落首行缩进 2 字符。页面设置：A4 纸，上下页边距为 2.54cm，左右页边距为 3.18cm。

一、出境活动整体情况

（一）个人信息处理者基本情况

1.基本情况简介，包括股权结构、实际控制人、境内外投资情况、组织架构和个人信息保护机构信息等。

2.整体业务与处理个人信息情况。

3.拟出境个人信息情况。

（1）个人信息出境涉及业务、个人信息收集使用、信息系统等情况;

（2）个人信息处理者和境外接收方处理个人信息的目的、范围、方式，及其合法性、正当性、必要性;

（3）出境个人信息的规模、范围、种类、敏感程度，处理敏感个人信息情况;

（4）拟出境个人信息在境内存储的系统平台、数据中心等情况，个人信息出境链路相关情况，计划出境后存储的系统平台、数据中心等;

（5）个人信息出境后向境外其他接收方提供的情况。

4.遵守个人信息保护相关法律法规的情况。

（二）境外接收方情况

1.境外接收方基本情况;

2.境外接收方处理个人信息的用途、方式等;

3.境外接收方履行责任义务的管理和技术措施、能力等。

（三）个人信息处理者认为需要说明的其他情况

二、拟出境活动的影响评估情况及结论

对照《个人信息出境标准合同办法》第五条规定事项，说明个人信息保护影响评估情况，重点说明评估发现的问题和整改情况。

综合影响评估情况和相应整改情况，对个人信息出境活动作出客观的影响评估结论，充分说明得出评估结论的理由和论据。

国家互联网信息办公室　香港创新科技及工业局公告

2023 年 3 号

落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局关于促进粤港澳大湾区数据跨境流动的合作备忘录》关于“共同制定粤港澳大湾区个人信息跨境标准合同并组织实施，加强个人信息跨境标准合同备案管理”的合作措施，国家互联网信息办公室与香港创新科技及工业局共同制定《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》，现予公布。

特此公告。

国家互联网信息办公室　王京涛

香港特区政府创新科技及工业局　孙东

2023 年 12 月 10 日

粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引

第一条 为促进粤港澳大湾区个人信息跨境安全有序流动，推动粤港澳大湾区高质量发展，落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局 关于促进粤港澳大湾区数据跨境流动的合作备忘录》（以下简称备忘录），国家互联网信息办公室、香港特别行政区政府创新科技及工业局共同制定本实施指引。

第二条 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》（以下简称标准合同，见附件 1）为备忘录下有关促进粤港澳大湾区个人信息跨境流动的便利措施。粤港澳大湾区个人信息处理者及接收方可以按照本实施指引要求，通过订立标准合同的方式进行粤港澳大湾区内内地和香港之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。

个人信息处理者及接收方应注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者香港特别行政区。

第三条 通过订立标准合同的方式开展个人信息跨境提供的，应当坚持自主缔约与备案管理相结合、保护个人信息权益与防范风险相结合，保障个人信息跨境安全、自由流动。

第四条 按照本实施指引，通过订立标准合同跨境提供个人信息的，应当履行标准合同列明的义务和责任，包括满足以下条件:

（一）个人信息处理者跨境提供个人信息前，应当按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意;

（二）不得向粤港澳大湾区以外的组织、个人提供。

第五条 个人信息处理者按照本实施指引，通过订立标准合同跨境提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容:

（一）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性;

（二）对个人信息主体权益的影响及安全风险;

（三）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。

第六条 标准合同应当严格按照本实施指引附件订立，合同生效后方可开展个人信息跨境提供。

个人信息处理者可以与接收方约定其他条款，但不得与标准合同相冲突。

第七条 跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化，延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续。

第八条 个人信息处理者及接收方应在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者香港特别行政区政府政府资讯科技总监办公室进行标准合同备案，提交如下材料:

（一）法定代表人身份证件影印件;

（二）承诺书（模板见附件 2）;

（三）标准合同。

个人信息处理者及接收方应当对所备案材料的真实性负责。

第九条 个人信息处理者及接收方接受属地监管机构的监督管理，包括但不限于:

（一）根据标准合同第二条第七项及第十项，个人信息处理者答复监管机构的询问及对合同的义务和责任的履行承担举证责任;

（二）根据标准合同第三条第十二项，接收方应接受监管机构的监督管理，包括服从监管机构作出的决定以及提供已采取必要行动的证明等;

（三）根据标准合同第六条第二项，个人信息处理者解除标准合同时，通知监管机构。

第十条 任何组织和个人发现个人信息处理者或接收方按照本实施指引进行粤港澳大湾区内的个人信息跨境流动，但不履行本实施指引及标准合同要求的义务和责任的，可以向国家互联网信息办公室、广东省互联网信息办公室或者

香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署投诉、举报。

收到投诉、举报的部门发现个人信息跨境活动存在较大安全风险或者发生个人信息安全事件的，可以要求个人信息处理者或者接收方整改；需要交由其他执法部门处置的，交由相关部门依法处置。

第十一条 个人信息处理者或接收方在处理个人信息时发生个人信息泄露等安全事件的，应立即采取补救措施，按照属地通知国家互联网信息办公室、广东省互联网信息办公室，或者香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署。

第十二条 以上规定并不影响内地履行个人信息保护职责的部门和香港个人资料私隐专员公署在职责范围内依法加强个人信息保护和监督管理工作，包括处理与个人信息保护有关的投诉、举报，调查、处理违法个人信息处理活动等。

第十三条 有关部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十四条 国家互联网信息办公室和香港特别行政区政府创新科技及工业局可以根据实际情况，经协商一致后对本实施指引及附件进行修订。

第十五条 本实施指引自发布之日起生效。

国家互联网信息办公室
澳门特别行政区政府经济及科技发展局
澳门特别行政区政府个人资料保护局

公　告

2024 年第 1 号

落实《中华人民共和国国家互联网信息办公室与澳门特别行政区政府经济财政司关于促进粤港澳大湾区数据跨境流动的合作备忘录》关于“共同制定粤港澳大湾区个人信息跨境标准合同并组织推动实施，加强个人信息跨境标准合同备案管理”的合作措施，国家互联网信息办公室与澳门特别行政区政府经济及科技发展局、澳门特别行政区政府个人资料保护局共同制定《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》，现予公布。

特此公告。

国家互联网信息办公室　王京涛
澳门特别行政区政府经济及科技发展局　戴建业
澳门特别行政区政府个人资料保护局　杨崇蔚
2024 年 9 月 10 日

粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引

第一条 为促进粤港澳大湾区个人信息跨境安全有序流动，推动粤港澳大湾区高质量发展，落实《中华人民共和国国家互联网信息办公室与澳门特别行政区政府经济财政司 关于促进粤港澳大湾区数据跨境流动的合作备忘录》（以下简称备忘录），国家互联网信息办公室、澳门特别行政区政府经济及科技发展局、澳门特别行政区政府个人资料保护局共同制定本实施指引。

第二条 《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同》（以下简称标准合同，见附件 1）为备忘录下有关促进粤港澳大湾区个人信息跨境流动的便利措施。粤港澳大湾区个人信息处理者及接收方可以按照本实施指引要求，通过订立标准合同的方式进行粤港澳大湾区内内地和澳门之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。

个人信息处理者及接收方应注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者澳门特别行政区。

第三条 通过订立标准合同的方式开展个人信息跨境提供的，应当坚持自主缔约与备案管理相结合、保护个人信息权益与防范风险相结合，保障个人信息跨境安全、自由流动。

第四条 按照本实施指引，通过订立标准合同跨境提供个人信息的，应当履行标准合同列明的义务和责任，包括满足以下条件:

（一）个人信息处理者跨境提供个人信息前，应当按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意;

（二）不得向粤港澳大湾区以外的组织、个人提供。

第五条 个人信息处理者按照本实施指引，通过订立标准合同跨境提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容:

（一）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性;

（二）对个人信息主体权益的影响及安全风险;

（三）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。

第六条 标准合同应当严格按照本实施指引附件订立，合同生效后方可开展个人信息跨境提供。

个人信息处理者可以与接收方约定其他条款，但不得与标准合同相冲突。

第七条 个人信息处理者及接收方应在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者澳门特别行政区政府个人资料保护局进行标准合同备案，提交如下材料:

（一）承诺书（模板见附件 2）;

（二）标准合同;

（三）属地监管机构要求的其他材料。

个人信息处理者及接收方应当对所备案材料的真实性负责。

第八条 跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化，延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并按照个人信息处理者属地法律法规要求履行备案手续和法定通知义务。

第九条 任何组织和个人发现个人信息处理者或接收方按照本实施指引进行粤港澳大湾区内的个人信息跨境流动，但不履行本实施指引及标准合同要求的义务和责任的，可以向国家互联网信息办公室、广东省互联网信息办公室或者澳门特别行政区政府个人资料保护局投诉、举报。

收到投诉、举报的部门发现个人信息跨境活动存在较大安全风险或者发生个人信息安全事件的，可以要求个人信息处理者或者接收方整改；需要交由其他执法部门处置的，交由相关部门依法处置。

第十条 个人信息处理者或接收方在处理个人信息时发生个人信息泄露等安全事件的，应立即采取补救措施，按照属地规定通知国家互联网信息办公室、广东省互联网信息办公室，或者澳门特别行政区政府个人资料保护局等相关监管实体。

第十一条 以上规定并不影响内地履行个人信息保护职责的部门和澳门特别行政区政府个人资料保护局在职责范围内依法加强个人信息保护和监督管理工作，包括处理与个人信息保护有关的投诉、举报，调查、处理违法个人信息处理活动等。

第十二条 有关部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十三条 国家互联网信息办公室和澳门特别行政区政府经济及科技发展局、澳门特别行政区政府个人资料保护局可以根据实际情况，经协商一致后对本实施指引及附件进行修订。

第十四条 本实施指引自公布之日起生效。

广东省互联网信息办公室发布《粤港澳大湾区个人信息跨境流动标准合同备案指南》

为落实《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》，便于粤港澳大湾区内内地个人信息处理者或接收方规范有序开展备案工作，广东省互联网信息办公室编制了《粤港澳大湾区个人信息跨境流动标准合同备案指南》，进一步优化备案流程，公布线上报送系统，规范标准合同、承诺书、经办人授权委托书等材料的内容、格式，并提供了可下载模板。

符合条件的个人信息处理者或接收方，通过订立《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同》的方式进行粤港澳大湾区内内地和香港、澳门之间的个人信息跨境流动，按照本指南以线上方式向广东省互联网信息办公室备案。请直接访问“数据出境申报系统”（网址：https://sjcj.cac.gov.cn），也可从中国网信网（https://www.cac.gov.cn）首页“全国网信政务办事大厅”栏目访问“数据出境申报系统”。

广东省互联网信息办公室

2025 年 11 月 28 日

粤港澳大湾区个人信息跨境流动标准合同备案指南

根据《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》等规定，为指导和帮助粤港澳大湾区内内地个人信息处理者或接收方规范有序备案《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同》（以下简称大湾区标准合同），特制定本指南。

一、适用范围

注册于广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市的个人信息处理者或接收方，可以通过订立大湾区标准合同的方式进行粤港澳大湾区内内地和香港、澳门之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。

通过订立大湾区标准合同跨境提供个人信息的，应当履行大湾区标准合同列明的义务和责任，包括满足以下条件:

（一）个人信息处理者跨境提供个人信息前，应当按照相关法律法规要求告知个人信息主体并取得个人信息主体的同意。

（二）不得向粤港澳大湾区以外的组织、个人提供。

（三）个人信息处理者跨境提供个人信息前，应当开展个人信息保护影响评估。

（四）大湾区标准合同应当严格按照模板订立，合同生效后方可开展个人信息跨境提供。

二、备案方式

个人信息处理者或接收方应当在大湾区标准合同生效之日起10个工作日内，通过线上方式备案。可直接访问“数据出境申报系统”（网址：https://sjcj.cac.gov.cn），也可从中国网信网（https://www.cac.gov.cn）首页“全国网信政务办事大厅”栏目访问“数据出境申报系统”。

（一）账号注册与登录。对于初次登录系统进行提交的个人信息处理者或接收方，点击“注册账户”，填写用户名、密码、手机号码等信息。注册成功后，登录系统进行基础信息录入，填写个人信息处理者或接收方单位名称、统一社会信用代码、单位注册所在地等。

（二）项目新建与填报。登录后选择“粤港澳大湾区个人信息跨境流动标准合同备案”模块，点击“信息填报”，选择“个人信息处理者”或“接收方”，上传备案材料。

三、备案流程

大湾区标准合同备案流程包括材料提交、材料查验及反馈备案结果、补充或者重新备案等环节。

（一）材料提交

个人信息处理者备案标准合同，应当提交如下材料:

（1）承诺书

（2）大湾区标准合同

（3）其他材料：法定代表人身份证件（影印件）、统一社会信用代码证件（影印件）、经办人身份证件（影印件）、经办人授权委托书等

备案材料均应加盖公章且为简体中文版，承诺书、大湾区标准合同、经办人授权委托书应使用系统中“粤港澳大湾区个人信息跨境流动标准合同备案”模块提供的可下载模板，不得自行增删或修改模板内容。个人信息处理者或接收

方对所提交材料的真实性负责，提交虚假材料的，注销备案编号，并依法追究相应法律责任。

（二）材料查验及反馈备案结果

广东省互联网信息办公室应当自个人信息处理者提交备案材料之日起10个工作日内完成材料查验，并向符合备案要求的个人信息处理者发放备案编号。需要补充完善材料的，个人信息处理者应当在10个工作日内提交补充完善材料；逾期未补充完善材料的，可以终止本次备案程序。

备案主体为接收方时，广东省互联网信息办公室在10个工作日内完成材料查验并通知接收方。

（三）补充或者重新备案

跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化，延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立大湾区标准合同，并履行相应备案手续和法定通知义务。

个人信息处理者在标准合同有效期内补充订立大湾区标准合同的，应当提交补充材料；重新订立大湾区标准合同的，应当重新备案。补充或者重新备案的材料查验时间为10个工作日。

四、咨询方式

咨询电话：020-87100793（来电请明确告知主体信息）

咨询时间：工作日上午9:00-11:30，下午14:30-17:30