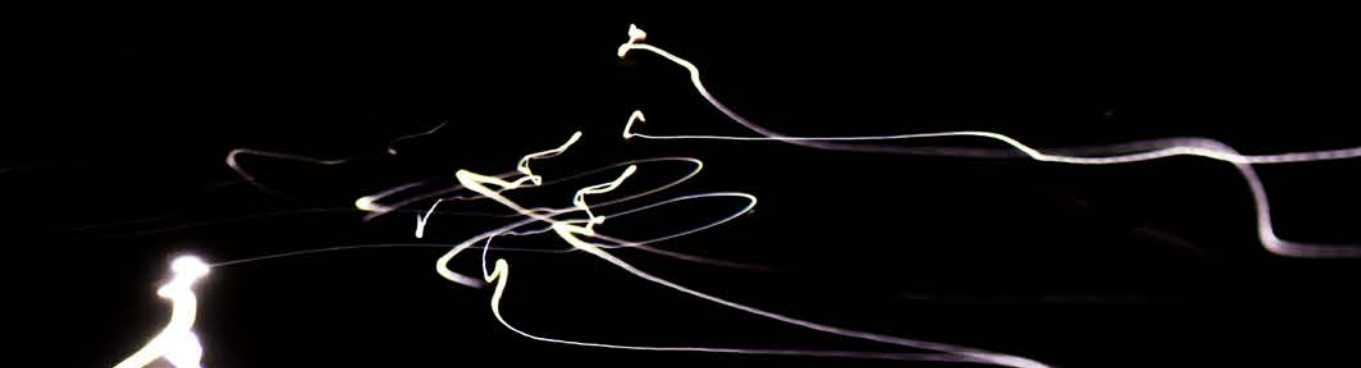

中倫律師事務所
ZHONG LUN LAW FIRM
中伦
网络安全
与数据保护
年度报告
CYBER
SECURITY
ANNUAL REPORT
a Zhonglun report

中伦研究院出品

CONTENTS | 目录



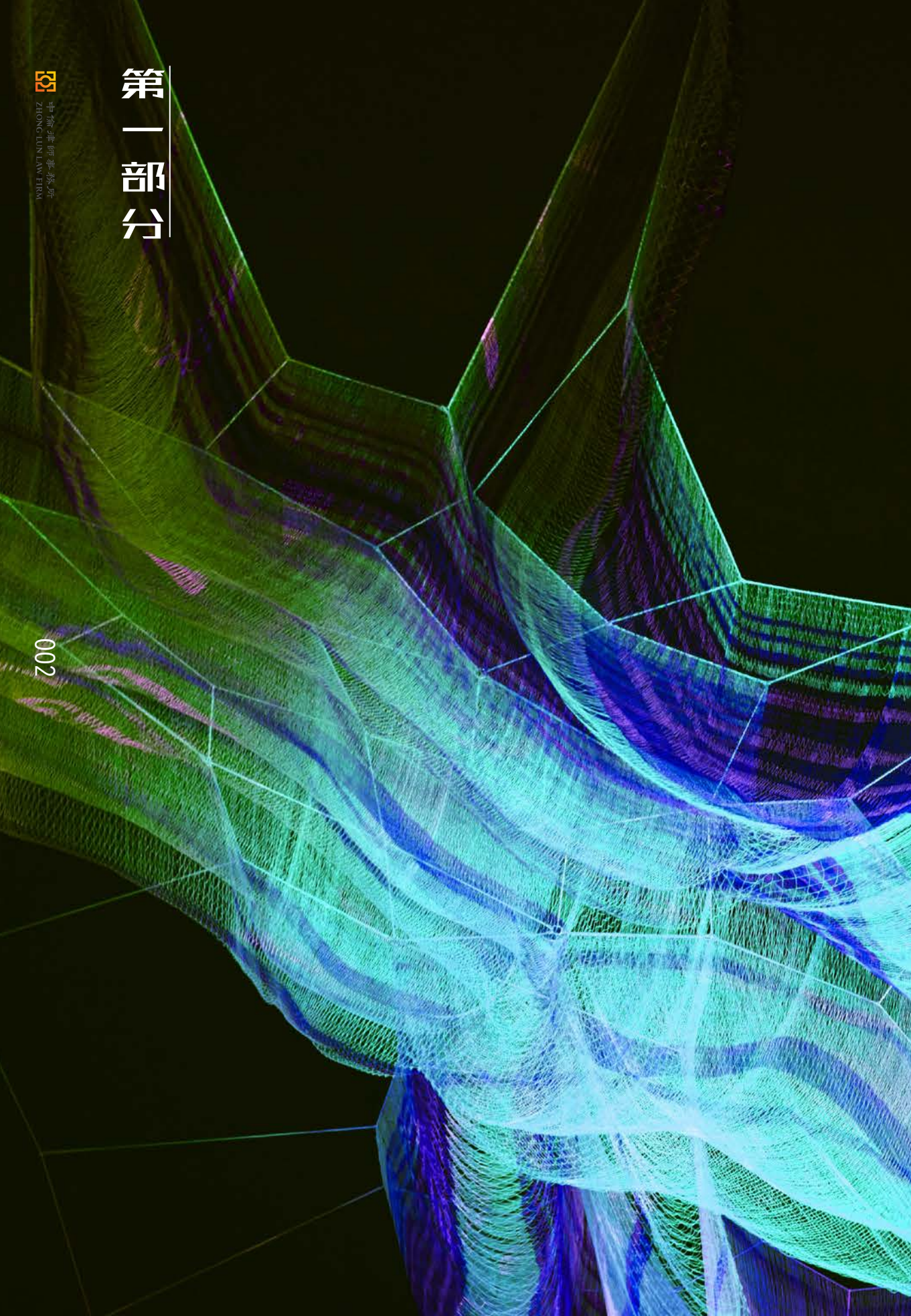
PREFACE | 前言

2017年6月1日，《中华人民共和国网络安全法》颁布生效，奠定了网络安全和数据保护的实证法基础。为保障《网络安全法》有效实施，一方面，以国家互联网信息办公室为主的多个监管部门制定了多项配套法规，进一步细化和明确了各项制度的具体要求、相关主体的职责以及监管部门的监管方式；另一方面，全国信息安全标准化技术委员会制定并公开了一系列以信息安全技术为主的重要标准，为网络运营者和监管部门提供了非常具有操作性的合规指引。与此同时，工信部、公安部等多个部委也在职权范围内制定了相应的规范性文件；国家质量监督检验检疫总局、国家食品药品监管总局、国家宗教事务局等部门也同样针对各自领域内的数据制定了具体的规范、标准和规定。

至今，《网络安全法》生效至今已逾两年，网络安全相关立法体系逐步完善，执法监管工作也进入稳步发展阶段，网络安全及数据合规问题在各领域企业中的重要性更为突出。

长期以来，中伦律师深度参与了网络安全和数据保护合规法律实践，从中积累了诸多经验。我们结合自身的实务经验，以2018年《中伦网络安全与数据保护法律评论》为基础，结合2019年的最新立法以及具有典型性或者创新性的代表案例推出此报告，力求全方位、多层次、宽领域地展现本年度网络安全及数据保护的全景图像，并针对相关议题进行深入探讨，向企业提出可行的合规建议，希冀促进我国网络安全和数据保护法律进程的进步。

第一部分

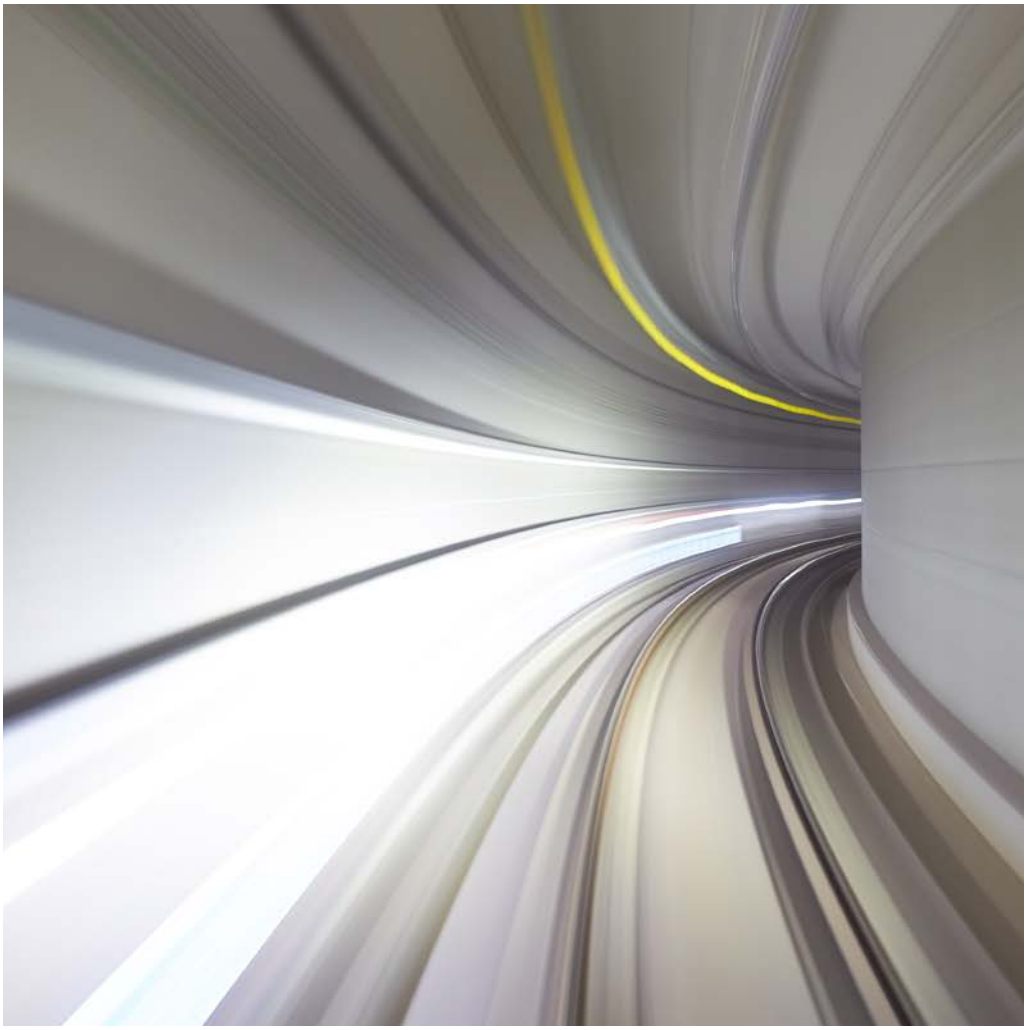


1

观察：2019年网络安全立法和执法状态

CHAPTER ONE

盘点与展望



《中华人民共和国网络安全法》(“《网络安全法》”)生效至今已逾两年,相较于中国“数据合规元年”之2018年,网络安全相关立法体系逐步完善,执法监管及企业合规措施落地等各方面工作均进入稳步发展阶段。在ABC时代(AI, Big Data, Cloud Computing)背景及国家强化网络安全建设的政策环境下,网络安全及数据合规与各行业的耦合度进一步提升,除以工信部、网信办、公安部等部门主导的APP个人信息保护执法行动、“净网行动”外,围绕人脸识别技术的讨论、针对数据爬取行业的起底、渗透在企业上市过程中的数据合规问题排查等,无不体现网络安全及数据合规问题在各领域企业合规工作中的突出地位。在岁末年初,我们将照例简要盘点本年度网络安全及数据保护的全景图像,并对下一年度的发展趋势进行展望,以期为企业数据合规工作提供参考。

SECTION 01

复盘:2019年网安立法及执法的全景观察

(一)《网络安全法》配套法规完善之“进阶”

《网络安全法》作为我国网络空间安全管理的框架性法律,其对网络运营者的责任义务要求需依托具体配套法规或实施细则而予以落实。相较去年,本年度配套法规的完善取得了“进阶性”成果,也做出了不少“进阶性”尝试。

“等保2.0”制度体系完成实质性构建。2019年12月1日,以《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》、《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》、《GB/T 25070-2019信息安全技术 网络安全等级保护安全设计技术要求》[1]三个网络安全领域的国家标准为代表的“等保2.0”制度正式生效[2],标志我国信息系统等级保护测评工作将适用全新的评估标准体系。“等保2.0”在保留五级安全等级评定标准的基础上,形成“安全通用要求”及“云计算/移动互联/物联网/工业控制系统扩展要求”的标准评定体系。这对尚未进行等保备案,或已进行等保评定而需每年进行再评估的信息系统运营者而言,无疑是重点合规工作。

《个人信息安全规范》与时俱进应时而变。2018年5月《GB/T 35273-2017信息安全技术个人信息安全规范》(“《个人信息安全规范》”)正式实施。在现有生效版本基础上,本年度《个人信息安全规范》经历了2月、6月、10月的三次草案/征求意见稿的调整尝试,在总结现行版本落实过程中发现的问题及经验并展开优化的同时,对大数据时代技术发展产生的个性化展示、数据汇聚融合、SDK/插件管理等为新型技术应用场景如何规范个人信息的收集和使用提出了新的尝试。

个人信息、重要数据分别管理的框架性变化。本年度《个人信息出境安全评估办法(征求意见稿)》[3]的发布,打破了2017年《个人信息和重要数据出境安全评估办法(征求意见稿)》[4]的立法框架。由于个人信息及重要数据所保护的法益不同,其保护规制路径也理应存在区别。目前的立法模式正逐步响应这种分开管理的监管框架,以出境安全评估为抓手进行管理。

面向CIIO的网络安全审查工作逐步完善。目前《关键信息基础设施安全保护条例(征求意见稿)》尚未落地,CII的识别标准和适用范围有待确定。本年度《网络安全审查办法(征求意见稿)》[5]的发布,表明国家重点关注并规范关键信息基础设施运营者(CIIO)采购网络产品和服务时的审查需要、审查流程、审查因素等。

儿童个人信息保护规范得以落实。本年度《儿童个人信息网络保护规定》,辅之以8月初教育部等八部门联合发布的《关于引导规范教育移动互联网应用有序

1.2019年5月13日,国家市场监督管理总局、国家标准化管理委员会发布。
2.等保1.0以1994年发布并于2011年修订的《中华人民共和国计算机系统安全保护条例》为开端,广泛应用于各行业指导企业开展信息系统安全等级保护的建设整改、等级测评等工作。2017年6月1日正式实施的《中华人民共和国网络安全法》规定“国家实行网络安全等级保护制度”,明确了网络安全等级保护制度的法律地位,也拉开了等保2.0的序幕。相应地,2018年公安部发布《网络安全等级保护条例(征求意见稿)》,深入推进实施网络安全等级保护制度。而《等保基本要求》等三个国家标准结合云计算、移动互联、物联网、工业控制和大数据等新技术新应用开展综合治理、系统监管、主动防控的等保2.0时代。
3.国家互联网信息办公室于2019年6月13日发布
4.国家互联网信息办公室于2017年4月11日发布
5.国家互联网信息办公室于2019年5月24日发布

健康发展的意见》，对面向未成年人尤其是在校学生提供产品或服务过程中收集其个人信息的运营者进行明确的行为约束及规范。在应对国内外日益增强的儿童个人信息保护的呼声中，我国已迈出了关键性一步。

（二）网安执法运动之“迭起”

今年以来，App个人信息保护问题始终是各行业监管的重点关注对象。年初[6]中央网信办、工业和信息化部、公安部、市场监管总局四部委在《关于开展App违法违规收集使用个人信息专项治理的公告》中明确提出，自今年1-12月内全国范围将组织开展App违法违规收集使用个人信息专项治理行动。在此基调下，相应立法及执法行动频频，包括成立App专项治理工作组，发布《App违法违规收集使用个人信息自评估指南》等[7]，“3.15晚会”上曝光典型案例，向用户量大且问题严重的App的运营者发送整改通知等。今年11月份以来，由工信部主导的“App用户权益执法行动”[8]，可视为对全年度App执法检查工作的“年度大考”。

公安机关不断加强网络安全执法监督工作。年中公安部部署了本年度网络安全执法检查工作，以国家关键信息基础设施、重要信息系统和大数据等相关应用系统为重点检查对象，组织网络安全技术检测和现场检查工作。同时，“净网2019”行动持续开展，各地网警支队陆续公布了行政执法案例，为企业网安合规工作划定实务“红线。”

各行业陆续开展内部审查及自律自管行动。中国人民银行、中国互联网协会、国家计算机病毒应急处理中心、各地消费者权益保护协会等行业单位及部门，陆续开展内部网络安全自查、自律等行动，从行业内部引导相应企业落实《网络安全法》的要求。

（三）密码产品管理之“放管”逻辑

《中华人民共和国密码法》于今年10月26日发布并将于明年1月1日正式施行。其响应国家“放管服”的改革要求，对于网络运营者密码产品管理采取“放管”措施：从立法层面正式取消了国家密码管理局负责实施的商用密码产品生产单位审批、商用密码产品销售单位许可、外商投资企业使用境外密码产品审批、境外组织和个人在华使用密码产品或者含有密码技术的设备审批。然而，取消上述行政审批并不意味着国家对于密码应用的完全放开，而是释放出监管重点正在从“管企业”向“管产品”转变的信号，例如增强CIIO的商用密码应用安全性评估和国家安全审查等。

6.2019年1月25日
7.包括《App违法违规收集使用个人信息自评估指南》、《App违法违规收集使用个人信息行为认定办法》（征求意见稿）及《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（草案）》
8.2019年11月4日，工业和信息化部发布《关于开展App侵害用户权益专项整治工作的通知》，即日起面向App服务提供者和App分发服务提供者，就App违规处理个人信息、过度索权、为用户账号注销设置障碍等八类侵害用户权益的突出问题，由工信部及地方通信管理局主导开展信息通信领域为期两个月的App专项整治行动。

(四)数据爬取业务之刑事“红线”

今年9月以来,公安部门加强对涉足互联网金融行业的大数据服务公司在网络安全及数据合规领域的执法力度。9月6日,摩羯科技、新颜科技两家数据服务提供商均面临警方调查,部分高管人员被要求协助调查,其他部分知名风控数据提供商也主动或被动停止了相应的数据提供服务。根据现有公开资料,尽管这类公司遭遇调查的主要原因系数据爬虫技术的使用边界问题,但数据爬虫背后连带的数据源合规、用户授权获取、合法对外提供个人金融信息、数据库维护、各环节员工的数据访问权限等常见的数据合规处理问题,因缺乏人员数据合规意识及技能培训、缺乏内部管理制度和技术保障措施导致公司数据库污染或非法对外提供个人信息等而导致的法律风险(甚至可能触碰个人信息非法采集及提供等刑事“红线”),都值得社会各界的高度关注,尤其是同样涉及大量数据获取、开发、分析、共享的企业的重视。

(五)行业标准及指南构建之合规“引路”

完善企业网络安全技术措施指引。2019年4月10日,公安部网络安全保卫局发布《互联网个人信息安全保护指南》。与《个人信息安全规范》相比,该指引加强了数据安全实现中技术措施的要求,并与等级保护制度的技术要求相结合,为企业数据合规工作提供更加全面的指引。

加强移动互联网应用程序(App)安全认证及合规管理指引。如今App成为网络运营者收集处理用户个人信息的主要渠道,相应行业单位及部门也以App为抓手展开合规指引工作。今年3月份国家认证认可监督管理委员会发布的《移动互联网应用程序(App)安全认证实施细则》、全国信息安全标准化技术委员会于5月份发布的《网络安全实践指南-移动互联网应用业务功能个人信息收集必要性规范》、国家标准化委员会于10月份发布的《信息安全技术 移动互联网应用程序(App)收集个人信息基本规范》(草案)等,共同组成了App安全认证及数据合规管理指引体系基础。

尽管这一系列标准或指引并非强制性国家标准,但其为企业提供了落实数据保护工作的行业良好实践规范(Good Practice)。采取上述标准或指引的推荐性措施,有助于企业落实法律法规的各项要求,亦有利于企业平衡数据处理活动的商业需求与数据保护的合规义务。

SECTION 02

展望：2020年国内立法发展及企业应对策略

在2020年，我们预计：

立法成果化：2019年度诞生的网络安全及数据合规领域的诸多“草案”及“征求意见稿”，预示着2020年将是本领域法律、行政法规成果“井喷”的一年。其中，已纳入十三届全国人大常委会立法规划的《数据安全法》、《个人信息保护法》，连同高度关注的《数据安全管理办法》及《个人信息出境安全评估办法》等配套法规的最终出台值得期待。

标准支撑完善化：有关数据出境管理、CII识别及安全保护、重要数据识别等一系列配套标准可能最终落地，为企业提供可操作性的合规指引。

隐私保护常态化：个人信息保护工作将从今年的阶段性执法运动的形式，逐步转化为日常常态化监管模式；对于隐私政策/通知等用户授权机制的审查要求，也将从“有无”进一步深入为“详略”的细化要求，切实评估各项功能涉及的个人信息处理活动的保护机制，切实维护个人信息主体权益。

跨境监管核心化：有关个人信息和重要数据出境的监管要求有望于明年落地，对于跨国企业而言，构建合规的全球IT架构，设计合法的数据本地化和跨境传输方案，将成为跨国企业合规工作的重中之重。

行业监管体系化：各个行业主管部门，尤其是金融、医疗健康、电子商务等数据敏感行业，将进一步完善行业内的网络安全和数据保护实施细则的立法和执法工作。

数据管理科学化：为应对商业发展需求，企业将从被动应对监管逐步转变为主动开展数据合规管理，启动数据资产管理战略，全盘化、体系化、科学化展开内部数据合规管理体系及外化合规成果建设工作。

[结语]

为帮助企业理解中国复杂的法律环境，寻求企业适当的合规路径，降低法律风险，中伦专业团队结合在网络安全和数据保护领域的广泛实践，将继续推出一系列网络安全和数据保护的回顾和总结文章，希望对我们的客户有所帮助。

CHAPTER TWO

现行网络安全法立法框架解读及合规建议

《中华人民共和国网络安全法》(以下简称“《网络安全法》”)及其配套的法律法规和标准,构成了目前国内网络安全及数据保护合规的核心法律体系。从衔接关系上看,《网络安全法》为框架性法律文件,为企业网络安全及数据合规工作划分制度板块及合规原则,而各项具体制度则对合规原则进行了进一步细化和落地,形成兼具包容性、延展性及适应性的操作细则。目前网络安全及数据保护合规体系覆盖网络安全等级保护制度、关键信息基础设施安全保护制度、个人信息和重要数据保护制度、互联网信息内容管理制度、数据出境管理制度等。

在上述制度框架的基础上,纵观2019年的立法成就,除重要数据保护、关键信息基础设施认定及保护标准等重大、复杂问题仍有待讨论外,其他制度版块均有代表性的制度成果发布,尤其是个人信息保护、数据出境管理、网络安全等级保护技术标准等。

以下我们将简要描述网络安全法立法框架,突出2019年最新立法成果,并为企业合规提供整体性建议。具体法律法规及标准内容,可参考本报告“第三部分:2019《网络安全法》配套法律法规和规范性文件的梳理”。

SECTION 01

以网络安全等级保护制度为核心的网络安全合规管理制度

网络安全等级保护制度（Multi-level Protection Scheme，以下简称“MLPS”）是基于《网络安全法》第二十一条的规定形成的网络安全保护等级测评、备案及保护措施的综合管理制度，以网络安全等级评定为基础，为不同等级的网络设定不同标准的网络安全保护要求，覆盖机构及人事安排、内部管理制度设计等组织管理措施，以及去标识化、匿名化、加密存储与传输、自动化决策及记录等技术保护措施，为《网络安全法》所设定的网络安全保护管理制度提供量化标准及实现路径。网络运营者应当按照《网络安全法》及等级保护配套制度的具体要求，落实公司内网络的等级保护合规义务。如相应系统的网络运营者未落实等级保护义务，则会因违反《网络安全法》的明确要求承担相应的行政责任，并可能因系统问题导致的个人信息泄露等安全事件对数据合作方及相关个人信息主体承担民事责任。

2019年12月生效的国家标准（《GB/T22239-2019信息安全技术网络安全等级保护基本要求》、《GB/T25070-2019信息安全技术网络安全等级保护设计技术要求》和《GB/T28448-2019信息安全技术网络安全等级保护测评要求》，联同2018年公布的《网络安全等级保护条例（征求意见稿）》，标志着中国等保2.0时代的开启。以《计算机信息系统安全保护条例》、《信息安全等级保护管理办法》等为代表的等保1.0时代将逐步退出时代舞台。

在等保2.0要求下，不同等级的系统应当适配不同程度的制度及技术保护措施。除了针对所有系统的普遍要求外，三级以上网络还应当落实特殊的保护义务。需注意的是，第三级以上网络应当在境内实施技术维护，不得境外远程技术维护。因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施。目前具体网络安全评估的实施细则尚未公布。

为应对等保2.0时代的到来，我们建议作为网络运营者的企业，应重视如下合规工作：

◆所有的网络运营者都应针对企业内网络、信息系统实施评估，以确定各自运营的信息系统所对应的等级，这一环节建议聘请具备相关经验的律师事务所、咨询公司等专业服务机构协助处理此类事务。

◆对于第二级以上网络，公司应当组织专业测评，并向公安机关备案。

◆一旦网络等级被确定下来，网络运营者应当遵循相关技术标准要求，履行网络基础设施、云计算平台/系统、大数据应用/平台/资源、物联网、工业控制系统和移动互联网络新应用场景的特殊保护义务。

◆密切关注立法与执法动态，加强与主管部门的沟通。

SECTION 02

关键信息基础设施安全保护制度

关键信息基础设施安全保护制度，是基于《网络安全法》第三十一条至第三十九条设置的、针对一旦遭到破坏、丧失功能或者数据泄露而可能严重危害国家安全或者公共利益等的信息系统（即关键信息基础设施）的网络安全保护及合规管理要求体系。对于关键信息基础设施运营者而言，需在遵守一般网络运营者义务的基础上，重点关注被认定为关键信息基础设施的信息系统的组织管理、运维安全、数据保护的合规义务，尤其是服务器部署安全、网络关键设备及网络安全专用产品采购、数据本地化存储要求等问题。例如，《网络安全法》第三十七条明确要求，关键信息基础设施的运营者在境内运营中收集的个人信息和重要数据应当在境内存储，如因业务需要确需向境外提供的，则需按照网信部门等制定的具体办法进行安全评估。

然而，尽管《网络安全法》为关键信息基础设施运营者设定了基本的合规要求框架，但针对关键信息基础设施的识别及认定标准、数据出境安全评估的具体落实方案及对应主管机构等实质内容法律法规仍未出台。作为该制度体系核心的《关键信息基础设施安全保护条例》、《信息安全技术 关键信息基础设施安全检查评估指南》、《信息安全技术 关键信息基础设施网络安全保护要求》等法规及标准，仅发布了征求意见稿版本，尚未形成约束性或者明确性的生效细则，这使得企业开展实际合规工作产生了一定局限。

对此，我们建议，对于企业自身业务或者企业客户的相关业务可能涉及国计民生、公共利益等重要行业的企业，应当自行评估处理上述业务的信息系统构成关键信息基础设施的可能性。经内部评估或者与主管机构沟通后认定存在较大可能构成关键信息基础设施的，应当尽快对照《网络安全法》的原则要求及现行征求意见稿列明的合规细则，提前匹配相关合规要求并计划下一步合规工作。

SECTION 03

个人信息保护及重要数据保护制度

《网络安全法》第四十一条至第四十五条规定了对网络运营者个人信息保护的要求，同时第二十一条、第三十七条等涉及到对重要数据的保护原则。

（一）个人信息保护制度

根据我国《网络安全法》第七十六条的规定，个人信息是指以电子形式记录的、可以单独或者与其他信息组合来识别自然人主体的信息，包括但不限于自然人的名字、生日、身份证号码、个人生物信息、地址、电话号码等。由全国信息安全标准化技术委员公布的、于2018年5月生效的《GB/T 35273-2017信息安全技术 个人信息安全规范》作为目前国内规范个人信息全生命周期管理的主要标准，为企业个人信息保护提供具体化指引。在生效半年并汲取相关实践经验后，2019年《个人信息安全规范》进行了若干修订并公布了两版征求意见稿及一版草案，目前最新的征求意见稿版本（2019年10月22日发布）相较于现行版本，强调了隐私政策的描述规范（包括应当增加概要、介绍控制者基本情况、各业务功能对应个人信息类型、个人敏感信息突出标识等）（5.5条）、个性化展示及退出要求（7.5条）、数据融合的合规考虑（7.6条）、对接入的第三方插件/SDK的管理（8.7条）等规范性要求。

同时，公安部于2019年4月发布了《互联网个人信息安全保护指南》，尽管不具备强制约束力，但其将《网络安全法》对于个人信息保护的原则性合规要求，转化为从管理机制（管理制度、机构及人员）、技术措施以及个人信息全流程管理（收集、保存、应用、删除、共享、披露、应急处置等）等层面进行指引。

在儿童个人信息保护方面，2019年也取得了突出的立法成就。《儿童个人信息网络保护规定》的出台，辅之以2019年8月教育部等八部门联合发布的《关于引导规范教育移动互联网应用有序健康发展的意见》，对面向未成年人尤其是在校学生提供产品或服务过程中收集其个人信息的运营者进行明确的行为约束及规范。

合规建议	环节	基本问题
1	收集	◆有无明确的个人信息收集处理规则 ◆个人信息收集处理规则的呈现形式及内容详尽程度是否符合当前个人信息保护相关法律法规要求以及行业良好实践
2		◆是否已取得个人信息主体的授权同意 ◆是否针对不同的应用场景、不同数据类型满足相应的授权同意要求（例如用于个人敏感信息收集的明示同意）
3		◆收集渠道和方式是否合法合规（尤其是涉及数据委托处理、数据爬取、数据融合等） ◆是否采取制度和技术双重措施来保证数据来源合法性
4	使用/处理	是否按照法律法规要求及与个人信息主体的约定（个人信息收集处理规则）等如实使用所收集的个人信息，未超出约定范围使用
5		对于数据融合、画像分析、市场营销等高合规风险的应用场景，是否满足相应的合规要求
6		是否存在非法交易个人信息等违法违规行为
7	管理	是否指定特定的网络安全及数据管理机构及负责人，并赋予相应的权限和资源
8		是否建立健全个人信息影响安全评估制度并定期实施评估工作
9		是否保障个人信息主体享有法律法规约定的权利（访问、更正、删除个人信息、注销账户等），实践操作与向个人信息主体公示的个人信息收集处理规则是否相符
10		是否基于必要原则和最小原则，做好对个人信息内外部访问权限的管控
11		是否已采取相应技术措施防止个人信息被非法拷贝、丢失、损坏或者盗窃
12		◆是否制定网络安全及个人信息安全事件应急预案 ◆是否做好事件发生后的风险管控措施及告知相关个人信息主体、以及报告主管机关的应对措施
13	对外提供	◆是否明确对外提供个人信息的处理规则（包括委托处理及合作共享） ◆对外提供个人信息的方式是否安全，是否具备一定制度及技术保护措施 ◆相关个人信息主体是否知悉并同意上述个人信息对外提供的相关处理规则相应安全措施
14		是否与相应数据合作第三方签订数据处理协议，以厘清双方在数据保护及合规处理方面的责任义务
15		◆是否存在跨境传输场景，所涉的个人信息是否为不可跨境传输的信息类型 ◆对于数据接收方是否做到审慎评估对方数据保护能力 ◆相关个人信息主体是否知悉并同意其个人信息的出境行为

（二）重要数据保护制度

《网络安全法》明确了关键信息基础设施运营者的数据本地化要求[9]，提出了重要数据这一新概念。在2017年发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》中重要数据进行了定义，指与国家安全、经济发展，以及社会公共利益密切相关的数据。随后，信安标委在《信息安全技术数据出境安全评估指南(征求意见稿)》中提出了《重要数据识别指南》，列举了各行业各领域涉及的重要数据范围。而2019年5月28日发布的《数据安全管理办法（征求意见稿）》进一步明确了重要数据的性质，即“一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据”、并列举了部分示例“如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等”，同时明确排除了企业生产经营和内部管理信息及个人信息作为重要数据的可能。

由于数据本地存储及数据出境安全评估制度均涉及重要数据，因此，重要数据的识别至关重要。然而目前有关重要数据的识别标准仍在制定当中。

《数据安全管理办法（征求意见稿）》作为小数据安全法对重要数据的保护原则提出了一些新要求，包括：

安全评估——网络运营者向第三方提供（包括共享、交易、公开披露、出境等）重要数据前，应当进行安全评估工作，并获得行业主管监管部门同意，行业主管监管部门不明确的，应经省级网信部门批准。

备案——以经营为目的收集重要数据的网络运营者应当向所在地网信部门进行备案。同时明确该备案内容仅限收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，而不包括具体的数据内容本身。

应当注意的是，上述办法仅为征求意见稿，其内容仍可能存在变动。关于重要数据识别范围及具体的安全评估及备案管理工作，仍有待出台相关细则。

9.《中华人民共和国网络安全法》第三十七条
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。

SECTION 04

数据本地化存储要求及数据出境合规管理制度

数据本地化存储要求及数据跨境转移是中国公司“走出去”、外国公司“走进来”所必须面临的重要问题。《网络安全法》要求关键信息基础设施运营者收集的个人信息和重要数据应当存储在中国境内（即数据本地化要求）。因业务需要，确需向境外提供的在境内收集的个人信息和重要数据的，应当事先进行安全评估。而2017年4月发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》（“旧

办法”）将数据出境限制的适用主体由《网络安全法》下的“关键信息基础设施”运营者扩展到含义更广泛的“网络运营者”，这意味着几乎所有的互联网运营商、网络新媒体企业以及利用互联网提供服务信息的传统企业（例如银行、保险公司等）都应履行相应的数据出境合规义务。自此以后，关于数据跨境传输的监管一直是网络运营者（尤其是跨国企业）的关注焦点，旧办法几易其稿，仍未获得多方利益相关方的认可。同时，在国际化和数字化的大时代背景下，数据跨境传输不可避免，其监管制度的落地一直是困扰跨国公司的一个重大问题。

而2019年发布的《个人信息出境安全评估办法（征求意见稿）》及《数据安全管理办法（征求意见稿）》重新定义了个人信息与重要数据的出境管理体系，相当于推倒了旧办法的监管架构，另起炉灶。本质上讲，个人信息与重要数据所保护的法益是不同的，其所对应的具体保护路径也应有所区别。个人信息与特定自然人的身份属性及经济属性密切相关，直接与个人合法权益相关；而重要数据与国计民生、社会公共利益密切相关，更多考虑国家及行业整体秩序。以2019年发布的《个人信息出境安全评估办法》（征求意见稿）为例，相较于2017年的出境安全评估旧办法，其体现了个人信息与重要数据分开管理的立法思维，在新办法的框架下，行政机构对数据跨境传输的监管将贯穿整个数据周期。

若上述法规最终依照现行征求意见稿的内容正式发布，则个人信息及重要数据出境监管将发生如下关键转变：

◆数据出境管理要求所适用的主体范围将从关键信息基础设施运营者扩展到网络运营者。

◆个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估，提交申报书、网络运营者与数据接收者签订的数据处理协议、个人信息出境安全风险及安全保障措施分析报告及国家网信部门要求提供的其他材料[10]。

◆重要数据出境前，网络运营者应当报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。[11]

以上为我们对国内现有网络安全及数据保护合规保护立法体系框架的初步解读，侧重于梳理2019年主要立法进展及企业整体性合规应对建议。具体合规体系解读、立法及执法趋势分析、核心应用场景的合规建议等，可详见本报告的第二部分。中伦团队也将一如既往地持续关注立法及执法趋势并进行相应解读，以期为企业提供更加切实有效的帮助。

10.《个人信息出境安全评估办法（征求意见稿）》第3条和第4条。
11.《数据安全管理办法》第28条。

CHAPTER THREE

2019年《网络安全法》执法案件汇总及分析

截至目前，于2017年6月1日起生效的《中华人民共和国网络安全法》（以下简称“《网络安全法》”）作为我国网络空间安全管理的基本法律及目前网络安全执法的最主要法律依据，正式实施已逾两年。《网络安全法》以网络运营者为主要规范对象，对网络运营者的网络运行安全、网络信息安全提出了若干制度性管理要求，重点包括网络信息内容管理制度、网络安全等级保护制度、关键信息基础设施的安全保护制度、个人信息和重要数据保护制度、网络产品和服务管理制度、网络安全事件管理制度等。

为保障《网络安全法》的落地实施，国家互联网信息办公室（以下简称“国家网信办”）等相关监管部门制定了多项配套法规，进一步细化和明确了各项制度的具体要求、相关主体的职责以及监管部门的监管方式。同时，全国信息安全标准化技术委员会（以下简称“信安标委”）亦制定并公开了一系列以信息安全技术为规范对象的国家推荐性标准（大部分处于征求意见稿阶段，有部分已正式生效，或者正式发布待实施）。

此外，于2018年11月1日正式生效的《公安机关互联网安全监督检查规定》，系作为公安部门加强对《网络安全法》落实情况的执法监管的重要依据。2019年5月13日，国家市场监督管理总局、国家标准化管理委员会发

布的《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》、《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》、《GB/T 25070-2019信息安全技术 网络安全等级保护安全设计技术要求》三个网络安全领域的国家标准于2019年12月正式生效，共同构筑新时代的网络安全等级保护制度，标志着等保2.0的正式到来。

上述法律法规，结合《网络安全法》颁布前已经生效的《全国人大常委会关于加强网络信息保护的决定》、《电信和互联网用户个人信息保护规定》等重要法规，共同构成目前我国网络安全法律保护体系。为确保上述相关法律法规的有效实施，监管部门开始了一系列的执法及执法检查工作。比如，国家互联网信息办公室（“中央网信办”）、工业和信息化部（“工信部”）、公安部、市场监管总局于1月25日联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，决定自2019年1月至12月，在全国范围组织开展App违法违规收集使用个人信息专项治理行动。对《网络安全法》的执法状况进行系统分析，有助于企业了解执法部门目前的执法重点和处罚措施，对于企业进行合规工作具有借鉴意义。

除了行政执法以外，《网络安全法》同时与刑事领域密切相关。《网络安全法》对于保障个人信息保护及信息系统安全做出了义务性规定，若相关主体未能遵守相应规定，则可能需承担相应的刑事责任。因此，对《网络安全法》内容相关的刑事案例的关注，有助于企业做好重点领域的刑事合规工作。

本文将以我们发布的2018年《<网络安全法>执法案例汇总及执法重点分析》为基础，结合2019年产生的案例素材以及以往具有典型代表性或者创新性的代表案例，扩充行政执法案例库，丰富刑事典型案例资源，并增补相应的结果分析，全方位、多层次、宽领域地展现《网络安全法》实施至今两年多以来的主要执法案例及多维度分析成果。

第一节 《网络安全法》行政执法案例综述

《网络安全法》正式实施以来，行政执法工作日趋常态化，且趋于频密，2019年行政执法主要处罚案例情况总结见《附件一：<网络安全法>行政执法相关处罚案例》

SECTION 01

主要行政监管行动

（一）四部门对App收集个人信息的专项治理行动

2019年1月，中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》[12]，并联合有关单位成立了App违法违规收集使用个人信息专项治理工作组，旨在打击App违法违规收集使用个人信息行为。截至4月16日，举报信息超过3480条，涉及1300余款App。对于30款用户量大、问题严重的App，工作组已向其运营者发送了整改通知[13]。截至9月15日，相关举报平台已收到近8000条举报信息[14]。

从截至4月16日所收到的举报问题来看，26%的App没有隐私条款或未在隐私条款中明确收集个人信息的目的、方式、范围；31%的App在申请打开收集个人信息相关权限时，未明确告知用户；20%的App收集与业务功能无关的个人信息，如金融借贷App收集用户通信录；19%的App未经用户同意，向他人提供设备ID、应用程序列表等个人信息；13%的App强制索要与业务功能无关的权限，如计算器、手电筒App强制要求打开地理位置权限。还有一些App存在不支持用户注销账户、更正或删除信息等问题[15]。

四部委高度重视个人信息保护工作，针对当前App强制授权、过度索权、超范围收集个人信息等网民反映强烈的问题，已采取或即将采取出台必要的管理规范和相关标准的形式进行规制。2019年5月，App专项治理工作组发布《App违法违规收集使用个人信息行为认定方法（征求意见稿）》。该征求意见稿与App专项治理工作组2019年3月发布的《App违法违规收集使用个人信息自评估指南》一脉相承，但又结合《个人信息安全规范》以及举报活动中频繁出现的严重违法违规现象，体现出执法机构规范的重点，对于企业评估合规状况、设定自身的合规红线有重大参考意义。2019年10月，结合评估工作实践和各方征求意见，陆续更新并公开《信息安全技术　个人信息安全规范（最新征求意见稿）》[16]、《移动互联网应用程序（App）收集个人信息基本规范（最新草案）》。[17]

14.App专项治理工作组："四部门抓紧推进App违法违规收集使用个人信息专项治理"，https://mp.weixin.qq.com/s/eF2L1cSoC-mp4eFD4DrNM8w，访问时间：2019年12月13日。

15.中央网信办："中央网信办：App专项治理行动已收到近8000条举报信息"，https://mp.weixin.qq.com/s/zX-unV7qksLogHTiO-ohFu7g，访问时间：2019年12月13日。

工信部："四部门抓紧推进App违法违规收集使用个人信息专项治理"，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057732/c6797025/content.html，访问时间：2019年12月13日。

16.App专项治理工作组："GB/T 35273《信息安全技术 个人信息安全规范》最新版征求意见稿"，https://mp.weixin.qq.com/s/XyJOp2hGujlSKbiLjnpUWA，访问时间：2019年12月13日。

17.App专项治理工作组："《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》最新版草案"，https://mp.weixin.qq.com/s/y8EUsg9-vDMMinVuHR2ZEA，访问时间：2019年12月13日。

（二）中央网信办开展网络生态治理专项行动

针对网络生态问题频发、各类有害信息屡禁不止等突出问题，中央网信办自2019年1月启动持续六个月的网络生态治理专项行动，分为启动部署、全面整治、督导检查、总结评估四个阶段，对各类网站、移动客户端、论坛贴吧、即时通信工具、直播平台等重点环节中的淫秽色情、低俗庸俗、暴力血腥、恐怖惊悚、赌博诈骗、网络谣言、封建迷信、谩骂恶搞、威胁恐吓、标题党、仇恨煽动、传播不良生活方式和不良流行文化等12类负面有害信息进行整治，集中解决网络生态重点环节突出问题，严厉查处关闭一批违法违规网站和账号[18]。

与此同时，为进一步加强网络生态治理，构建天朗气清的网络空间，中央网信办会同有关部门起草了《网络生态治理规定（征求意见稿）》[19]，以期通过立法方式巩固专项治理成果，持续化监督网络生态发展。

（三）市场监管总局开展“守护消费”行动以打击侵害消费者个人信息违法行为

2019年4月1日至9月30日，市场监管总局依照《消费者权益保护法》、《电子商务法》、《网络安全法》、《侵害消费者权益行为处罚办法》等法律法规的相关规定，在全国范围内开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动，重点打击侵害消费者个人信息的违法行为。[20]

本次行动重点关注违法行为多发的房产租售、小贷金融、教育培训、保险经纪、美容健身、装饰装修、旅游住宿、快递、电话营销、网站或APP运营等行业和领域。本次行动主要查处3类违法行为：一是未经消费者同意，收集、使用消费者个人信息；二是泄露、出售或者非法向他人提供所收集的消费者个人信息；三是未经消费者同意或者请求，或者消费者明确表示拒绝的，向其发送商业性信息。

行动期间，全国市场监管部门共立案查办各类侵害消费者个人信息案件1474件，查获涉案信息369.2万条，罚没款1946.4万元，移送公安机关案件154件。

（四）国家市场监督管理总局等部门开展2019网络市场监管专项行动（“网剑行动”）

2019年6月，国家市场监督管理总局、国家发展和改革委员会、工业和信息化部、公安部、商务部、海关总署、国家互联网信息办公室、国家邮政局等部门联合发起了2019网络市场监管专项行动（“网剑行动”），着力规范电子商务主体资格，严厉打击网络市场突出问题，落实电子商务经营者责任，维护良好网络市场秩序。

具体来说，此次专项行动的重点任务主要如下：（一）着力规范电子商务主体资格，营造良好准入环境；（二）严厉打击网上销售假冒伪劣产品、不安全食品及假

18.中央网信办：“国家网信办启动网络生态治理专项行动 剑指12类违法违规互联网信息”，http://www.-cac.gov-.cn/2019-01/03/c_1123942483.htm，访问时间：2019年12月13日。
19.中央网信办：“国家互联网信息办公室关于《网络生态治理规定（征求意见稿）》公开征求意见的通知”，http://www.-cac.gov-.cn/2019-09/11/c_1569729939897372.htm，访问时间：2019年12月13日。
20.市场监管总局：“市场监管总局开展“守护消费”行动 打击侵害消费者个人信息违法行为”，http://ww-w.samr.gov.cn/zfjc-j/sjdt/g-zdt/201904/t20190410_292709.html，访问时间：2019年12月13日。

药劣药，营造放心消费环境；（三）严厉打击不正当竞争行为，营造公平竞争的市场环境；（四）深入开展互联网广告整治工作，营造良好广告市场环境；（五）依法打击其他各类网络交易违法行为，有效净化网络市场环境；（六）强化网络交易信息监测和产品质量抽查，营造良好消费环境；（七）落实电子商务经营者责任，营造诚信守法经营环境。

本次专项行动明确了网络市场中存在的问题，综合运用行政指导、行政约谈、行政处罚等手段，督促电子商务经营者、特别是平台经营者履行法定责任和义务，加强了部门间协同监管和联合惩戒，有助于净化网络市场环境，规范网络交易行为[21]。

（五）工信部网络安全管理局开展2019年电信和互联网寒夜网络安全行政检查工作

2019年5月，工信部网络安全管理局主导开展2019年电信和互联网行业网络安全行政检查工作[22]，检查对象为依法获得电信主管部门许可的基础电信企业、互联网企业、互联网域名注册管理和服务机构（以下统称“网络运行单位”）建设与运营的网络和系统。行动将通过自查自纠、检查评估、整改问责等阶段手段，以电信和互联网行业网络基础设施为重点关注对象，即通过公共互联网收集、存储与处理用户信息和网络数据的重要信息系统，包括但不限于互联网数据中心、公共云服务平台、工业互联网平台、企业门户网站、即时通信系统、软件应用商店、公众视频监控平台等。检查内容包括网络安全管理落实情况、网络安全防护技术手段、仍然存在的漏洞等风险隐患等。

（六）工业和信息化部开展APP侵害用户权益专项整治工作

当下，APP违规收集个人信息、过度索权、频繁骚扰、侵害用户权益等问题日益突出，工信部在2019年11月组织开展了APP侵害用户权益专项整治行动工作[23]。这次整治工作主要面向两类对象：一是APP服务提供者，主要检查是否存在侵害用户个人信息等合法权益的现象；二是APP分发服务提供者，含应用商店和基础电信企业营业厅等承担APP分发功能的各类企业，主要检查是否落实《移动智能终端应用软件预置和分发管理暂行规定》等有关要求。具体来说，工信部主要针对以下8个问题展开整治工作：

第一，“私自收集个人信息”。即APP未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前，收集用户个人信息。

第二，“超范围收集个人信息”。即APP收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息，如通讯录、位置、身份证、人脸等。

21.国家市场管理总局：“市场监管总局等部门关于印发2019网络市场监管专项行动（网剑行动）方案的通知”，，http://gkml.samr.gov.cn/nsjg/wjs/201906/t20190620_302494.html，访问时间：2019年12月13日。

22.工信部：“关于做好2019年电信和互联网行业网络安全行政检查工作的通知”，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c6983820/content.html，访问时间：2019年12月13日。

23. 工信部：“工业和信息化部关于开展App侵害用户权益专项整治工作的通知”，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057714/c7506181/content.html，访问时间：2019年12月13日。

第三，“私自共享给第三方”。即APP未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

第四，“强制用户使用定向推送功能”。即APP未向用户告知，或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。

第五，“不给权限不让用”。即APP安装和运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。

第六，“频繁申请权限”。即APP在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。

第七，“过度索取权限”。即APP在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

第八，“账号注销难”。即APP未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

SECTION 02

主要执法主体

根据《网络安全法》的规定，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在各自职责范围内负责网络安全保护和监督管理工作。具体而言，网络安全法的行政执法部门主要有中央网信办、工信部、公安部、国家保密局、国家密码管理局以及各行业主管部门等。其中，最主要的执法机构为中央网信办、工信部和公安部。

基于条文本身可知，上述执法主体间存在着权责不清、交叉执法的问题；而在具体执法案例中，尽管各部门间对于网络安全监管方向存在初步可感知的差异，但仍未有明晰的领域界限，网络安全监管“九龙治水”现象仍然存在。

SECTION 03

主要执法依据

根据附件总结的《网络安全法》行政执法案例，主要执法依据如下表所示（附表2）

序号	条目 《网络安全法》	主要内容
1	第21条、第59条	网络安全等级保护制度、网络安全保护义务
2	第56条	网络安全风险或安全事件的约谈制度
3	第22条第3款、第41条、第42条、第43条、第64条	个人信息保护
4	第24条、第61条	网络实名制
5	第47条、第50条、第68条	网络用户发布信息管理
6	第22条、第60条	网络产品和服务的法定要求：不得设置恶意程序、终止提供安全维护
7	第46条、第67条	禁止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

附表2：《网络安全法》行政执法案例的主要执法依据

其中，从执法案例数量上看，因未按要求管理用户发布的信息而根据《网络安全法》第47、50、68条作出的处罚案例，因未落实网络安全等级保护制度，未履行网络安全保护义务而根据《网络安全法》第21、56、59条作出的处罚案例，以及因未履行个人信息保护的法律责任而违反《网络安全法》第22、41、42、43、64条作出的处罚案例，系目前工信部、公安部、中央网信办及其地方对应部门已作出的执法案例中前三多的案例类型。

SECTION 04

主要责任主体

根据附件一总结的《网络安全法》行政执法案例，主要责任主体为网络运营者和网络用户。根据《网络安全法》第76条第3款的规定，网络运营者是指网络的所有者、管理者和网络服务提供者。结合附件案例，具体而言，责任主体主要集中在以下三类：具有信息发布功能的网站及平台的运营者；网络科技/技术公司；学校、学院及其他事业单位。

从领域分布来看，考虑到网络使用与业务发展的密切程度，案例所涉及的责任主体主要集中于科技、通信传媒、教育等领域，少部分属于电商、政务、酒店服务、快消、农业等领域。在我们收录的行政执法案例中，可以看到，相比2018年，除了科技公司一直属于监管重点外，“网络直播平台”、“电商平台”、“即时通讯平台”等也被列入强监管范围，涉及领域不断拓展。

除上述作为主要责任主体的网络运营者之外，利用网络发布违法犯罪活动信息的组织或个人也成为《网络安全法》行政执法的规制对象，如在微信群中转发散布谣言、发布炸药制作方法、传播涉暴力恐怖、淫秽信息、宗教极端、民族分裂的文字、图片等的个人也会依法承担相应的行政拘留甚至刑事责任。

24.责令整改是否为行政处罚措施存有争议，此处暂列为行政处罚措施。

SECTION 05

主要处罚措施

根据附件总结的《网络安全法》行政执法案例，处罚措施集中在责令整改[24]、警告、罚款（包括单位和直接负责人）、责令停产停业（包括停业整顿、关闭网站、暂停有关系统运行、停止更新、暂停新用户注册）、行政拘留、刊发道歉声明六类，有单罚亦有并罚。其中最主要的处罚措施为责令整改，在附件总结的案例中，多数案例均涉及责令整改；其次为罚款，对单位的罚款从一万到五十万不等。另外，目前对于一些未产生严重后果但存在较大安全风险而引发市场关注的不合规行为，监管部门往往倾向于先行约谈整改。

其中，在2019年，除了常规的约谈及督促整改以外，执法机关对于存在问题的企业所提出的整改要求不断细化，处罚措施趋于多样化，包括高额罚款、产品下架、服务平台限期停止服务等。可以看到，执法机关一方面在不断加强执法力度，另一方面也通过更为因地制宜的整改措施，以查促改，推动国内网络运营秩序及环境的健康发展。

SECTION 06

主要处罚地域

在附件收录的《网络安全法》行政执法案例中，处罚地区主要集中在浙江、江苏、上海、广东、北京等发达地区，安徽、山东、广西、湖南等地也有发生。随着《网络安全法》及配套法规的深入落实，执法案例将覆盖更多省份及地区，执法范围已基本覆盖全国。

附件一：《网络安全法》行政执法相关处罚案例

为更清晰展现《网络安全法》自正式实施以来的相关执法案例，综合把握执法情况发展脉络及典型案例，在本期汇总整理的行政执法相关处罚案例中，我们收录了2019年起由国家层面机关以及各地地方主管机关采取的主要执法检查行动和处罚案例。基于本文汇总分析的案例成果，可以初步感知，2019年发生的执法行

动存在着以下显著特征：

第一，关注的法律问题层面：执法案例更加集中于个人信息保护、用户信息发布管理层面，高度关注网络用户个人信息安全及网络环境净化；

第二，执法主体层面：执法主体主要为公安机关，工信部（及其地方所属的通信管理局）以及各级网信办参与执法行动的活跃度提升，金融管理机关也有参与执法；

第三，执法对象层面：除了一直属于监管重点的科技公司外，网络直播平台、电商平台、即时通讯平台等受监管关注的频度不断提升，执法对象涉及领域不断拓宽；

第四，处罚措施层面：除了常规的约谈及督促整改以外，整改要求不断细化，处罚措施趋于多样化，包括高额罚款、产品下架、服务平台限期停止服务等。

以下是自2019年1月1日以来围绕《网络安全法》所开展的行政执法相关处罚案例一览表。

25. 详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
1	网络安全运行管理制度	《网络安全法》第21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	《网络安全法》第56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。 《网络安全法》第59条 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，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。 《网络安全法》第六十一条 网络运营者违反本法第二十四条	未落实网络安全等级保护制度、不履行网络安全保护义务	2019-09	江苏省无锡市公安局	江苏省无锡市	科技	无锡某科技公司正在开发、测试的网络平台遭黑客攻击破坏造成不良影响。经查，该公司安全意识淡薄，未落实网络安全等级保护制度，未采取技术防护措施，未制订网络安全事件应急处置预案等。2019年9月，无锡警方依据《网络安全法》第21条、第25条、第59条规定，对该公司予以罚款5万元，对直接负责的主管人员倪某某予以罚款2万元。[25]
					2019-05	重庆市永川区公安局	重庆市	医疗	在了解重庆永川某私立医院服务器突然陷入瘫痪，医院业务全面“停摆”后，重庆永川警方对该私立医院进行调查后发现，医院HIS、LIS、PACS、EMR等后台系统业务以及微信公众号后台、医院网站等主要系统业务全部放置在同一套服务器中，医院未安装边界防护设备、未安装日志行为审计设备，未设置数据安全备份策略等其

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
1	网络安全运行管理制度	份和加密等措施； （五）法律、行政法规规定的其他义务。 《网络安全法》第二十四条 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，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、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。						他网络安全技术措施，使医院业务在互联网上长期处于“裸奔”状态。对此，公安部门对医院未按照网络安全等级保护制度的要求履行安全保护义务的行为进行查处，并按照《网络安全法》第59条之规定，对医院处以罚款一万元，对直接负责的主管人员处以罚款五千元的行政处罚。[26]
					2019-05	广东省广州市公安局	广东省广州市	酒店	广州市海某悦酒店在提供互联网上网服务（WiFi）的过程中，虽然安装了互联网公共上网服务场所安全管理系统，但擅自停止了互联网安全保护技术措施，导致安全管理系统没有正常运行。广州警方根据《互联网安全保护技术措施规定》第十四条第（一）项之规定，依法对该司作出警告的行政处罚，并责令限期改正。[27]
					2019-02	江苏省无锡市公安局	江苏省无锡市	市政	无锡某图书馆因安全责任意识淡薄、网络安全等级保护制度落实不到位、管理制度和技术防护措施严重缺失，导致网站遭受攻击破坏。无锡公安机关依据《网络安全法》第21条、第59条规定，对上述单位予以5万元罚款，对相关责任人予以2万元罚款，同时责令限期整改安全隐患，落实网络安全等级保护制度。[28]
					2019-02	江苏省南京市公安局	江苏省南京市	科研	南京某研究院因安全责任意识淡薄、网络安全等级保护制度落实不到位、管理制度和技术防护措施严重缺失，导致网站遭受攻击破坏。南京公安

26.详见“重庆网警：某医院未履行等级保护制度被罚款1万元”，http://www.sohu.com/a/312780954_100150040，访问时间：2019年12月13日。
27.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
28.公安部网络安全保卫局：“江苏网警发布‘净网2019’专项行动行政执法典型案例”，http://www.cyberpolice.cn/wfjb/html/g-zdt/20190510/4594.shtml，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
									机关依据《网络安全法》第21条、第59条规定，对上述单位予以5万元罚款，对相关责任人予以5千元罚款，同时责令限期整改安全隐患，落实网络安全等级保护制度。[29]
				网络安全漏洞等安全风险信息未采取技术措施或者未充分保障安全事件整改	2019-08	中国银行保险监督管理委员会	北京市	金融	2019年8月9日，中国银行保险监督管理委员会针对中信银行股份有限公司未向监管部门报告重要信息系统运营中断事件、信息系统控制存在较大安全漏洞而未做到有效的安全控制等包含网络安全在内的多项问题，根据相关法规作出行政处罚（银保监罚决字〔2019〕12号），没收违法所得33.6677万元，罚款2190万元，合计2223.6677万元。[30]
					2019-07	湖南省长沙市公安局	湖南省长沙市	科技	2019年7月2日，长沙市公安局高新分局网安大队工作中发现长沙某科技有限公司网站被攻击入侵，主页被篡改存有大量涉黄信息和广告信息。经查，该网站未落实安全技术措施、未制定内部安全管理制度、未明确网络安全责任人。高新网安大队依据《中华人民共和国网络安全法》第21条、第59条规定，对该公司及直接负责主管人员周某分别予以罚款10000元和5000元，并责令立即整改到位。[31]

29.公安部网络安全保卫局："江苏网警发布'净网2019'专项行动行政执法典型案例"，http://www.cyberpolice.cn/wfjb/html/gzdt/20190510/4594.shtml，访问时间：2019年12月13日。
30.中国银行保险监督管理委员会："中国银行保险监督管理委员会行政处罚信息公开表（银保监罚决字〔2019〕12号）（中信银行股份有限公司）"，http://www.cbirc.gov.cn/cn/doc/9103/910305/ybjhcf/10DC795A790442BFAB0042CA48E3A478.html，访问时间：2019年12月13日。
31.详见"公安机关'净网2019'网络安全相关典型案例"，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-01	上海市通信管理局	上海市	科技 电脑 好传媒	市通信管理局在网络安全回头看专项复查中发现，上海聚力传媒技术有限公司在接到《上海市通信管理局网络安全威胁通报（2018年第36期）》并责令改正的要求后，未对其移动互联网APP应用“PP体育”存在的安全风险采取补救措施，未落实整改要求；上海匹匹扣网络科技有限公司在接到上海市通信管理局网络安全威胁通报（2018年第42期）并责令改正的要求后，未对其移动互联网APP应用“旅游圈”存在的安全风险采取补救措施，未落实整改要求。对此，市通信管理局依据《网络安全法》有关规定，对两家企业分别处以罚款人民币五万元，并对两家企业直接负责的网络安全主管人员季某和李某分别处以罚款人民币一万元。[32]
					2019-01	广东省深圳市公安局	广东省深圳市	通讯、科技	2018年12月28日，深圳网警在深圳市“护网2018”网络攻防演习中，发现中国XX通信集团广东有限公司深圳分公司微信公众号“深圳XX营业厅”对应的后台系统存在1处SQL高危系统漏洞，可导致大量会员信息、宽带订购信息、手机套餐信息、手机充值信息泄漏。2019年1月17日，深圳网警再次组织警力对该公司开展网络安全检查，发现该公司仍未对存在的系统漏洞进行处置。深圳警方根据《公安机关办理行政案件程序规定》第一百三十八条第一款，《中华人民共和国网络安全法》第二十一条第二项、第二十五条、第五十九条第一款之规定，决定给予中国XX通信集团广东有限公司深圳分公司行政警告处罚并责令限期五日改正。[33]

32.详见“上海市通信管理局通报一批网络安全违规典型案例”：http://www.sohu.com/a/298148186_100150040，访问时间：2019年12月13日。
33.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
				网络安全管理制度未建立/健全	2019-09	江苏省宿迁市公安局	江苏省宿迁市	科技	包某某(男,30岁)、赵某某(男,26岁)、顾某某(男,24岁)、颜某某(男,28岁,均为沭阳人)4人合伙在宁港经济开发区顾某某家厂房搭建设备,对外提供网络服务,今年9月6日因未落实网络安全管理制度和技术防护措施,被宿迁警方责令限期整改。9月21日,包某某等人未整改到位,宿迁警方依据《网络安全法》第21条、第59条规定,对包某某等4人分别予以罚款5千元。[34]
					2019-09	江苏省连云港市公安局	江苏省连云港市	能源	连云港警方在对辖区电力企业开展网络安全执法检查中发现,某光伏电站、某风力发电有限公司、某新能源有限公司等10家单位不同程度存在网络安全管理制度不完善、技术防护措施不到位、未开展网络安全等级保护工作等问题。 2019年9月,连云港警方依据《网络安全法》第21条、第59条规定,对该光伏电站等单位分别予以警告,责令限期整改,落实网络安全等级保护制度。[35]
					2019-09	江苏省常州市公安局	江苏省常州市	科技	常州警方在受理外地公安机关协查时发现,常州某互联网数据中心未落实信息安全管理制度,未采取屏蔽过滤等技术保护措施,致使犯罪嫌疑人租用并利用该公司提供的服务器,非法传播大量盗版视频及淫秽色情视频,造成严重后果。2019年9月,常州警方依据《网络安全法》第47条、第68条规定,对该互联网数据中心予以罚款10万元,对直接负责的主管人员予以罚款1万元,没收其违法所得7200元。[36]

34. 详见“公安机关‘净网2019’网络安全相关典型案例”,https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw,访问时间:2019年12月13日。
35. 详见“公安机关‘净网2019’网络安全相关典型案例”,https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw,访问时间:2019年12月13日。
36. 详见“公安机关‘净网2019’网络安全相关典型案例”,https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw,访问时间:2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-01	上海市通信管理局	上海市	科技、娱乐	市通信管理局核查发现，本市某网络音频FM公司未按照《网络安全法》有关要求制定网络安全事件应急预案；同时，企业网络安全事件管理不到位，未制定事件报告和处置制度，未对安全事件制定通报流程，在发生安全事件后未按照规定向市通信管理局等主管部门报告有关情况。市通信管理局针对上述问题约谈企业主要负责人，要求其牢固树立网络安全责任意识，严格落实企业安全管理，完善应急预案和事件报告制度，切实履行网络运营者的安全保护义务。
2	个人信息保护制度	《网络安全法》第22条 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。 《网络安全法》第41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	《网络安全法》第64条 网络运营者、网络产品或者服务的提供者违反规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。	未获取个人信息收集、使用的用户同意及授权；未充分保障用户个人信息安全	2019-11	工信部	全国	科技、娱乐	针对媒体公开报道和用户曝光的“ZAO”App用户隐私协议不规范，存在数据泄露风险等网络数据安全问题，工信部网络安全管理局对北京陌陌科技有限公司相关负责人进行了问询约谈，要求其严格按照国家法律法规以及相关主管部门要求，组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。同时，要进一步加强新技术新业务安全评估，切实采取有效措施，积极防范自有业务平台被利用实施电信网络诈骗等风险隐患。[37]

37.工信部：“网络安全管理局就‘ZAO’App网络数据安全问题开展问询约谈”，http://www.miit.gov-.cn/n1146290/n1146402/n1146440/c7392862/content.html，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
		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。 《网络安全法》第42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。 《网络安全法》第43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。			2019-11	天津市公安局武清分局	天津市	科技、医疗	“健康天津”APP涉嫌无隐私协议收集用户位置信息等违法违规行为，经天津市公安局武清分局网安支队受案调查，依据《网络安全法》第41条、第64条规定，对该APP运营单位“天津健康医疗大数据有限公司”处以行政警告并责令限期整改。[38]
					2019-11	上海市公安局徐汇分局	上海市	科技	“趋势密码”APP未经用户同意收集使用精准定位等个人信息，涉嫌超范围收集用户信息等违法违规行为，经上海市公安局徐汇分局网安支队受案调查，依据《网络安全法》第64条第一款，对该APP运营单位“上海益秋投资管理有限公司”处以行政警告。[39]
					2019-11	成都市公安局	四川省成都市	科技	“简讯”APP涉嫌无隐私协议收集用户位置信息等违法违规行为，经成都市公安局网安支队受案调查，依据《网络安全法》第64条第一款规定，对该APP运营单位“成都市黑领科技有限公司”处以行政警告并处罚款贰仟元。[40]
					2019-09	江苏省苏州市公安局	江苏省苏州市	科技、生活	苏州某软件公司运营的一款生活类APP应用涉嫌侵害公民个人信息。经查，该APP应用的软件代码存在获取用户部分敏感权限功能，可以收集与其提供的服务无关的用户信息。2019年9月，苏州警方依据《网络安全法》第41条、第64条规定，对该软件公司予以罚款1千元，对公司法人予以罚款1万元，责令限期整改。[41]

38.详见“公安机关开展APP违法采集个人信息集中整治”，http://www.zjtbzx.gov.cn/show-29-3129-1.html，访问时间：2019年12月13日。
39.详见“公安机关开展APP违法采集个人信息集中整治”，http://www.zjtbzx.gov.cn/show-29-3129-1.html，访问时间：2019年12月13日。
40.详见“公安机关开展APP违法采集个人信息集中整治”，http://www.zjtbzx.gov.cn/show-29-3129-1.html，访问时间：2019年12月13日。
41.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-09	工信部信息通信管理局	全国多地	通信	5月17日，工信部信息通信管理局针对近期“95”号码和移动转售业务“170”“171”等号段拨打骚扰电话严重扰民、群众举报投诉居高不下等突出问题，分别集中约谈了南京颢志苍信息科技有限公司等20家呼叫中心企业和远特（北京）通信技术有限公司等10家移动转售企业。各被约谈企业签订了《整改承诺书》，郑重承诺将严格贯彻落实工业和信息化部的整改要求，全面排查，立行立改，坚决整改到位，在整改完成前不再开通相关业务或申请新的码号资源。[42] 此外，5月22日，信息通信管理局就骚扰电话管控不力问题约谈了中国电信集团公司和广东、江苏、浙江、四川等问题突出的四省电信公司。中国电信集团公司和参会四省电信公司签订了《整改承诺书》，承诺将提高思想认识，切实履行企业主体责任，组织全面排查，切实堵住管理漏洞，并对问题严重的基层单位及责任人严肃问责，坚决整改到位。[43]
					2019-09	江苏省常州市公安局	常州	科技、娱乐	常州某网络科技公司运营的一款漫画类APP应用涉嫌侵害公民个人信息。经查，该网络科技公司对个人信息保护工作重视不够，未向被收集者明示收集、使用信息的目的、方式和范围。2019年9月，常州警方依据《网络安全法》第41条、第64条规定，对该网络科技公司予以警告，责令限期整改。[44]

42.工信部信息通信管理局：“信息通信管理局集体约谈骚扰电话问题突出企业”，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057714/c6960229/content.html，访问时间：2019年12月13日。
43.工信部信息通信管理局：“工业和信息化部就骚扰电话管控不力问题约谈中国电信”，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057714/c6968595/content.html，访问时间：2019年12月13日。
44.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-09	江苏省常州市公安局	江苏省常州市	交通、生活、科技	常州某智能停车场管理公司运营的一款停车类APP应用涉嫌侵害公民个人信息。经查，常州某智能停车场管理公司面向司机提供停车服务，在运营过程中采集司机个人信息，但未向被收集者明示收集、使用信息的目的、方式和范围。2019年9月，常州警方依据《网络安全法》第41条、第64条规定，对该智能停车场管理公司予以警告，责令限期整改。[45]
					2019-09	江苏省常州市公安局	江苏省常州市	金融	张某（男，36岁）、高某某（男，29岁，均为南京人）以1000元的价格在网上向他人（另案查处）购买公民个人信息，用于常州公司电话推销股票配资及微信推广农产品业务。2019年9月，常州警方依据《网络安全法》第44条、第64条规定，对张某、高某某分别予以罚款1万元。[46]
					2019-07	APP专项治理工作组	全国多地	科技	APP专项治理工作组通报了同花顺、墨迹天气等40家企业在个人信息收集使用、公开有效联系方式等方面存在合规问题的情况，责令其限期整改。[47]
					2019-07	工信部	全国多地	科技	工信部在近期执法调查中发现，饿了么、小红书、网易考拉等App未经用户同意收集个人信息，未明确告知用户收集、使用信息的目的、方式和范围，误导用户同意收集使用个人信息等，责令其运营者尽快整改。[48]

45.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
46.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
47.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
48.工信部：“工业和信息化部关于电信服务质量的通告（2019年第2号）”，http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c7021505/content.html，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-05	北京市公安局朝阳分局	北京市	科技、金融	警方工作中发现北京淘金者科技有限公司旗下一款产品牛股王APP，存在超范围采集用户个人信息及手机权限的情况。经现场检查，牛股王APP在获取读取手机状态和身份、发现已知帐户、拦截外拨电话、开机时自动启动四项权限中存在超范围采集用户个人信息的情况。对此，朝阳警方依据《网络安全法》第41条、第64条，对该公司给予行政警告处罚。[49]
					2019-05	广东省深圳市公安局	广东省深圳市	科技	2019年5月22日，深圳网警在工作中发现，深圳中维世纪科技有限公司开发的查看视频监控“NXXIP”移动应用在未明示收集、使用信息的目的、方式和范围的情况下，获取该应用的用户通讯录信息，存在超范围收集公民个人信息的行为，涉嫌违反《中华人民共和国网络安全法》第二十二条第三款、第四十一条至第四十三条、第六十四条之规定。依法给予中维世纪科技有限公司责令改正并处警告的行政处罚。[50]
					2019-04	中国人民银行武汉分行	湖北省武汉市	金融	中国人民银行武汉分行于2019年4月向交银国际信托有限公司发出《行政处罚决定书》（武银罚字〔2019〕第14号），针对后者未经同意查询个人信息和企业的信贷信息的现象，作出罚款人民币29万元的处罚。[51]

49.详见“北京警方发布‘净网2019’行政执法案例”，https://baijiahao.baidu.com/s?id=1640088245605529135&wfr=spider&for=pc，访问时间：2019年12月13日。
50.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
51.中国人民银行武汉分行：“中国人民银行武汉分行行政处罚信息公示表（2019.4.19）”，http://wuhan.pbc.gov.cn/wuhan/123472/123493/123502/3811247/index.html，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-02	江苏省扬州市公安局	江苏省扬州市	教育	扬州公安机关接群众举报，对本地某教育培训中心存在骚扰推销行为开展突击检查。现场查获记录学生及家长个人信息的纸质材料80余页，后经鉴定共计3025条公民个人信息。经传唤该培训中心法人孟某某（男，40岁，扬州人）及现场正在电话营销的工作人员，查清非法获取多所学校学生姓名及家长电话，用以推销课程的违法事实。今年2月，扬州公安机关依据《网络安全法》第44条、第64条规定，对该教育培训中心予以罚款6万元。[52]
					2019-02	江苏省无锡市公安局	江苏省无锡市	电商	经调查发现，无锡某企业在互联网运营的某销售平台存在管理员弱口令，该平台服务器存有姓名、手机号等公民个人信息，极易引发数据泄露。今年2月，无锡公安机关依据《网络安全法》第42条、第64条规定对未履行数据保护义务、侵害公民个人信息依法得到保护权利的无锡市某国有企业予以警告并责令改正，对系统运维部门负责人予以警告。[53]
					2019-01	上海市通信管理局	上海市	科技、旅游	市通信管理局发现本市某在线旅游服务企业在其互联网信息系统内以明文形式存储游客的身份证件信息、护照信息、手机号码等个人信息，未按照《网络安全法》有关法律要求，采取技术措施和其他必要措施保障其收集的用户个人信息安全；且企业未明确个人信息在使用、传输和存储过程中的防护要求，存在严重的用户信息安全风险。市通信管理局在组织有关网络安全

52.中国人民银行武汉分行：“中国人民银行武汉分行行政处罚信息公示表（2019.4.19）”，http://wuhan.pbc.gov.cn/wuhan/123472/123493/123502/3811247/index.html，访问时间：2019年12月13日。
53.公安部网络安全保卫局：“江苏网警发布‘净网2019’专项行动行政执法典型案例”，http://www.cyberpolice.cn/wfjb/html/gzdt/20190510/4594.shtml ，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
									专业机构对相关漏洞进行现场记录和分析取证后，对企业负责人进行了严肃约谈通报，责令其立即采取技术防护措施，完善数据安全管理制度，确保其收集、存储的个人信息和数据安全，保障互联网用户的合法权益。[54]
					2019-01	上海市通信管理局	上海市	科技、电商	市通信管理局监测发现本市某宽带接入服务单位的某电子商城平台存在严重安全漏洞，外部人员可利用相关漏洞查看商城用户的姓名、地址、手机号码等个人信息，从而导致用户信息泄露等严重风险。市通信管理局组织有关网络安全专业机构对相关问题进行了现场记录和分析取证，并按照《网络安全法》有关精神对企业负责人进行严肃约谈通报，责令其立即采取补救措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。[55]
3	网络实名制	《网络安全法》第24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。	《网络安全法》第61条 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，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、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。	未落实真实身份信息登记、发布审核等	2019-09	山东省菏泽市公安局	山东省菏泽市	科技	2019年9月16日，菏泽市东明县某网络科技公司网站因网络安全防护工作落实不到位，大量注册用户未落实实名认证，网站存在严重安全隐患。网安部门在现场检查中发现，该网站自上线运行以来，始终未落实网络安全等级保护制度、不履行网络安全保护义务、未要求注册用户提供真实身份信息、留存网络日志少于六个月。根据《网络安全法》第五十九条第一款、第六十一条之规定，山东省菏泽市公安局网安支队决定给予该网络科技公司和直接负责的主管人员法定代表人李某某行政处罚决定，对公司处六万元罚款，对法定代表人李某某处五千元罚款，责令停业整顿。[56]

55.详见“上海市通信管理局通报一批网络安全违规典型案例”：http://www.sohu.com/a/298148186_100150040，访问时间：2019年12月13日。
56.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-06	北京市公安局海淀分局	北京市	科技	警方工作中发现北京奇客创想科技股份有限公司旗下的7k7k应用分发平台为用户提供信息发布、与用户签订协议或者提供服务时，未要求用户提供真实身份信息。针对此情况，海淀警方对该平台开展现场安全检查，立即约谈该公司主要负责人，发现该平台有130款APP开发者信息不完整，违反了《网络安全法》第24条之规定。海淀警方依据《网络安全法》第61条给予该公司责令限期整改的行政处罚。[57]
					2019-01	北京市公安局昌平分局	北京市	科技	警方工作中发现运营商北京千秋大业信息科技有限公司存在未按要求留存接入用户真实身份信息的情况，立即对该运营商开展现场检查。经核查，该公司于2018年因未按要求留存用户真实信息已被公安机关给予行政警告并责令限期改正。因其逾期未改，昌平警方依据《计算机信息网络国际联网安全保护管理办法》第21条之规定给予该公司罚款9000元、公司主管人员罚款3000元的行政处罚。[58]
	用户信息发布管理制度	《网络安全法》第47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。	《网络安全法》第68条 网络运营者违反本法第四十七条规定，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、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可	未对平台内用户发布的违法信息和有害信息采取处理措施（包括对内容传输停止等措施，对外向主管部门报告）	2019-09	江苏省扬州市公安局	江苏省扬州市	政务	扬州某市级单位因工作需要，在互联网申请免费邮箱，后将该邮箱账号、密码以通知形式公布在该单位网站上。此后，该邮箱长期无人管理维护，导致被不法分子利用，多次接受、转发涉及邪教等违法有害信息。2019年9月，扬州警方依据《网络安全法》第21条、第59条规定，对该单位予以警告，责令限期整改。[59]

57.详见“北京警方发布‘净网2019’行动执法案例”，https://baijiahao.baidu.com/s?id=1640088245605529135&wfr=spider&for=pc，访问时间：2019年12月13日。
58.详见“北京警方发布“净网2019”行动执法案例”，https://baijiahao.baidu.com/s?id=1640088245605529135&wfr=spider&for=pc，访问时间：2019年12月13日。
59.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
		《网络安全法》第50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。	以责令暂停相关业务、停业整顿、关闭网站、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。		2019-07	湖南省郴州市桂阳县公安局	郴州桂阳市	科技	2019年7月11日，郴州桂阳市公安局网安大队工作中发现桂阳某网站出现赌博APP下载链接。经调查，该网站未对用户上传的“惠创金服”和“惠创国际”的两个涉嫌赌博的APP进行内容审核。桂阳网安大队依据《中华人民共和国网络安全法》第47条、第68条规定，对该网站运营者予以警告处罚，并责令立即整改。[60]
					2019-06	北京市公安局朝阳分局	北京市	科技	警方工作中发现“猫途鹰”网存在违法信息、公司审核措施落实不到位的情况，违反《网络安全法》第47条之规定。朝阳警方依据《网络安全法》第68条之规定对该公司罚款10万元。[61]
					2019-05	中央网信办、教育部、全国扫黄打非办等部门	全国多地	科技、教育	今年1月至4月，国家网信办会同教育部、全国扫黄打非办等有关部门开展教育类移动应用程序专项整治。根据网民举报线索，专项整治行动对国内教育类移动应用程序信息服务组织巡查，查实“作业狗”“口袋老师”“初中知识点大全”等20余款程序传播淫秽色情等违法违规信息，存在过度商业营销和娱乐化等不良行为。国家网信办已清理下架上述程序，关停违法违规情况严重的应用服务，约谈部分程序运营方，督促删除内容低俗及与学习无关的文章5.5万余篇，关停420余个专栏以及320多个违规账号，全面整改，规范运营，落实企业主体责任。同时，还清理下架以青少年为主要用户的二次元和社交类违法违规程序1.21万款。[62]

60.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
61.详见“北京警方发布“净网2019”行政执法案例”，https://baijiahao.baidu.com/s?id=1640082456055291 35&wfr=spider&for=pc，访问时间：2019年12月13日。
62.详见“‘作业狗’‘口袋老师’等教育类APP因涉黄低俗被整治”，https://www.chinacourt.org/index.php/article/detail/2019/05/id/3924956.shtml，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-05	广东省深圳市公安局	广东省深圳市	科技、直播	2019年5月30日，深圳网警对深圳果酱时代科技有限公司以“百得新科技（香港）有限公司”（法人代表崔某）的名义，从2017年7月至今在境外运营两个直播平台的案件进行调查。经查，该公司从2016年8月份开始经营国内外十几个直播平台，同时在香港注册百得新科技有限公司，通过该公司经营海外直播平台，但该公司所有工作人员办公地点在深圳果酱时代科技有限公司。调查发现该公司后台有大量涉黄信息及图片，其行为已构成对法律、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的违法行为。深圳警方依据《中华人民共和国网络安全法》第六十九条之规定，决定给予深圳市果酱时代科技有限公司罚款5万元、直接负责的主管人员罚款1万元的行政处罚。[63]
					2019-04	天津市网信办	天津市	科技、图像	经查，视觉中国网站（域名：vcg.com）在其发布的多张图片中刊发敏感有害信息标注，违反了《网络安全法》第47条之规定。天津市网信办依据《网络安全法》第68条第一款之规定，对网站运营主体汉华易美（天津）图像技术有限公司作出从重罚款的处罚。[64]
					2019-04	中央网信办	全国多地	科技、通讯	针对即时通信工具传播违法违规信息、匿名注册、欺诈诱骗、为线下违法违规活动提供平台服务等行业乱象，国家网信办启动即时通信工具专项整治工作，从应用展现、服务导向、商业模式、注册机制、信息内容、群组管理等方面，对

63.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
64.天津网信办：“天津市网信办依法对视觉中国网站做出行政处罚”，https://mp.weixin.qq.com/s/VSbrKoIkRyagVvquJxHZ3Q，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
									各类即时通信工具进行深入巡查和测试。首批清理关停“比邻”“聊聊”“密语”等9款传播淫秽色情信息，或为招嫖卖淫、售卖淫秽色情音视频等提供推广和平台服务的即时通信工具。[65]
					2019-04	广东省深圳市公安局	广东省深圳市	科技	2019年4月20日，深圳网警对互联网数据中心运营商深圳易信科技股份有限公司存在违法信息高发的问题进行调查，发现该公司未按照法律规定落实用户实名登记、日志留存、违法信息防治、等级保护措施，导致相关机房托管的两个网站被黑客入侵并植入博彩页面（分别有61个和237个页面被篡改）。深圳警方根据《中华人民共和国网络安全法》第二十五条、第五十九条之规定，决定给予深圳易信科技股份有限公司警告的行政处罚。[66]
					2019-02	中央网信办	全国多地	科技	中央网信办依据《网络安全法》、《互联网新闻信息服务新技术新应用安全评估管理规定》和《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》等法规性文件的管理精神及要求，连续约谈约见“微信7.0版”、“聊天宝”、“马桶MT”、“多闪”等四款社交类新功能新应用企业负责人，责成有关企业履行和完善安全机制程序，依法开展安全评估工作。[67]

65.中央网信办：“国家网信办启动小众即时通信工具专项整治 首批清理关停9款违法违规APP”，http://www.cac.gov.cn/2019-04/16/c_1124373996.htm，访问时间：2019年12月13日。
66.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
67. 中央网信办：“国家网信办约谈约见四款新发布社交类应用企业”，http://www.cac.gov.cn/2019-02/01/c_1124077140.htm，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
					2019-02	广东省广州市公安局	广东省广州市	科技、生活	2019年2月，广州警方在接到群众举报有人通过社交软件“X伴”APP发布招嫖信息后，对其运营公司广州十柒道科技贸易有限公司开展现场检查，发现该APP实际为2018年11月被行政处罚并下架的“睡X”APP“改头换面”而来。在现场检查发现，“X伴”APP后台上存在未经实名认证而发布的信息量高达22万余条，其中含有违法内容的信息有100余条。针对广州十柒道科技贸易有限公司存在的违法行为，广州警方根据《网络安全法》第六十一条之规定，依法对该司处以罚款十万元、对法人代表薛某处以罚款一万元的行政处罚，并责令限期改正。受到处罚后，该公司主动下架了“X伴”APP。[68]
4	网络产品和服务管理制度	《网络安全法》第22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。	《网络安全法》第60条 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。	未能及时全面检测和完善网络服务	2019-08	江苏省无锡市公安局	江苏省无锡市	科技、房地产	无锡某房产信息技术服务公司运营的房产交易网站存在管理员弱口令等隐患，网站服务器存有手机号、身份证、家庭住址及房产交易记录等公民个人信息6万余条，极易引发数据泄漏。2019年8月，无锡警方依据《网络安全法》第42条、第64条规定，对该房产信息技术服务公司予以警告，责令限期整改。[69]
					2019-06	广东省广州市公安局	广东省广州市	科技	2019年6月，广州市某公司会员积分测试系统遭黑客非法入侵，网站首页被篡改张贴违法有害信息，造成恶劣影响。经查，本次遭受攻击的信息系统为该公司于2015年前搭建的测试系统，已多年处于无人维护的状态，但该系统仍然在线可通

68. 详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。
69.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

序号	法律制度	法律规定		具体执法案例					
		法律要求	法律责任	具体事由	公告时间	执法部门	发生地区	领域标签	案例描述
									过互联网访问，并存在弱口令、远程命令执行等多个高危漏洞，导致被黑客入侵并篡改。同时，该单位还未依法落实留存网络日志技术措施的问题。针对该公司不履行网络安全保护义务的行为，广州公安机关依法对其作出行政处罚，并责令其限期改正。[70]

70.详见“公安机关‘净网2019’网络安全相关典型案例”，https://mp.weixin.qq.com/s/Z6aHl72AhTDsNQUTxbXNTw，访问时间：2019年12月13日。

第二节 刑事典型案例及工作发展综述

本节选取了部分与《网络安全法》内容紧密相关的、具有较大影响力或者指导意义的刑事案例，具体可详见《附件二：<网络安全法>相关的刑事典型案例》。

SECTION 01

主要适用法规

《网络安全法》与《刑法》及相关司法解释在个人信息保护、计算机信息系统安全层面形成了较为明确的内容对应（附表1）：

		个人信息保护	计算机信息系统安全
《网络安全法》	第47条 禁止发布违法信息	第44条禁止非法获取/对外提供个人信息	第27条 禁止危害网络安全
《刑法》及相关司法解释	《中华人民共和国刑法》第三百六十四条第一款、第四款规定：传播淫秽的书刊、影片、音像、图片或者其他淫秽物品，情节严重的，处二年以下有期徒刑、拘役或者管制。向不满十八周岁的未成年人传播淫秽物品的，从重处罚。	第253条之一 【侵犯公民个人信息罪】	第285条、第286条 【非法侵入计算机信息系统罪】 【非法侵入计算机信息系统罪；非法获取计算机信息系统数据、非法控制计算机信息系统罪；提供侵入、非法控制计算机信息系统程序、工具罪】 第二百八十六条之一【拒不履行信息网络安全管理义务罪】
		《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》

SECTION 02

公安部部署组织全国公安机关开展“净网2019”专项行动

2019年1月，公安部部署组织全国公安机关开展“净网2019”专项行动，严厉打击侵犯公民个人信息、黑客攻击破坏等网络违法犯罪活动。在本年度中，全国各地公安机关一方面聚焦重点，打击网络违法犯罪，努力全面铲除网络违法犯罪赖以生存的网上土壤，最大程度打击和遏制违法犯罪活动；另一方面按照国家治理

体系和治理能力现代化的要求，积极推动有关政策、法律、机制和措施的健全完善，从源头上规范网络空间秩序、防范治理网络违法乱象。截至今年10月31日，共侦破涉网案件45743起，抓获犯罪嫌疑人65832名，取得了显著成效。其中侦破侵犯公民个人信息类案件2868起，抓获犯罪嫌疑人7647名；侦破黑客类案件1361起，抓获犯罪嫌疑人2133名；侦破网络诈骗类案件21933起，抓获犯罪嫌疑人22743名；侦破网络赌博类案件5797起，抓获犯罪嫌疑人9490名；侦破网络色情类案件2406起，抓获犯罪嫌疑人4512名；破获了一系列人民群众关心关切的重点热点典型案件，打掉多个利用“暗网”倒卖公民信息的犯罪团伙，捣毁一批为“套路贷”提供技术、数据服务的科技公司，斩断多条非法生产、销售针孔摄像头等偷拍器材的黑色产业链条，清剿了多张制售迷奸药物的犯罪网络。同时，针对互联网企业及联网单位开展安全监督检查17万余家次，清理违法有害信息445万余条，关闭网络账号60万余个，约谈整改相关网站及APP 3.7万余家次，行政查处9.1万家次[71]。

71.公安部：《公安部通报“净网2019”转向行动典型案例》，网址：http://www.cac.gov.cn/2019-11/14/c_1575264987750271.htm

附件二：《网络安全法》相关的部分刑事典型案例

随着现代通讯技术和互联网技术的快速发展，公民个人信息极易泄露并被用于交易，计算机信息系统的安全性随时经受考验。为保障互联网环境下公民个人信息及计算机信息系统的安全，《网络安全法》第44条、第27条分别对这两部分的安全保障义务进行规定，明确了行政责任的范畴；与此同时，《刑法》第253条之一、第285-286条分别为公民个人信息、计算机信息系统安全划定刑事合规“红线”，更进一步突出国家对于网络安全及数据合规工作的重视态度。尽管目前，在公开的判决书内公开援引、提及《网络安全法》的情况相对较少，但随着责任范围的逐步明确，任何构成网络运营者的个人及组织均需重视并遵守《网络安全法》的相关要求，以避免承担行政责任乃至进一步的刑事责任。

本附件主要收录与《网络安全法》条款内容明确相关的、涉及个人信息保护、信息系统安全以及违法信息传播的部分刑事典型案例，以2019年发生及作出判决的案例为主，其中重点关注公安部“净网2019”专项行动开展以来的案例成果及进展，以展现上述领域较为常见或者具有创新性的案例场景，明确刑事监管红线。

序号		法规条文（现行）	《网络安全法》的对应规定	判决时间	发生地区	判决法院	领域标签	案情简介	备注
1	侵犯公民个人信息罪	《刑法》第253条之一：违反国家有关规定，**向他人出售或者提供公民个人信息**，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。 违反国家有关规定，**将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的**，依照前款的规定从重处罚。 窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。 **单位犯前三款罪的，对单位判处罚金**，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。	《网络安全法》第44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。**	尚未判决	北京市房山区	尚未判决	科技	2019年8月，有人向北京警方举报称，其经常接到培训公司的精准推销电话，对方可以准确说出其工作职位和公司运营业务，并推销相关培训课程，自己生活工作已受到严重滋扰。接到举报线索后，网安总队立即开展网上侦查，发现这些精准推销电话多来自于房山区的两家咨询公司。对此，网安总队会同房山分局成立专案组开展工作。经查，该公司员工通过在网上购买、交换等方式获取了大批特定客户个人信息，然后雇佣业务员专门向目标客户推销培训课程。在获取犯罪证据后，专案组于8月19日开展集中打击行动，依法对两家涉案公司进行查处，现场起获涉案电脑90余台、手机100余部、U盘等存储介质20余个，提取并鉴定涉及工商法人代表信息类的公民个人信息80余万条。目前，涉案人员因涉嫌侵犯公民个人信息罪已被房山分局依法刑事拘留。[72]	公安部“净网2019”专项行动
2				尚未判决	河北省邯郸市	邯郸市丛台区人民法院	科技	2018年6月，邯郸市丛台区某小区居民到丛台区公安分局网安大队反映情况：在小区X号楼XX室中，有一伙年轻人白天频繁出入，行事神神秘秘，疑似搞传销。网安大队接报后，立即开展侦查。为避免打草惊蛇，侦查员化装成物业工作人员，以清查出租房屋为名对该户进行检查，发现有8人正在办公卡间内接打电话，办公桌上零散放置的印有包含姓名、电话、购买过的保健品、收货住址等公民个人信息的纸张，在房间墙角处还堆放着近一米高的A4纸张（已用过），有近万张之多。2018年6月29日，专案组抓获犯罪嫌疑人王某新等9人，查扣手机10部、电脑9台、硬盘3块。根据前期扎实的侦查取证工作，市县两级网安民警从10部手机、9台电脑、3块硬盘、数十万条聊天记录中，梳理出涉案人员关系脉络，最终确定王某新先后从浙江嘉兴姚某，河北张家口范某、祁某，湖南长沙王某强，北京郭某丹等处非法获取大量公民个人信息。2018年7月至10月，先后抓获以上5名犯罪嫌疑人，查获其电子设备。2019年6月27日，邯郸市丛台区人民法院对王某新等五人涉嫌侵犯公民个人信息犯罪依法开庭审理。[73]	公安部“净网2019”专项行动

72.详见“北京警方侦破多起网络侵犯公民个人信息违法犯罪案件”，https://mp.weixin.qq.com/s/35MXRIFqYRskwoawnvZtaw，访问时间：2019年12月13日。
73.详见“邯郸侵犯20余省公民个人信息案件利益链条”，https://mp.weixin.qq.com/s/s7xn7tG23yhhFxNMXSdq5w，访问时间：2019年12月13日。

序号		法规条文（现行）	《网络安全法》的对应规定	判决时间	发生地区	判决法院	领域标签	案情简介	备注
3				尚未判决	天津	尚未判决	科技	2019年9月初，天津市河东区多名居民在安装某贷款类手机App后，出现被非法采集通讯录、通话记录、短信等信息的情况。天津市公安局河东分局、天津市公安局网络安全保卫总队立即就此抽调精干警力组成专案组立案侦查。经过细致调查，专案组发现，该手机App的网站备案公司、软件著作权公司、服务器租赁公司均系同一伙人经营，职责明确、分工细致、团伙作案。经过公检法部门的三方会商，11月14日，天津市公安局河东分局组织60余名警力，会同河东区检察院工作人员飞赴外地，与专案组前期侦查警力会合，开展集中收网行动。11月15日凌晨6时许，在当地警方密切配合下，专案组兵分四路实施抓捕，分别将以葛某、朱某、李某平为首的22名涉案嫌疑人成功抓获。经查，为骗取公民个人信息，自2019年4月起，该团伙设计经营手机贷款App，在未明确告知用户的情况下，非法采集注册用户的通讯录、通话记录、短信息等隐私数据，仅非法采集的用户短信息初步统计就达246万多条。[74]	
4				尚未判决	广东省肇庆市	尚未判决	科技	2019年10月，封开公安民警在“净网2019”专项行动中走访各辖区派出所并开展网络安全宣传工作。工作中接到一群众反映最近总是接到一个“陌生女人”的来电咨询汽车抵押、贷款事项，并且收到大量的汽车抵押、无息贷款的短信等信息。民警凭借职业敏感性，判断这个事情背后可能隐藏着一批涉嫌侵犯公民个人信息的犯罪团伙。网安民警根据线索开展案件经营工作，成功挖掘出一个涉及汽车抵押领域的侵犯公民个人信息犯罪团伙，并经过侦查取证，掌握到该团伙通过QQ群、微信群等渠道获取需要查询公民汽车抵押信息的客户，然后把客户信息发给可以查询公民汽车抵押信息人员，再把查询结果反馈给客户，收取客户60元到80元不等的佣金。短短一个月时间，嫌疑人已经非法查询并出售公民个人信息1500余条，涉案金额达2万余元。[75]	公安部“净网2019”专项行动
5				2019-11	全国各地	江苏常州天宁法院	科技	2018年5月初，常州天宁警方通过网上巡查发现，某网络聊天软件上有人大肆贩卖公民的个人信息，涉及交易信息量和金额特别巨大。经专案组深度研判，警方逐步查明掌握一个盘踞全国、覆盖10多个省市的通过网络贩卖公民个人信息的特大犯罪网络。而这个网络甚至延伸到了境外，部分中间商从国内潜逃至越南、缅甸等东南亚国家，大肆倒卖公民个人信息。很快，这起案件被公安部挂牌督办。鉴于案情重大、涉	

74.详见“天津破获一起利用手机App骗取公民个人信息案件”，https://mp.weixin.qq.com/s/Zb7yqAzfraidiVL1iV6EKA，访问时间：2019年12月13日。
75.详见“封开警方侦破获一起涉嫌侵犯公民个人信息团伙案件抓获涉案人员4名”，https://mp.weixin.qq.com/s/9ybb22KH_LcHzLbgp7WptQ，访问时间：2019年12月13日。

序号		法规条文（现行）	《网络安全法》的对应规定	判决时间	发生地区	判决法院	领域标签	案情简介	备注
								案人员遍布境内外，专案组在江苏省公安厅网安总队、公安部网安局的大力支持下，抽调100余名警力，先后分赴全国多省市开展集中收网行动，一举抓获犯罪嫌疑人40名，打掉信息源头13个，查获公民各类信息约6万余条，涉案总价值200余万元。而境外中间商经公安部统一指挥，由无锡警方集中出境抓获4人。 经审查，该团伙中13人为牟利，利用工作的便利从单位内部非法获取公民各类信息约6万余条后，通过网络聊天软件以每条1元到1000元不等的价格出售给中间商，中间商再将购得的上述信息通过微信并以每条加价2元到500元不等的价格转卖给下游中间商以及散户，谋取暴利。目前，经江苏常州天宁法院公开开庭审理，瞿某、董某等30名被告人涉嫌侵犯公民个人信息案件，被告人被判处有期徒刑七个月至四年半不等的实刑。[76]	
6	非法获取计算机信息系统数据罪	《刑法》第285条：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。	《网络安全法》第27条：任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。	尚未判决	广东省东莞市	尚未判决	科技	2019年9月，东莞市公安局网警支队民警通过侦查发现，东莞市某科技公司开发的网络服务器管理软件系统以及全国使用该系统的2400多台服务器被非法入侵、控制。办案民警经侦查发现，犯罪嫌疑人陈某通过编写脚本木马攻击目标网站，取得服务器的管理员控制权。在广东省公安厅网警总队的统筹部署下。 9月25日，东莞网警联合南城分局，在深圳市某小区抓获犯罪嫌疑人陈某。经审讯，陈某对其非法控制计算机信息系统和侵犯公民个人信息的犯罪事实供认不讳。公安机关经过侦查发现，陈某利用部分网站“弱口令”等系统管理漏洞，通过系列犯罪手段，在互联网上非法入侵过20个网上贷款网站平台，从中非法获取网络公民个人信息约70万条，并通过“暗网”某论坛发帖贩卖，非法营利12000元人民币。[77]	

76. 详见“常州警方破获特大侵犯公民个人信息案”，https://mp.weixin.qq.com/s/JmnwrWA584LNpx8qzSA3fw，访问时间：2019年12月13日。
77.详见“广西壮族自治区信息安全测评中心网络安全事件周报”，https://mp.weixin.qq.com/s/W4aD57SYiLLAyC9tcwr31Q，访问时间：2019年12月13日。

第二部分

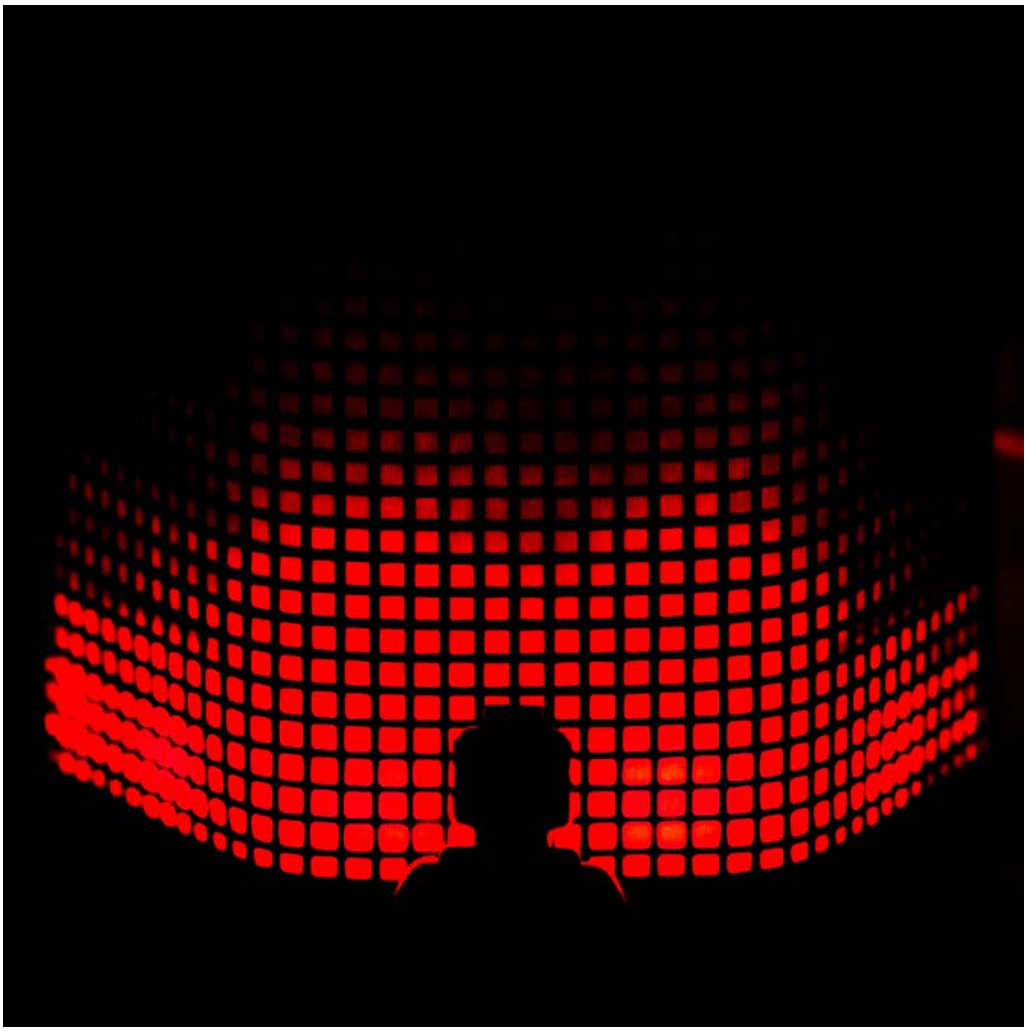
2

回顾：网络安全与数据保护合规制度专题解析

CHAPTER ONE

《中华人民共和国密码法》解析[78]

78.原文标题为《密码法的“放管”之道》，作者陈际红、陈璇、罗芸，网址：http://www.zhonglun.com/Content/2019/11-05/1631342516.html。



2019年10月26日，第十三届全国人民代表大会常务委员会第十四次会议审议通过并公布了《中华人民共和国密码法》（以下简称“《密码法》”），该法将于2020年1月1日起施行。在此之前，密码管理领域位阶较高的法律渊源可以追溯至国务院于1999年10月发布的《商用密码管理条例》（以下简称“《条例》”）。此后，国家密码管理局和全国人大常委会分别于2017年4月和2019年7月5日发布了《中华人民共和国密码法（草案征求意见稿）》及《中华人民共和国密码法（草案）》（以下简称“《密码法（草案）》”）。基于《密码法（草案）》基础上完善并颁布的《密码法》，填补了我国密码领域长期存在的法律空白，是迄今我国在密码管理领域的第一部综合性法律。

SECTION 01

适用对象：从“商用密码”到“密码”；从“技术和产品”到“技术、产品和服务”

条文对比		
《商用密码管理条例》（1999年10月7日生效）	《密码法（草案）》（2019年7月5日发布）	《密码法》（2020年1月1日生效）
商用密码，对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。（第2条）（1999年10月7日生效）	**密码**的科研、生产、经营、进出口、检测、认证、使用和监督管理等活动。（第2条） **密码**，是指使用特定变换对数据等信息进行加密保护或者安全认证的**产品、技术和服务**。（第3条）	**密码**，是指采用特定变换的方法对信息等进行加密保护、安全认证的**技术、产品和服务**。（第2条）

《条例》由于受时代背景的限制，监管范围主要为密码产品。随着信息技术的发展以及日趋明显的行业分工，多种多样的密码技术、密码产品和密码服务层出不穷，《密码法》适用和监管的对象从“商用密码”到“密码”，且不再仅仅局限于密码产品和密码技术，而延伸至密码服务。

需要指出的是，《密码法》中的密码与我们日常生活中所提及的“密码”并不完全等同，生活中经常接触到的“密码”只是进入个人设备或软件的口令或“通行证”，是一种初级的身份认证手段。而《密码法》中的密码的功能体现在对信息的“加密保护”和“安全认证”，且系通过采用特定变换的方法来实现。

SECTION 02

密码的分类：密码分类及用途

条文对比		
《商用密码管理条例》（1999年10月7日生效）	《密码法（草案）》（2019年7月5日发布）	《密码法》（2020年1月1日生效）
商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理。（第3条）	密码分为**核心密码、普通密码和商用密码**。国家对密码实行**分类管理**。（第6条） **核心密码、普通密码用于保护国家秘密信息**，核心密码保护信息的最高密级为绝密	国家对密码实行**分类管理**。密码分为**核心密码、普通密码和商用密码**。（第6条） **核心密码、普通密码用于保护国家秘密信息**，核心密码保护信息的最高密级为绝密

条文对比		
《商用密码管理条例》（1999年10月7日生效）	《密码法（草案）》（2019年7月5日发布）	《密码法》（2020年1月1日生效）
	级，普通密码保护信息的最高密级为机密级。**核心密码、普通密码属于国家秘密。**密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码的科研、生产、检测、装备、使用和销毁等实行严格统一管理。（第7条）**商用密码用于保护不属于国家秘密的信息。**公民、法人和其他组织均可依法使用商用密码保护网络与信息安全。（第8条）（第10条）	级，普通密码保护信息的最高密级为机密级。**核心密码、普通密码属于国家秘密。**密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。（第7条）**商用密码用于保护不属于国家秘密的信息。**公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。（第8条）

在信息化和数字化高速发展的今天，密码的应用已经渗透到国民经济和社会生活的方方面面，甚至日益成为维护国家网络空间主权、安全和发展利益的保障和战略性资源。由于不同密码所保护的对象不同，为充分发挥不同密码在保护网络和信息安全中的核心支撑作用，《密码法》中对密码实行分类管理，明确了密码的分类层级，按照要保护信息的密级重要性排列依次为：核心密码、普通密码和商用密码，并对各自的管理和使用分别进行专章规定，使得立法体例和法律适用更加清晰科学。

尽管商用密码在《条例》中被认定为国家秘密，但《密码法》明确规定，核心密码、普通密码属于国家秘密，商用密码用于保护不属于国家秘密的信息，不属于国家秘密。

核心密码保护信息的最高密级为绝密级，因此核心密码可以用于保护国家绝密级、机密级、秘密级信息；普通密码保护信息的最高密级为机密级，因此普通密码可以用于保护机密级、秘密级信息；商用密码用于保护不属于国家密码的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

SECTION 03

密码活动的监管：《密码法》的“放”与“管”

（一）《密码法》之“放“：

条文对比		
《商用密码管理条例》（1999年10月7日生效）	**《密码法（草案）》（2019年7月5日发布）**	**《密码法》（2020年1月1日生效）**
商用密码技术属于国家秘密。**国家对商用密码**产品的科研、生产、销售和使用**实行专控管理**。（第3条） 商用密码的**科研**任务由国家密码管理机构**指定的单位承担**。商用密码指定科研单位必须具有相应的技术力量和设备，能够采用先进的编码理论和技术，编制的商用密码算法具有较高的保密强度和抗攻击能力。（第5条） 商用密码产品由国家密码管理机构指定的单位生产。**未经指定，任何单位或者个人不得生产商用密码产品**。商用密码产品指定生产单位必须具有与生产商用密码产品相适应的技术力量以及确保商用密码产品质量的设备、生产工艺和质量保证体系。（第7条） 商用密码产品由国家密码管理机构许可的单位**销售**。**未经许可，任何单位或者个人不得销售**商用密码产品。（第10条） 任何单位或者个人只能**使用**经国家密码管理机构认可的商用密码产品，**不得使用自行研制的或者境外生产**的密码产品。（第14条）	核心密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定对**核心密码、普通密码的科研、生产、检测、装备、使用和销毁**等实行严格统一管理。（第7条） 公民、法人和其他组织均可**依法使用商用密码**保护网络与信息安全。（第8条） 国家鼓励商用密码技术的研究开发和应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。（第21条）	核心密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定**对核心密码、普通密码实行严格统一管理**。（第7条） 公民、法人和其他组织**可以依法使用商用密码保护网络与信息安全**。（第8条） 国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。（第21条）

为了加强商用密码管理，保护信息安全，《条例》对商用密码的科研、生产、销售、使用、安全和保密管理进行了全方位的严格管理。然而，《条例》及其配套规定对密码产品各环节的严格审批要求已经不能适应密码技术和应用的需要，为了贯彻落实“放管服”的改革要求，在《密码法》颁布之前，我国已逐步放宽了商用密码的市场准入，削减密码管理领域的行政许可数量。具体表现为：

2017年9月29日，国务院发布《关于取消一批行政许可事项的决定》（国发〔2017〕46号），取消了国家密码管理局负责实施的商用密码产品生产单位审批、商用密码产品销售单位许可、外商投资企业使用境外密码产品审批、境外组织和个人在华使用密码产品或者含有密码技术的设备审批4项行政许可事项。

2017年12月1日，国家密码管理局发布《关于废止和修改部分管理规定的决定》（“第32号公告”），对《商用密码产品销售管理规定》、《商用密码产品使用管理规定》和《境外组织和个人在华使用密码产品管理办法》三部管理规定予以废止，对《商用密码科研管理规定》、《商用密码产品生产管理规定》和《电子认证服务密码管理办法》三部管理规定的部分条款予以修订。

《密码法》的发布标志着从立法层面正式取消了国家密码管理局负责实施的商用密码产品生产单位审批、商用密码产品销售单位许可、外商投资企业使用境外密码产品审批、境外组织和个人在华使用密码产品或者含有密码技术的设备审批。

然而，应当注意到，取消上述行政审批并不意味着国家对于密码应用的完全放开，而是释放出监管重点正在从“管企业”向“管产品”转变的信号：

根据国家密码管理局于2017年10月11日发布的《关于做好商用密码产品生产单位审批等4项行政许可取消后相关管理政策衔接工作的通知》（国密局字〔2017〕336号，“336号通知”），生产、销售的商用密码产品仍应当依法办理《商用密码产品型号证书》，并且对商用密码产品销售企业继续实施商用密码产品销售登记备案制度。商用密码产品型号证书制度在《密码法》生效后是否会保留并继续实行，还具有一定的不确定性，仍有待法律实施中进行观察。

此外，外商投资企业、境外组织和个人使用的密码产品或者含有密码技术的设备需要从境外进口的，仍应当依法办理《密码产品和含有密码技术的设备进口许可证》[79]，且进口商应当在进口密码产品时披露进口密码产品的最终用户和最终用途[80]。

（二）《密码法》之“管”：

不难看出，上述商用密码监管实践体现了监管部门对于密码的管理方式从重事前审批转化为侧重于事中事后监管，与此同时监管部门还通过如下制度设计实

79. 密码局、海关总署于2013年12月31日联合发布《关于调整〈密码产品和含有密码技术的设备进口管理目录〉的公告》（“国家密码管理局、海关总署联合公告2013年第27号”），该公告公布了《密码产品和含有密码技术的设备进口管理目录》。鉴于列入该目录的产品必须办理《进口许可证》，因此，可以理解为目录中的产品属于密码产品和含有加密技术的设备。

80. 根据336号通知附件3《取消“外商投资企业使用境外密码产品审批”后的事中事后监管措施》的规定，在取消“外商投资企业使用境外密码产品审批”行政许可事项后，将采取措施加强事中事后监管：“一、在密码产品进口许可审批中强化对进口密码产品最终用户的和最终用途的审核。完善密码产品进口许可审批流程和相关文本，加强对进口密码产品最终用户和最终用途登记审核与分类管理。二、加大对取得密码产品进口许可证的单位“双随机”抽查力度。全面落实“双随机一公开”制度，完善对取得密码产品进口许可证的单位抽查的内容和方式，加强对进口密码产品最终用户和最终用途的审查，适时向社会公布抽查情况和抽查结果，对抽查中发现的问题提出整改要求，并对整改情况进行核查。……”

现多维度的“管”，体现了不偏废“放”或“管” 的监管态度，确保“放”与“管“”两个轮子一起转。

1.进出口管制清单制度

条文对比

《商用密码管理条例》（1999年10月7日生效）	《密码法（草案）》（2019年7月5日发布）	《密码法》（2020年1月1日生效）
进口密码产品以及含有密码技术的设备或者出口商用密码产品，必须报经国家密码管理机构批准。任何单位或者个人不得销售境外的密码产品。（第13条）	国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。商用密码进口许可和出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。 大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。（第28条）	国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。商用密码进口许可清单和出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。 大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。（第28条）

根据国际通行做法，商务部和国家密码管理局对于商用密码进出口实行清单管理制度，即对涉及国家安全、社会公共利益且具有加密保护功能的商用密码等实施进口许可、出口管制清单制度，此举对于防止利用商用密码从事违法犯罪活动具有重要意义。

2.商用密码产品和服务的检测、认证制度

条文对比

《商用密码管理条例》（1999年10月7日生效）	《密码法（草案）》（2019年7月5日发布）	《密码法》（2020年1月1日生效）
国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范和规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。 商用密码检测、认证机构应当依法取得相关资质，并依照法律、行政法规的规定和商用密码检测认证技术规范和规则开展商用密码检测认证。（第25条） 涉及国家安全、国计民生、社会公共利益的商用密码产品列入网络关键设备和网络安全专用产品目录，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。 用于网络关键设备和网络安全专用产品的商用密码服务，应当由商用密码认证、检测机构安全认证合格或者安全检测符合要求后，方可提供。（第26条）	国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。商用密码检测、认证机构应当依法取得相关资质，并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证。商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。（第25条） 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。（第26条）	网络关键设备和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23条）

根据《密码法》的规定，用于网络关键设备和网络安全专用产品的商用密码服务实行强制检测、认证制度；其他商用密码从业单位实行自愿检测、认证制度。商用密码产品检测认证适用《中华人民共和国网络安全法》（以下简称“《网络安全法》”）的有关规定，体现了与《网络安全法》的衔接和协调。

条文对比			
《密码法（草案）》（2019年7月5日发布）	《密码法》（2020年1月1日生效）	《网络安全审查办法（征求意见稿）》（2019年5月21日）	《关键信息基础设施安全保护条例（征求意见稿）》（2019年7月10日）
法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，开展商用密码应用安全性评估。 关键信息基础设施的运营者和国家机关采购、使用涉及商用密码的网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。(第27条)	法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。(第27条)	运营者采购网络产品和服务时，应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告。可能导致以下情况的，应当向网络安全审查办公室申报网络安全审查： (一) 关键信息基础设施整体停止运转或主要功能不能正常运行； (二) 大量个人信息和重要数据泄露、丢失、毁损或出境； (三) 关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁； (四) 其他严重危害关键信息基础设施安全的风险隐患。(第6条)	存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。 关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。(第53条)

由于仅对涉及国家安全、国际民生、社会公共利益的商用密码产品以及使用网络关键设备和网络安全专用产品的商用密码服务实行强制检测、认证制度，且实践当中主管部门会通过发布并适时更新《网络关键设备和网络安全专用产品目录》来界定管理范围，因此既可以较好地实现标准化和检测、认证的支撑作用，也可以一定程度上平衡密码产业发展。

3.关键信息基础设施运营者的商用密码应用安全性评估和国家安全审查

《密码法》对涉及国家安全、国计民生、社会公共利益，列入网络关键设备和网络安全专用产品目录的产品以及关键信息基础设施运营者（以下称“CIIO“）采购产品和服务，规定了相应的管制措施，体现了职能转变和“放管服”要求与保障国家安全的平衡。从相关《密码法》的条文中不难看出其与《网络安全法》、《关键信息基础设施安全保护条例（征求意见稿）》及《网络安全审查办法（征求意见稿》等配套法规均有衔接。除此之外，《密码法》还与《网络安全等级保护条例（征求意见稿）》的相关规定呼应，例如，第三级以上网络应当采用国家密码管理部门认可的密码技术、产品和服务，必须委托密码应用安全性测评机构开展密码应用安全性评估，且应将评估结果报相关主管部门备案。

SECTION 04

外资利好：外资的市场参与平等地位的确立

条文对比	
《密码法》（2020年1月1日生效）	
各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位。国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。（第21条）	国家鼓励在外商投资过程中基于自愿原则和商业规则开展技术合作。技术合作的条件由投资各方遵循公平原则平等协商确定。行政机关及其工作人员不得利用行政手段强制转让技术。（第22条）

81. 商用密码产品型号证书制度在《密码法》生效后是否会保留并继续实行，还具有一定的不确定性，仍有待法律实施中进行观察。。

《条例》于1999年颁布以来，国家密码管理机构曾经限制外资企业获得商用密码产品生产资格和商用密码产品销售资格，所以至今只有极少数的外资企业获得了相应证书。此次《密码法》的颁布，明确规定了对于从事商用密码研究、生产、销售、服务、进出口的外商投资企业应当依法平等对待。自2017年国家密码管理局取消大部分行政审批至《密码法》对相关市场的进一步放开，外商投资企业在国内已经获取与中资企业一样的待遇，意味着：

外资企业可以在中国生产、销售、使用境内商用密码产品，前提是已经就该密码产品取得有效的《商用密码产品型号证书》[81]。

外资企业可以通过规定的流程就符合条件的密码产品申请《商用密码产品型号证书》。

对于进口境外密码产品以及含有密码技术的设备，仍然需要取得《密码产品和含有密码技术的设备进口许可证》。

此外，作为对外国投资者就强制技术转让问题的担忧的回应，《密码法》专门规定禁止强制商用密码技术转让，该规定是今年3月较早发布的《中华人民共和国外商投资法》中禁止强制技术转让规定在密码管理领域的体现，有利于保护外国投资者的权益以及激发外商投资企业的投资热情。

总体而言，《密码法》的颁布有利于外资企业公平地进入市场竞争，外国投资者可以充分利用此番红利，找到自身的价值定位，与中国企业积极开展商用密码技术合作，共同开拓相关市场。

结语

《密码法》作为密码管理领域的首部基础性法律，其出台可以有效提升密码管理的科学性和规范化，也将有力地促进密码技术进步、产业发展和规范应用，可以预计密码产业的蓬勃发展将给企业带来新的发展机遇。

CHAPTER TWO

网络安全实施规范解读

《网络安全法》颁布之后，为了落实相关基本法律要求，国家网信办、工信部、国家市场监督管理总局、国家标准化管理委员会等部门相继发布了实施《网络安全法》的规范性文件，针对实践中的问题提出了具体指导标准，在法规层面上明确网络运营者的合规要求和主管部门的监管态度，对企业的网络安全合规具有重要意义。

第一节 《网络安全审查办法（征求意见稿）》解读[82]

82.原文标题为《国家安全更聚焦|<网络安全审查办法（征求意见稿）>出新招》，作者陈际红、吴佳蔚、刘洋，网址：http://www.zhonglun.com/Content/2019/06-10/1034293236.html。

2019年5月24日0时，国家互联网信息办公室（“国家网信办”）会同国家发展和改革委员会等12部局联合起草并发布《网络安全审查办法（征求意见稿）》（“新《审查办法》”），并随即发布了英文版。相较于2017年国家网信办发布的《网络产品和服务安全审查办法（试行）》（“原《审查办法》”），新《审查办法》在适用范围、适用原则、审查内容和审查程序等诸多方面均有较大幅度的变更。因此，新《审查办法》并没有在原《审查办法》办法上做修补性质的修改，而是另起炉灶，由国家网信办会同国家发展和改革委员会等12部局联合发布。

SECTION 01

更加聚焦国家安全

网络安全审查制度法律基础来源于《国家安全法》第五十九条，国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的网络信息技术产品和服务得以进行国家安全审查；以及，来源于《网络安全法》第三十五条，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。因此，网络安全审查制度的立法目标应当锁定于维护国家安全。相较于原《审查办法》，新《审查办法》立法价值更加聚焦于国家安全，而非保护企业和用户的合法权益，例如：

新《审查办法》明确适用于“关键信息基础设施运营者采购网络产品和服务”的活动，而一般不会延伸至一般的网络运营者。

把数据安全界定为“大量个人信息和重要数据泄露、丢失、毁损或出境”，而非“非法收集、存储、处理、使用用户相关信息的风险”。

删除了“产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险”的内容。

在《网络安全法》的体系下，为保障网络产品和服务安全，除了网络安全审查制度外，还有“网络关键设备和网络安全专用产品安全认证和安全检测”制度。 两个制度体系的立法目标不一，涵盖重点不同，后者可以看成是一个广泛适用的网络产品安全制度，前者是一个保障国家安全的、增强性的网络产品安全制度。

SECTION 02

设定CIIO为安全审查的主要抓手

原《审查办法》规定，网络产品和服务提供者应当对网络安全审查工作予以配合，并对提供材料的真实性负责。因此，可以理解，原审查制度中审查机构面对的向对方主要是“网络产品和服务提供者”，但关于网络安全审查的申报责任和配合义务等问题却规定的不甚清晰。

而在新《审查办法》中，设定关键信息基础设施运营者（Critical Information Infrastructure Operator，**“CIIO”**）为整个审查流程的抓手，CIIO要承担如下责任：

应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告；

通过契约或其他方式要求产品和服务提供者配合网络安全审查，采购合同应约定在网络安全审查通过后方可生效；

向网络安全审查办公室申报网络安全审查；

进入特别审查程序需要提供补充材料的，予以配合；

加强安全管理，督促网络产品和服务提供者认真履行网络安全审查中作出的承诺；

当然，违法责任的板子也会打在CIIO身上，CIIO“违反本办法规定的，依照《中华人民共和国网络安全法》第六十五条的规定处理”。

SECTION 03

安全审查的内容更加丰富

原《审查办法》实施近两年，有实施中的经验和问题要总结，更为重要的是，在此期间，国际环境发生了重要变化，国家安全的内涵也进一步的在演进，政治、外交、贸易等非技术因素导致产品和服务供应中断的可能性增强。

新《审查办法》下，安全审查程序中有两个环节，一是CIIO自行判断是否应向网络安全审查办公室申报网络安全审查；二是网络安全审查主管机构评估采购活动可能带来的国家安全风险。相对于CIIO的自查环节，网络安全审查主管机构评估侧重于国家安全风险，更多考虑产品和服务受到非技术因素而供应中断的可能性，产品和服务提供者受外国政府资助、控制等的情况，具体如下：

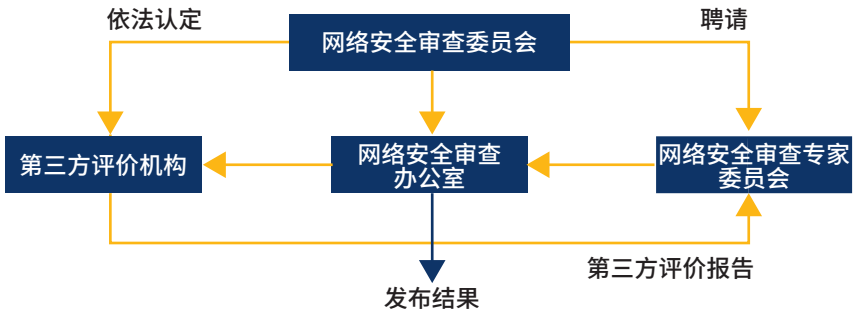
运营者申报网络安全审查考虑因素	网络安全审查主管机构评估国家安全风险考虑因素	评析
关键信息基础设施整体停止运转或主要功能不能正常运行； 关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁；	对关键信息基础设施持续安全稳定运行的影响，包括关键信息基础设施被控制、被干扰和业务连续性被损害的可能性； 产品和服务的可控性、透明性以及供应链安全，包括因为政治、外交、贸易等非技术因素导致产品和服务供应中断的可能性； 对国防军工、关键信息基础设施相关技术和产业的影响； 产品和服务提供者遵守国家法律与行政法规情况，以及承诺承担的责任和义务； 产品和服务提供者受外国政府资助、控制等情况；	美国《确保信息通信技术与服务供应链安全》行政令第一条（a）款规定“交易涉及由外国对手拥有的、控制或受其管辖或指导的人设计、开发、制造或供应的信息和通信技术或服务”，因此“产品和服务提供者受外国政府资助、控制等情况”一定程度上是对上述规定的回应，体现了ICT供应链安全对于国家安全的重要意义83。
大量个人信息和重要数据泄露、丢失、毁损或出境；	导致大量个人信息和重要数据泄露、丢失、毁损、出境等的可能性；	
其他严重危害关键信息基础设施安全的风险隐患。	其他可能危害关键信息基础设施安全和国家安全的因素。	

83. ICT供应链安全可以参照信安标委颁布的《信息安全技术 ICT供应链安全风险管理指南》（征求意见稿）予以评估。

SECTION 04

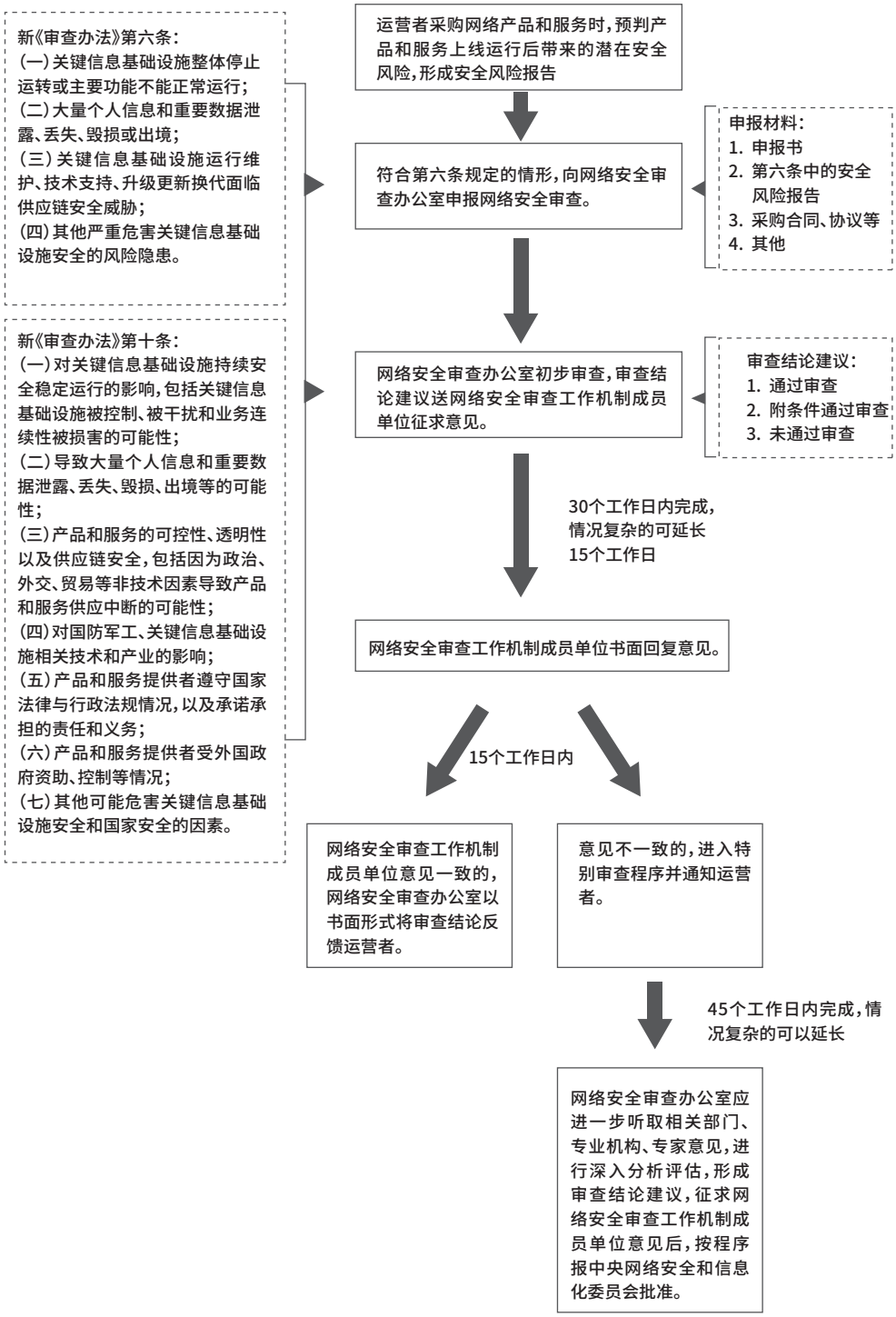
审查程序更清晰

对原《审查办法》诟病比较多的问题之一，就是审查中的程序规定和时限规定不清晰。原来的网络安全审查框架基本如下：



新《审查办法》下，中央网络安全和信息化委员会统一领导网络安全审查工作，国家网信办等12个部局组成国家网络安全审查工作机制单位。同时，在国家网

信办设立网络安全审查办公室，负责组织制定网络安全审查相关制度规定和工作程序、组织网络安全审查、监督审查决定的实施，具体如下：



结语

首先，关于网络安全审查行为的定性。其是否构成具体行政行为？是否赋予相对方司法救济的权利？按照行政法的基本原则，有具体行政行为就应该有救济程序，包括行政复议渠道和司法救济渠道。但是，关于国家安全审查行为，从目前世界范围内的立法实践来看，有直接将国家安全审查排除在司法审查范围之外的实践，也有将其视为正常的行政行为并按照国内法赋予相对方司法救济权的实践。而最近通过的《中华人民共和国外商投资法》第三十五条规定，国家针对外商投资进行安全审查的安全审查决定为最终决定。参照外商投资法的立法思路，我们倾向于认为网络安全审查行为不具有司法救济的渠道。

其次，关于重要数据的定义和范围。按照审查办法的规定，“大量重要数据泄露、丢失、毁损或出境”是审查的一个因素。而目前关于重要数据的具体定义和范围大小，仍存在不小的争议。从维护国家安全的立法目的上看，重要数据不应该泛化为一般的商业性数据，而应聚焦在和国家安全息息相关的数据范围之内，这样的监管才符合立法的本意。

最后，为了进一步降低企业网络安全和风险，建议相关企业开展整体的网络安全合规工作，包括网络产品和服务采购制度、等级保护及网络安全制度建设、个人信息和重要数据制度建设等。

第二节 《网络安全漏洞管理规定》解读[84]

2019年6月18日，工业和信息化部发布《公开征求对<网络安全漏洞管理规定（征求意见稿）>的意见》（以下简称“《意见》”），旨在加强网络安全漏洞管理。值得强调的是，《意见》指出《网络安全漏洞管理规定（征求意见稿）》（以下简称“《漏洞管理规定（征求意见稿）》”、“本规定”）拟以规范性文件形式发布，明确了其法律位阶。《漏洞管理规定（征求意见稿）》全文共十二条，系统地规范了网络产品、服务、系统的网络安全漏洞验证、修补、防范、报告和信息发布等行为。比较明显的是，本规定依然蕴含事件导向性立法的意味，背后的纠纷事件值得关注和探讨。

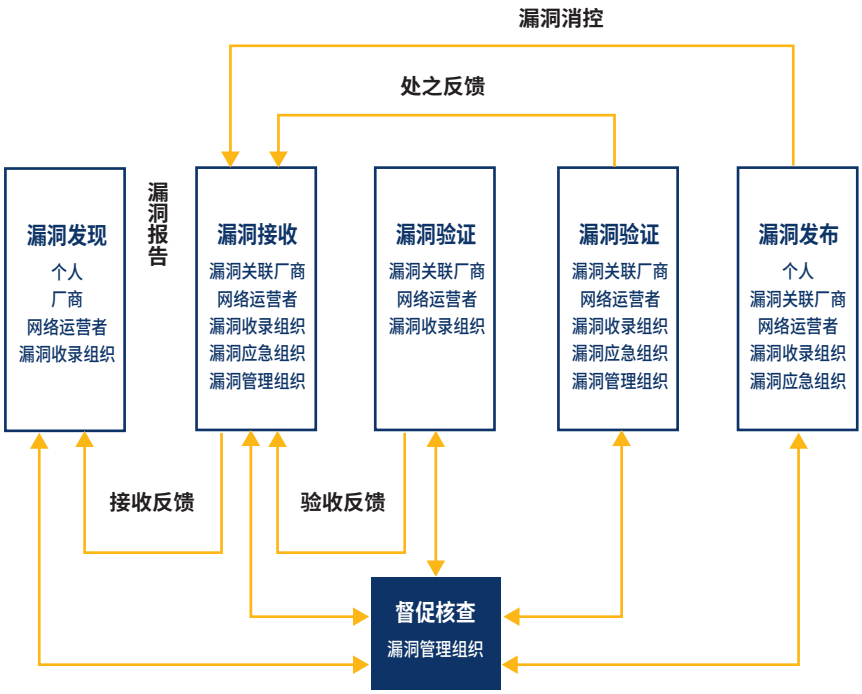
84.原文标题为《敲黑板！<网络安全漏洞管理规定>逐条解读》，作者刘新宇、宋海新、张功俐，网址：http://www.zhonglun.com/content/2019/06-19/1711082330.html。

SECTION 01

重点速览

（一）明确不同主体发现或发布网络安全漏洞应采取的不同措施

根据《信息安全技术网络安全漏洞管理规范（征求意见稿）》（以下简称“《漏洞管理规范（征求意见稿）》”），网络安全漏洞全生命周期的管理包括漏洞发现、漏洞接收、漏洞验证、漏洞处置、漏洞发布等多个环节。具体如下图所示（来源：《漏洞管理规范（征求意见稿）》）：



漏洞生命周期管理流程

从内容上看，《漏洞管理规定（征求意见稿）》根据主体身份的不同，重点规定了各主体从漏洞接收到漏洞发布之间各个环节应采取的主要措施，但是并未就漏洞发现本身涉及的问题进行详细规范。

1、网络产品、服务提供者和网络运营者发现和发布网络安全漏洞的要求

主体	网络产品、服务提供者和网络运营者
适用情形	发现或获知其网络产品、服务、系统存在漏洞
相关措施	立即对漏洞进行验证 在**规定的期限**内采取漏洞修补或防范措施 （1）网络产品应在90日内 （2）网络服务或系统应在10日 （如有需要）在**规定的期限**内告知用户或相关技术合作方**相关漏洞风险及其需要采取的漏洞修补或防范措施**，并向工业和信息化部网络安全威胁信息共享平台**报送相关漏洞情况** （1）采取漏洞修补或防范措施后5日内 （2）告知的方式：向社会发布；通过客服等方式

2、第三方组织或个人向社会发布网络安全漏洞信息的要求

主体	第三方组织或个人（包括漏洞收集平台在内）
适用情形	通过网站、媒体、会议等方式向社会发布漏洞信息
相关措施	**原则：**必要、真实、客观、有利于防范和应对网络安全风险 **强调“三不得”+“一同步”** **1.“三不得”：** **一不得在“官宣”前抢先向社会发布，**即不得在网络产品、服务提供者和网络运营者向社会或用户发布漏洞修补或防范措施之前发布相关漏洞信息； **二不得夸大影响，营造恐慌气氛，**即不得刻意夸大漏洞的危害和风险； **三不得提供乘人之危的方法、程序和工具，**即不得发布和提供专门用于利用网络产品、服务、系统漏洞从事危害网络安全活动的方法、程序和工具。 **2.“一同步”：** 应当在发布漏洞信息时同步发布漏洞修补或防范措施。 **内控管理职责——防范漏洞泄露和内部人员违规发布漏洞信息。** 明确漏洞管理部门和责任人； 建立漏洞信息发布内部审核机制； 采取防范漏洞信息泄露的必要措施； 定期对内部人员进行保密教育； 制定内部问责制度。

（二）明确不同主体违反本规定要求应承担的法律责任

《漏洞管理规定（征求意见稿）》第八条和第九条分别规定了网络产品、服务提供者和网络运营者，以及第三方组织违反本规定要求应承担的相应法律责任。

主体	情形	法律责任
网络产品、服务提供者和网络运营者	未按《漏洞管理规定（征求意见稿）》规定采取漏洞修补或防范措施并向社会或用户发布的	由工业和信息化部、公安部等有关部门按职责组织对其进行约谈； 给予行政处罚，如给予警告，处以罚款等 （处罚依据：《网络安全法》第五十六条、第五十九条和第六十条等）
第三方组织	违反《漏洞管理规定（征求意见稿）》规定向社会发布漏洞信息	由工业和信息化部、公安部等有关部门组织对其进行约谈； 给予行政处罚，如给予警告，处以罚款，责令暂停相关业务，停业整顿，关闭网站，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以罚款等； 构成犯罪的，依法追究刑事责任； 给网络产品、服务提供者和网络运营者造成经济或名誉损害的，依法承担民事责任。 （处罚依据：《网络安全法》第六十二条和第六十三条等）

（三）鼓励第三方组织和个人向漏洞收集平台报送漏洞有关情况

根据《漏洞管理规定（征求意见稿）》第十条的相关规定，监管部门鼓励第三方组织和个人及时向漏洞收集平台报送获知网络产品、服务、系统存在的漏洞情况。不同于网络产品、服务提供者和网络运营者应向网络安全威胁信息共享平台报送相关漏洞情况，第三方组织和个人报送漏洞信息主要通过漏洞收集平台，如国家信息安全漏洞共享平台和国家信息安全漏洞库。其中国家信息安全漏洞共享平台设置了《CNVD原创漏洞积分评分细则》和积分兑换等白帽子积分奖励计划，用于进一步肯定漏洞报送者（白帽子）在防范漏洞安全风险的积极作用。

SECTION 02

逐条解读

第一条：为规范网络安全漏洞（以下简称“漏洞”）报告和信息发布等行为，保证网络产品、服务、系统的漏洞得到及时修补，提高网络安全防护水平，根据《国家安全法》《网络安全法》，制定本规定。

解读

本条明确了**《漏洞管理规定（征求意见稿）》的立法目的和立法依据。从立法目的看，两个细分目的和一个整体目的相结合。**

第一个细分目的，规范网络安全漏洞报告和信息发布等行为。报告的主体包括网络产品、服务提供者网络运营者和第三方组织或个人，报告的内容主要为网络安全漏洞相关情况，漏洞信息发布规制的主体主要为第三方组织或个人，发布规制的路径主要为通过网站、媒体、会议等方式向社会发布；

第二个细分目的，保证网络产品、服务、系统的漏洞得到及时修补。根据工业和信息化部网络安全管理局发布的《2018年第四季度网络安全威胁态势分析与工作综述》，网络安全漏洞仍然是网站和系统面临的主要安全威胁之一。其发现和获知且经验证后应采取的主要措施就在于修补，及时处置漏洞的威胁。

整体目的，提高网络安全防护水平，提高网络安全防护水平能够及时应对网络安全漏洞，有效防范网络安全漏洞被违法违规利用等带来的网络安全风险和威胁。

从立法依据看，本规定明确立法依据为《国家安全法》和《网络安全法》，上位法的重要性也突出了本规定的重要性。而且，将《国家安全法》明确作为上位法依据，更强调及时发现、有效处置网络安全漏洞对维护国家安全具有重要意义。关于《网络安全法》的具体条文依据，行为规则主要见于第二十二条第一款、第二十五条、第二十六条。

第二条：中华人民共和国境内网络产品、服务提供者和网络运营者，以及开展漏洞检测、评估、收集、发布及相关竞赛等活动的组织（以下简称“第三方组织”）或个人，应当遵守本规定。

本条明确了**《漏洞管理规定（征求意见稿）》的适用范围。**适用范围具体包括两个要点：

第一个要点，地域限制，中华人民共和国境内；

第二个要点，规制对象，网络产品、服务提供者和网络运营者，以及开展漏洞检测、评估、收集、发布及相关竞赛等活动的组织或个人，基本将网络安全漏洞发现、接收、验证、处置和发布的各类主体均纳入到规制范围。

第三条：网络产品、服务提供者和网络运营者发现或获知其网络产品、服务、系统存在漏洞后，应当遵守以下规定：

（一）立即对漏洞进行验证，对相关网络产品应当在90日内采取漏洞修补或防范措施，对相关网络服务或系统应当在10日内采取漏洞修补或防范措施；

（二）需要用户或相关技术合作方采取漏洞修补或防范措施的，应当在对相关网络产品、服务、系统采取漏洞修补或防范措施后5日内，将漏洞风险及用户或相关技术合作方需采取的修补或防范措施向社会发布或通过客服等方式告知所有

可能受影响的用户和相关技术合作方，提供必要的技术支持，并向工业和信息化部网络安全威胁信息共享平台报送相关漏洞情况。

解读

本条明确了**网络产品、服务提供者和网络运营者发现或获知存在网络安全漏洞时应采取的措施。**

本条的直接上位法条文依据为《网络安全法》第二十二条第一款，“……网络产品、服务的提供者……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。”具体措施包括对网络安全漏洞进行验证、修补或防范和漏洞相关情况的发布、告知和报送两项措施。

第一项措施，对网络安全漏洞进行验证、修补或防范。具体应采取两步操作：

第一步，验证，时间要求为立即，具体环节包括技术验证、确认和反馈，涉及的主体主要包括网络产品、服务提供者和网络运营者，如果涉及其他漏洞厂商和网络运营者，也应及时通知相关厂商和网络运营者共同进行验证；

第二步，修补或防范，根据网络安全漏洞的类型、来源和危险程度不同，具体措施主要包括发布补丁、升级版本、增加防火墙、新增安全策略、临时处置建议等。值得注意的是，这里对相关网络产品采取漏洞修补或防范的时间要求为90日内，相关网络服务或系统要求为10日内，其考虑因素包括硬件产品修补的复杂程度、产品召回、厂商实地查看耗时等。

第二项措施，漏洞相关情况的发布、告知和报送。具体包括两点操作：

第一点，漏洞相关情况的发布或告知。该点操作具体包括四个小点要求：

前提条件，即需要用户或相关技术合作方采取漏洞修补或防范措施，如不需要则不用进行该项操作。未决问题在于，如何判定是否需要？谁来判定？

首先，时间要求，对相关网络产品、服务、系统采取漏洞修补或防范措施后5日内。

其次，内容要求，漏洞风险及用户或相关技术合作方需采取的修补或防范措施。

再次，发布或告知对象及方式，向社会发布或通过客服等方式告知所有可能受影响的用户和相关技术合作方。

最后，技术支持要求，为用户和相关技术合作方提供必要的技术支持，如指导升级补丁、升级软件版本等；

第二点，漏洞相关情况的报送，具体包括两个要点：

首先，报送对象，工业和信息化部网络安全威胁信息共享平台（The Information Sharing Platform of Cyber Security Threat，英文简称“ISPCST”），负责统一

汇集、存储、分析、通报、发布网络安全威胁信息。制定相关接口规范，与相关单位网络安全监测平台实现对接。坚持科学认定、有效处置的原则，组织网络安全专业机构对威胁信息进行认定，通知相关单位及时处置网络安全隐患，消除网络安全风险。ISPCST平台面向电信主管部门、基础电信企业、互联网企业、网络安全企业、网络安全专业机构等用户，共同建立网络安全威胁信息上报、认定、处置、共享的管理体系，构建国家公共互联网网络安全威胁信息资源库，切实提升我国网络安全威胁监测与处置水平。其官方网址为http://cstis.org.cn/；

其次，报送内容，相关漏洞情况。具体报送内容需关注工业和信息化部网络安全威胁信息共享平台的报送要求，并建议关注正在制定的《信息安全技术　网络安全漏洞发现与报告管理指南》等相关国家、地区和行业标准。

第四条：工业和信息化部、公安部和有关行业主管部门按照各自职责组织督促网络产品、服务提供者和网络运营者采取漏洞修补或防范措施。

本条明确了**工信部、公安部和有关行业主管部门的职责要求。**

本条的直接上位法条文依据为《网络安全法》第八条第一款，“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。”具体到公安部的职责，《公安机关互联网安全监督检查规定》第十六条规定，“公安机关对互联网服务提供者和联网使用单位是否存在网络安全漏洞，可以开展远程检测。”

第五条：工业和信息化部、公安部、国家互联网信息办公室等有关部门实现漏洞信息实时共享。

本条明确了**网络安全漏洞信息实时共享的要求。**

有关部门实时共享网络安全漏洞信息，有利于构建网络安全漏洞信息资源库，切实提升我国网络安全威胁监测与处置水平。而且，网络安全漏洞信息实时共享，有助于未发现和获取网络安全漏洞信息的网络产品、服务提供者和网络运营者及时接收网络安全漏洞信息，采取修补或防范措施，避免漏洞的影响和损失的扩大。

第六条：第三方组织或个人通过网站、媒体、会议等方式向社会发布漏洞信息，应当遵循必要、真实、客观、有利于防范和应对网络安全风险的原则，并遵守以下规定：

（一）不得在网络产品、服务提供者和网络运营者向社会或用户发布漏洞修补

或防范措施之前发布相关漏洞信息；

（二）不得刻意夸大漏洞的危害和风险；

（三）不得发布和提供专门用于利用网络产品、服务、系统漏洞从事危害网络安全活动的方法、程序和工具；

（四）应当同步发布漏洞修补或防范措施。

本条明确了**第三方组织或个人发布网络安全漏洞信息的原则和要求。**

网络漏洞信息发布不当，可能会危害国家安全、社会安全、企业安全和用户安全。本条的直接上位法条文依据为《网络安全法》第二十六条，“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。”具体规制内容沿用了《漏洞管理规范（征求意见稿）》第5.5条的思路，包括网络安全漏洞发布对象、发布方式、发布的原则要求和发布的具体要求四点。

第一点，发布对象，第三方组织或个人，即开展漏洞检测、评估、收集、发布及相关竞赛等活动的组织和个人。

第二点，发布方式，通过网站、媒体、会议等方式向社会发布，主要指向公开发布的形式。

第三点，发布的原则要求，遵循必要、真实、客观、有利于防范和应对网络安全风险的原则。漏洞信息涉及的目标对象、风险情况描述等应真实客观，不得发布虚假、容易引起误解和恐慌和用于打击竞争对手等不正当竞争目的等的网络安全漏洞信息。

第四点，发布的具体要求，包括“三不得”和“一同步”。

“三不得”规范了发布时间、发布的真实客观性和发布内容，具体包括：

第一，发布时间要求，不得在网络产品、服务提供者和网络运营者向社会或用户发布漏洞修补或防范措施之前发布相关漏洞信息。该项要求与本规定第三条第二项相关联，参照了《中国互联网协会漏洞信息披露和处置自律公约》（以下简称**“《漏洞披露和处置自律公约》”**）第十一条适时披露原则的精神，但对具体时间节点进行了明确规定。需要探讨的点在于，该项似乎隐含如果该等漏洞信息无需用户或相关技术方采取漏洞修补或防范措施，网络产品、服务提供者和网络运营者可以不向社会或用户发布，由此也能限制第三方组织或个人向社会发布网络安全漏洞信息；

第二，发布的真实客观性要求，沿用了《漏洞管理规范（征求意见稿）》5.5.1b）条和《漏洞披露和处置自律公约》第十一条客观原则要求的思路，漏洞信息涉及的目标对象、风险情况描述等应真实客观，不得将漏洞潜在风险作为网络攻击事件进行发布和诱导，不得刻意夸大漏洞的危害和风险，避免引起媒体舆论和社会公

众的误读和恐慌；

第三，发布内容要求，沿用了《漏洞管理规范（征求意见稿）》5.5.1c)条的思路，旨在防止为相关漏洞被违法违规利用提供帮助的行为。需要进一步探讨的是，这里的“专门”的限定是否有必要?实践中有多大概率会专门发布从事危害网络安全活动的方法、程序和工具。

“一同步”，即同步发布漏洞修补或防范措施，意味着在网络产品、服务提供者和网络运营者发布漏洞修补或防范措施之外，漏洞发布者也需要发布漏洞修补或防范措施。未决问题在于，漏洞发布者发布的漏洞修补或防范措施是否可以与网络产品、服务提供者和网络运营者发布漏洞修补或防范措施保持一致?还是需要提出同等保护效果或者更有效的修补或防范措施?

第七条：第三方组织应当加强内部管理，履行下列管理义务，防范漏洞信息泄露和内部人员违规发布漏洞信息：

（一）明确漏洞管理部门和责任人；

（二）建立漏洞信息发布内部审核机制；

（三）采取防范漏洞信息泄露的必要措施；

（四）定期对内部人员进行保密教育；

（五）制定内部问责制度。

本条明确了**第三方组织加强内部管理防范漏洞信息泄露和内部人员违规发布漏洞信息的要求。**

与本规定第六条一致，本条的直接上位法条文依据依然为《网络安全法》第二十六条。具体来说，本条沿用了《漏洞管理规范（征求意见稿）》5.5.1d)条的思路，旨在加强内部管理，确保漏洞发布和扩散渠道可控可追溯。具体包括以下五项管理义务要求：负责部门和负责人，内部审核机制、采取防范泄漏的必要措施、内部人员定期保密教育、内部问责制度。

需要指出的是，如何对履行管理义务进行判定。对于第三方组织而言，需要落实而且需要做好留痕以备检查和免于承担责任或减轻责任承担的证明，如组织架构及具体负责人职责、审核机制的文本及执行环节的具体审批操作、采取措施的说明、保密教育的内容、频率和参与情况、内部问责制度文本等。

第八条：网络产品、服务提供者和网络运营者未按本规定采取漏洞修补或防范措施并向社会或用户发布的，由工业和信息化部、公安部等有关部门按职责依据《网络安全法》第五十六条、第五十九条、第六十条等规定组织对其进行约谈或给予行政处罚。

本条明确了**网络产品、服务提供者和网络运营者的违规责任承担。**

第一个要点，规制对象，网络产品、服务提供者和网络运营者。

第二个要点，违规情形，未按本规定采取漏洞修补或防范措施并向社会或用户发布的，这里具体指向本规定第三条。

第三个要点，监管部门，工业和信息化部、公安部等有关部门。

第四个要点，责任依据，《网络安全法》第五十六条、第五十九条、第六十条等规定。

第五个要点，具体责任形式，约谈或行政处罚。根据上述《网络安全法》规定，这里的行政处罚根据具体情形不同，主要包括警告、处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款或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等。

第九条：第三方组织违反本规定向社会发布漏洞信息，由工业和信息化部、公安部等有关部门组织对其进行约谈，或依据《网络安全法》第六十二条、第六十三条等规定给予行政处罚；构成犯罪的，依法追究刑事责任；给网络产品、服务提供者和网络运营者造成经济或名誉损害的，依法承担民事责任。

本条明确了**第三方组织违规发布网络安全漏洞信息的责任承担。**

第一个要点，规制对象，第三方组织。需要探讨的是，本规定第二条和第六条对于向社会发布网络安全漏洞信息的规制对象均为第三方组织和个人，此处并未将个人纳入违规发布信息的责任承担范围。

第二个要点，违规情形，违规向社会发布漏洞信息。

第三个要点，监管部门，工业和信息化部、公安部等有关部门。

第四个要点，责任依据，《网络安全法》第六十二条、第六十三条等规定。

第五个要点，责任形式，行政责任，包括约谈，或行政处罚。这里的行政处罚，根据情节不同，具体包括警告、处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、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五千元以上五万元以下罚款等；刑事责任，构成犯罪的，依法追究刑事责任；民事责任，给网络产品、服务提供者和网络运营者造成经济或名誉损害的，依法承担民事责任。可能涉及的民事责任承担形式，包括侵权、不正当竞争等。

第十条：鼓励第三方组织和个人获知网络产品、服务、系统存在的漏洞后，及时向国家信息安全漏洞共享平台、国家信息安全漏洞库等漏洞收集平

台报送有关情况。漏洞收集平台应当遵守本规定第六条、第七条规定。

本条明确了**监管部门对第三方组织和个人及时报送漏洞有关情况的鼓励态度和漏洞收集平台的规范要求。**

第一个要点，监管部门鼓励对第三方组织和个人及时报送漏洞有关情况的鼓励。这里的报送平台，包括国家信息安全漏洞共享平台、国家信息安全漏洞库等漏洞收集平台。

国家信息安全漏洞共享平台（China National Vulnerability Database，英文简称**“CNVD”**），是由国家计算机网络应急技术处理协调中心（中文简称**“国家互联应急中心”**，英文简称**“CNCERT”**）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。建立CNVD的主要目标即与国家政府部门、重要信息系统用户、运营商、主要安全厂商、软件厂商、科研机构、公共互联网用户等共同建立软件安全漏洞统一收集验证、预警发布及应急处置体系，切实提升我国在安全漏洞方面的整体研究水平和及时预防能力，进而提高我国信息系统及国产软件的安全性，带动国内相关安全产品的发展。CNVD在其官网发布了漏洞处理策略和《中国互联网协会漏洞信息披露和处置自律公约》。其官方网址为https://www.cnvd.org.cn/。

国家信息安全漏洞库（China National Vulnerability Database of Information Security ，英文简称"CNNVD"），于2009年10月18日正式成立，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，面向国家、行业和公众提供灵活多样的信息安全数据服务，为我国信息安全保障提供基础服务。其官方网址为http://www.cnnvd.org.cn/index.html。

第二个要点，漏洞收集平台的规范要求。国家信息安全漏洞共享平台、国家信息安全漏洞库等漏洞收集平台应当遵守本规定第六条、第七条规定，即向社会发布网络安全漏洞信息的要求和加强内部管理，防范漏洞信息泄露和内部人员违规发布漏洞信息的要求。

第十一条：任何组织或个人发现涉嫌违反本规定的情形，有权向工业和信息化部、公安部举报。

本条明确了**违反《漏洞管理规定（征求意见稿）》的举报要求。**

第一个要点，明确举报主体可以是任何组织或个人，意味着对举报主体没有设置限制，排除了举报主体不适格的障碍。

第二个要点，明确接受举报的部门为工业和信息化部和公安部。这里并未将网信办纳入接受举报的部门范围，需要进一步探讨。

值得注意的是，本条并未对举报人的信息保护进行说明。根据《网络安全法》

第十四条的规定，“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”，建议本规定项下亦应按照《网络安全法》的规定，对举报人的信息予以保密保护。

第十二条：本规定自印发之日起施行。

本条明确了《漏洞管理规定（征求意见稿）》正式生效的具体时间。考虑到目前本规定仅处于征求意见稿阶段，具体实施时间有待关注正式稿正式出台的时间。需要指出也需要重点关注的是，与此前网信办发布的系列文件不同，本规定的实施时间将与印发时间同步，未设置过渡期，需要提前做好相应合规准备。

结语

作为规范性文件，《网络安全漏洞管理规定（征求意见稿）》规定了网络产品、服务的提供者、网络运营者、第三方组织和个人验证、修补、防范和报告和信息发布等行为，有助于有效防范、及时处置和适当披露网络安全漏洞信息，有利于降低网络安全漏洞带来的网络安全风险和因不当发布网络安全漏洞信息带来的对国家安全、网络安全、企业安全和用户安全的不利影响。其一旦印发即开始执行，未设置过渡期，需要相关主体提前做好相应合规准备，避免正式稿出台后的措手不及。

85.原文标题为《等保2.0国家标准颁布，看十大“硬核”变化》，作者陈际红、韩璐、刘洋，网址：http://www.zhongluncom/Content/2019/05-27/1456463868.html。
86.《中华人民共和国计算机系统安全保护条例》第九条规定，“计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。”

第三节

“等级保护2.0国家标准”解读[85]

2019年5月13日，国家市场监督管理总局、国家标准化管理委员会发布的《信息安全技术　网络安全等级保护基本要求》（GB/T　22239-2019）（“《等保基本要求》”）、《信息安全技术　网络安全等级保护测评要求》（GB/T　28448-2019）、《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）三个网络安全领域的国家标准于2019年12月1日正式生效，共同构筑新时代的网络安全等级保护制度，标志着等保2.0的正式到来。

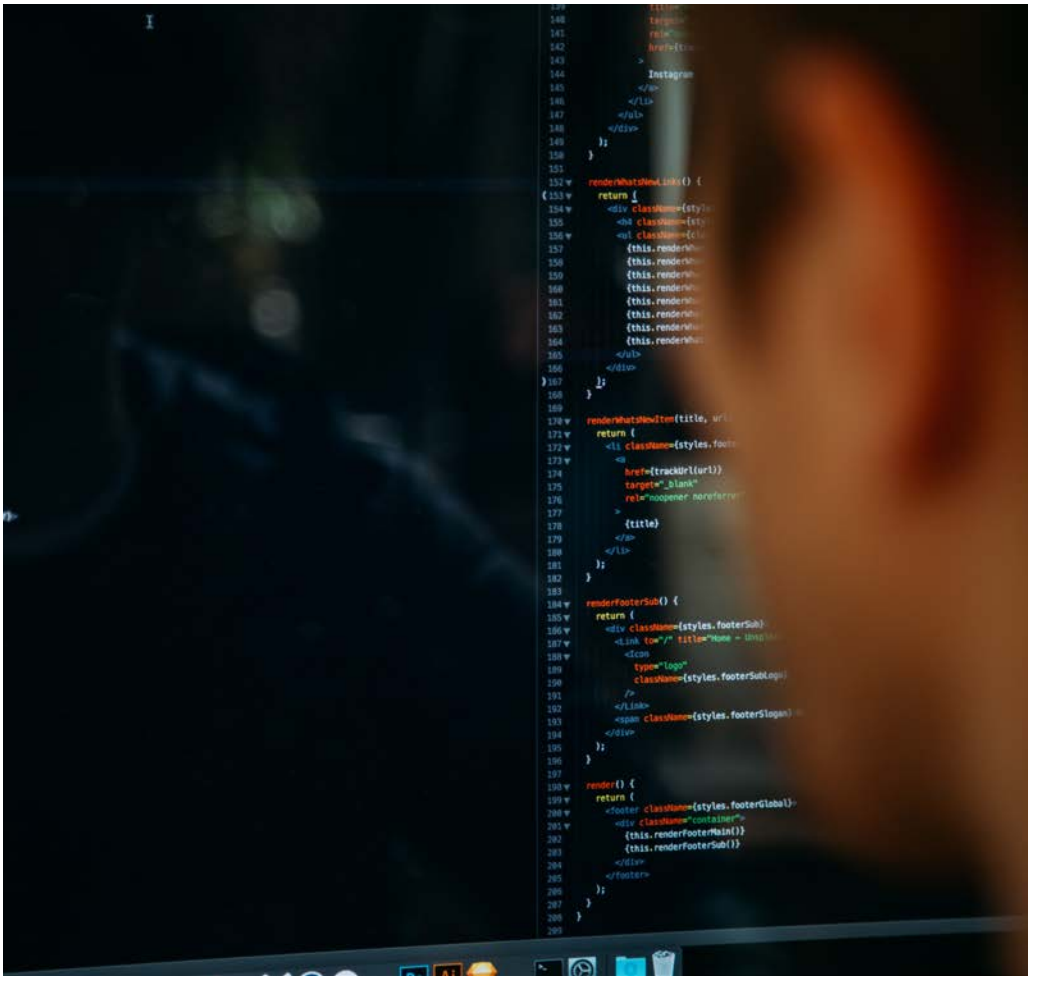
SECTION 01

等保1.0迈入等保2.0时代

等保1.0以1994年发布并于2011年修订的《中华人民共和国计算机系统安全保护条例》[86]为开端，广泛应用于各行业指导企业开展信息系统安全等级保护的建

设整改、等级测评等工作。2016年6月1日正式实施的《中华人民共和国网络安全法》规定“国家实行网络安全等级保护制度”[87]，明确了网络安全等级保护制度的法律地位，也拉开了等保2.0的序幕。相应地，2018年公安部发布《网络安全等级保护条例（征求意见稿）》，深入推进实施网络安全等级保护制度。而本次《等保基本要求》等三个国家标准的正式颁布，更是顺应当前加强网络安全的国家要求，结合云计算、移动互联、物联网、工业控制和大数据等新技术新应用开展综合治理、系统监管、主动防控的等保2.0时代。

87.《中华人民共和国网络安全法》第二十一条规定，“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）…（五）。”第三十一条规定，“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。”



网络安全等级保护制度法律框架

类别	等保1.0体系	等保2.0体系
法律	无	《中华人民共和国网络安全法》 《中华人民共和国保守国家秘密法》
行政法规	《中华人民共和国计算机信息系统安全保护条例》	《《网络安全等级保护条例（征求意见稿）》
部门规章	《信息安全等级保护管理办法》（公通字[2007]43号） 《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）	《《网络安全等级保护条例（征求意见稿）》
国家标准	《信息系统安全等级保护基本要求》（GB/T 22239-2008） 《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2008） 《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010） 《信息安全技术 信息系统安全等级保护测评准则》	《计算机信息系统安全保护等级划分准则（GB 17859-1999）(上位标准) 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058)（正在修订） 《信息安全技术 网络安全等级保护定级指南》(GB/T 22240)（正在修订） 《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019) 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019） 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019） 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018） 《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）

通过以上对比可知，现行网络安全等级保护体系（即等保2.0体系）相较等保1.0顶层设计与法律位阶均有所提升，顺应了“没有网络安全就没有国家安全”[88]的新时期新网络安全形势。

88.人民网：“习近平谈网络安全：没有网络安全就没有国家安全”，http://cpc.people.com.cn/xuexi/n1/2018/0817/c385476-30234135.html，2019年5月22日访问。

（一）等保对象及适用范围两个全覆盖

	等保1.0	等保2.0	评析
保护对象	信息系统	基础信息网络 云计算平台/系统 大数据应用/平台/资源 物联网（IoT） 工业控制系统 采用移动互联技术的系统	适应新技术的发展，将云计算、移动互联、物联网、工业控制系统等新兴技术和应用场景纳入了等级保护范围，构成“安全通用要求+新型应用安全扩展要求”，覆盖所有保护对象。
适用范围	/	各地区、各单位、各部门、各企业、各机构。	除个人及家庭自建自用的网络外，适用范围覆盖全社会。

（二）主动防控的管控思路

等保2.0仍遵循五个安全保护等级的划分，基本沿用等保1.0对不同级别的安全保护能力的描述，但在二级以上的安全保护能力的表述上，增加了对安全事件的处置；在三级以上的安全保护能力的表述上，增加对攻击行为的监测，均体现了等保2.0进行主动防控的特点。有可能被定级为二级或三级以上的网络运营者，应加强对安全事件的处置管理，开展对攻击行为的监测。

安全保护能力等级	等保1.0	等保2.0
第一级	应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在**系统**遭到损害后，能够恢复部分功能。	除将等保1.0中的“系统”替换为“自身”外，无变化： “在**自身**遭到损害后，能够恢复部分功能。”
第二级	应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾害、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在**系统**遭到损害后，能够在一段时间内恢复部分功能。	除将等保1.0中的“系统”替换为“自身”外，另增加“**处置**安全事件”的表述： “能够发现重要的安全漏洞和处置安全事件，在**自身**遭到损害后，能够在一段时间内恢复部分功能。”

安全保护能力等级	等保1.0	等保2.0
第三级	应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。	除将等保1.0中的“系统”替换为“自身”外，另增加“监测攻击行为和处置安全事件”的表述： “能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。”
第四级	应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。	除将等保1.0中的“系统”替换为“自身”外，另增加“监测攻击行为和处置安全事件”的表述： “能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。”
第五级	略[89]	略

89.《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)注：“第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本标准中进行描述。”

（三）优化安全通用要求

等保1.0中的安全通用要求共计10项，技术要求和管理要求各占5项。等保2.0较之于等保1.0，同样规定了10项安全通用要求，技术要求和管理要求依旧各占5项，但是在具体架构上进行了整合，并调整了相应名称，具体如下：

	等保1.0	等保2.0	评析
技术要求	物理安全	安全物理环境	等保2.0在技术要求上进行架构的调整，将原“网络安全”的内容拆分为“安全通信网络”、“安全区域边界”的两个部分，并将“主机安全”、“应用安全”、“数据安全及备份恢复”整合到“安全计算环境”中，同时新增“安全管理中心”的要求。 此外，等保2.0管理要求架构上沿袭等保1.0的规定，仅对名称进行了微小调整。
	网络安全	安全通信网络	
		安全区域边界	
	主机安全	安全计算环境	
	应用安全		
	数据安全及备份恢复		
	/	安全管理中心	
管理要求	安全管理制度	安全管理制度	
	安全管理机构	安全管理机构	
	人员安全管理	安全管理人员	
	系统建设管理	安全建设管理	
	系统运维管理	安全运维管理	

(四)新增安全扩展要求

相较于征求意见稿,本次正式发布的等保2.0在整体框架上存在较大变化,不再将安全通用要求与针对云计算、移动互联、物联网、工业控制和大数据[90]等不同等保对象的安全扩展要求分列为六个单独的标准,而是按照不同等级要求分列各等级下各新技术新应用应当满足的控制点要求,作为新增的安全扩展要求进行规定。我们将各等保对象不同等级的安全扩展要求逐一作了对比,各控制点要求逐级增加[91],具体内容如下:

90. 《等保基本要求》附录H规定了大数据的安全控制措施内容。
91. 该表仅对比核心控制点,对于控制点相同的不同等级具体要求有所区别。

安全要求等级	云计算	移动互联	物联网	工业控制系统	大数据
第一级	安全物理环境 安全通信网络 安全区域边界 安全计算环境 安全建设管理	安全物理环境 安全区域边界 安全计算环境 安全建设管理	安全物理环境 安全区域边界 安全运维管理	安全物理环境 安全通信网络 安全区域边界 安全计算环境	安全通信网络 安全计算环境 安全建设管理
第二级	相较第一级, 增加: 安全运维管理	同第一级	同第一级	相较第一级, 增加: 安全建设管理	相较第一级, 增加: 安全物理环境 安全运维管理
第三级	相较第二级, 增加: 安全管理中心	相较第一级 及第二级, 增加: 安全运维管理	相较第一级 及第二级, 增加: 安全计算环境	同第二级	同第二级
第四级	同第三级	同第三级	同第三级	同第二级 及第三级	同第二级 及第三级

92.《中华人民共和国网络安全法》第十六条规定，“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。”

（五）强化可信计算

《网络安全法》第十六条规定“推广安全可信的网络产品和服务”[92]。《网络安全等级保护条例（征求意见稿）》第十四条也规定“国家鼓励……采取主动防御、可信计算、人工智能等技术”。等保2.0中增加“可信验证”的控制点，亦是对上述法律法规的具体回应。本次等保2.0新标准强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求，例如第四级安全保护能力等级要求可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。这也体现了等保2.0主动防控、动态防控的管控思路。

（六）新增“安全管理中心”控制点

等保2.0对二级以上安全要求增加了“安全管理中心”的新控制点，以此将“系统管理员”、“审计管理员”、“安全管理员”等人员职责逐一落实到技术层面上。其中第二级安全要求仅包括系统管理和审计管理两个方面，而第三级和第四级均要求系统管理、审计管理、安全管理、集中管控四个方面全方位覆盖，具体如下：

控制点	等级要求		安全要求
系统管理	第二级	第三级及第四级	1)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； 2)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
审计管理			1)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； 2)应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理	/		1)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； 2)应通过安全管理员对系统的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

控制点	等级要求		安全要求
集中管控	/		1)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； 2)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； 3)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； 4)应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； 5)应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； 6)应能对网络中发生的各类安全事件进行识别、报警和分析； 7)应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的一致性。（第四级特殊要求）

（七）增加“个人信息保护”控制点

等保2.0新增了“个人信息保护”的控制点，以第三级安全要求为例，包括：(1) 应仅采集和保存业务必需的用户个人信息；(2) 应禁止未经授权访问和非法使用用户个人信息。虽然等保2.0对“个人信息保护”仅做简要表述，但毋庸置疑的是，个人信息保护是网络安全等级保护的重要制度。近期，中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，开展个人信息专项治理工作，个人信息的监管风险日益加重。相应地，企业应当依据《网络安全法》及其配套法律法规对个人信息保护相关规定，开展个人信息保护合规治理工作。

（八）调整管理制度、机构、人员的控制点

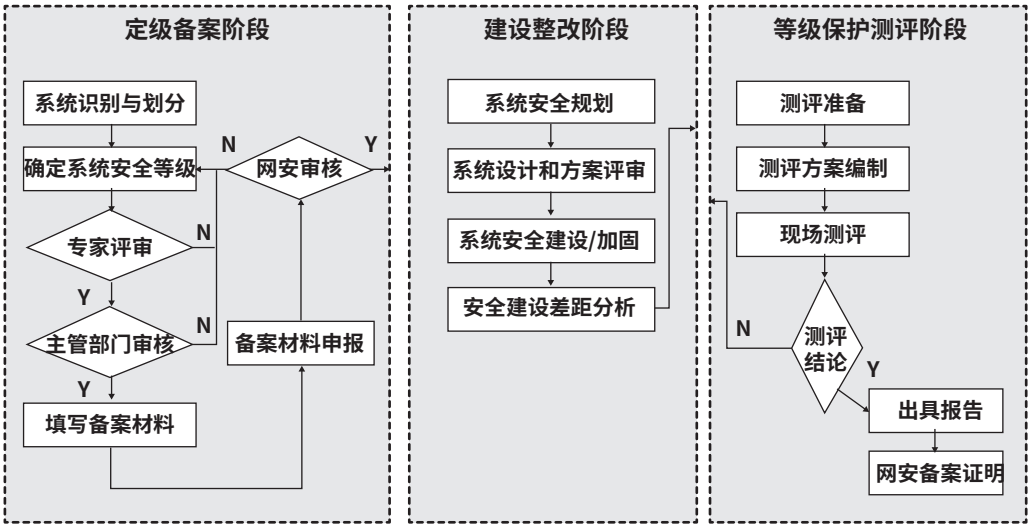
等保2.0调整了安全管理制度、机构、人员的控制点，以第三级安全要求为例：

控制点	等保2.0
安全管理制度	管理制度方面，应形成安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系； 将记录表单纳入安全管理制度体系，突出记录和可追溯的作用； 制定和发布方面，取消对安全管理制度的论证和审定，简化发布流程； 评审和修订方面，取消由信息安全领导小组负责的要求。

控制点	等保2.0
安全管理机构	在岗位设置方面，将表述调整为“成立指导和管理网络安全工作的委员会或领导小组，最高领导由单位主管领导担任或授权”，具体要求不受影响； 人员配备方面，取消“关键事务岗位配备多人共同管理”的规定； 授权和审批方面，取消“审批文档的记录和保存”； 沟通和合作方面，不再要求聘请信息安全专家作为常年完全顾问。
安全管理人员	取消人员考核的要求； 对外部人员的访问管理设置更加具体的管理规定，包括外部人员介入受控网络访问系统的审批控制及离场后的清除访问权限。

（九）定级及测评方式变化

等保1.0要求企业进行“自主定级、自主保护”。等保2.0下加强了主管部门审核及第三方专家评审的作用，某种程度上改变定级方式可能改变目前企业疏于等保定级的现状，增加更多的强制性和必要性。同时，等保1.0对于第四级系统每半年进行一次测评的要求，变为每年进行一次测评，与第三级系统的测评要求保持一致。等保2.0的具体定级流程及具体实施流程如下：



（十）各方职责分工

环节	企业	主管部门
定级	确定等级保护对象，确定安全保护等级，编制定级备案材料。	审查定级方法、工作过程、内容、结论等是否符合规定；组织专家对等级保护对象的定级情况进行评审。
备案	整理备案材料，向属地公安机关网安部门备案。	受理备案，实施备案审核，发放备案证明。
建设整改	依据等级保护国家标准和行业标准，开展安全技术和管理体系建设。	组织专家对等级保护对象的建设方案进行评审；审查等级保护对象的安全建设整改工作；对关键信息基础设施的安全建设工作重点审查。
等级测评	定期选择公安部公布的全国等级保护测评推荐目录中具有资质的测评机构，开展等级测评工作。	审查等级保护对象等级测评工作是否符合规定；对关键信息基础设施实行重点审查。
监督检查	接受并配合公安机关、上级主管部门的监督检查；定期开展安全自查工作。	定期针对等级保护对象开展网络安全执法检查；关键信息基础设施实施重点保护。

SECTION 02

企业合规建议

（一）明确落入等级保护的范围

由于等级保护对象及范围的全覆盖性，大部分企业的内部网站及信息系统，对外的网站、应用程序都会被纳入等级保护的范围。企业应当盘点自身业务是否涉及运营云计算平台/系统、大数据应用/平台/资源、物联网和工业控制系统等，并及时将上述系统纳入网络安全等级保护工作范畴。

（二）尽快开展等级保护合规工作

我国日益加强对网络安全违法违规活动的执法，2018年公安部组织开展安全监督检查14.4万家次，发现整改安全风险、管理问题等134.6万处，依法查处互联网企业3.4万余家次[93]。近期，江苏泰州某事业单位就因不履行网络安全保护义务而

受到查处[94]。鉴于网络安全执法的严峻态势，建议相关企业尽快开展等级保护合规工作，建立企业内部管理制度、安全技术措施，设置相应的管理机构和管理人员，开展等保定级、备案、测评、整改等一系列合规工作。

（三）开展网络安全整体合规工作

除积极开展网络安全等级保护工作外，企业还应当重视《网络安全法》及其配套法律法规构建的系统性的网络安全相关义务，主要包括：

- 落实网络安全等级保护制度；
- 履行网络运营者网络安全保护义务；
- 关键信息基础设施认定和网络安全保护义务的履行；
- 个人信息和重要数据的保护；
- 数据本地化存储和跨境数据传输的安全评估；
- 落实网络产品和服务的网络安全审查制度；
- 网络传播内容的管理；
- 落实《网络关键设备和网络安全专用产品目录》及安全认证检测制度。

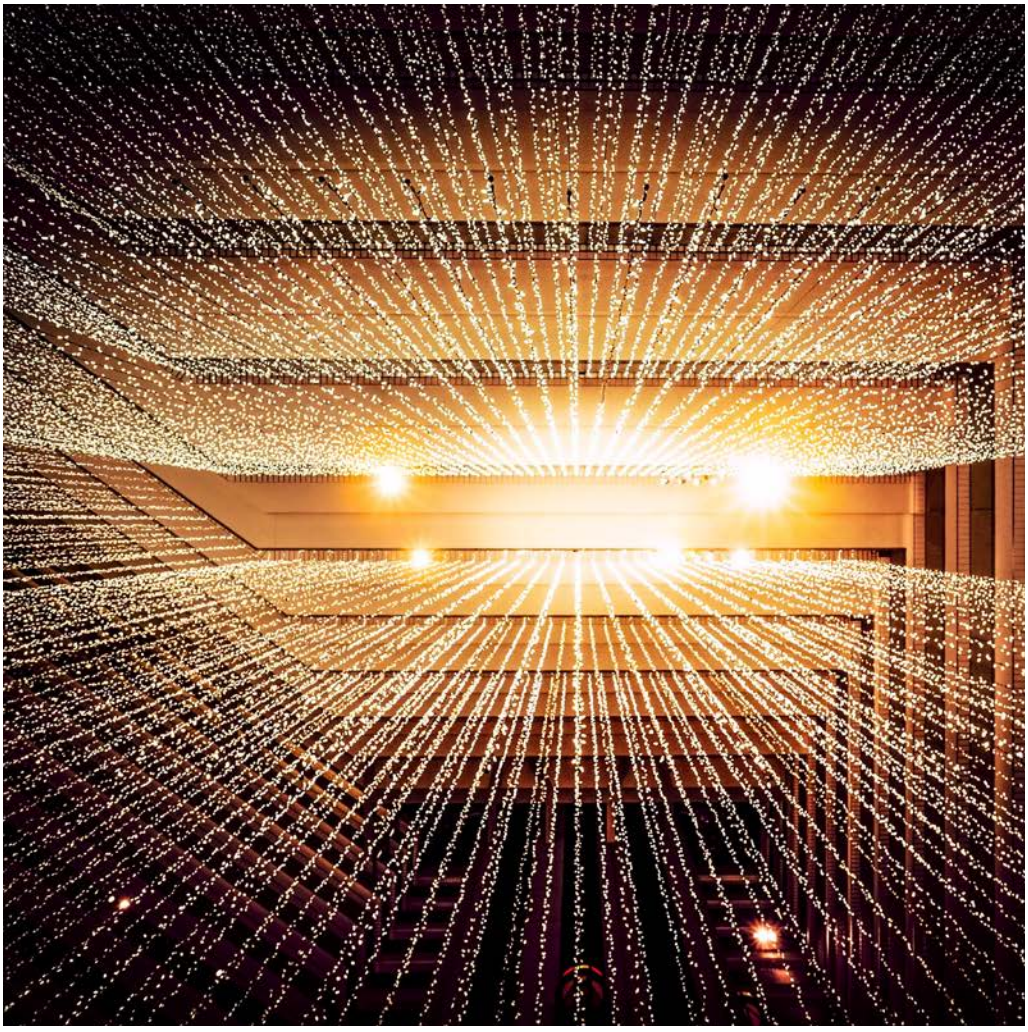
结语

若相关企业违反上述法律要求，可能引发民事侵权、行政处罚，甚至是刑事责任。因此，我们建议相关企业可以开展整体的网络安全和数据保护合规工作，以防范上述风险。建议企业尽快着手实施网络安全与数据保护的整体合规工作，对企业目前的合规现状进行摸底评估，有效识别相应法律风险，并针对合规漏洞建立健全整体的合规体系。对于企业而言，有效的系统合规梳理工作包括合规现状尽职调查与差距分析、风险识别及合规建议、合规方案的实施和优化三个阶段，做到组织、流程、制度和培训各环节环环相扣，同时应当与企业所在行业、产品及服务的特性有针对性的落实相关合规义务。

93.中华人民共和国公安部官网："公安部'净网2018'专项行动取得显著成效"，http://www.mps.gov.cn/n2253534/n2253535/c6422823/content.html，2019年5月20日访问。
94.江苏网警："江苏网警发布'净网2019'专项行动执法典型案例（二）"，https://mp.weixin.qq.com/s/ZRKmO-hJfFo-jZcXl3TjBx-A?scene=25#wechat_redirect，2019年5月20日访问。

CHAPTER THREE

数据保护



对于现代企业而言，数据就像血液一样贯穿于业务（模式分析、隐私条款、业务界面、DPA设计）、产品（数据存储、产品界面、个人信息）、并购（数据审查）、员工（入职、离职）、合作伙伴（尽调）等各个方面，流淌在企业的每个“毛细血管”中，成为几乎可以与劳动力和资本相提并论的生产要素，在很大程度上决定了企业在市场中的竞争和成长。其中，个人信息是重要的组成部分，在企业合规中尤为重要，这也是落实《网络安全法》的重要组成部分，个人信息的收集、处理的合规性已经成为影响企业成功与否的新挑战。

第一节

《数据安全管理办法(征求意见稿)》解读[95]

国家互联网信息办公室于2019年5月28日发布《数据安全管理办法(征求意见稿)》[96](以下简称"管理办法"),向社会公开征求意见。该管理办法在继承《中华人民共和国网络安全法》(以下简称"《网络安全法》")原则性规定的基础上,着重规范了网络运营者对于个人信息和重要数据的安全管理义务。在个人信息保护部分,吸收了近年来广泛适用的国家标准《信息安全技术个人信息安全规范》(GB/T 35273-2017)中的若干规定,于法规层面上明确了网络运营者的合规要求及主管部门的监管态度,同时提出了收集个人敏感信息备案制的新要求;在重要数据保护部分,进一步明确了重要数据的性质,提出了收集重要数据的备案制以及向第三方提供重要数据的批准制的新要求。

SECTION 01

进一步明确"数据活动"的监管

在本次管理办法中,对利用网络开展数据收集、存储、传输、处理、使用等活动统一规范为"数据活动"。除纯粹家庭和个人事务外,在中国境内开展数据活动的行为都将受管理办法的制约。同时,除境内数据监管外,对于来源于境外的数据安全风险和威胁,国家也将采取一定监测、防御、处置措施。

在《网络安全法》确定的"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[97]"的原则性规定的基础上,管理办法进一步明确了个人信息和重要数据安全保护工作在中央网络安全和信息化委员会领导下,由国家网信部门统筹协调、指导监督。地(市)及以上网信部门将负责指导监督本行政区内的个人信息和重要数据安全保护工作。

《网络安全法》要求网络运营者应当采取一定技术措施确保网络安全及数据安全[98],同时制定网络安全事件应急预案并及时处置安全事件[99]。在此基础上,管理办法进一步明确了网络运营者的数据安全保护义务,在立法层面上新增建立数据安全管理责任和评价考核制度、制定数据安全计划、开展数据安全风险评估、组织数据安全教育培训的合规义务。

95.原文标题为《小数据安全法出台|<数据安全管理办法(征求意见稿)>解析》,作者陈际红、韩璐,网址:http://www.zhonglun.com/Content/2019/05-29/1520544924.html。

96.《数据安全管理办法(征求意见稿)》原文请见http://www.moj.gov.cn/news/content/2019-05/28/zlk_235861.html

97.《中华人民共和国网络安全法》第八条 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。

98.《中华人民共和国网络安全法》
第十条 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。
第四十二条 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。

99.《中华人民共和国网络安全法》
第二十五条 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。

SECTION 02

广泛吸收国家标准的成熟规定，效力上升为规章

2018年5月，全国信息安全标准化技术委员会（以下简称**“信安标委”**）发布的《信息安全技术个人信息安全规范》（GB/T 35273-2017）（以下简称**“规范”**）正式实施，该规范作为企业落地《网络安全法》中个人信息保护原则要求的实践指引，被各个行业及企业在数据合规工作中广泛采用，也成为监管部门管理和执法的重要参考依据。今年2月1日，信安标委再次发布该规范的《信息安全技术个人信息安全规范（草案）》，结合了2017年、2018年的隐私评审[100]工作成果，及2019年四部委开展的App违法违规收集使用个人信息专项治理行动[101]的监管要求，对市场上比较集中的过度收集用户个人信息，强制授权、“一揽子授权”等突出问题提出了相应的合规标准。

可以看出本次管理办法在个人信息部分，很大程度上吸收了现行规范的合规要求，同时采纳了规范修订草案中的新增要点，将国家标准层级上的部分核心措施提升到法规层面，既明确了网络运营者在法规层级上的合规义务，又减少了规范作为国家标准适用的压力。

（一）不得捆绑授权，应当区分核心业务功能

具体而言，本次管理办法要求网络运营者不得以打包授权，捆绑授权等形式强迫、误导个人信息主体同意其收集个人信息。在继承了《网络安全法》对于个人信息收集、使用的“明示”+“同意”的原则性要求基础上[102]，进一步吸收了规范修订草案对于通过区分核心业务功能和扩展业务功能来保障个人信息主体选择同意权的核心要求，从法规层面明确了网络运营者既不能以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，违背个人信息主体的自主意愿默认或捆绑授权；也不能因个人信息主体仅提供核心业务功能所必须的个人信息，便拒绝向其提供核心业务功能服务。具体业务功能区分方法及交互式界面的设计建议企业参考规范新修订草案“附录C保障个人信息主体选择同意权的方法”的相应内容。

（二）禁止歧视行为

规范将个人信息处理是否可能对个人信息主体合法权益造成不利影响，导致歧视性待遇作为个人信息安全影响评估工作的主要内容之一。本次管理办法明确了网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等。

100.2017年7月至9月，中央网信办、工信部、公安部和国家标准委针对国内互联网领先企业的10款App组织了首次App隐私政策专项评审工作。2018年12月，全国信息安全标准化技术委员会对40款网络产品和服务的隐私条款进行了2018年隐私条款专项评审工作。

101.2019年1月25日中央网信办、工业和信息化部、公安部、市场监管总局联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，决定自2019年1月起至12月，在全国范围组织开展持续时间长达一年的App违法违规收集使用个人信息专项治理行动，旨在解决目前App强制授权、过度授权、超范围收集个人信息等突出问题。具体解读请参考以往文章《实施半年后再修订：《信息安全技术个人信息安全规范》应时而变》。

102.《中华人民共和国网络安全法》
第四十一条　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。
第四十二条　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。

（三）明示定推功能并提供退出机制

与此同时，管理办法吸收了规范修订草案对于定向推送、个性化展示的个人信息应用场景的操作规范和退出机制，从法规层面上要求网络运营者应当以明显方式标明“定推”字样，并为用户提供停止接收定向推送信息的功能，保证了个人信息主体对于定向推送的自主选择，避免形成信息孤岛。同时，将规范修订草案对于个人信息主体可以删除或匿名化处理定推活动所依赖的个人信息的操作建议直接上升至法规层面，并明确用户选择停止接收定向推送信息时，网络运营者应删除已经收集的设备识别码等用户数据和个人信息，这就从定向推送的深层基础上严格控制网络运营者对用户画像的使用界限，提出了用户可以拒绝产品或服务提供者收集其个人信息进行特定画像处理和定推服务的合规要求。管理办法在此基础上明确开展定向推送活动的规则及其内容应当满足一定的原则性要求，即遵守法律、行政法规，尊重社会公德、商业道德、公序良俗，诚实守信，严禁歧视、欺诈等行为。

上述严禁歧视行为、明示定推功能并提供退出机制的要求，与《电子商务法》对于向消费者提供个性化展示应当同时提供不针对其个人特征的选项的立法原则保持一致[103]，均为保障用户在使用网络产品及服务时不受数据、算法歧视，并获得自主选择的权利。

（四）原则性规定收集未成年人个人信息的行为规范

未成年人的个人信息一直是立法执法保护的重点。今年4月20日提交审议的《民法典人格权编（草案）》二审稿[104]对此明确了收集使用未成年人等无民事行为能力人或者限制民事行为能力人的个人信息的，应当征得其监护人同意的立法原则。

本次管理办法明确规定对于收集14周岁以下未成年人个人信息应当事先获得其监护人的同意。而对于收集、使用年满14周岁的未成年人个人信息的情况并未进行规定，对收集无民事行为能力人或者限制民事行为能力人的个人信息的情况也未有明确说明。而目前现行的《个人信息安全规范》对于收集年满14周岁的未成年人个人信息的，强调应当事先获得未成年人或其监护人的明示同意，而对于不满14周岁的，则应当事先征获得其监护人的明示同意。鉴于未成年人个人信息的敏感度，我们仍建议企业参照《个人信息安全规范》的相关推荐标准进行相应的合规工作。

（五）规定向第三方提供个人信息须征得授权同意的例外，促进数据的有序流动

本次管理办法在继承《网络安全法》对于个人信息主体同意的原则性要求的

103.《电子商务法》第十八条“电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益”

104.来源：http://www.npc.gov.cn/npc/cwhhy/13jcwh/2019-04/21/content_2085573.htm

前提下，吸收了规范对于向第三方提供个人信息无需征得授权同意的规定，统一简化为五大类例外情形，在具体内涵上与规范保持一致，具体对比如下：

《数据安全管理办法(征求意见稿)》	《信息安全技术个人信息安全规范》(GB/T 35273-2017)	《信息安全技术个人信息安全规范（草案）》
第二十七条 网络运营者向他人提供个人信息前，应当评估可能带来的安全风险，并征得个人信息主体同意。下列情况除外： （一）从合法公开渠道收集且不明显违背个人信息主体意愿； （二）个人信息主体主动公开； （三）经过匿名化处理； （四）执法机关依法履行职责所必需； （五）维护国家安全、社会公共利益、个人信息主体生命安全所必需。	8.5 共享、转让、公开披露个人信息时事先征得授权同意的例外 以下情形中，个人信息控制者共享、转让、公开披露个人信息无需事先征得个人信息主体的授权同意： a）与国家安全、国防安全直接相关的； b）与公共安全、公共卫生、重大公共利益直接相关的； c）与犯罪侦查、起诉、审判和判决执行等直接相关的； d）出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的； e）个人信息主体自行向社会公众公开的个人信息； f）从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。	8.5 共享、转让、公开披露个人信息时事先征得授权同意的例外 相较现行规范增加“a)与个人信息控制者履行法律法规规定的义务相关的”的情形。

值得注意的是，规范对收集、使用个人信息无需征得个人信息主体的授权同意提供了几类具体情形，在规范修订草案中还删除了“履行合同必要”之例外情形。但在本次管理办法中并未明确收集、使用个人信息无需征得授权同意的例外。相反地，管理办法明确规定了仅当用户知悉收集使用规则并明确同意后，网络运营者方可收集个人信息。

由此可见，个人信息主体的授权同意仍将是收集和使用个人信息的法定前提。

（六）从法规层面明确DPO的职责要求

规范修订草案中增加了对于个人信息保护负责人的任职条件、职责要求、汇报对象等内容。本次管理办法吸收了相应具体要求，从个人信息保护负责人上升为数据安全责任人（DPO），同时在规范意图要求所有个人信息控制者均设置个人信息保护负责人的要求上缩小了适用范围，将以非经营为目的收集数据，以及收集除个人敏感信息外其他个人信息的网络运营者明确排除在外，即仅约束以经营为目的收集重要数据或个人敏感信息的网络运营者应任命DPO的合规义务。

SECTION 03

将重要数据纳入监管

《网络安全法》明确了关键信息基础设施运营者的数据本地化要求[105]，提出了重要数据这一新概念。 在2017年发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》中重要数据进行了定义，指与国家安全、经济发展，以及社会公共利益密切相关的数据。随后，信安标委在《信息安全技术　数据出境安全评估指南(征求意见稿)》中提出了《重要数据识别指南》，列举了各行业各领域涉及的重要数据范围。本次管理办法进一步明确了重要数据的性质，即“一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据”并例举了部分示例“如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等”，同时明确排除了企业生产经营和内部管理信息及个人信息作为重要数据的可能。

可以看出，本次管理办法仍未对重要数据的具体识别方式进行规定。尽管本次管理办法规定企业生产经营和内部管理信息将不属于重要数据的范畴，但各行业主管部门对本行业内涉及的重要数据的监管重点仍不会松懈。我们建议现阶段企业具体判断重要数据类别时，应当同时考量横纵两个维度：以风险导向及性质作为横向的宏观判断标准，以及《重要数据识别指南》中各行业内重要数据范围的纵向判断标准。如企业因生产经营涉及大量测绘数据，则仍应当考虑地理数据作为行业主管部门自然资源部（原国土资源部）的监管重点，应当作为重要数据予以管控。

105.《中华人民共和国网络安全法》第三十七条
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。

SECTION 04

新增个人敏感信息和重要数据备案管理制度

2019年5月8日，天津市互联网信息办公室发布《天津市数据安全管理办法（暂行）》的征求意见稿，提出建立重要数据和个人信息的备案制度。此次管理办法提出在全国范围内对以经营为目的收集重要数据和个人敏感信息网络运营者应当向所在地网信部门进行备案。同时明确该备案内容仅限收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，而不包括具体的数据内容本身。鉴于管理办法第十四条明确了网络运营者从第三方间接收集个人信息应当履行与直接收集个人信息同等的保护责任和义务，则网络运营者即便不直接向个人信息主体收集其个人敏感信息，而是从第三方处获得个人敏感信息的，也应当履行相应的备案义务。

尽管该备案制可以作为政府监管的抓手，从一定程度上加强企业完善收集使用重要数据和个人敏感信息的合规义务，并落实企业发生数据安全事件的追责管理，但从实践操作来讲，网络运营者覆盖面极广，涉及数据收集、处理的业务类型繁多，同时考虑到数据动态性和时效性的特点，企业若针对每项数据收集新需求完成逐一备案，将势必增加相应成本，同时对地方网信部门的备案管理要求也将显著增加。与此同时，如落实备案制，还须在立法层面上首先确定重要数据的具体分类标准和适用范围。

SECTION 05

新增向第三方提供重要数据的批准管理制度

本次管理办法明确了网络运营者向第三方提供（包括共享、交易、公开披露、出境等）重要数据前，应当进行安全评估工作，并获得行业主管监管部门同意，行业主管监管部门不明确的，应经省级网信部门批准。同时，管理办法提出“向境外提供个人信息按有关规定执行。”可以看出，网信办在《个人信息和重要数据出境安全评估办法》迟迟未出台的情况下，有意将重要数据与个人信息的出境管理进行分割，实行不同的监管原则。预计个人信息出境的具体管理办法也将陆续推出。

SECTION 06

首次规范“爬虫”技术等自动获取数据的行为

目前市场上利用爬虫技术大量自动获取数据的行为已屡见不鲜。本次管理办法针对此类采取自动化手段访问收集网站数据的行为进行了规制，要求其不得妨碍网站正常运行，如严重影响网站运行，网站有权要求停止自动化访问收集，该行为即应停止。管理办法同时明确如自动化访问收集流量超过网站日均流量三分之一，则视为严重影响网站运行的情形。需注意的是，该条款仅列举了严重影响网站运行的情形之一，其他利用自动化访问收集的行为若从结果上导致网站运营受严重影响，也应当在网站要求时及时停止该行为，避免违规风险。

SECTION 07

首次针对AI技术自动合成信息进行规制

今年2月，电视剧《射雕英雄传》中黄蓉一角换脸某知名女星的视频引发热议。而主张人脸识别技术侵犯个人隐私和公民权利为由的英国首例警用人脸识别案也于近日开庭审理。现今大数据、人工智能等技术广泛应用，一定程度上也催发了技术滥用导致的违法违规行为，不仅涉及侵犯自然人的人格权益，严重的还可能造成恶劣的社会影响，危害国家安全和社会公共利益。对此，今年4月提交审议的《民法典人格权编（草案）》二审稿对此类AI技术所导致的社会问题亦作出了回应[106]，要求任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权。同时针对自然人声音等其他人格权的许可使用和保护也进行了规范。

据了解，近年来国内外诸多媒体机构均推出了自己的“人工智能写手”，如腾讯财经推出了“Dreamwriter”，新华社推出“快笔小新”、“媒体大脑”等[107]。本次管理办法顺应时代要求，规定利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息不得以谋取利益或损害他人利益为目的，同时应当以明显方式标明“合成”字样。

106.来源：http://www.npc.gov.cn/npc/cwhhy/13jcwh/2019-04/21/content_2085573.htm

107.来源：https://m.mp.oeeee.com/a/BAAFRD0000020190528165378.html?&layer=4&share=chat&isndappinstalled=0

SECTION 08

明确平台对于接入第三方应用的数据安全保障义务

目前，应用程序中接入/嵌入第三方产品或服务的场景十分常见，一旦发生合规漏洞，平台商和第三方往往无法明确双方的责任和义务，而数据主体往往很难去追究第三方产品或服务提供商的责任。

此前规范修订草案细化了平台商对第三方应用收集个人信息的管理机制。本次管理办法从法规层面商进一步明确了网络运营者对于第三方应用接入的管理义务，同时将对个人信息的安全保障义务扩大到了所有数据。同时明确第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。网络运营者应当在与第三方签订的合同中明确双方的数据安全责任及安全措施，同时完善企业内部数据安全管理制度，妥善留存个人信息安全影响评估报告，对第三方应用接入管理、审计记录等，并对第三方应用运营者及时督促整改，必要时停止其接入。以充足的技术措施和制度手段证明平台商充分履行了审慎义务。

SECTION 09

提出开展自愿性数据安全管理认证和应用程序安全认证机制

2019年1月25日中央网信办等四部委联合发布的《关于开展App违法违规收集使用个人信息专项治理的公告》提出将开展App个人信息安全认证工作，鼓励App运营者自愿通过App个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。

本次管理办法将监管部门治理违法违规收集使用个人信息的思路，延用至所有数据的安全管理当中，旨在通过鼓励搜索引擎、应用商店等优先推荐通过认证的应用程序的市场选择机制引导消费者选用安全的应用产品，进一步规范网络运营者的数据安全治理工作，形成解决数据安全问题的长效治理机制。

管理办法同时提出具体数据安全管理认证和应用程序安全认证工作将由国家网信部门会同国务院市场监督管理部门共同指导国家网络安全审查与认证机构进行，预计相应具体认证办法也将陆续出台。

SECTION 10

明确监管部门约谈整改的处理机制

《网络安全法》规定了省级以上人民政府有关部门发现网络存在较大安全风险或者发生安全事件时，可以依照规定的权限和程序对网络运营者的法定代表人或主要负责人进行约谈[108][13]。本次管理办法在此基础上进一步明确了网信部门如发现网络运营者数据安全管理责任落实不到位，可以按照规定的权限和程序约谈网络运营者的主要负责人，并督促整改。结合近年来网络安全和数据保护相关执法行动，网信部门的约谈整改已成为监管的主要措施之一。根据本次管理办法第三十七条罚则的规定，对于违反本办法规定的网络运营者，监管部门可根据情节给予公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚，构成犯罪的，也将依法追究刑事责任。

108.《中华人民共和国网络安全法》第五十六条 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。

SECTION 11

明确主管部门对于数据负有保密责任

《网络安全法》规定网信及有关部门在履行网络安全保护职责中获取的个人信息、隐私和商业秘密应当严格保密，除用于维护网络安全的需要外，不得用于其他用途。同时，今年4月提交审议的《民法典人格权编（草案）》二审稿中亦明确了国家机关及其工作人员对履职过程中知悉的自然人隐私、个人信息等的保密义务。

在此立法原则基础上，管理办法明确了国务院有关主管部门对网络运营者提供的数据负有安全保护责任的要求。相应的，在此法律制度规范下，有关主管部门因履行维护国家安全、社会管理、经济调控等职责需要而要求提供相关数据的，网络运营者也应当予以配合。

结语

在2018年9月公布的“十三届全国人大常委会立法规划”中，《数据安全法》被列为“条件比较成熟、任期内拟提请审议的法律草案”，网络运营者应当积极关注立法进展，提前做好合规准备。

第二节

四部门对App收集个人信息的专项治理述评[109]

2019年1月，中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》（以下简称《公告》），并联合有关单位成立了App违法违规收集使用个人信息专项治理工作组，旨在打击App违法违规收集使用个人信息行为。截至4月16日，举报信息超过3480条，涉及1300余款App。对于30款用户量大、问题严重的App，工作组已向其运营者发送了整改通知。

从举报的问题来看，26%的App没有隐私条款或未在隐私条款中明确收集个人信息的目的、方式、范围；31%的App在申请打开收集个人信息相关权限时，未明确告知用户；20%的App收集与业务功能无关的个人信息，如金融借贷App收集用户通信录；19%的App未经用户同意，向他人提供设备ID、应用程序列表等个人信息；13%的App强制索要与业务功能无关的权限，如计算器、手电筒App强制要求打开地理位置权限。还有一些App存在不支持用户注销账户、更正或删除信息等问题[110]。

109. 原文标题为《四部门重拳出击APP个人信息乱象，企业如何有效应对?》，作者陈际红、韩璐，网址：http://www.zhonglun.com/Content/2019/03-04/1704042531.html。

110. “四部门抓紧推进App违法违规收集使用个人信息专项治理”，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057732/c6797025/content.html，访问时间：2019年5月8日。

四部委高度重视个人信息保护工作，针对当前App强制授权、过度索权、超范围收集个人信息等网民反映强烈的问题，已采取并即将采取出台必要的管理规范和相关标准的形式进行规制[111]。2019年5月5日，App专项治理工作组发布《App违法违规收集使用个人信息行为认定方法（征求意见稿）》（以下简称《认定方法》）并公开征求意见。该《认定方法》与App专项治理工作组2019年3月发布的《App违法违规收集使用个人信息自评估指南》（以下简称《指南》）一脉相承，但又结合《个人信息安全规范》（以下简称《规范》）以及举报活动中频繁出现的严重违法违规现象，体现出执法机构规范的重点，对于企业评估合规状况，设定自身的合规红线有重大参考意义。

111.如公安部已颁布的《App违法违规收集使用个人信息自评估指南》，正在修订中的《个人信息安全规范》，以及日前市场监管总局下发的《网络交易监督管理办法》（征求意见稿）中关于网络经营者在经营活动中收集消费者信息的规定（第22条）等。

SECTION 01

《公告》解读

本次公告主要列明了APP运营者的主要合规义务、App隐私政策和个人信息收集使用情况评估方式、APP运营者的法律责任及开展自愿性App个人信息安全认证等要点。

（一）APP运营者的合规义务

公告指出，App运营者收集使用个人信息时应当严格履行《中华人民共和国网络安全法》（以下简称“《网络安全法》”）规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。《网络安全法》规定网络运营者应承担的个人信息保护合规义务主要包括：

建立健全用户信息保护制度（第四十条）；

建立个人信息的收集、使用规则及制度（第四十一条、第四十二条、第四十四条）；

建立个人信息泄露事件的报告制度（第四十二条）；

建立个人信息的删除和更正制度（第四十三条）；

建立对用户发布的信息管理制度（第四十七条）；

建立网络信息安全投诉、举报制度（第四十九条）。

《网络安全法》规定网络运营者在收集个人信息时应满足“知情同意”原则（第四十一条）。公告强调App运营者应当获得个人信息主体的自主选择同意，即明示同意，同时要求App运营者不以默认、捆绑、停止安装使用等手段变相强迫用户授权（禁止强制授权），进一步提高了App运营者获得个人信息主体授《网络安全法》规定网络运营者在收集个人信息时应当向个人信息主体明示收集权的合规要求。

使用规则（第四十一条）。公告在此原则性规定的基础上，要求App运营者应当

以通俗易懂、简单明了的方式向个人信息主体展示其个人信息收集使用规则，即从用户友好的角度来设计用户隐私政策，避免目前绝大多数用户难以理解晦涩难懂、长篇大段的隐私协议而草草点击同意授权的乱象。可以看出，各部委以行业良好实践规范作为本次专项治理的审查要求，旨在提高App市场上个人信息保护的合规标准。

同时，公告指出App运营者应当遵循合法、正当、必要的原则，不得收集与所提供服务无关的个人信息（禁止过度收集），不得违反法律法规与用户约定收集使用个人信息（禁止超范围收集），并倡导App运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项（禁止强制推送），进一步落实个人信息主体对于其个人信息的实际控制权。

（二）App隐私政策和个人信息收集使用情况评估

公告指出，本次专项治理行动将由全国信息安全标准化技术委员会（以下简称“信安标委”）、中国消费者协会、中国互联网协会、中国网络空间安全协会，组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估，评估规模预计将达上千款App。上述专业机构也将编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，作为本次评估工作的主要依据。

此次信安标委将联合各专业机构针对App如何区别基本功能与附加功能、如何鉴别所收集信息为必要信息、以及违法违规收集使用个人信息的评估要点出台更为细致的合规指引，不难看出本次制定的相关评估规范也将对企业合规工作产生重要影响。

（三）APP运营者的法律责任

公告指出，有关主管部门将在此次专项治理行动中加强对违法违规收集使用个人信息行为的监管和处罚，包括责令App运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。根据《网络安全法》的规定，单位违法违规收集使用个人信息的，还将对直接负责的主管人员和其他直接责任人员进行处罚。涉及犯罪的，还应当根据《刑法修正案（九）》及两高相关司法解释的规定承担相应的刑事责任。公安机关也将在本次专项治理行动中开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。

结合目前我国个人信息保护相关立法框架，违法违规收集使用个人信息的处罚规定具体如下：

违法违规行为	执法依据	处罚规定
提供的应用软件，设置恶意程序，或者含有法律、行政法规禁止发布或者传输的信息。	《网络安全法》第六十条	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。
强制、过度收集个人信息。	《网络安全法》第六十四条 《中华人民共和国消费者权益保护法》第二十九条	由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 处罚机关应当记入信用档案，向社会公布。
未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息。	《网络安全法》第六十四条 《中华人民共和国消费者权益保护法》第二十九条	由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 处罚机关应当记入信用档案，向社会公布。
未采取措施删除或者更正违反法律法规规定收集、使用的个人信息。	《网络安全法》第六十四条 《中华人民共和国消费者权益保护法》第二十九条	由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 处罚机关应当记入信用档案，向社会公布。
泄露、篡改、毁损收集的个人信息。	《网络安全法》第六十四条 《中华人民共和国消费者权益保护法》第二十九条	由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 处罚机关应当记入信用档案，向社会公布。
发生或可能发生个人信息泄露、毁损、丢失的情况时，未立即采取补救措施，未及时告知用户并向有关主管部门报告。	《网络安全法》第六十四条 《中华人民共和国消费者权益保护法》第二十九条	由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 处罚机关应当记入信用档案，向社会公布。

违法违规行为	执法依据	处罚规定
非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的行为。	《网络安全法》第六十四条	由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。
强制、过度收集个人信息。	《网络安全法》第六十四条 《中华人民共和国消费者权益保护法》第二十九条	由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 处罚机关应当记入信用档案，向社会公布。
非法方式获取、非法出售或者非法向他人提供个人信息，情节严重构成犯罪的行为。	《刑法修正案（九）》	处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。单位犯罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员判处相应处罚。
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。	《网络安全法》第六十八条	由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万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、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。
应用软件下载服务提供者不履行安全管理义务。	《网络安全法》第六十八条	由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万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、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。
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，采取停止传输、消除等处置措施。	《网络安全法》第六十九条	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。
拒绝、阻碍有关部门依法实施的监督检查。	《网络安全法》第六十九条	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。
拒不向公安机关、国家安全机关提供技术支持和协助。	《网络安全法》第六十九条	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。
拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成了严重后果。	《刑法修正案（九）》、《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；单位犯罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员依照前款的规定处罚。

112.来源于国家认监委http://www.cnca.cn/xxgk/tpxw/201901/t20190125_57029.shtml。

除此之外，为加强APP的规范管理，国家网信办于去年先后出台《移动互联网应用程序信息服务管理规定》《互联网直播服务管理规定》《互联网群组信息服务管理规定》等相关法规，明确移动应用程序开发者、运营者及接入者各自应当承担的企业主体责任。企业还应当遵守各行业主管部门对本行业的特殊监管政策。

（四）开展自愿性App个人信息安全认证

公告提出，四部委将开展App个人信息安全认证工作，鼓励App运营者自愿通过App个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。据了解[112]，市场监管总局将会同网信办等部门建立App个人信息安全认证制度，按照App运营商自愿申请的原则，由具备资质的认证机构依据相关国家标准对App收集、存储、传输、处理、使用个人信息等活动进行评价，符合要求后颁发安全认证证书并允许认证标识。此举旨在通过鼓励搜索引擎和应用商店优先推荐获证App等方式，引导消费者选用安全的App产品，透过市场选择机制的引领作用进一步规范App运营商的研发和推广行为、提升个人信息保护意识和能力，形成解决App违法违规使用个人信息问题的长效治理机制。

SECTION 02

《认定方法》解读

《认定方法》规定了主要的App违规情形，以下逐一进行解读。

（一）没有公开收集使用规则的情形

条文	对应《指南》评估点	法律依据	评析
1.没有隐私政策、用户协议，或者隐私政策、用户协议中没有相关收集使用规则的内容；	1.是否有隐私政策。 2.隐私政策是否单独成文。	《网络安全法》第22条、第41条 《消费者权益保护法》第29条	此处所指的“收集使用规则”基本与《指南》中提及的隐私政策一致，同时在一定程度上扩大了范围，也将用户协议中的相关规则纳入其中，实质要求与《指南》关于隐私政策公开性、易读性的要求一致，提出了对于公开收集使用规则的底线要求。
2.在App安装、使用等过程中均未通过弹窗、链接等方式提示用户阅读隐私政策，或隐私政策链接无效、文本无法正常显示；			
3.进入App主功能界面后，多于4次点击、滑动才能访问到隐私政策；	3.隐私政策是否易于访问。		
4.其他违反公开收集使用规则要求的情形。	N/A		

（二）没有明示收集使用个人信息的目的、方式和范围的情形

条文	对应《指南》评估点	法律依据	评析
1.收集使用信息的目的违反合法、正当、必要原则，如仅仅以改善程序功能、提高用户体验、定向推送等为目的收集用户个人信息；	5.是否明示收集个人信息的业务功能 20.是否向用户明示收集、使用个人信息的目的、方式、范围。 21.若使用Cookie及其同类技术收集个人信息，是否向用户明示。	《网络安全法》第22条、第41条 《消费者权益保护法》第29条	此处所指的“未明示收集使用个人信息的目的、方式和范围”所涉及的授权文本不仅包括隐私政策、亦包括单独的弹窗提示中涉及收集使用用户个人信息的授权文本，文本本身应简明易读，其实质内容应满足合法、正当、必要原则，收集规则发生变化以及涉及到实践中对用户影响最大的个人敏感信息的收集时应明确向用户通知并取得其同意，要求收集信息、调取访问权限时明确、清晰地对应到具体的业务功能。
2.没有逐一列出收集个人信息的类型、频率，特别是针对个人敏感信息；	6.业务功能与所收集个人信息类型是否一一对应。 7.是否明示各项业务功能所收集的个人信息类型。 8.是否显著标识个人敏感信息类型。 20.是否向用户明示收集、使用个人信息的目的、方式、范围。		
3.收集使用个人信息的目的、方式和范围发生变化，未以适当方式通知用户，适当方式包括更新隐私政策并提醒用户重新阅读授权等；	18.隐私政策更新 20. 是否向用户明示收集、使用个人信息的目的、方式、范围。		
4.在申请可收集个人信息的权限时，未告知收集使用的目的，如在申请调阅通讯录时没有说明原因；	20.是否向用户明示收集、使用个人信息的目的、方式、范围。		
5.每次要求用户提供个人敏感信息时，如身份证号、银行卡号等，未同步实时说明原因；	20.是否向用户明示收集、使用个人信息的目的、方式、范围。		
6.有关收集使用规则的内容晦涩难懂、冗长繁琐；	4.隐私政策是否易于阅读。 20.是否向用户明示收集、使用个人信息的目的、方式、范围。		
7.其他没有明示收集使用个人信息的目的、方式和范围的情形。	N/A		

（三）未经同意收集使用个人信息的情形

条文	对应《指南》评估点	法律依据	评析
1.未经同意就开始收集个人信息，如App首次运行、提示用户阅读隐私政策前就开始收集个人信息；	20. 是否向用户明示收集、使用个人信息的目的、方式、范围。 23.收集个人信息前是否征得用户自主选择同意。	《网络安全法》第22条、第41条 《消费者权益保护法》第29条	部分旨在实现用户的选择同意原则，列举了未经过授权环节即收集个人信息以及超限收集（实际收集情况与隐私政策及其他授权文本不符）的显著违规现象，以及容易引起用户反感的：明确拒绝之后依然继续收集或持续索要授权，未经同意或者未使用APP时仍持续收集和擅自修改权限设置的情形。对于使用行为中利用用户信息进行定向推送的退出机制亦做出了规定，这一点与《规范》的修订版本以及《互联网个人信息安全保护指南》的相关规定有密切联系。
2.用户明确拒绝后，仍收集个人信息，如用户不同意被收集地理位置信息时仍然收集；	28.是否在用户明确拒绝后继续索要权限、打扰用户。	《电子商务法》第18条	
3.实际收集使用的个人信息超出用户授权的范围	25.实际收集的个人信息类型是否超出隐私政策所述范围。		
4.利用用户信息和算法定向推送新闻、广告等，未提供终止定向推送的选项；	11.个人信息的使用规则。[113]		
5.未经用户同意，私自调用可收集用户个人信息权限；	23.收集个人信息前是否征得用户自主选择同意。 26.收集与业务功能有关的非必要信息，是否经用户自主选择同意。	《网络安全法》第22条、第41条 《消费者权益保护法》第29条	
7.未经用户同意私自更改用户设置的权限，包括App更新时将用户设置的权限恢复到默认状态；	23.收集个人信息前是否征得用户自主选择同意。 26.收集与业务功能有关的非必要信息，是否经用户自主选择同意。 29.App更新是否更改系统权限设置。	《电子商务法》第18条	
8.用户明确拒绝App收集个人信息请求，App仍频繁征求用户同意，干扰用户正常使用；	28.是否在用户明确拒绝后继续索要权限、打扰用户。		
9.违背与用户约定，不按隐私政策中的收集使用规则收集使用个人信息；	25.实际收集的个人信息类型是否超出隐私政策所述范围。		
10.其他未经同意收集使用个人信息的情形。	N/A		

113. 如果App运营者将个人信息用于用户画像、个位化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。

（四）违反必要性原则，收集与其提供的服务无关的个人信息的情形

条文	对应《指南》评估点	法律依据	评析
1.实际收集的个人信息类型与现有业务功能无关，无关是指该类信息并非实现现有业务功能所必需；	27.是否收集与业务功能无关的个人信息。	《网络安全法》第22条、第41条 《消费者权益保护法》第29条	此处所指“与其服务无关的个人信息”主要是为了实现必要性原则的落地，几个条文并未区分核心、附加业务功能，而是直接采用“现有业务功能”的说法，禁止超出现有业务功能所必须的个人信息收集行为：收集频率非必要、申请无关信息收集权限；同时，对于易强迫用户做出选择的消极的收集行为进行了明确：一揽子授权、拒绝时影响其他业务功能、新增功能扩张同意范围时要求统一接受、游客模式拒绝提供所有服务。
2.在用户使用业务功能时，收集个人信息的频率等超出所使用的业务功能需要；	25.实际收集的个人信息类型是否超出隐私政策所述范围。 26.收集与业务功能有关的非必要信息，是否经用户自主选择同意。 27.是否收集与业务功能无关的个人信息。		
3.捆绑多项业务功能一揽子征求用户同意，不同意则不提供任何单一服务；	24.是否存在将多项业务功能和权限打包，要求用户一揽子接受的情形。		
5.如提供未经注册即可使用（如支持浏览、游客模式）的业务功能，用户若不同意收集此类业务功能所需以外的个人信息，App拒绝提供所有服务；	23.收集个人信息前是否征得用户自主选择同意。 24.是否存在将多项业务功能和权限打包，要求用户一揽子接受的情形。 27.是否收集与业务功能无关的个人信息。		
6.新增业务功能时，需收集的个人信息超出原有同意范围，如用户不同意收集，则拒绝提供原有业务功能，新增业务功能将取代原有业务功能的除外；	27.是否收集与业务功能无关的个人信息。		
8.其他收集与其提供的服务无关的个人信息的情形。	N/A		

（五）未经同意向他人提供个人信息的情形

条文	对应《指南》评估点	法律依据	评析
1.未经同意，且未做匿名化处理，从客户端直接向第三方提供个人信息，包括App客户端嵌入第三方代码、插件（如sdk）等方式向第三方提供；	22.若存在嵌入第三方代码插件收集个人信息的功能，是否向用户明示。	《网络安全法》第42条 《消费者权益保护法》第29条	本部分主要是对于未经同意向他人提供个人信息这一高危处理动作进行规制，明确界定两种违规方式：未经同意且未经匿名化处理直接提供和间接提供个人信息给第三方。
2.数据传输至App服务器后，未经同意，且未经匿名化处理，向第三方提供其收集的个人信息；	14.对外共享、转让、公开披露个人信息规则。		
3.其他未经同意向他人提供个人信息的情形。	N/A		

（六）未按法律规定提供删除或更正个人信息功能的情形

条文	对应《指南》评估点	法律依据	评析
1.未提供更正、删除个人信息，注销用户账号的功能；	15.用户权利保障机制。 30. 是否支持用户注销账号。 31. 是否支持用户查询、更正或删除个人信息。	《网络安全法》第43条、第49条 《电子商务法》第24条、第59条	本部分主要对于法律明确规定的更正、删除、注销账号的权利进行了规定，明确未提供该等功能、实践中无法保障及时有效落实更正、删除、注销权利的情形均为明确的违规。
2.对于提供在线操作方式、客服电话、电子邮件等方式的，进行相关操作未响应的；	32.是否及时反馈用户申诉。		
3.需人工处理的，受理后未在承诺时限内（无承诺时限的，以15个工作日为限）完成核查和处理的；	3.需人工处理的，受理后未在承诺时限内（无承诺时限的，以15个工作日为限）完成核查和处理的； 32.是否及时反馈用户申诉。		
4.更正、删除或注销操作提示完成后，依然未能更正、删除个人信息，注销用户账号的；	15.用户权利保障机制 30. 是否支持用户注销账号。 31. 是否支持用户查询、更正或删除个人信息。 32.是否及时反馈用户申诉。		
5.其他未采取措施予以删除或者更正的情形。	N/A		

（七）侵犯未成年人在网络空间合法权益的情形

条文	对应《指南》评估点	法律依据	评析
1. 未经监护人同意，收集使用14周岁以下(含)未成人个人信息；	20. 是否向用户明示收集、使用个人信息的目的、方式、范围 23.收集个人信息前是否征得用户自主选择同意	《网络安全法》第22条、第41条	《指南》中并未明确提及未成年人个人信息保护的内容[114]，该条的设置反映了群众和国家对于未成年人个人信息收集使用的关切，特别是其中涉及的定向推送活动。
2. 未经监护人同意，利用14 周岁以下(含)未成年人信息和算法开展个性化推送新闻、时政信息、广告等定向推送活动。	11.个人信息的使用规则[115]		

通过上述条文的分析，可以发现，本《认定方法》草案较之《指南》，旨在对以下明显的违规行为进行规制：隐私政策不够简明易得；未明示收集使用个人信息目的、方式和范围；违反必要性原则，收集与其提供的服务无关的个人信息；未经同意向他人提供个人信息；未提供删除、更正、注销的权利设置及配套有效的响应机制。在一定程度上对《网络安全法》及《指南》关注的规制重点提出了底线要求。除此之外，《认定方法》草案还格外强调了定向推送活动的选择退出机制和未成年人个人信息保护的内容，其中定向推送活动的选择退出机制与《个人信息安全规范》的修订部分以及《互联网个人信息安全保护指南》所体现的部分条款密切相关，涉及该等业务的企业应密切关注。

114. 但该内容在《规范》中有直接提及："5.5 c)收集年满14的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意。"
115. 如果App运营者将个人信息用于用户画像、个位化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。

SECTION 03

合规建议及应对策略

本次专项治理行动规模之大、范围之广、执法力度之强，或创下近年之最。四部门联合执法，四协会全面评估，公安部门严厉打击，市场监督部门安全认证，持续时间长达一年的综合治理，加强处罚违法违规行为的同时匹配规范性引导和政策性鼓励，这一系列的组合拳重击势必解决目前App强制授权、过度授权、超范围收集个人信息等突出问题，达到规范App市场的预期监管效果。

对于App开发者、运营者而言，着手调整产品设计环节的隐私保护，规范个人信息收集和使用规则，严格落实信息安全管理责任是目前亟待处理的问题。同时，应用商店、网盘、论坛贴吧等社交平台及云服务企业等网络平台运营者应当切实落实主体责任，针对平台接入的App及其发布信息进行真实性、安全性、合法性等审核，建立信用管理制度；督促应用程序提供者保护用户信息；发布合法信息内

容，建立健全安全审核机制；发布合法应用程序，尊重和保护应用程序提供者的知识产权。并通过服务协议，明确双方的权利义务，规避合规风险。App运营者及网络平台运营者应当配合有关部门依法进行监督检查，设置便捷的投诉举报入口，及时处理公众投诉举报。电信运营商、云服务提供商、域名管理机构亦有义务配合实施网信办等主管部门对相关违法违规APP的关停处罚。

除上述个人信息保护制度外，企业还应当重视《网络安全法》及其配套法律法规构建的系统性的网络安全和数据保护义务，主要包括：

落实网络安全等级保护制度；

网络传播内容的管理；

履行网络运营者网络安全保护义务；

关键信息基础设施认定和网络安全保护义务的履行；

个人信息和重要数据的保护；

数据本地化存储和跨境数据传输的安全评估；

网络产品和服务提供者的网络安全义务；

落实网络安全审查制度；

落实《网络关键设备和网络安全专用产品目录》及安全认证检测制度。

结语

建议企业尽快着手实施网络安全与数据保护的整体合规工作，对企业目前的合规现状进行摸底评估，有效识别相应法律风险，并针对合规漏洞建立健全整体的合规体系。对于企业而言，有效的系统合规梳理工作包括合规现状尽职调查与差距分析、风险识别及合规建议、合规方案的实施和优化三个阶段，做到组织、流程、制度和培训各环节环环相扣，同时应当与企业所在行业、产品及服务的特性有针对性的落实相关合规义务。

第三节

《信息安全技术个人信息安全规范（草案）》解读[116]

2019年2月1日，全国信息安全标准化技术委员会（以下简称“信安标委”）发布了《信息安全技术 个人信息安全规范（草案）》（以下简称“规范”），面向全社会公开征求意见。这次修订于2018年12月开始，距离2018年5月正式实施刚过半年，这其实是一件“好事”，说明它是一部“活”的规范。

116.原文标题为《实施半年后再修订：<信息安全技术个人信息安全规范>应时而变》，作者陈际红、韩璐，网址：http://www.zhonglun.com/Content/2019/03-04/1704042531.html。

SECTION 01

修改背景

事实上，《信息安全技术个人信息安全规范》已经被各个行业和企业在数据合规工作中广泛采用，为企业落地《网络安全法》提供了良好的实践指引，也成为监管部门管理和执法的重要参考依据。本次修订也是对新近相关立法的接轨。于2019年元旦正式实施的《电子商务法》规定，电子商务经营者“根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的，应当同时向该消费者提供不针对其个人特征的选项”。在此原则性规定的基础上，本次规范新增个性化展示及退出的相关机制，进一步细化电子商务及其他应用场景下对于个性化展示的操作规则，明确了产品及服务提供者利用其信息优势向用户定向推送时应当履行的合规义务。

与此同时，本次修订亦是对现今技术快速发展的积极回应。针对同一场景中多个企业都能同时获得用户个人信息的场景，规范在之前“委托处理”、“共同个人信息控制”两类场景的基础上，增加了日常生活中已十分常见的平台接入/嵌入第三方产品或服务的技术应用场景，为新型技术应用如何规范个人信息的收集和使用提出了切实可行的实操建议。

更为重要的是，本次修订也是对于过去两年执法成果的回应。规范结合了2017年、2018年的隐私评审[117]工作成果，并总结了近一年来规范适用中的经验，对市场上比较集中的几类违反个人信息保护原则的现象，如过度收集用户个人信息，强制授权、“一揽子授权”等突出问题提出了相应的合规标准。

117.2017年7月至9月，中央网信办、工信部、公安部和国家标准委针对国内互联网领先企业的10款App组织了首次App隐私政策专项评审工作。2018年12月，全国信息安全标准化技术委员会对40款网络产品和服务的隐私条款进行了2018年隐私条款专项评审工作。

SECTION 02

区分基本业务功能和扩展业务功能，保障个人信息主体选择同意权

《网络安全法》实施后，为了符合个人信息收集、使用的“明示”+“同意”的原则性要求（第四十一条、第四十二条），一些APP在首次安装时，往往将所有服务和业务功能捆绑在一起，通过用户对隐私政策的接受来获得“一揽子授权”，强迫用户一次性授权同意各项业务功能所收集的多种个人信息。用户若想使用其基本功能，必须全盘接受所有个人信息的收集和使用，否则只能退出软件，用户自身的选择同意权并未得到充分的体现。

本次规范提出产品和服务提供者应当区分产品的基本业务功能和扩展业务功能，明确过度收集、强迫收集、捆绑授权个人信息等乱象不符合法律和监管要

求。规范增加了“附录C保障个人信息主体选择同意权的方法”，明确了不同业务功能应用场景下不同的告知和明示统一的方法，并例举了交互式界面的设计模板。

规范要求产品和服务提供者应当根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求，来划定产品或服务的基本业务功能，而不应将改善服务质量、提升用户体验、研发新产品单独作为基本业务功能。当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不得违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。

产品和服务提供者收集基本业务功能所必要的个人信息时，除告知用户所必要收集的个人信息类型外，还应当告知用户拒绝提供授权所产生的影响，即企业可拒绝向用户提供该业务功能。而对于扩展业务功能所需的个人信息，产品和服务提供者应当允许个人信息主体对扩展业务功能逐项选择同意，如个人信息主体不同意收集扩展业务功能收集所必要的个人信息，不得拒绝提供基本业务功能或降低基本业务功能的服务质量。

2019年1月25日中央网信办、工业和信息化部、公安部、市场监管总局联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》(以下简称“公告”)，决定自2019年1月起至12月，在全国范围组织开展持续时间长达一年的App违法违规收集使用个人信息专项治理行动，旨在解决目前App强制授权、过度授权、超范围收集个人信息等突出问题。其中公告指出，本次专项治理行动将由全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，组织相关专业机构，编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，作为本次评估工作的主要依据。

而本次规范修订正与上述四部门联合开展个人信息专项治理的工作要求相一致，为公众提供了区分基本业务功能和扩展业务功能的判断标准及方式，为企业自查及合规整改提供了良好指引。

SECTION 03

明确平台商对于接入的第三方产品或服务收集个人信息的管理义务

2018年5月正式实施的《个人信息安全规范》对“委托处理”、“共同个人信息控制”两类场景的合规操作进行了规定。目前，应用程序中接入/嵌入第三方产品或服务的应用场景十分常见，一旦发生合规漏洞，平台商和第三方往往无法明确双方的责任和义务，而数据主体往往很难去追究第三方产品或服务提供商的责任。为

顺应新技术、新产品形态的发展，本次规范结合了行业良好实践及主管部门的监管态度，提出平台商作为个人信息控制者应当履行一定的合规义务，具体如下：

应建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件；

应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施；

应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅；

应要求第三方根据本标准相关规定要求向个人信息主体征得收集个人信息的授权同意，核验其实现本项要求的方式；

应要求第三方产品或服务建立响应个人信息主体请求、申诉等的机制，并妥善留存、及时更新，确保个人信息主体查询、使用；

应督促和监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；

涉及第三方嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜开展技术检测确保其个人信息收集、使用行为符合约定要求，并对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定行为的及时切断接入。

去年12月，某旅游住宿类应用软件因用户使用平台内嵌小程序时，未向用户告知个人信息收集使用规则，便默认开通会员等问题，被工信部约谈并要求立即整改。可见，对于此类第三方产品或服务嵌入的问题，平台商应尽更为严格的合规义务。建议产品和服务提供商完善相应的管理机制和工作流程，明确双方在个人信息保护合规问题上的责任和义务。

SECTION 04

新增个性化展示及退出机制

针对目前较为常见的基于用户画像作定向推送、个性化展示等个人信息应用场景，规范首次阐释了“个性化展示”的定义，并细化了相应的操作规则。“个性化展示”是基于特定个人信息主体（用户）的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

对于“个性化展示”的操作规则，规范划分为“向个人信息主体推送新闻或信息服务的个性化展示“，”电子商务经营者提供商品或者服务搜索结果的个性化展示“以及普遍意义上”向个人信息主体提供业务功能的过程中使用个性化展示“三

大应用场景。其中，针对电子商务场景下的个性化展示，规范与2019年1月1日正式实施的《电子商务法》的立法原则保持一致，即“电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益”（《电子商务法》第十八条）。

同时，对于产品推送新闻或提供信息服务的应用，规范要求个人信息控制者应当以显著方式标明“个性化展示”或“定推”等字样向用户明示，并为个人信息主体提供简单直观的退出个性化展示模式的选项。此举一定程度上保证了个人信息主体对于定向推送的自主选择，避免形成信息孤岛。同时，对于普遍意义上的个性化推送，规范还建议个人信息控制者宜建立机制保证个人信息主体可以删除或匿名化处理个性化展示活动所依赖的个人信息。这就从定向推送的深层基础规范了产品或服务提供者对用户画像的控制界限，提出了用户可以拒绝产品或服务提供者收集其个人信息进行特定的画像处理的良好实践模式。

SECTION 05

细化个人信息安全事件报告制度

《网络安全法》要求网络运营者“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“（第四十二条）。《国家网络安全事件应急预案》也对特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件四个等级的网络安全事件应对措施进行了详细规定。

但实践操作中，一旦发生个人信息泄露等安全事件，企业往往无法判断告知个人信息主体及上报监管部门的界限。本次修订试图弥补相应细则的缺失，提出了判断”告知“及”上报“的依据，即通过确认个人信息泄露的程度、对个人信息主体所造成的影响，涉及的个人信息数量（超过100万人的个人信息）和影响范围（关系国计民生、公共利益的）等几个因素来判断。对于像基因、生物特征信息、疾病等个人敏感信息的泄露、毁损、丢失的安全事件，应当向个人信息主体逐一告知，并依照规范的要求向网信部门报告。

SECTION 06

进一步细化个人信息控制者的组织管理要求

组织措施是数据合规中重要的方面。本次修订明确了个人信息控制者应当任

命个人信息保护负责人，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作，同时要求企业应为个人信息保护负责人和个人信息保护工作机构提供必要的资源，保障其独立履行职责。规范对个人信息保护负责人和个人信息保护工作机构应履行的职责也作了详细规定。

于此同时，规范提倡个人信息控制者建立、维护和更新所收集、使用的个人信息处理活动记录，将所涉及个人信息类别、数量、来源、处理目的、使用场景，以及委托处理、共享、转让、公开披露、是否涉及出境、各环节相关的信息系统、组织或人员等情况形成系统的活动记录，不仅对于企业内部合规整改工作提供参考，更是为企业一旦发生个人信息泄露等安全事件时的责任分担提供有效依据。此要求与GDPR中的数据处理活动的记录要求也是一致的。

去年11月，某知名房地产经纪公司员工冒用客户信息办理北京居住证一案在北京朝阳法院开庭审理。针对房屋中介侵犯客户个人信息的违法行为，法院认为房地产经纪公司主要利用信息优势地位，为房地产市场租售双方提供信息匹配的居间服务，在利用客户信息获取利益的同时，需承担高于一般主体的保管义务。而作为管理者，公司未建立信息安全管理制度和操作规程，未对客户信息安全进行风险提示、未对客户敏感信息进行加密处理，亦未采取任何实际有效的措施防控风险，导致员工可轻易将业主个人信息泄露用于非法目的。本案侵权事实的发生与公司内部监管漏洞直接相关，公司管理存在过错，应承担侵权责任，确定经济损失赔偿金10万元[118]。

基于此案所暴露出的房地产中介行业存在的普遍问题，朝阳法院对北京市住房和建设委员会出具了司法建议书，建议完善房地产中介行业管理制度，并提出房地产中介机构应当建立健全公民个人信息安全管理制度和从业人员信息操作规范，设立信息传输时的加密处理机制，规范履行合同过程中对公民个人信息的保护，明确信息保管的责任人等。

由此可见，产品或服务提供者建立健全内部数据合规体系，尤其是健全个人信息内部操作规范，提高自身的合规审慎义务，已经成为企业必不可少的合规重点。规范在此现实意义下，提倡企业建立、维护和更新所收集、使用的个人信息处理活动记录，并明确了活动记录的具体内容，为企业合规提供了更为详细的指引。

118.来源：http://finance.sina.com.cn/chanjing/gsnews/2018-11-20/doc-ihnyuqhi4219644.shtml

SECTION 07

个人信息的汇聚融合

所谓个人信息的汇聚融合，对于数据控制者而言，就是把不同产品线、不同来

源或基于不同目的所收集的数据聚集在一起，形成“大”数据，以增强企业的数据能力，或者是更好地了解和服务客户。目前在业界“企业平台化”和“市场精准化”的趋势下，数据汇聚融合行为已经非常普遍，也是不可逆转的技术方向。但是，数据的汇聚融合，很有可能侵犯数据主体的合法权益，比如超范围使用、非授权目的的使用等。基于此，规范并没有“封杀”数据汇聚融合，而是提出了具体的要求：

非获得授权业务的必要，一般应采用间接画像；

数据加工处理后，如仍具备个人识别（单独或结合）能力，则还应作为个人信息对待，受授权范围的约束；

如数据的汇聚融合的使用行为超出了已获得授权的范围，则应当重新获得授权；

应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估（PIA）。

SECTION 08

意外地删除无需征得授权同意之“履行合同必要”的情形

本次规范针对原有个人信息控制者收集、使用个人信息无需征得个人信息主体的授权同意的几类情形作了两处修改：一是将“法律法规规定的其他情形”修改为“与个人信息控制者履行法律法规规定的义务相关的”；二是删除了履行合同必要之例外，即“ 根据个人信息主体要求签订和履行合同所必需的情形”。

对于第一处的修订，我们认为个人信息控制者收集、使用个人信息，将其“征得授权同意的例外”的条件界定为与个人信息控制者履行其法律义务相关而不论其它场景，是合适的，也可以避免该例外的滥用。

对于第二处删除“征得授权同意的例外”之“履行合同必要”，我们认为该修订可能会带来不必要的社会成本。一般情况下，可以认为合同的各方基于履行合同义务而向合同相对方提供签约和履约所必要的个人信息，这是善意履约的表现。于此同时，提供个人信息的一方一般也具有相应的心理预期。在GDPR中也有基于“履行合同必要”而无需另行征得个人信息主体的授权同意的类似规定。尽管有专家质疑此类例外规定与《网络安全法》所确定的“授权同意”规则相冲突，但我们理解所谓的“授权同意”规则，应当既包括书面合同的授权同意，也包括通过实际行为作出的授权同意，签约、履约即是如此，因此它们之间并没有实质性冲突。

同时，我们也担心“履行合同必要”作为“征得授权同意的例外”可能会导致一系列滥用问题，尤其是对于C端消费者面对大平台的情形。对此，我们建议对该例

外的适用增加一个条件限定，即："根据个人信息主体要求签订和履行合同所必需的，且该个人信息的收集和使用符合一般个人信息主体的理解和预期。" 如此，既可以消除滥用之担忧，又便利于商业交易。

结语

《网络安全法》规定了我国个人信息保护的基本框架，即"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"。国家标准《个人信息安全规范》在此基础上结合国际通用的个人信息和隐私保护理念，提出了"权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与"七大原则，为企业完善内部个人信息保护制度及实践操作规则提供了更为细致的指引，自其正式发布以来被广泛应用于各行各业的合规实践中。尽管《个人信息安全规范》属于国家推荐标准，但其作为监管部门网络安全管理和执法的参考依据的重要性不言而喻。建议企业结合《个人信息安全规范》的良好实践指引，逐步提高个人信息保护水平，为其产品与服务保驾护航。

第四节

《个人信息出境安全评估办法（征求意见稿）》述评[119]

119.原文标题为《打造中国版的SCC | <个人信息出境安全评估办法（征求意见稿）>评析》，作者陈际红。

2019年6月13日，国家互联网信息办公室发布《个人信息出境安全评估办法（征求意见稿）》，邀请社会各界在7月13日前提出意见。自2017年4月发布《个人信息和重要数据出境安全评估办法（征求意见稿）》（"旧办法"）后，关于数据跨境传输的监管一直是网络运营者（尤其是跨国企业）的关注焦点，旧办法几易其稿，仍未获得多方利益相关方的认可。同时，在国际化和数字化的大时代背景下，数据跨境传输不可避免，其监管制度的落地一直是困扰跨国公司的一个重大问题。

SECTION 01

推倒《个人信息和重要数据出境安全评估办法》架构，另起炉灶

《个人信息出境安全评估办法（征求意见稿）》（"新办法"）与旧办法相比，有以下实质性变化，可以说是另起炉灶：

（一）个人信息和重要数据分开监管

个人信息跨境传输的监管主要关乎于个人信息主体的权利行使，而重要数据的保护则以国家安全和公共利益为主要考量，二者的价值取向不同，立法重点也应当不同。因此，个人信息和重要数据分开监管是一个恰当的思路，且制定个人信息跨境保护机制中，可以设定恰当的民事权利义务和便利的个人信息主体行权渠道为主要思路。而对于重要数据的跨境监管，应当以行政监管为主要手段。

（二）摒弃了原有的两层安全评估机制

旧办法就数据出境规定了自评估和监管机构评估的两层架构，涉及数据出境的网络运营者，均要自行组织对数据出境进行安全评估，出境数据达到法定标准的，网络运营者应报请行业主管或监管部门组织安全评估。而在新办法中，个人信息出境前，网络运营者均需要向网信部门申报个人信息出境安全评估。

（三）删除了事先经数据主体同意的要求

旧办法要求，个人信息出境前，应向个人信息主体说明数据出境的事项并经其同意，而新办法则仅要求网络运营者告知个人信息主体数据出境的情况。

这些变化反映了最近国际形势的变化及监管部门监管思路的演变。

SECTION 02

中国版的“标准合同条款SCC”机制若隐若现

从《个人信息出境安全评估办法（征求意见稿）》条款中，不难看出GDPR“标准合同条款SCC”的影子。欧盟委员会根据95指令第26条第4款，先后通过了4个版本的标准合同条款，即SCC2001C、SCC2004C、SCC2001P以及SCC2010P。欧盟对SCC的基本思路是通过合同的权利义务安排，弥补跨境传输后对数据法定保护的不足，设定一个基于合同条款的、对数据主体充分保护的机制。

在保障标准合同条款执行机制方面，通过合同条款设定数据控制者和处理者面向数据主体的民事义务，及面向监管机关的行政义务。如果数据控制者或处理者违反合同条款的义务和责任，则会面临民事赔偿责任和行政处罚责任。

在新办法中，采用了与SCC类似的机制：

网络运营者与境外个人信息接收者需要签订数据合同，且需要向网信部门申报；

数据合同应当规定数据出境的明确场景（目的、类型、保存时限）；

数据合同中应当明确规定网络运营者和数据接收方所承担的责任和义务；

数据合同中应当设定个人信息主体是个人信息主体权益条款的受益人，且具

有索赔的权利；

赋予个人信息主体知情权，应个人信息主体的请求，网络运营者应提供数据合同的副本；

赋予监管机构的监管和处罚权力，网信部门可以检查数据合同规定义务的履行情况、是否存在违反国家规定或损害个人信息主体合法权益的行为等。

基于该机制与SCC实质的类似性，可以将新办法确定的数据跨境机制称为中国版的SCC。

但是，中国版的SCC与GDPR的SCC机制也存在着实质性差异。GDPR的SCC机制，主要依赖于通过合同设定民事权利和义务来督促数据控制者达到较高的数据保护水准，而行政监管行为的介入以事后或事件驱动为主要方式。而在中国的监管方案中，行政监管的有形之手会贯穿整个数据周期。对此，下文会做详细的介绍。

SECTION 03

未解决的难点：数据主体如何行使权利？

新办法规定，个人信息主体是合同中涉及个人信息主体权益的条款的受益人，个人信息主体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。对此，我们理解数据合同是双方合同，即网络运营者和数据接收者之间的合同。而根据合同的相对性原则，合同所设定的权利义务关系仅约束于合同双方，对第三方并不产生效力。因此，新办法的框架下，个人信息主体作为受益人及赋予损害赔偿的请求权，是否会产生法律上的障碍？

第三方受益人规则赋予受益于合同履行的非合同相对方对合同违约方提起诉讼的权利，可请求法院强令其履行义务的权利。在我国，运用第三方受益人规则还缺乏理论上的研究及司法上的实践，其是否可行，仍待立法和司法实践。

SECTION 04

有形之手的行政监管贯穿整个数据周期

与GDPR项下的SCC机制不同，在新办法的框架下，行政机构对数据跨境传输的监管贯穿整个数据周期，这也可能是目前中国数据保护水平和司法有效性的现状所决定的。

网信部门作为主要的数据监管部门，对数据跨境传输会有以下监管节点：

省级网信部门在收到个人信息出境安全评估申报材料并核查其完备性后，应

当组织专家或技术力量进行安全评估；

网络运营者应当每年12月31日前将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门；

发生较大数据安全事件时，应及时报所在地省级网信部门；

定期组织检查网络运营者的个人信息出境记录；

出现违法情况，网信部门可以要求网络运营者暂停或终止向境外提供个人信息；

接受对违反本办法向境外提供个人信息的行为的举报。

需要讨论的一个问题是，效率和安全的平衡问题。在当今时代，各种类型企业都有数据跨境传输的需求，因此，在保障数据安全的前提下，努力保持数据传输的便利性应当是立法的一个价值取向。在新办法确定的制度下，跨境数据传输的便利性、效率都会打折扣，企业的运营成本也会显著提高。另一方面，面对如此大量的安全评估需求，监管部门的监管能力和行政成本也是需要考虑的问题。

基于此，我们建议建立一个例外的机制，对于中小企业或小规模、偶尔的跨境数据传输，应当从新办法的严格要求的程序中剥离出来，给予豁免。

SECTION 05

问题与思索

新办法中也有几个问题值得讨论。

一是关于境外机构的监管。按照新办法第二十条规定，境外机构经营活动中，通过互联网等收集境内用户个人信息，应当在境内通过法定代表人或者机构履行本办法中网络运营者的责任和义务。跨境电商作为目前常见的一种电子商务方式，交易双方身处不同的法域，通过跨境交付的方式完成交易。而对于境外的网络运营机构，是否要进行一致性的监管是值得思考的。我们认为，对于有目的开拓中国市场的境外机构，比如说有中文语言、人民币支付或境内物流，则可纳入监管范围；而对于无意于开拓中国市场的机构，即使发生了零星的跨境交易，也无须进行监管。境外机构在境内受监管的联系主体，不必是其法定代表人，任命能够代表公司的代表即可。

二是关于救济权利。新办法规定，网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的，可以向国家网信部门提出申诉。那么对于申诉结果仍存在异议的，网络运营者是否享有诉权?我们认为，如若将网信部门的评估行为认定为行政行为的话，就应当赋予诉权。

三是关于境外接收者向第三方的数据传输。新办法规定，境外接收者不得将接收到的个人信息传输给第三方，但满足特定条件的可以向第三方传输。向第三

方传输只是一个行为界定，产生的后果可能是数据共享、数据转让、数据公开和数据委托处理等。对于允许向第三方传输的例外情形的规定，还应当细化到不同的场景，据此确定具体的条件，不能一概地给予例外。唯有此，才符合网络安全法所规定的授权同意的要求。

结语

国家互联网信息办公室在5月28日发布的《数据安全管理办法（征求意见稿）》提出将重要数据的出境评估及行业主管部门或网信部门的批准作为重要数据出境的基本监管原则。此次《个人信息出境安全评估办法（征求意见稿）》提出的个人信息出境监管新框架，进一步体现了监管部门的监管新思路。

第五节 《互联网个人信息安全保护指南》述评[120]

120.原文标题为《管理措施和技术措施的平衡：<互联网个人信息安全保护指南>》，作者陈际红、吴佳蔚，网址：http://www.zhonglun.com/Content/2019/04-26/1522255455.html。

2019年开年伊始，作为主要执法机构之一的公安部于2019年4月发布了《互联网个人信息安全保护指南》（以下简称《保护指南》），旨在有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，供互联网服务单位在个人信息保护工作中参考。实际上，公安部早在2018年11月30日发布了《互联网个人信息安全保护指引（征求意见稿）》（以下简称《保护指引》），作为保护指南的前身，保护指引主要结合了《个人信息安全规范》和《信息系统安全等级保护基本要求》两部国家标准的要求对于个人信息保护工作进行规范。最终出台的保护指南的文本与保护指引相比，整合了《个人信息安全规范》和《网络安全法》关于等级保护、内容治理、重要数据以及跨境数据传输方面的要求，还就安全事件响应部分另设单节，对于《网络安全法》中关于安全事件管理的环节进行了更为具化的落实，呈现出技术措施和管理措施相结合的趋势。

SECTION 01

适用范围

保护指引	保护指南	评析
本指引规定了个人信息安全保护的安全管理机制、安全技术措施和业务流程的安全。 本指引适用于指导个人信息持有者在个人信息生命周期处理过程中开展安全保护工作，也适用于网络安全监管职能部门依法进行个人信息保护监督检查时参考使用。	本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。 适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。	保护指南与保护指引的范围基本相同，仅在适用对象方面有所区分，保护指南明确适用对象包括互联网企业和专网或非联网环境控制和处理个人信息的组织或个人，删除了保护指引中原有的执法监督检查时参考使用的环节，强调了保护指南的参考作用。

SECTION 02

规范性引用文件

保护指引	保护指南	评析
下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。 凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。 GB/T22239—2008 信息安全技术 信息系统安全等级保护基本要求 GB/T25069—2010　信息安全技术 术语 GB/T35273—2017　信息安全技术 个人信息安全规范	下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。 GB/T25069—2010　信息安全技术 术语 GB/T35273—2017　信息安全技术 个人信息安全规范 GB/T22239 信息安全技术 网络安全等级保护基本要求（信息系统安全等级保护基本要求）	保护指南最终删除了等保基本要求规范的日期限制，我们理解这与等保标准的修订进程有关，企业需要保持密切关注。

SECTION 03

术语和定义

保护指引	保护指南	评析
3.1个人信息[121] 3.2个人信息主体 3.3个人信息生命周期：包括个人信息主体收集、保存、使用、委托处理、共享、转让和公开披露、销毁个人信息在内的全部生命历程。 3.4个人信息持有者：对个人信息进行控制和处理的组织或个人。	相较保护指引新增： 3.9个人信息处理系统 处理个人信息的计算机信息系统，涉及个人信息生命周期一个或多个阶段（收集、保存、应用、委托处理、共享、转让和公开披露、删除）。	保护指南最终就个人信息的定义引用了网安法的规定（保护指引引用了个人信息安全规范），并新增了个人信息处理系统的定义，除此之外，二者并无显著区别。但它们都提出了个人信息持有和持有者的概念，持有者包括个人信息安全规范中提及的控制者和处理者，此外还对个人信息生命周期进行了定义。

121.关于保护指南和保护指引中与《个人信息安全规范》基本一致的定义我们不再赘述，仅在此列明其新设的定义，以下条文皆同。

保护指引	保护指南	评析
3.5个人信息持有：对个人信息及相关资源、环境、管理体系等进行计划、组织、协调、控制的相关活动或行为。 3.6个人信息收集 3.7个人信息使用 3.8个人信息删除		

SECTION 04

管理机制

保护指引	保护指南	评析
4.1管理制度 4.1.1管理制度内容 4.1.2管理制度制定发布 4.1.3管理制度执行落实 4.1.4管理制度评审改进 4.2管理机构 4.2.1管理机构的岗位设置 4.2.2管理机构的人员配置 4.3管理人员 4.3.1管理人员的录用 4.3.2管理人员的离岗 4.3.3管理人员的考核 4.3.4管理人员的教育培训 4.3.5外部人员访问	新增： 4.1 基本要求 个人信息处理系统的安全管理要求应满足GB/T 22239相应等级的要求。	保护指南最后增加了4.1满足等级保护相应规定的总体要求，其他的要求基本保持不变，仅在内部顺序和内容组织上进行了微调。

SECTION 05

技术措施

保护指引	保护指南	评析
5.1基本要求 应按照GB/T 22239—2008 7.1第三级的物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复要求进行安全保护，并满足以下要求：	5.1 基本要求 个人信息处理系统其安全技术措施应满足GB/T 22239相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务，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。	与4.管理机制的修改思路保持一致，保护指南强调了应满足等保技术标准相应等级的要求，与保护指引统一采取第三级等保这一较高标准的要求不同，要求处理系统按照其相应等级履行义务，给予企业根据自身的保护等级和风险大小予以适当保护的空间，更加符合网安法等级保护制度。
5.1.1 网络和通信安全 5.1.1.1 网络架构 5.1.1.2 通信传输 5.1.1.3 边界防护 5.1.1.4 访问控制 5.1.1.5 入侵防范	5.2 通用要求 5.2.1 通信网络安全 5.2.1.1 网络架构 5.2.1.2 通信传输 5.2.2 区域边界安全 5.2.2.1 边界防护	就通用要求而言，基本源自等级保护标准中与数据保护相关的内容，具体内容上保护指南与之前相差不大，仅做了体系上和逻辑上的微调。 保护指南新增了关于个人信息云

保护指引	保护指南	评析
5.1.1.6 恶意代码和垃圾邮件防范 5.1.1.7 安全审计 5.1.2 设备和计算 5.1.2.1 身份鉴别 5.1.2.2 访问控制 5.1.2.3 安全审计 5.1.2.4 入侵防范 5.1.2.5 恶意代码防范和程序可信执行 5.1.2.6 资源控制 5.1.3 应用和数据 5.1.3.1 身份鉴别 5.1.3.2 访问控制 5.1.3.4 软件容错 5.1.3.5 资源控制 5.1.3.6 数据完整性 5.1.3.7 数据保密性 5.1.3.8 数据备份恢复 5.1.3.9 剩余信息保护 5.2 增强要求 5.2.1 云计算安全增强要求 5.2.2 物联网安全扩展增强要求	5.2.2.2 访问控制 5.2.2.3 入侵防范 5.2.2.4 恶意代码防范 5.2.2.5 安全审计 5.2.3 计算环境安全 5.2.3.1 身份鉴别 5.2.3.2 访问控制 5.2.3.3 安全审计 5.2.3.4 入侵防范 5.2.3.5 恶意代码防范和程序可信执行 5.2.3.6 资源控制 5.2.4 应用和数据安全 5.2.4.1 身份鉴别 5.2.4.2 访问控制 5.2.4.3 安全审计 5.2.4.4 软件容错 5.2.4.5 资源控制 5.2.4.6 数据完整性 5.2.4.7 数据保密性 5.2.4.8 数据备份恢复 5.2.4.9 剩余信息保护 5.3扩展要求 5.3.1 云计算安全扩展要求 新增：a)应确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定； 5.2.2 物联网安全扩展增强要求	平台存储的要求，一是确保数据本地化存储（云计算的IDC要在境内），二是如需出境，则还要遵循数据出境的监管规定。

SECTION 06

业务流程

	保护指引	保护指南	评析
6.1收集	个人信息的收集行为应满足以下要求： a)个人信息收集前，应向被收集的个人信息主体公示本机构收集的目的、范围、方法和手段、处理方式等信息； b)个人信息收集应获得个人信息主体的同意和授权； c)个人信息收集应执行收集前签署的约定和协议，不应有超范围收集的现象； d)应确保收集个人信息过程的安全性： 1）收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全	个人信息的收集行为应满足以下要求： a)个人信息收集前，应当遵循合法、正当、必要的原则向被收集的个人信息主体公开收集、使用规则，明示收集、使用信息的目的、方式和范围等信息； b)个人信息收集应获得个人信息主体的同意和授权，不应收集与其提供的服务无关的个人信息，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息； c)个人信息收集应执行收集前签署的约定和协议，不应超范围收集；	1.增加了网安法项下规定的收集原则，使用明示而非公示的表述，结合了APP自查指南的规定，对于收集无关信息，捆绑授权的现象进一步作出了禁止； 2.对于生物识别信息等个人敏感信息进一步做出了降低风险进行收集的要求； 3.对于大规模收集公民的敏感数据进行了禁止，与网安法项下的重要数据制度或可相关； 4.与《个人信息安全规范》相比，强调了等保及内容管理相关的技术措施。

	保护指引	保护指南	评析
	性； 2）收集个人信息时，信息在传输过程中应进行加密等保护处理； 3）收集个人信息的系统应落实网络安全等级保护要求； 4）收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。	d）不应大规模收集或处理我国公民的种族、民族、政治观点、宗教信仰等敏感数据； e）个人生物识别信息应仅收集和使用摘要信息，避免收集其原始信息； f）应确保收集个人信息过程的安全性： 1）收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全性； 2）收集个人信息时，信息在传输过程中应进行加密等保护处理； 3）收集个人信息的系统应落实网络安全等级保护要求； 4）收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。	
6.2保存	个人信息的保存行为应满足以下要求： a）收集到的个人信息应采取相应的安全加密存储等安全措施进行处理； b）应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限； c）应对保存的个人信息在超出设置的时限后予以删除； d）保存信息的主要设备，应对个人信息数据提供备份和恢复功能，确保数据备份的频率和时间间隔，并使用不少于以下一种备份手段： 1）具有本地数据备份功能； 2）将备份介质进行场外存放； 3）具有异地数据备份功能。	个人信息的保存行为应满足以下要求： a）在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定； b）收集到的个人信息应采取相应的安全加密存储等安全措施进行处理； c）应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限； d）应对保存的个人信息在超出设置的时限后予以删除； e）保存信息的主要设备，应对个人信息数据提供备份和恢复功能，确保数据备份的频率和时间间隔，并使用不少于以下一种备份手段： 1）具有本地数据备份功能； 2）将备份介质进行场外存放； 3）具有异地数据备份功能。	1.增加了境内运营收集的个人信息本地化存储的要求； 2.与《个人信息安全规范》相比增加了备份的一些技术要求。
6.3应用	个人信息的应用应满足以下要求： a）对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息； 注：经过匿名化或脱敏的方式处理的个人信息数据可用于历史、统计或科学目的，可以超出与信息主体签署的相关使用协议和约定，但应提供适当的保护措施	个人信息的应用应满足以下要求： a）对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息；注：经过处理无法识别特定个人且不能复原的个人信息数据，可以超出与信息主体签署的相关使用协议和约定，但应提供适当的保护措施进行保护。	1.采取了网络安全法项下关于匿名化的表述； 2.增加了修改权删除权的行使效果描述； 3.关于自动化处理的用户画像进行了基本的规定，与《个人信息安全规范》7.10约束信息系统自动决策相比，对于可能对用户带来法律后果的应用提出了更进一步明确授权的要求（7.10仅要求提供申诉的

	保护指引	保护指南	评析
	进行保护。 b)个人信息主体应拥有控制本人信息的权限，包括：1） 允许对本人信息的访问； 2） 允许对本人信息的修改，包括纠正不准确和不完整的数据； c)应对个人信息的接触者设置相应的访问控制措施，包括： 1）对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限； 2） 对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等； 3） 对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。 d)应对必须要通过界面展示的个人信息进行去标识化的处理。	b)个人信息主体应拥有控制本人信息的权限，包括：1) 允许对本人信息的访问； 2) 允许通过适当方法对本人信息的修改或删除，包括纠正不准确和不完整的数据，并保证修改后的本人信息具备真实性和有效性； c)完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利；如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据； d)应对个人信息的接触者设置相应的访问控制措施，包括： 1) 对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限； 2) 对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等；3） 对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。 e)应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化的处理。	权利），但在实践中可能需要具体分析（如司法决策可能无需用户明确授权）；此外与《个人信息安全规范》2019修改草案7.4个性化展示及退出的规定也有所差异，仅确保其有反对或拒绝的权利（7.4还包括显著标识、提供不针对选项以及增强控制能力），这一点需要进一步关注《个人信息安全规范》的修订情况。
6.4删除	a)个人信息相关存储设备，应在个人信息超过保存时限之后进行删除； b)个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复； c)对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除； d) 废弃存储设备，应在进行删除后再进行处理。	a)个人信息在超过保存时限之后应进行删除，经过处理无法识别特定个人且不能复原的除外； b)个人信息持有者如有违反法律、行政法规的规定或者双方的约定收集、使用其个人信息时，个人信息主体要求删除其个人信息的，应采取措施予以删除； c)个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复； d)对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除； e)废弃存储设备，应在进行删除后再进行处理。	1.增加了匿名化的例外； 2.增加了个人信息主体有权要求非法收集使用个人信息的删除。

	保护指引	保护指南	评析
6.5 第三方委托处理	a) 在对个人信息委托处理时，不应超出该信息主体授权同意的范围； b) 在对个人信息的相关处理进行委托时，应对受托方的数据安全能力进行评估； c)对个人信息进行委托处理时，应签订相关协议要求受托方符合本规范； d)应向受托方进行对个人信息数据的使用和访问的授权； e)受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。	a)在对个人信息委托处理时，不应超出该信息主体授权同意的范围； b)在对个人信息的相关处理进行委托时，应对委托行为进行个人信息安全影响评估； c)对个人信息进行委托处理时，应签订相关协议要求受托方符合本文件； d)应向受托方进行对个人信息数据的使用和访问的授权； e)受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。	基本一致。
6.6 共享和转让	如存在个人信息共享和转让行为时，应满足以下要求： a)共享和转让行为应经过合法性、必要性评估； b)在对个人信息进行共享和转让时应进行安全影响评估，应对受让方的数据安全能力进行评估，并按照评估结果采取有效的保护个人信息主体的措施； c)在共享、转让前应向个人信息主体告知转让该信息的目的、数据接收方的类型等信息； d)在共享、转让前应得到个人信息主体的授权同意； e)应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记； f)在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，例如访问、更正、删除、注销等。	个人信息原则上不得共享、转让。如存在个人信息共享和转让行为时，应满足以下要求： a)共享和转让行为应经过合法性、必要性评估； b)在对个人信息进行共享和转让时应进行个人信息安全影响评估，应对受让方的数据安全能力进行评估确保受让方具备足够的数据安全能力，并按照评估结果采取有效的保护个人信息主体的措施； c)在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息； d)在共享、转让前应得到个人信息主体的授权同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外； e)应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记； f)在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，例如访问、更正、删除、注销等； g)当个人信息持有者发生收购、兼并、重组、破产等变更时，个人信息持有者应向个人信息主体告知有关情况，并继续履行原个人信息持有者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意。	根据《个人信息安全规范》对于授权同意的例外和收购、兼并、重组、破产等变更进行了增补规定。

	保护指引	保护指南	评析
6.7 公开披露	个人信息原则上不得公开披露。如存在该行为，应满足以下要求： a)公开披露行为应经过合法性、必要性评估； b)应对该行为进行安全影响评估，并按照评估结果采取有效的保护个人信息主体的措施； c)在披露前应向个人信息主体告知披露的目的、类型等； d)在公开披露前应得到个人信息主体的明示同意； e)应记录公开披露的信息内容，将公开披露情况中包括公开披露的日期、数据量、目的和数据接收方的基本情况在内的信息进行记录。	个人信息原则上不得公开披露。如经法律授权或具备合理事由确需公开披露时，应充分重视风险，遵守以下要求： a)事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施； b)向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外； c)公开披露个人敏感信息前，除6.7 b)中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容； d)准确记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等； e)承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任； f)不得公开披露个人生物识别信息和基因、疾病等个人生理信息； g)不得公开披露我国公民的种族、民族、政治观点、宗教信仰等敏感数据分析结果。	1.补充了公开这一高危处理动作的例外情形； 2.补强了关于个人敏感信息告知的内容，要求对于生物识别信息等个人生理相关的个人敏感信息不得公开披露； 3.要求公开披露的持有者需要承担公开披露造成个人信息主体合法权益造成损害的责任； 4.不得公开我国公民的敏感数据分析结果与网安法项下的重要数据制度或可相关。

SECTION 07

应急处置

保护指引	保护指南	评析
6.8 应急处置 a)应建立健全网络安全风险评估和应急工作机制； b)应制定网络安全事件应急预案； c)应定期组织相关个人信息事件安全事件演练； d)应制定相关制度信息，在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制； e)应对进行个人信息处理的相关内部人员进行应急响应培训和应急演练； f)应了解知晓应急处置策略和规程；	7.1应急机制和预案 a)应建立健全网络安全风险评估和应急工作机制，在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制； b)应制定个人信息安全事件应急预案，包括应急处理流程、事件上报流程等内容； c)应定期（至少每半年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程，留存应急培训和应急演练记录； d)应定期对原有的应急预案重新评估，修订完善。	将应急处置分为应急机制和预案、处置与相应两个部分，对于应急机制中的培训对象、应急培训演练的周期、评估审计机制做出了详细规定。

保护指引	保护指南	评析
g)应记录信息安全事件信息，在应急事件发生后对事件内容进行记录，包括发现事件的人员、事件、涉及的个人信息和人数、发生事件的系统名称等； h)应对事件造成的影响进行评估，并采取必要的措施对事态进行控制； i)应将事件的情况告知受影响的个人信息主体。	7.2处置和响应 a)发现网络存在较大安全风险，应采取措施，进行整改，消除隐患；发生安全事件时，应及时向公安机关报告，协助开展调查和取证工作，尽快消除隐患； b)发生个人信息安全事件后，应记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门； c)应对安全事件造成的影响进行调查和评估，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； d)应按《国家网络安全事件应急预案》等相关规定及时上报安全事件，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式； e)应将事件的情况告知受影响的个人信息主体，并及时向社会发布与公众有关的警示信息。	根据网络安全法项下关于安全事件管理的规定和《国家网络安全事件应急预案》对于处置和响应进一步细化，强调了事件发生前风险隐患的自查整改和发生时的及时汇报；细化了事件记录的要求和技术措施所达到的效果；对于安全事件的上报项目进行了明确规定；并且要求向社会发布警示。

结语

2019年开年伊始，就个人信息安全保护治理行动，各部门动作频频。继1月份中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，及由此成立的App违法违规收集使用个人信息专项治理工作组发布的《App违法违规收集使用个人信息自评估指南》之后，作为主要执法机构之一的公安部应时而动，发布《互联网个人信息安全保护指南》。结合公安部日前开展的旨在打击违法违规收集使用个人信息、涉嫌赌博、直播领域低俗表演等问题开展专项治理的“净网2019”专项行动，不难看出，公安部将在本年度的重点工作中加强对于互联网服务单位信息安全管理义务和个人信息保护义务的监督管理。

经过对保护指南征求意见阶段的文本和正式指南文本的比较，公安部门在对于个人信息保护的规范文件上呈现出了与网络安全法其他制度尤其是等级保护制度结合更为紧密的趋势，企业外部的个人信息不合规操作很可能导致公安部门对整个企业的等级保护义务落实情况进行彻底的清查，从而导致更高的合规风

险。此外，指引加强了关于个人信息安全事件和网安法项下安全事件管理义务的联系，细化了关于个人信息安全事件的具体要求。最后，保护指南还体现出公安部门对于数据本地化与跨境转移以及与个人信息相关的重要数据的初步管理态势，建议企业持续跟进配套法规的更新。

简言之，在企业进行数据合规工作中，《个人信息安全规范》和《互联网个人信息安全保护指南》都是值得参考的指引性文件，一个着重于管理措施，一个增强了技术措施的指引，两个相互补充，相得益彰。

第六节 未成年人个人信息保护述评[122]

随着以教育、学习为主要应用场景的移动互联网应用（“APP”）快速发展，在提高教学水平、满足学生个性化学习需求的同时，一些数据滥用、强制授权、平台垄断等乱象也日益凸显。2019年8月10日教育部等八部门联合发布了《关于引导规范教育移动互联网应用有序健康发展的意见》[123]，针对近两年教育类APP的监管工作提出了总体部署方案，从备案管理、内容审核、数据保护、网络安全等多个层面提出了规范性意见。2019年8月22日，国家互联网信息办公室（“网信办”）发布了《儿童个人信息网络保护规定》[124]，作为《中华人民共和国网络安全法》（“《网络安全法》”）的配套法规，对14周岁以下未成年人[125]的个人信息保护进行规范，并在2019年10月1日实施。

SECTION 01 在校学生个人信息保护焦点事件不断

近期，国内外均发生了学校部署人脸识别系统用于日常考勤及纪律管理，从而引发较大争议的事件。人脸识别技术的合理运用、学生个人信息（尤其是面部识别特征等个人敏感信息）收集及使用的合规性问题值得相关企业重点关注。

（一）国内某大学利用人脸识别技术管理学生日常考勤引起舆论关注

国内某大学于今年8月下旬在学校各大校门、学生公寓、试点教室等部分场所安装了人脸识别系统收集学生的面部识别特征等个人敏感信息，以支持门禁管理、日常考勤等管理目的，引发了社会舆论的高度关注[126]。从个人信息保护角度出发，该应用场景涉及的个人信息主体数量较大、数据类型高度敏感、数据使用目的

122.本文综合了两篇文章的内容，第一篇标题是《儿童个人信息保护新规出台，与COPPA的明示同意区别有哪些》，作者陈际红、吴佳蔚、罗芸，网址：http://www.zhonglun.com/Content/2019/06-06/1404027237.html；第二篇标题是《未成年人个人信息保护：案例、监管与合规》，作者陈际红、韩璐、薛泽涵，网址：http://www.zhonglun.com/Content/2019/09-29/0909467556.html。

123.该规定由教育部、中央网信办、工业和信息化部、公安部、民政部、市场监管总局、国家新闻出版署、全国“扫黄打非”工作小组办公室等八个部门联合发布，于发布之日（2019年8月10日）起生效，详见http://www.cac.gov.cn/2019-09/05/c_1569218551238246.htm。

124.详见http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

125.《儿童个人信息网络保护规定》第二条 本规定所称儿童，是指不满十四周岁的未成年人。

126.中国药科大学新闻网《我校在江苏省高校中率先全面使用人脸识别系统》http://news.cpu.edu.cn/d4/b4/c243a119988/page.htm 人民网《中国药科大学用人脸识别考勤引争议 校方回应》：http://js.people.com.cn/n2/2019/0903/c360307-33317868.html?-from=singlemessage

多样，主要存在以下争议：

第一，通过收集学生面部识别特征等个人敏感信息以实现日常考勤与课堂纪律管理，是否满足《网络安全法》规定的正当、必要的原则[127]，以及《GB/T 35273-2017　信息安全技术-个人信息安全规范》（"《个人信息安全规范》"）规定的最小必要要求[128]；

第二，学校及相应系统供应商对学生面部识别特征等个人敏感信息的收集和使用是否已具备合法基础，即是否获得学生或其监护人[129]的授权同意。进一步来说，面对学校与学生之间"不对等"的主体关系，如何满足相应授权同意的真实有效；

第三，学校在收集个人信息前是否履行了对相应系统供应商数据安全能力的审核义务，是否明确规定了第三方供应商的数据保护义务。

（二）瑞典某学校利用人脸识别技术统计学生课程考勤违反GDPR

2019年8月21日，瑞典数据保护机构根据欧盟通用数据保护条例（General Data Protection Regulation, "GDPR"）对瑞典一所学校利用人脸识别系统收集学生面部识别特征等个人信息的行为处以200,000瑞典克朗（约人民币15万元）的罚款[130]，这也成为了瑞典历史上的第一个GDPR处罚案例。

在这一事件中，该校收集了参与课堂学习的22名学生的面部识别特征以进行自动化课程登记，相应数据均存储在未连接互联网的本地计算机中，在收集此类生物识别数据前也已征得学生监护人的明确同意。尽管如此，瑞典数据保护机构经调查认为，该校所获得的学生监护人的"同意"在学校和学生之间构成的"不对等"关系下作出，不应视为自愿的"同意"，因此不能作为个人数据处理合法化的依据。同时，该校为统计课堂出勤记录可以采取保护学生个人数据的其他方式进行，为此收集面部识别特征等高度敏感性数据超出了实现目的所必需，并不满足GDPR对于个人数据处理的目的限制和数据最小必要基本原则。此外，瑞典数据保护机构认为学校在进行相应个人数据处理活动前，未进行任何数据保护影响评估，尤其缺乏此类数据处理行为对数据主体权利影响的评估。

目前国内个人信息保护相关立法及执法态度均借鉴了域外数据保护相关法律的立法原则。尽管该事件为域外执法案例，但对于向境外提供产品或服务的境内企业，以及利用新兴技术从事教育行业的相关企业而言，其指导意义是不言而喻的。对于收集个人信息尤其是学生的个人信息，一刀切的授权同意已经不再满足日趋严格的执法要求，建议企业结合数据应用场景、使用目的、手段必要性、授权同意的真实意思表示、双方权利分配等因素，多方位综合判断数据处理合法依据是否有效。同时，在收集个人信息之前，相关企业应当进行数据保护影响评估工

127.《中华人民共和国网络安全法》第四十一条 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。

128.《个人信息安全规范》5.2收集个人信息的最小必要要求
对个人信息控制者的要求包括：
a) 收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该等信息的参与，产品或服务的功能无法实现；
b) 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；
c) 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

129.对于未满14周岁的未成年人应当获得其法定监护人的授权同意。

130. 本事例相应事实描述，主要参考瑞典数据监管局针对本案的执法决定书：https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf。

作，以明确风险并采取一定技术和制度措施有效降低风险。

SECTION 02

国内有关未成年人个人信息保护的立法及监管趋严

（一）《儿童个人信息网络保护规定》于2019年10月1日正式生效

2019年8月22日，网信办发布了《儿童个人信息网络保护规定》，作为《网络安全法》的配套法规对14周岁以下未成年人（“儿童”）的个人信息保护进行了统一规范，其作为国家层面发布的儿童个人信息保护专门立法对各行业各领域涉及儿童个人信息的收集、处理活动的企业均具有约束力，该规定已于2019年10月1日正式生效。

1.儿童个人信息保护的基本框架

从立法框架及其内容上看，该规定沿袭了《网络安全法》对个人信息保护的基本原则，吸纳了《个人信息安全规范》对于个人信息收集、使用、转移、共享、存储、披露、删除等全生命周期的合规保护逻辑及规范要求，突出了儿童个人信息保护的特殊监管要求，同时强调了儿童监护人的监护职责，网络运营者与监护人协同共治的管理思路。对于违反该规定的相关企业，网信部门可依据职责进行约谈，作出处罚并记入信用档案，予以公示。

可以预见，《儿童个人信息网络保护规定》将作为执法检查的合规重点，相关企业应当及时排查风险，部署相应的合规措施。为此，我们梳理了儿童个人信息保护核心排查重点如下：

合规要点	具体要求
规则设定及专岗设置	**【规则】**设置专门的儿童个人信息保护规则和用户协议； **【岗位】**指定专人负责儿童个人信息保护。
告知及授权同意	**【基本要求】**收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意； **【拒绝】**向儿童监护人征得同意时，应当同时提供拒绝选项； **【告知】**向儿童监护人明确告知以下事项：收集处理目的、方式和范围；存储地点、期限和超期存储方式；信息安全保障措施；拒绝后果；用户反馈渠道和方式；用户行权途径和方式，等等。如前述事项发生实质性变化的，需再次征得同意。
数据收集	**【约定目的及范围】**不得违反法律及行政法规规定和双方约定的目的和范围收集、使用儿童个人信息。因业务需要确需超出约定目的和使用范围的，应当再次征得儿童监护人同意。

合规要点	具体要求
数据存储	**【期限】**不得超过实现其收集、处理目的所必需的存储期限； **【加密】**采取加密等措施存储儿童个人信息。
内部管理	**【权限管理】**以最小授权为原则，严格设定内部信息访问权限，控制儿童个人信息知悉范围，记录数据访问情况； **【审批及记录】**工作人员访问儿童个人信息的，应当经过儿童个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。
数据转移	**【事前安全评估】**向委托方/第三方转移儿童个人信息的，应自行或者委托第三方机构进行安全评估； **【签署数据处理协议】**与委托方/第三方合作处理儿童个人信息的，应当通过签署数据处理协议明确双方责任、处理事项、处理期限、处理性质和目的等儿童个人信息保护相关义务，委托行为不得超出授权范围。
个人信息主体权利	**【更正权】**积极采取措施响应、更正儿童或其监护人发现的已收集、处理的个人信息中的错误； **【删除权】**当以下情形发生时，积极响应儿童或其监护人提出的个人信息删除要求： 企业违反法律、行政法规规定或者双方约定目的范围； 超出目的范围或者必要期限收集、处理儿童个人信息； 儿童监护人撤回同意； 儿童或者监护人通过注销方式终止使用企业提供的产品或者服务的。
安全事件应对	**【数据主体告知+主管部门报告】**当发生儿童个人信息泄露、损毁、丢失等信息安全事件的，启动应急预案，立即向主管部门报告，并以任何可能方式向受影响的儿童及其监护人告知。

2.保护规定中对于同意的具体规定

在《儿童个人信息网络保护规定》中，获得监护人的明示同意是收集、使用儿童（14周岁以下）个人信息的前提。美国早在1998年通过了《儿童在线隐私保护法》（Children' s Online Privacy Protection Act，以下简称“COPPA”），适用于美国司法辖区内在线收集13岁以下儿童的个人信息的个人或实体，说明了相关隐私政策的要求、同意的设置以及保护隐私安全的责任规则等内容。其中获得父母“可验证的同意”（verifiable consent）亦是该制度的核心之一，在落实的过程中监管机构对于企业如何完成COPPA合规付出了诸多努力，尤其针对同意的要求、落实及其适用例外通过制定合规指引等形式配合法案进行了明确的规定。

（1）保护规定中对于同意的具体规定

同意的规定	同意的例外
《儿童个人信息网络保护规定（征求意见稿）》第七条 网络运营者收集、使用儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的明示同意。明示同意应当具体、清楚、明确，基于自愿。	《儿童个人信息网络保护规定（征求意见稿）》第十九条 网络运营者收集、使用、转移、披露儿童个人信息，有以下情形之一的，可以不经过儿童监护人的明示同意： （一）为维护国家安全或者公共利益； （二）为消除儿童人身或者财产上的紧急危险； （三）法律、行政法规规定的其他情形。

由于儿童主体的特殊性，对其个人信息的处理必须满足明示同意的条件，这也与《个人信息安全规范》相符。但由于明示同意的规定较为严格，如果不明确规定例外情形的话，无疑会造成个人信息控制者的额外负担，也不利于保障儿童以及国家的相关利益。

（2）美国COPPA关于同意的规定和例外

同意的规定[131]	同意的例外[132]
（A）要求向儿童收集个人信息的任何网站或提供在线服务的运营商或实际知晓其网站或服务向儿童收集个人信息的运营商或在线服务运营商， （i）在其网站上通知，运营商向儿童收集了哪些信息，运营商如何使用这些信息，以及运营商对此类信息的披露的情形；并且 （ii）**获取可验证的父母同意**，以收集，使用或披露儿童的个人信息。	以下情况下，并不要求根据第（1）（A）（ii）款作出的可验证的父母同意： （A）从儿童收集的在线联系信息，该信息仅用于一次性直接响应儿童的特定要求，不用于再次联系儿童，并且运营者不得以可检索的形式保存； （B）父母或儿童的姓名或在线联系信息的请求，仅限于获得父母同意或根据本节提供通知的目的，如在合理的时间后没有获得父母同意，运营者不以可检索的形式保留此类信息； （C）从儿童收集的在线联系信息，该信息仅用于直接针对儿童的特定请求作出一次以上的回复，并且不得重新联系该儿童将该信息用于该请求范围之外的目的： （i）如果在对儿童作出初步回应之后的任何其他答复之前，运营者采取合理措施向父母提供从儿童收集的在线联系信息，其使用目的以及父母可以要求经营者不可进一步使用该等信息并且不能以可检索的形式留存该等信息；或 （ii）在委员会认为适当的情况下，根据在此规定的条例中，在没有通知父母时，结合儿童获得信息和服务的利益，以及对儿童的安全和隐私的风险； （D）儿童的姓名和在线联系信息（在保护网站儿童参与者安全的合理必要范围内）： （i）仅用于保护此类安全的目的； （ii）不得用于重新联系儿童或任何其他用途；并且 （iii）如果运营者采取合理措施向父母提供从儿童收集的姓名和在线联系信息，使用目的以及父母可以要求经营者不可进一步使用该等信息并且不能以可检索的形式留存该等信息；或 （E）该网站的运营者或在线服务所需收集，使用或传播该等信息是以下所必需： （i）保护其网站的安全性或完整性； （ii）采取预防措施以避免责任； （iii）回应司法程序；或 （iv）在其他法律规定允许的范围内，向执法机构提供信息或就与公共安全有关的事项进行调查。

131.15 U.S.C. § § 6502. (b) (1).
132.15 U.S.C. § § 6502. (b) (2).

(3) FTC的合规指引

美国联邦贸易委员会(Federal Trade Commission，简称FTC)是COPPA唯一的监管机构。FTC为COPPA制定了包括《企业六步合规计划》(A Six-Step Compliance Plan for Your Business)在内的合规指南[133]，为企业遵守COPPA提供了实用指引。

133.Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business，链接：https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance，访问日期：2019年06月04日。

合规指南规定 ——“可验证的同意”	合规指南规定 —— 同意的例外
在收集、使用和披露儿童个人信息前，必须征得其父母的可验证的同意。COPPA将这个问题留给企业，但是须通过清晰可用的技术设计，合理选择一个方法以确保作出同意的是儿童的父母，而非儿童本人，这点非常重要。 可接受的方法包括： （1）父母签署一个同意表格并通过传真、邮箱或电子扫描方式邮寄； （2）让父母使用信用卡、借记卡或其他在线支付系统等可以向账户持有人提供每笔单独交易的通知的系统； （3）使父母可以通过免费号码与经过相关知识培训的人员通话； （4）使父母可以与经过相关知识培训的人员进行视频会议； （5）使父母提供政府颁发的可在数据库中查询的ID复印件，但要在完成认证程序后删除认证记录； （6）使父母回答一系列对于父母之外的人很难回答的问题； （7）验证由父母提供的父母的驾照和父母本人照片，通过人脸识别技术进行对比。 如果仅将儿童的个人信息用于内部目的而不会披露，可以使用 “电子邮件+”的方法。根据该方法，向父母发送电子邮件并让他们回复以表示同意。然后，必须通过电子邮件，信件或电话向父母发送确认。如果使用“电子邮件+”，必须让父母知道他们可以随时撤销他们的同意。 必须让父母选择允许收集和使用他们孩子的个人信息，而不能捆绑式同时同意向第三方披露该信息。如果对父母已经同意的收集，使用或披露做法进行了更改，必须向父母发送新通知并征得父母的同意。	一般而言，在收集儿童的个人信息之前，必须获得家长的可验证同意。但是，该要求有一些有限的例外情况，允许在未经父母同意的情况下收集信息。但是在每个例外情况下可能收集的信息范围很窄。不能再收集任何例外之外的信息。此外，如果根据其中一个例外收集信息，则不能将其用于任何其他目的或将其披露。 （1）事由：**获得可验证的父母同意** 可收集**儿童和父母的姓名和在线联系信息**，如果未在合理时间内获得同意，则必须删除其联系信息。必须在直接通知中告知父母相关信息（包括链接到隐私政策）； （2）事由：**主动向父母通知他们的儿童参与或接受不收集个人信息的网站或服务** 可收集**家长的在线联系信息**，但必须在直接通知中告知父母相关信息（包括链接到隐私政策）； （3）事由：**直接回应儿童的特定一次性请求（例如，如果儿童想要参加比赛）** 可收集**儿童的在线联系信息**，不能使用这些信息来再次联系该儿童，响应请求后，必须将其删除。无需直接通知； （4）事由：**直接回应儿童的多次特定要求（例如，如果儿童想要收到时事通讯）** 可收集**儿童和父母的在线联系信息**，不能将此信息与从儿童收集的任何其他信息相结合。但必须在直接通知中告知父母相关信息（包括链接到隐私政策）； （5）事由：**为保护儿童的安全** 可收集**儿童和父母的姓名和在线联系信息**，但必须在直接通知中告知父母相关信息（包括链接到隐私政策）； （6）事由：**保护您网站或服务的安全性或完整性，防范责任，回应司法程序，或在法律允许的情况下，向执法部门提供信息** 可收集**儿童的姓名和在线联系信息**，无需直接通知； （7）事由：**为站点或服务的内部操作提供支持** **包括：维护或分析网站的运作，执行网络通信，验证网站用户或个性化内容，提供内容相关广告或频次上限，保护用户或网站的安全性或完整性，法律或监管合规，或根据前文一次性联系或多次联系儿童的例外的请求。** **可收集持久标识符**（又称“单一标识符”），不能使用该信息与特定人员联系，包括通过行为广告，收集特定人员的个人资料或用于任何其他目的。如果收集持久标识符以外的个人信息，则不能使用此例外。无需直接通知；

合规指南规定 —— “可验证的同意”	合规指南规定 —— 同意的例外
	（8）事由：**如果确实知道某主体的信息是通过导向儿童的网站收集的，但他们之前的注册表明此该主体是13岁或以上，此例外仅适用于：只收集持久标识符而不收集其他个人信息;此主体已确定与网站或服务进行交互以触发收集;并且已经对该主体进行了年龄筛选，表明他或她已经13岁或以上。可直接收集持久标识符而无需直接通知。**

其中关于同意的环节，该合规指引列出了非常明确具体的路径供企业参考，同时对于同意的例外亦进行了事由（目的）、收集数据类型、直接通知以及其他限制条件方面的明确规定。

（4）比较与评析

	同意的规定	同意的例外
《保护规定》	监护人的明示同意	**• 为维护国家安全或者公共利益; •为消除儿童人身或者财产上的紧急危险; • 法律、行政法规规定的其他情形。**
COPPA	父母的可验证的同意（并且在合规指引中明确了具体的实践方法）	出于通知以获得可验证同意的目的收集; •出于特定的响应儿童一次或多次请求的目的收集（目的和数据类型均有严格限制）; •**保护儿童安全**（目的和数据类型均有严格限制）; •保护其网站的安全性或完整性;采取预防措施以防范责任;**回应司法程序;或在法律其他规定允许的范围内，向执法机构提供信息或就与公共安全有关的事项进行调查**（目的和数据类型均有严格限制）。

《保护规定》和COPPA均规定了监护人的明确同意为处理儿童个人信息的前提，并且也均规定了同意的例外情形。最大的区别为，**COPPA经过近20多年的实施，在合规实施的颗粒度和落实程度方面更胜一筹：在同意方面，其合规指引直接列举了明确的验证父母同意的途径;在例外情形层面，除了与《保护规定》相同或近似的公共安全、保护儿童安全以及法律法规另行规定外，对于企业正当的不会对儿童权益造成实质性影响的行为（如保护网站安全完整等）严格限定的同时也允许该等例外情形发生。《保护规定》只是草案，相对而言规定较为概括，在接下来**

的正式文本制定以及相关标准出台的过程中，COPPA的上述操作具有一定的借鉴意义。涉及儿童个人信息处理的企业可尝试吸收学习上述合规要求，厘清企业收集儿童数据的事由，并探讨是否会落入可能的例外情形中，为自身即将面临的合规义务做好准备。

（二）《关于引导规范教育移动互联网应用有序健康发展的意见》

2019年8月10日，教育部、中央网信办、工业和信息化部、公安部、民政部、市场监管总局、国家新闻出版署、全国“扫黄打非”工作小组办公室等八个部门联合发布了《关于引导规范教育移动互联网应用有序健康发展的意见》，并于同日生效。

作为国家层面发布的首个全面规范教育App的政策文件[134]，相比于此前发布的《教育部办公厅关于严禁有害APP进入中小学校园的通知》[135]以及《教育部等六部门关于规范校外线上培训的实施意见》[136]，该意见不止于中小学，也不局限于校外，而是覆盖各学段教育和各类应用场景的教育移动互联网应用，包括APP、公众号和小程序等移动互联网平台（统称为**“教育APP”**）。

134.教育部发布会解读《关于引导规范教育移动互联网应用有序健康发展的意见》http://www.gov-.cn/xinwen/2019-09/05/-content_5427621.htm
135.详见http://www.moe.gov.cn/srcsite/A06/s3321/201901/t20190102_365728.html
136.详见http://www.moe.gov.cn/srcsite/A06/s3325/201907/t20190715_390502.html

1、监管对象及责任主体

从监管对象来看，该意见界定了教育App的内涵和外延，提出教育App是以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的教育移动互联网应用。从使用场景来看，教育App大致分为三类：1）市场竞争提供、师生自主选用；2）学校企业合作、学校组织应用；3）学校自主开发、部署校内使用。

从责任主体来看，该意见不仅针对教育移动应用提供者（即教育APP运营者），提出了备案管理、内容审核、数据保护、网络安全等多个层面的规范性要求，同时针对教育、网信、电信、公安、市场监管、扫黄打非等职能部门进行协同联动的监管体系建设和“互联网+教育”领域的集中治理工作的整体部署。此外，该意见明确了教育行政部门和学校在教育App推荐、选用及运维中的责任。

2、近两年“互联网+教育”领域的立法及监管安排

教育部将于近期制定并出台教育移动互联网应用备案管理办法，明确备案方式、内容、对象和时间，实现“一省备案、全国有效”和全程网上办理，并于2019年底，落实并完成教育APP的备案工作。

由教育行政部门牵头，会同网信部门、电信主管部门、公安部门等多部门开展教育移动应用专项治理行动，集中治理利益绑架、信息泄露、低俗信息等问题。

教育行政部门将着手建立推荐机制，形成推荐名单，并向社会公开。同时，建立常态化的监测预警通报机制，教育移动应用的选用退出机制、负面清单和黑名单制度，推动将黑名单信息纳入全国信用信息共享平台。

2020年底，建立健全教育移动应用管理制度、规范和标准，形成常态化的多部门协同治理监管机制，各部门执法重点如下：

监管部门	“互联网+教育”领域执法重点
教育行政部门	牵头负责教育APP治理工作，统筹协调 指导和监督教育APP进校管理，健全教育APP选用机制。
网信部门	依据职责重点做好教育APP提供者、应用商店等APP分发平台提供者、移动终端制造商的内容审核、数据保护监管工作。
电信主管部门	ICP备案等相关电信业务经营许可资质的审批及监管工作。
新闻出版部门	教材、教辅等网络出版物的监管工作。
民政部门	教育类民办非企业单位的登记管理工作。
市场监管部门	线上盈利性教育机构的登记管理；依法查处违法收费、虚假、违法广告等行为。
公安部门	持续开展“净网”专项行动； 网络安全等级保护的监管工作； 网络实名制的监管工作； 打击整治侵犯公民个人信息罪、发布、传播涉黄涉赌等违法有害信息等相关违法犯罪活动。
全国“扫黄打非”工作小组办公室	将查处教育App纳入低俗信息专项整治行动，作为“净网”专项行动工作重点进行部署； 对相关应用侵权盗版行为予以打击；对传播低俗等不良信息行为予以整治。

3、教育APP提供者的合规要求

该意见针对教育APP提供者、应用商店等APP分发平台提供者、移动终端制造商提出了备案管理、内容审核、数据保护、网络安全等多个层面的规范性要求，具体如下：

监管部门	“互联网+教育”领域执法重点
备案管理	获得ICP备案等相关电信业务经营许可； 取得网络安全等级保护定级备案证明、等级测评报告； 向机构住所地的省级教育行政部门进行教育业务备案，登记单位基本信息和所开发的教育移动应用信息。
内容审核	以未成年人为主要用户的教育移动应用应当限制使用时长、明确适龄范围，对内容进行严格把关； 具备论坛、社区、留言等功能的教育移动应用应当建立信息审核制度。
数据保护	遵循《网络安全法》基本要求，建立个人信息自收集到使用的全生命周期管理机制；

监管部门	“互联网+教育”领域执法重点
数据保护	按照“后台实名、前台自愿”的原则，对注册用户进行身份信息认证（实名制要求）； 收集使用未成年人信息应当取得监护人同意、授权; 收集使用个人信息应当明示收集使用信息的目的、方式和范围，并经用户同意； 不得以默认、捆绑、停止安装使用等手段变相强迫用户授权。
网络安全保障	教育APP及后台系统应当统一落实网络安全等级保护要求； 鼓励参加网络安全认证及检测。
广告发布管理	广告应与服务内容相契合； 如为教学、管理工具要求统一使用的教育APP，不得植入商业广告和游戏。
进校合作管理	推荐使用的教育移动应用应当遵循自愿原则，不得与教学管理行为绑定，不得与学分、成绩和评优挂钩。如为教学、管理工具要求统一使用的教育APP，不得向学生及家长收取任何费用。确需选用第三方应用的，不得签订排他协议，或实际由单一应用垄断业务。

结语

纵观2019年网络安全与数据保护领域的执法行动，自2019年1月中央网信办、工信部、公安部、市场监管总局四部门联合开展App个人信息专项治理工作[137]以来，从全国范围到地方监管的执法力度日益加强。2019年7月，App专项治理工作组先后两次向社会公布了50款违法违规收集使用个人信息的App[138]。2019年6月至9月，上海市通信管理局共监测处置了App应用12000余个，分批次对44家运营单位进行了约谈通报[139]。2019年9月，国家计算机病毒应急处理中心公布《移动APP违法违规问题及治理举措》，曝光多个APP涉嫌超范围收集个人信息、恶意扣费、远程控制等违法违规行为[140]。2019年9月16日至22日，由中央宣传部、中央网信办等十部门联合主办的国家网络安全宣传周活动举办，更加显现出国家对网络安全、数据保护的高度重视。

面对日趋严格的网络安全与数据保护执法大环境，尤其是近期密集出台的有关未成年人、个人信息保护的立法与监管活动，对产品及服务提供者如何平衡商业发展与网络安全与数据保护合规风险提出了严峻挑战。结合上述国内外未成年人个人信息保护立法及监管趋势，我们建议相关企业**优化个人信息授权机制，以“制度+技术”双重保障防范风险，**具体如下：

第一，结合《网络安全法》、《互联网个人信息安全保护指南》、《儿童个人信息网络保护规定》、《个人信息安全规范》等法律法规及配套国家标准，针对以儿童为主要对象的产品或服务，尤其在使用人脸识别等新兴技术时，应以合规高标准设计个人信息收集、使用的授权同意机制，包括充分告知收集处理规则、获取儿童监护人的明示授权同意，识别监护关系和监护人授权同意的有效性，并通过一定技

137.2019年1月25日，中央网信办等四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，开展为期一年的App个人信息专项治理工作。详见http://www.-cac.gov-.cn/2019-01/25/c_1124042599.htm?-from=sin-glemessage

138.2019年7月11日、16日，App专项治理工作组向社会公布了50款违法违规收集使用个人信息的App并督促其运营者限期30日内进行全面整改工作。

139.2019年9月17日，上海市通信管理局召开2019年电信和互联网行业网络安全工作大会，对本年度电信和互联网行业网络安全行政检查的总体情况进行了通报，详见https://news.si-na.com.cn/o/2019-09-17/doc-iicez-zrq6444914.shtml

140.详见http://ww-w.cverc.org.cn/zx-dt/re-port20190918-5.htm

术措施满足业务功能的逐一授权。企业应当从自身业务模式特点入手，设计有效的识别及身份认证机制，确保相应个人信息处理活动具备合法依据。

第二，在收集个人信息之前，相关企业应当针对数据处理活动的全流程进行数据保护影响评估，并采取一定技术和制度措施有效降低风险，充分保障数据安全。

第三，对于面向儿童提供的产品及服务，还应当采取一定的有害内容预防措施进行内容过滤，同时采取网络使用时长控制等网络沉迷防控手段。对于面向全年龄段用户的产品及服务建议设置儿童模式，并将相应儿童个人信息分割独立存储，以降低网络安全和儿童个人信息保护合规风险。

第四，对于非APP的教育类产品，相关企业也应当对标教育APP的最新监管要求，完善网络安全及个人信息保护制度并优化相应技术措施，以从容应对教育行业的监管变化。

141.本文原标题为《许孩子一个春天|速评<儿童个人信息网络保护规定（征求意见稿）>》，作者周洋、王东蓉，网址：http://www.zhonglun.com/content/2019/06-03/1623322353.html。
142.参见《儿童个人信息网络保护规定（征求意见稿）》第2条。

第七节

《儿童个人信息网络保护规定（征求意见稿）》述评[141]

2019年5月31日，国家互联网信息办公室发布了《儿童个人信息网络保护规定（征求意见稿）》（下称“《规定》”）。不同于美国针对儿童个人信息和隐私保护专门制定了COPPA等法律，此前我国关于儿童个人信息保护的主要规定散落于国家推荐性标准和指南中，而没有效力层级较高的专门性法律法规。此次《规定》使得被忽视的儿童个人信息保护得到了应有的重视。

SECTION 01

《规定》的适用范围——是否有长臂管辖尚不明确。

《规定》适用于在我国境内通过网络从事收集、存储、使用、转移、披露儿童个人信息等活动[142]。该适用范围将众多涉及儿童个人信息的联网游戏、社交网络应用程序、在线定位服务、联网玩具或其他物联网设备等网络运营者都纳入其中。此外，在“在中华人民共和国境内”的语境下，我们理解除了在中国注册成立的网络运营者在中国境内的行为显然受《规定》的管辖外，那些在境外注册但通过网络向中国儿童收集个人信息的行为是否也受《规定》的管辖仍需明确。

SECTION 02

明确“儿童”为不满14周岁的未成年人——未明确14岁以上未成年人的个人信息网络保护。

《规定》明确了“儿童”是指不满14周岁的未成年人[143]，这与《最高人民法院关于审理拐卖妇女儿童犯罪案件具体应用法律若干问题的解释》中儿童年龄的认定标准一致[144]。也与《信息安全技术 个人信息安全规范》（下称“**《规范》**”）中关于收集未成年人信息应征得监护人明示同意的年龄相同[145]。设立儿童个人信息保护中的年龄标准应考虑到儿童对其信息的独立处理能力、家长对儿童相关活动的干预程度以及儿童权利保护与网络运营者义务承担之间的平衡，因此绝不能与儿童是否拥有民事行为能力混为一谈。该年龄标准的设置既要考虑儿童的心智和辨认是非的能力，以保护儿童权利，同时也要避免年龄设置过高，将不合理地加重企业义务。COPPA将儿童定义为不满13岁的自然人[146]；欧盟《通用数据保护条例》（General Data Protection Rules，下称“GDPR”）保护的对象为16岁以下的儿童，同时规定成员国可以降低年龄标准，但不能低于13岁[147]。考虑到不满14周岁的未成年人在生理和心理上比较不成熟，且缺乏相应的法律意识，难以应对网络风险，《规定》对其进行了特殊保护。然而《规定》未将那些已满14周岁的未成年人纳入适用范围，如何对其个人信息进行保护仍待进一步明确。

SECTION 03

确立了网络运营者在开展涉及儿童个人信息活动的过程中应遵循的原则——强调网络运营者的安全保障义务

《规定》要求网络运营者在开展涉及儿童个人信息活动时应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则[148]，承袭了《网络安全法》与《规范》中关于收集、使用个人信息应依据的原则[149]，并进一步将“安全保障”纳入其中，强调了网络运营者对儿童个人信息的安全保障义务。

SECTION 04

鼓励行业自律——未明确行业规范的效力如何

《规定》鼓励互联网行业组织指导推动网络运营者制定儿童个人信息保护的行业规范、行为准则[150]，以适应不同行业的特点，从行业自律的角度提高监管的灵活性。但《规定》未明确说明该等行业规范、行为准则的效力。COPPA“安全港”条款

144.参见《最高人民法院关于审理拐卖妇女儿童犯罪案件具体应用法律若干问题的解释》第9条。
145.参见《信息安全技术 个人信息安全规范》第5.5(c)条。
146.参见15 U.S.C. § 6501(1).
147.参见GDPR Art. 8(1).
148.参见《儿童个人信息网络保护规定（征求意见稿）》第3条。
149.参见《网络安全法》第41条，《信息安全技术 个人信息安全规范》第5.1、5.2、5.3条。
150.参见《儿童个人信息网络保护规定（征求意见稿）》第4条。

则把行业自律与法律规范相结合，运营者遵守那些由行业自治组织颁发的并经美国联邦贸易委员会（Federal Trade Commission，下称**“FTC”**）审核批准的行业自治规范可以视为遵守FTC根据COPPA所制定的规章[151]，以此加强了行业规范对网络运营者的监督作用。

151.参见15 U.S.C. § 6503(a), 6503(b)(1).
152.参见《儿童个人信息网络保护规定（征求意见稿）》第5条。
153.参见《网络安全法》第21条。
154.参见《信息安全技术 个人信息安全规范》第10.1(b)条。
155.参见《数据安全管理办法（征求意见稿）》第17条。
156.参见《儿童个人信息网络保护规定（征求意见稿）》第7条。
157.参见《儿童个人信息网络保护规定（征求意见稿）》第8、11条。
158.参见《儿童个人信息网络保护规定（征求意见稿）》第14、15条。
159.参见《信息安全技术 个人信息安全规范》第5.5(c)条。

SECTION 05

网络运营者应设置专门的儿童个人信息保护规则与用户协议，并设立个人信息保护专员或指定专人负责儿童个人信息保护——加强公司治理。

《规定》要求网络运营者应制定专门的儿童个人信息保护规则与用户协议，该用户协议应简洁、易懂；同时应设立个人信息保护专员或者指定专人负责儿童个人信息保护[152]，强调落实对儿童个人信息的保护工作。目前部分以儿童为主要受众的跨国公司，如迪士尼、三丽鸥已有专门的儿童隐私保护政策，并在网页中加以显著标明，而专门的儿童用户协议目前在行业实践中较为少见。从公司治理角度，《规定》要求网络运营者应设立的个人信息保护专员或者指定专人负责儿童个人信息保护，与《网络安全法》中的“网络安全负责人”[153]，《规范》中的“个人信息保护负责人”[154]以及近期出台的《数据安全管理办法（征求意见稿）》中的“数据安全责任人”[155]分别在不同的领域发挥作用。

SECTION 06

网络运营者收集、使用儿童个人信息应征得儿童监护人的明示同意——未明确监护人同意是否应可验证

《规定》要求网络运营者收集、使用儿童个人信息时，首先应以显著、清晰的方式对儿童监护人履行告知义务；其次应取得该监护人的明示同意，且对明示同意提出“具体、清楚、明确、基于自愿”四点要求[156]；当告知事项发生实质性变化，或当网络运营者因业务需要，超出目的和范围使用儿童个人信息的，应当再次征得儿童监护人的明示同意[157]。此外，网络运营者和第三方共同使用儿童个人信息，或者向第三方转移儿童个人信息的应当征得儿童监护人的明示同意[158]。

监护人同意是儿童个人信息保护中的重要内容，是一项一般性要求：《规范》规定“收集年满14的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意”；[159]《未成年人网络保护条例（送审稿）》规定“通过网络收集、使用未成年人个人信息的，应当遵循合法、正当、

必要的原则，明示收集、使用信息的目的、方式和范围，并经未成年人或其监护人同意”；[160]《信息安全技术 个人信息保护指南（征求意见稿）》规定“个人信息管理者不应要求未满16周岁的未成年人提交个人信息，当发现信息提交者未满16周岁时，应给出明确提示并停止收集行为，为提供必要服务确需收集其个人信息的，应征得其监护人的同意”。[161]实践中存在着如何通知监护人以及验证该同意来源于儿童监护人的困境。COPPA及其配套规则对此作出了详细的规定：首先应尽合理努力，在现有技术条件下保证儿童监护人收到通知；其次通知的内容应包括作出该通知的原因、收集的个人信息的类型以及如何对该信息作出披露、在线隐私政策的链接、监护人作出同意的方式等内容；再有，监护人的同意必须是可验证的同意，具体方法包括电话、视讯、回答问题等，确保同意由儿童的监护人所授予。[162]同样，GDPR规定，在考虑技术可行性的前提下，运营商应作出“合理努力”以核实相关同意是由儿童的监护人作出或授权的。[163]

160.参见《未成年人网络保护条例（送审稿）》第16条。
161.参见《信息安全技术 个人信息保护指南（征求意见稿）》第5.1.4条。
162.参见16 CFR § 312.4, 312.5.
163.参见GDPR Art. 8(2).
164.参见《儿童个人信息网络保护规定（征求意见稿）》第19条。
165.参见《信息安全技术 个人信息安全规范》第8.5条。
166.参见《儿童个人信息网络保护规定（征求意见稿）》第17、18条。
167.参见《儿童个人信息网络保护规定（征求意见稿）》第18条。

SECTION 07

明确无需取得监护人明示同意的例外情形——数量上减少，实质上预留了解释空间

《规定》允许网络运营者在“（一）为维护国家安全或者公共利益；（二）为消除儿童人身或者财产上的紧急危险；（三）法律、行政法规规定的其他情形”[164]这三种情形下收集、使用、转移、披露儿童个人信息，可以不经过儿童监护人的明示同意。与《规范》相比，虽然从数量而言无需取得监护人明示同意的例外情形减少了，[165]但实质上《规定》中的第三项兜底条款似乎为可能出现的例外情况预留了一定的解释空间。

SECTION 08

明确监护人享有要求更正、删除儿童个人信息以及撤回同意的权利——未明确监护人是否有权撤销14岁以上未成年人所作出的同意

除强调监护人的明示同意外，基于儿童对成年人的依赖性，《规定》明确赋予了监护人要求更正、删除儿童个人信息的权利。[166]此外，在《规定》所列删除情形中，提到了“儿童监护人撤回同意的”，[167]可以认为“撤回同意”同样是监护人享有的权利之一。上述权利提高了监护人对儿童相关活动的干预程度。由于《规定》仅针对14岁以下儿童个人信息网络保护，对于那些14岁以上未成年人是否可作出同意，以及监护人是否有权撤销该等同意，尚不明确。

SECTION 09

处罚措施与《网络安全法》相对应——明确约谈机构为国家网信办；处罚力度较轻，威慑力有限

针对网络运营者的违法行为，《规定》提出了约谈、警告、没收违法所得、罚款、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照、记入信用档案，并予以公示等执法措施，[168]与《网络安全法》第56、64、71条的规定保持一致，[169]并将约谈实施主体从省级以上人民政府有关部门上升到国家互联网信息办公室，没有将约谈权力下放到地方；明确警告等处罚措施的实施主体为国家互联网信息办公室和其他有关部门；对网络运营者整改措施的实施增加了“及时性”要求。而从处罚力度而言，美国法院对于那些已经被认定违反COPPA的运营者可以就每次违反判处至多42,530美元的民事罚款，[170]GDPR的罚金则可能高达20,000,000欧元或企业上一财年全球营业额的4%。[171]可以看出，作为我国首部儿童个人信息保护的专门性立法，《规定》的处罚措施与COPPA、GDPR相比力度较轻。

168.参见《儿童个人信息网络保护规定（征求意见稿）》第24、25、26条。
169.参见《网络安全法》第56、64、71条。
170. 参见16 CFR § 312.9, 1.98(a).
171.参见GDPR Art. 83(5).

结语

此次《规定》的颁布是一份特殊的儿童节礼物，在当前儿童个人信息泄露严重的背景下为网络运营者敲响了警钟。儿童个人信息保护具有其特殊性，一方面应考虑儿童的人权与自由，另一方面也应考虑相关法律法规对产业发展可能产生的效果，因此既不能放松对儿童个人信息的保护，也不能对网络运营者作出过多限制，以实现赋权与保护之间的平衡

CHAPTER FOUR

核心应用场景下合规分析

在大数据时代，数据合规不再是躲在身后的可有可无的“影子”，而是运营发展过程中不可回避的“显性”问题，数据的无形性、技术性和复合性特点也为各行各业带来了前所未见的困难和阻碍。寻求规范化是企业稳健发展的必经途径，只有培养积极的合规心态，尽早的布局以及开展数据合规工作，专业处理数据合规问题，才能让企业健康发展。

第一节

大数据爬虫应用合规分析[172]

2019年，魔蝎科技、新颜科技等多家现金贷相关的数据源公司被查处，涉事高管被警方控制，魔蝎、新颜、天机、有盾、聚信立、白骑士等多家知名数据风控相关公司都已经主动或被动地停止了与爬虫相关的数据业务[173]。此次大数据执法风暴大有持续发酵之势头，相比2017年《中华人民共和国网络安全法》（“以下简称《网安法》”）实施后的首轮整顿可能更为严厉和彻底。此次行动源于银监会、互联网金融风险专项整治、P2P网贷风险专项整治工作领导小组办公室等监管机构主导的现金贷溯源性整肃，以及公安机关在全国范围开展的扫黑除恶行动，即打掉“套路贷”和暴力催收的数据源头[174]。法律依据为《网安法》、《刑法修正案九》等法律法规中关于禁止非法收集、使用个人信息的规定，以及上述专项整治工作领导小组办公室于2017年下发的《关于规范整顿“现金贷”业务的通知》所提出的红线要求：“不得暴力催收和不得非法侵犯公民个人信息”。

172.本文原标题为《执法风暴下的大数据爬虫合规之路》，作者陈际红、吴佳蔚、刘元兴，网址http://www.zhonglun.com/Content/2019/10-17/1122497264.html。

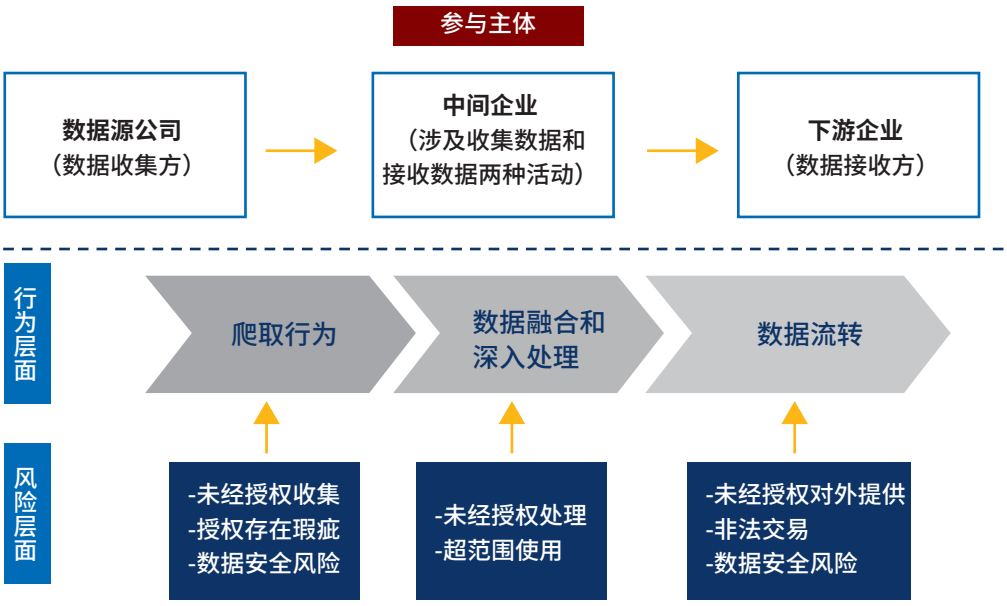
173.徐徜徉：《大数据风控行业“地震”：多家公司被调查，同盾科技否认实控人“跑路”》，财经新媒体，http://news.caijingmobile.com/article/detail/404093?source_id=40，访问时间：2019年9月20日。

174.蒋琳，李玲：《行业震荡！大批数据公司被查：是爬虫之错还是暴力催收的“锅”？》，南都记者采写，https://new.qq.com/omn/20190912/20190912A0QJHC00.html，访问时间：2019年9月20日。

SECTION 01

爬虫合规误区与风险

面对这一轮监管利剑，很多大数据公司噤若寒蝉，主要原因是不清楚大数据行业的合规边界，尤其是如何收集数据（特别是利用爬虫技术）及如何使用数据的边界和红线。基于法律规定和近期的执法背景，我们就关于数据产业链中涉及数据爬取和后续处理、流转的“六个常见做法和合规误区”做出分析，意在厘清大数据爬虫的合规边界与红线。其中，数据爬取行为分为“企业与用户、企业与第三方平台”两个场景，数据交易行为分为“数据提供方企业和数据接收方企业”两个维度。在数据产业链上下游中，企业在两端，从参与角色上来说，既可能是上游数据源企业（数据提供方），也有可能是下游数据使用企业（数据接收方）；从参与行为上来说，可能涉及数据爬取行为，内部对于该等数据的使用亦可能涉及数据融合场景，还可能涉及数据交易在内的流转行为（提供或接收）。



企业参与数据产业链上下游中的角色、行为、风险

（一）数据爬取行为

1.场景1：企业与用户

（1）常见做法1：未经授权进行爬取

合规误区：公开网站上用户信息是公开的，不需要用户授权同意；已经获得用户的同意，爬取用户通讯录中的第三人联系信息并进行后续使用。

风险分析：通过公开网站中爬取的个人信息，如果不是个人信息主体自行向社会公众公开或者公共机构主动明示公开的信息，则仍然需要获得个人信息主体的授权，用户通讯录中的第三人联系信息往往不可能直接获得该第三人的授权，该等缺乏授权的收集行为明显不具有合法性和正当性（《网安法》【第四十一条】、【第六十四条】，《个人信息安全规范》【第5.4条】）。

（2）常见做法2：模糊收集措辞，概括性授权收集

合规误区：意在收集的个人信息范围和类型难以穷尽列举，可以使用“等个人信息”表述模糊处理。

风险分析：爬虫采集协议文本使用“等个人信息”表述。

违反了相关规定的“透明度”的要求。（《网安法》【第二十二条、四十一条】、《个人信息安全规范》【第5.3条】及《App违法违规收集使用个人信息自评估指南》【评估要点7、20、23】的规定）

实践中该等描述往往伴随着超出使用目的范围的过度收集之嫌，可能违反最小必要原则。（《网安法》【第四十一条】及《个人信息安全规范》【第4条】、《App违法违规收集使用个人信息自评估指南》【评估要点7、25、26、27】）

（3）常见做法3：内部数据融合，超出范围使用

合规误区：在有效授权下爬取的数据，或者从上游数据源公司获得的爬取数据，可以放心进入企业自身数据库进行内部数据融合处理，可以进行超出原有授权采集目的进行使用而没有限制措施。

风险分析：现有法律法规没有对数据融合做出专门性规定，但信安标委于今年6月份发布的《个人信息安全规范（征求意见稿）》7.5明确提及数据融合——基于不同业务目的所收集的个人信息的汇聚融合，一、应遵守7.3“个人信息的使用限制”的要求；二、应根据汇聚融合后个人信息的使用目的，开展个人信息安全影响评估，采取适当的个人信息保护措施。可见数据融合处理和使用不是无限制的，应当遵循“合法性、正当性、必要性”原则，即要有合法性和正当性基础（用户授权同意等），对自身爬取数据、从第三方获得的爬取数据和自身对数据进行融合处理等行为也要在必要的范围内，并采取个人信息安全保护措施，否则可能会违反《网安法》的相关规定，遭到行政监管和处罚的风险。（《网安法》【第二十二、四十一、四十二条、六十四条】、《个人信息安全规范（征求意见稿）》【7.3、7.5】）

2.场景2：企业与第三方平台

（1）常见做法4：未经被爬取平台的授权直接爬取

合规误区：平台上用户数据属于用户，已经获得用户授权，爬取平台上用户数据不需要平台授权同意。

风险分析：（1）非法收集个人信息的风险

对被爬取平台而言，未经被爬取平台授权的数据爬取行为存在一定的安全风险，因此可能遭到被爬取平台基于平台安全的合法正当理由的封阻；未经第三方平台授权，通过破解技术爬取用户数据的行为可能构成《网安法》项下的窃取或以其他非法方式获取个人信息的违法行为（《网安法》【第四十四、六十四条】、脉脉案中确定的三重授权原则）。

（2）不正当竞争及其他风险

未经授权直接爬取第三方平台数据的行为，很可能构成“不劳而获”和“搭便车”、“侵犯商业秘密”（同业爬虫）、“妨碍、破坏正常运营”（破解爬虫）的不正当竞争情形。破解爬虫，可能构成“非法侵入他人网络、窃取网络数据的违法行为”，亦有可能构成“危害计算机信息系统安全的其他行为”，由此可能面临相应行政监管的风险，也有构成“非法获取计算机信息系统数据罪”或“破坏计算机信息系统罪”的刑事风险。（《反不正当竞争法》【第二、九、十二条】、《网安法》【第二十七条】、《计

算机信息系统安全保护条例》【第七条】以及《刑法》【第二百八十五条、二百八十六条】）

近期监管机构的立法亦试图规范不正当的爬取行为，2019年5月28日，网信办发布关于《数据安全管理办法（征求意见稿）》，其中【第十六条】规定：网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

2019年9月9日，美国联邦第九巡回上诉法院判决维持了地区法院支持数据爬取方hiQ的初审裁定。其中的焦点认定是：因为公开数据缺少相应的保护措施（例如密码），hiQ 爬取LinkendIn公开数据的爬虫行为不构成CFAA意义上的“未经授权”或“超出授权”行为，该案对我国数据爬虫纠纷审判实践具有借鉴意义。

（二）数据交易行为

1.维度1：数据提供方企业

常见做法5：将具有授权瑕疵的爬取数据整合后提供给下游数据使用企业

合规误区：无论是否存在授权瑕疵，爬取数据均可在被整合后提供给下游数据使用企业；在对外提供过程中，下游数据使用企业使用数据的情形和目的是下游数据使用企业自己的事情，与提供方无关，无需进行严格审查。

风险分析：如果上述情节严重到一定程度，很可能构成侵犯公民个人信息罪。为完成数据交易需要经过“数据爬取和数据提供”两个行为，具有授权瑕疵的数据爬取行为可能构成“窃取或者以其他方法非法获取公民个人信息”，数据提供行为则可能构成“向他人出售或者提供公民个人信息”。（《刑法》【第二百五十三条之一】、《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》【第五条】）

结合目前的执法趋势和背景，企业对外的数据交易行为，很有可能由于非法获取数据的交易行为而面临相应的刑事责任。

2.维度2：数据接收方企业

常见做法6：下游数据使用企业使用数据源公司非法爬取的数据。

合规误区：上游数据源公司（数据提供方）非法爬取的数据，责任由数据源公司（数据提供方）自己承担，与下游数据使用企业（数据接收方）无关。

风险分析：下游数据使用企业（数据接收方）在不对上游数据源公司（数据提供方）的数据来源合法性和数据收集授权范围进行审查和确认的情形下，购买和使用其非法爬取的数据，如果情节严重到一定程度，很可能构成侵犯公民个人信息罪。（具体法律风险后果，同【常见做法5】）。（《刑法》【第二百五十三条之一】、《最

高人民法院　最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》【第五条】）

结合目前的执法趋势和背景，下游数据使用企业很有可能由于执法机关对于上游数据合作方的调查，而面临相应的刑事责任。

SECTION 02

爬虫上下游企业合规建议

爬虫技术是中立的，最近的执法趋势实质打击的是对于爬虫技术的非法利用以至于损害公民个人信息权利的乱象。近期，国外HiQ vs LinkedIn爬虫案，二审终于落锤，维持了一审裁定，也让爬虫行业看到了“正当发展”的些许安慰和希望。爬虫业态在诞生和发展中长期处于灰色地带，在相关合规保护义务和追求效率刺激创新发展之间需要找到一个平衡，这是未来爬虫业态的正途。结合目前严格的执法趋势来看，无论是作为上游数据源公司（数据提供方）还是下游数据使用企业（数据接收方），企业均应就目前的合规形势进行应对之策的考量，以下是我们的简要建议：

（一）上游数据源公司（数据提供方）

1.针对爬取行为本身

就爬取而言，采取对自身爬取数据的合规瑕疵进行详细评估并更新授权文本（应遵循最小必要原则并对用户进行充分通知并取得其同意，并在后续使用中不得超出原授权范围）、与被爬取平台进行合作等措施降低风险；

爬虫使用技术手段应该懂得克制，遵守网站的Robot协议及适用协议，应当充分衡量其承受能力，不能影响其正常运营；

爬取的数据在存储、传输、内部使用融合等方面均应满足《个人信息安全规范》的要求。

2.内部数据融合

将爬取的数据归入自身数据库进行数据融合应该注意以下几点：

对爬取数据与原有内部数据进行融合处理后产生的信息，如（单独或结合）仍具备个人识别能力，则还应作为个人信息对待，对其处理应遵循收集个人信息时获得授权同意的范围；

如融合处理后产生的是个人敏感信息，还应遵守对个人敏感信息的保护要求；

如数据的汇聚融合的使用行为超出了已获得授权的范围，则应当重新获得授

权；

非获得授权业务的必要，在融合使用时，一般应采用无需定位到具体个人的间接画像（如推送商业广告时）；

遵循风险规制路径，进行事前、事中、事后的动态风控评估和控制，采取适当的个人信息保护和安全措施。

3.作为数据输出方

在对外提供过程中，对下游合作方使用数据的情形和目的进行严格审查；

并结合下游合作方的具体身份和具体场景对于用户进行明确的通知，取得用户的同意；

同时通过尽职调查、数据处理协议以及脱敏、匿名化处理等措施控制涉及非法出售公民个人信息的风险以及后续可能涉及的安全风险。

（二）下游数据使用企业（数据接收方）

作为数据接收方，应该参照《个人信息安全规范》5.3 b)的要求：

严格审核上游数据源公司数据来源，特别是爬虫产品数据来源的合法性及授权同意范围，要求其保证数据来源合法合规；

通过尽职调查和合同承诺等措施控制此处涉及的非法获得公民个人信息的风险以及后续可能涉及的安全风险；

遵循三重授权原则，如果对获得数据使用超出原有授权目的，要再次获得用户授权，真正做到通过获取外部数据实现自身数据的补强，达成数据融合的正当性。

结语

随着多家不同行业的数据公司被查，表明监管部门已经拓展了执法的宽度和深度，不再限于与互金相关的数据风控公司，也不再限于爬虫，形成了“网安部门联合多个部门，针对大数据行业乱象展开新一轮的大规模整治行动”[175]的监管画面，重在打击数据产业链上下游中的违法违规行为。面对这波更大、更严的监管整顿，企业应该重点关注数据产业链上下游中关涉自身的数据合规问题，尤其要严守数据爬虫的风险边界和合规红线。

175.米格、本妹：《大数据公司从业者被抓，几十家被列入调查名单》，一本财经，https://m.huxiu.com/article/270674.html，访问时间：2019年9月20日。

第二节

互联网贷款导流业务监管合规分析[176]

176.本文原标题为《互联网贷款导流：业务模式与监管新规》，作者刘新宇、陈嘉伟，网址http://www.zhonglun.com/Content/2019/03-19/1346294333.html。

互联网贷款导流业务正越来越受到互联网流量巨头们的青睐，包括BATJ以及新浪、饿了么、滴滴、蘑菇街、抖音等互联网平台纷纷布局贷款导流业务以实现自身流量变现。贷款导流业务是指互联网平台为包括持牌金融机构等在内的资金方提供的借款用户导流服务。导流业务的资金方通常包括了银行、消费金融公司、小额贷款公司等，有的导流方也会同P2P平台合作向P2P平台导流借款用户。资金方和导流方本身的角色不是固定的，有的资金方也会充当导流方的角色，将多余的流量推荐给其他资金方以实现对于流量的高效利用。

SECTION 01

贷款导流业务的兴起原因：传统金融机构与互联网平台的双向需求

对于网络贷款业务而言，资金、流量、风控三者缺一不可。部分传统金融机构本身空有资金和放贷业务资质，但缺乏线上获客的渠道、能力，资金利用效率不高，以往传统的线下推广获客方式对于其业务规模增长的助力有限。而对于互联网平台而言，为资金方发放贷款进行导流是其实现自身流量变现的一条有效渠道。一方面，部分导流方本身并不具备放贷业务资质，只能选择向具备放贷资质的机构输出流量。另一方面，部分互联网巨头虽然通过早期积累获得了相应的放贷业务牌照，但仍然可能受到业务规模限制的影响无法完全消化其积累的用户流量，例如各地监管对于小额贷款公司通常会有一定的资金杠杆限制，因此选择对外输出多余的流量。贷款导流业务正是基于这一背景产生，通过导流业务合作，实现行业内部资金与流量的有效结合。此外，近年来，受现金贷等相关监管政策的影响，对于场景的需求也成为金融机构等资金方同互联网平台合作的重要考量点。

SECTION 02

贷款导流业务与传统助贷业务的区别

助贷业务是指助贷机构向金融机构等资金方推荐借款用户的行为，广义上来说，导流业务也属于助贷业务的类型之一，但其与传统助贷业务的区别主要在于各自角色分工以及是否承担兜底责任的不同。

（一）不同的角色分工：导流方通常仅负责营销获客，而助贷机构还需承担风控责任

导流业务模式下导流方通常仅负责营销获客，类似于向资金方提供的广告投放服务，由资金方自行负责借款用户的筛选、风控等。而对于传统助贷业务而言，助贷机构不仅需进行获客，也会根据资金方的进件要求对用户进行初期的筛选、风控，再推送给资金方，资金方负责发放贷款。近年来，随着监管对于金融机构风控能力要求的加强，部分金融机构也会对助贷机构推荐的借款用户再进行一轮复核、筛选。

由于传统助贷业务下，助贷机构已经对借款用户进行了一轮筛选，所以其推荐给资金方的更多是标准化的资产，对于资金方而言，很多情况下仅是进行形式上的风控，其放款的审批通过率也通常较高。而导流业务下，资金方获得的仅是流量，其还面临着流量向用户转化的问题，因此选择高转化率的流量合作方对于主要依靠导流方进行互联网获客的金融机构而言显得至关重要。

（二）是否承担兜底责任：导流方通常无须兜底，助贷机构则相反

导流业务模式下由于导流方并不负责风控环节，因此导流业务与传统助贷业务在风险承担上的责任分配也不一致。导流业务下，导流方通常并不需要向金融机构等资金方承担兜底责任。而对于传统助贷业务而言，助贷机构通常需要向资金方兜底，常见的兜底方式包括了保证金、无限连带责任担保等。在《关于规范整顿“现金贷”业务的通知》（即“141号文”）下发后，监管要求“银行业金融机构不得接受无担保资质的第三方机构提供增信服务以及兜底承诺等变相增信服务”。因此，当前助贷业务合作中，助贷机构借助保险公司或者担保公司向金融机构提供担保的模式也受到越来越多的关注。

SECTION 03

贷款导流业务的三种主要模式

互联网平台在布局贷款导流业务时，根据合作的资金方的不同，主要可以分为以下三种模式：

第一，自营+外部合作模式。该种模式下，互联网平台同时向集团内部金融机构以及外部合作机构导流借款用户。互联网平台自身通过投资、新设等方式取得相应的金融牌照后，依托集团内部其他业务板块积累下来的流量开展贷款业务，本质上是集团内部不同业务板块之间的合作。除向集团内部机构导流外，通常情况下该类互联网平台也会同时向外部机构导流，一则是因为各个机构本身可能存

在一定的业务规模限制，如前文提到的对于小贷公司的资金杠杆限制，导致无法完全消化积累的流量。二则该类平台可能会对用户的优劣程度进行划分，将较为优质的用户优先向集团内部金融机构导流，而将不符合自身要求的用户向外部合作机构导流。

第二，纯外部合作/贷款超市模式。该种模式下，互联网平台仅向外部合作机构导流。该类型互联网平台可能由于切入金融业务较晚，不具备相应的金融牌照而无法直接发放贷款。或者由于自身战略定位原因，并不充当资金方的角色，仅向外部合作机构进行导流。部分互联网平台的导流业务更类似于“贷款超市”模式，用户可以通过其提供的入口选择不同的资金方进行贷款。

第三，联合贷款模式。该种模式下，导流的借款用户由互联网平台集团内部机构和其他外部合作机构共同出资向其发放贷款。联合贷款业务要求联合贷款的各资金方都应当具备相应的放贷业务资质。此前网传的《关于就联合贷款模式征求意见的通知》就将联合贷款业务的合作机构限定为“经中国银监会批准设立，持有金融牌照并获准经营贷款业务的银行业金融机构”。

SECTION 04

收费方式：CPA or CPS

CPA是按照每个导流用户的有效行为计费的方式，而CPS是按照贷款额来计算导流费用。

对于传统助贷业务而言，由于助贷机构实质上承担了风控角色，因此资金方与助贷机构之间的费用结算，一般由资金方直接向助贷机构提出固定的资金成本。如果资金方需要向助贷机构支付相应的服务费，往往也会根据助贷机构推荐的资产表现情况设置浮动费率。

对于导流业务而言，CPA和CPS是较为常见的两种收费方式。CPA收费方式下，用户每次完成有效注册、绑卡或者交易等行为，资金方将按照固定的有效CPA单价向导流方支付导流费用。CPS收费方式下，资金方按照用户获取的贷款金额的一定比例来支付导流费用。

市场上除了CPA以及CPS的收费方式外，导流业务常见的收费方式还包括CPC（按照每个有效点击计费）、CPD（按照每个有效下载计费）、CPM（千人展示成本）等。

SECTION 05

数据之争：API or H5

导流方在与资金方合作的过程中，关于用户数据对接一般采用API或者H5的方式。二者的主要区别在于收集、获取用户数据方式的不同。

API模式下双方通过系统进行对接，导流方通过系统接口向资金方传输用户数据。而H5模式下，导流的属性更为纯粹，导流方并不接触核心的用户数据，用户仅仅是通过导流方提供的入口跳转至资金方处申请借款。

H5模式相对容易操作，采用H5的对接方式有助于双方业务合作快速上线。但对于导流方而言其无法通过沉淀用户数据获得更多的价值。而在API模式下，导流方通过系统接口向资金方传输用户数据。一方面资金方对于获取的数据是否经过导流方加工篡改可能存在一定的担忧。另一方面，API合作模式下，资金方也会更加关注导流方在收集、共享用户数据时的合法合规性问题。

SECTION 05

贷款导流业务的监管合规要求

（一）导流业务资质

当前监管对于从事贷款导流业务机构的资质、业务规范并没有明确的要求。此前流传的《关于做好网贷机构分类处置和风险防范工作的意见》（即“175号文”）要求“积极引导部分机构转型为网络小贷公司、助贷机构或为持牌资产管理机构导流等”。对于该条规定，不少人也抱着是否是监管为“助贷机构”、“导流机构”正名的想法。而近期据媒体报道，银保监会收到互联网金融风险专项整治工作领导小组办公室来函，提请银保监会在日常监管中关注互联网机构为银行、信托、保险等持牌机构提供引流、营销宣传等服务的合法合规性。监管信号已经发出，不排除下一步互联网导流业务将迎来更为明确具体的规制。

监管的暂时缺位是否意味着互联网平台在经营导流业务时可以不承担任何责任呢?导流业务类似于互联网广告行为，导流方作为“广告”的发布者，应当尽到一定的审查义务，比如对于金融机构资质的真实性、“广告”内容的合法性进行一定的审查，对于未尽到必要审查义务的导流机构应当要求其承担相应的责任。但实践中，这种审查义务的边界确实难以把握，导流方也很难做到对所有相关内容的真实性、准确性进行完全审查。

如果导流方涉及由自身发放贷款，则需要取得相应的放贷业务资质。在当前我国法律体系下，具备放贷业务资质的机构通常包括了银行、消费金融公司、小额

贷款公司、信托及汽车金融公司。P2P平台定位于信息中介，其本身不具备放贷业务资质，部分导流方向P2P平台导流时，资金方通常是P2P平台的投资人。

（二）个人信息安全保护问题

在导流业务中如何通过协议签署、授权同意环节设计等操作合法合规地收集、共享用户个人信息对于导流方及资金方而言显得至关重要。

近年来，个人信息安全问题越来越受到重视，导流业务中，涉及到导流方、资金方向用户收集信息的行为，也涉及到导流方和资金方之间关于用户信息的传输、共享行为。按照《网络安全法》的规定，网络运营者应当遵循合法、正当、必要的原则收集、使用个人信息，并且应当公开收集、使用个人信息的规则、目的、方式和范围，取得被收集者的同意。同时，在向他人提供个人信息时也应当取得被收集者同意。参考《信息安全技术 个人信息安全规范》（GB/T 35273-2017）的标准，导流方及资金方还应当按照是否涉及收集用户个人敏感信息、是否涉及核心功能与附加功能的区分来设计用户授权同意收集、共享其个人信息的操作。同时，违反个人信息保护的相关规定可能还会涉及刑事责任承担的问题。我国《刑法》规定“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金”、“窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚”。

（三）跨区域展业限制

通过互联网平台提供的导流服务拓展业务开展区域对于诸多城商行、农商行而言是与互联网平台进行导流合作的重要原因之一，但与此同时，城商行、农商行也面临着跨区域展业的问题。

此前浙江银保监局下发《关于加强互联网助贷和联合贷款风险防控监管提示的函》要求“城商行、民营银行开展互联网联合贷款业务，应坚守‘立足当地、服务当地、不跨区域’的定位”、“开展互联网联合贷款业务，辖内城商行、民营银行法人原则上只能经营本行有分支机构的地域的客户，辖内城商行分行原则上只能经营省内的客户”。其后银保监会发布了《关于推进农村商业银行坚守定位 强化治理 提升金融服务能力的意见》要求“严格审慎开展综合化和跨区域经营，原则上机构不出县（区）、业务不跨县（区）。应专注服务本地，下沉服务重心，当年新增可贷资金应主要用于当地”。监管的一系列动作似乎意味着对于城商行、农商行通过互联网平台的导流服务跨区域展业的负面态度。而如果部分城商行、农商行受限于跨区域展业的要求退出导流市场，对于导流方而言，可选择的外部资金合作机构范围

也将进一步缩减。

结语

广义上的“助贷”市场当前主要包括三种业务模式：一是以“获客+风控”为核心特征进行标准化资产输出的传统助贷业务；二是仅提供“营销获客”服务的纯导流业务；三是依靠技术输出帮助传统金融机构提高信贷服务能力的业务模式。互联网贷款导流业务一方面有助于实现行业内部资金和流量的结合，但另一方面也面临着用户转化率的限制以及容易造成“多头借贷”等问题。在笔者看来，三种业务模式并无本质上的优劣之分，对于从业机构而言，自身技术实力、用户积累以及角色定位等实际情况才是选择何种业务模式的首要因素。与此同时，在整个互联网金融领域，监管政策的影响力早已不言而喻，诸多从业机构还应当适时根据监管政策导向及时调整相关业务，确保合法合规经营。

第三节 银行互联网贷款业务合规分析[177]

177.本文原标题为《地方银保监局下发监管提示函，银行互联网贷款业务路在何方》，作者刘新宇、张倩文，网址：http://www.zhonglun.com/Content/2019/01-15/1050353873.html。

2019年1月9日，中国银行保险监督管理委员会浙江监管局（以下称“浙江银保监局”）对各银保监分局、杭州银行和各城市商业银行杭州分行下发了《关于加强互联网助贷和联合贷款风险防控监管提示的函》（浙银保监便函〔2019〕9号）（以下称“监管提示函”或“该函”）。监管提示函的内容虽然仅有三条，但在行业内引发了不小的震动。

SECTION 01

监管提示函重点内容

（一）监管要求的重申

监管提示函再次重申了141号文中已经明确的以下几点：

不得将授信审查、风险控制等核心环节外包。

不得以任何形式为无放贷资质的机构提供放贷资金，不得与无放贷业务资质的机构共同出资发放贷款。

不得接受无担保资质的第三方机构提供增信服务以及兜底承诺等变相增信

服务。

（二）监管要求的新增

除上述重申的监管要求以外，该函增加了针对城商行、民营银行开展互联网联合贷款业务方面的属地化要求：

要按照客户身份证地址、主要业务经营地、主要居住生活地等维度，建立统一的属地经营规则，按照异地授信管理相关文件的精神严格管控异地授信。

辖内城商行、民营银行法人原则上只能经营本行有分支机构的地域的客户，辖内城商行分行原则上只能经营省内的客户。

SECTION 02

监管提示函的影响

当前，几乎所有商业银行均或多或少地参与或开展互联网贷款业务。以放贷主体为标准，可以将银行互联网贷款的业务模式划分为直接贷款和联合贷款两大类。监管提示函对于以上两类业务模式均产生了直接而重大的影响。

（一）直接贷款

1、业务模式

市场上虽然也存在部分传统商业银行通过手机银行或直销银行推出自主研发的纯线上信贷产品，直接获取C端客户。但有目共睹的是，受制于金融领域的强监管态势和传统银行科技力量相对薄弱等因素，传统银行的互联网化发展之路一直举步维艰，大部分直销银行的发展事实上非常有限。

相对来说，更常见的业务模式是商业银行与金融科技公司合作推出信贷产品。银行看中的一方面是金融科技公司在获客方面的经验和数据积累，另一方面是在反欺诈、网络风险防范等领域的技术和风控能力。因此，银行与金融科技公司的合作重点在于获客和风控两个层面。

2、监管提示函的要求

监管提示函针对银行与金融科技公司的合作提出了以下要求：

在内部管理层面，进一步明确“参与银行应开发与业务匹配的风控系统、风控模型，配备专业人员。应独立开展客户准入、风险评测、贷款额度和贷款利率确定、贷后资金用途管理。”

在外部合作的权利义务层面，银行要进一步梳理完善与合作机构合作的协议条款，明确各自权利义务和职责边界，明确银行与合作机构在客户信息共享、风险

防控、不良处置化解、贷款核销、消费者保护等领域的权利义务。

3、主要影响

在线上获客方面，此前银行更多地依赖于流量巨头输送贷款用户。但该业务合作模式中，风控、贷中管理、贷后催收和兜底责任一般由合作机构承担，银行更多地异化为单纯的放贷资金提供方，在“核心业务不得外包”的监管要求下，逐渐被淘汰。

目前比较典型的合作模式是由金融科技公司为银行输出风控技术，金融科技公司向银行提供技术服务、量身定制风控模型系统等，由银行使用前述系统和技术对客户进行反欺诈验证、信用评估、风险评估、核定信贷额度与价格等。在现有监管体系下，风控输出的业务模式可能会被更广泛的采用。

（二）联合贷款

1、业务模式

自141号文提出了“不得以任何形式为无放贷资质的机构提供放贷资金，不得与无放贷业务资质的机构共同出资发放贷款”后，实际上目前主要的联合放贷模式是传统银行与互联网银行的联合放贷。典型的互联网银行包括微众银行、网商银行、新网银行等。

2、监管提示函的要求

除了重申141号文的监管规定外，此次下发的函针对联合贷款业务又提出了以下新增要求：

不具备互联网贷款的核心风控能力和条件的银行，不得开展联合贷款业务。

明确各自权利义务和职责边界，明确银行与合作机构在客户信息共享、风险防控、不良处置化解、贷款核销、消费者保护等领域的权利义务。

对于无法提供贷款审查审批基本资料，或者所提供信息无法满足贷款审查审批需要的合作机构，不得与其开展联合贷款业务。

城商行、民营银行开展互联网联合贷款业务，应坚守“立足当地、服务当地、不跨区域”的定位，将长期可持续发展作为目标，通过互联网渠道引入在自身营销、服务和风险管控能力范围内的客户。要按照客户身份证地址、主要业务经营地、主要居住生活地等维度，建立统一的属地经营规则，按照异地授信管理相关文件的精神严格管控异地授信。开展互联网联合贷款业务，辖内城商行、民营银行法人原则上只能经营本行有分支机构的地域的客户，辖内城商行分行原则上只能经营省内的客户。

3、主要影响

目前，互联网银行贷款业务上大多数作为发起行，与传统银行合作开展联合

放贷模式进行，即互联网银行（即推荐行）负责精准获客、风险管理、运营服务，基于共同的贷款条件和统一的借款合同，按约定比例出资，联合传统银行（即被推荐银行）向符合条件的借款人发放贷款。像微粒贷等信贷产品即采用了以上业务模式，客户获取的贷款资金主要来自于各传统银行。

对于被推荐行来说，除了放贷规模和利润的提升外，对于其核心风控能力、客户积累等方面并无多大裨益。在与有资质的机构开展联合贷款业务时，被推荐行此前仍不能摆脱沦为资金通道的局面，在“不具备互联网贷款的核心风控能力和条件的银行，不得开展联合贷款业务”的要求下可能将受到遏制。

而对于推荐行来说，监管提示函的打击更为严重，主要体现在资金来源和属地化要求两个层面：

（1）资金来源

就目前发展情况来看，互联网银行的信贷业务资金大部分主要来自于注册资本和同业资金。

根据《中国人民银行关于改进个人银行账户分类管理有关事项的通知》（银发[2018]16号），银行账户分为I、II、III类账户，II类账户较I类账户少了转账（向非绑定账户转账）功能，且仅可进行小额取现。III类账户仅能办理小额消费及缴费支付。按照监管规定，互联网银行通过非现场渠道仅能开设功能受限的II类账户，使得互联网银行吸储功能受到制约。

	Ⅰ类账户	Ⅱ类账户	Ⅲ类账户
开户方式	柜面开户/远程视频柜员机和智能柜员机（但需现场核实身份信息）	银行柜面和网上银行、手机银行、直销银行、远程视频柜员机、智能柜员机等电子渠道	银行柜面和网上银行、手机银行、直销银行、远程视频柜员机、智能柜员机等电子渠道
开户条件	直接开户	绑定Ⅰ类银行账户或者信用卡账户	绑定已实名制验证的账户
账户功能	全功能银行账户：办理存款、购买理财产品、支取现金、转账、消费和缴费支付	办理存款、购买理财产品、限定金额的消费和缴费支付、限额向非绑定账户转出资金	小额消费和缴费支付
限额	无限额	与个人绑定账户转账无限额；消费及支付单日不超过1万元	账户余额限制：不超过2000元

由于缺少线下网点，线上远程开户受限，尽管互联网银行通过各种优惠措施，但吸收存款依然存在诸多困难。现阶段互联网银行资金来源多数依赖于股东资金以及同业资金，客户存款占比较低，资金渠道单一。

而监管提示函对于城商行等资金不得出省的要求则很大程度上遏制了互联网银行与城商行联合放贷业务的发展。

(2) 属地化要求

自2014年民营银行牌照放开以来，监管部门已批准筹建了17家民营银行，其中多家民营银行属于互联网银行。据公开渠道获取的信息显示，部分互联网银行基本信息如下：

银行	开业时间	背后主要股东	主要信贷产品类型
深圳前海微众银行	2014/12/16	腾讯	个人消费类
浙江网商银行	2015/05/28	蚂蚁金服	小微及三农类
四川新网银行	2016/12/28	新希望；小米	个人消费类
吉林亿联银行	2017/05/03	中发金控；美团子公司金快科技	个人消费类
江苏苏宁银行	2017/06/15	苏宁云商	个人消费类
百信银行	2017/09/05	百度；中信银行	个人消费类

根据对上表及行业实践的总结，互联网银行具有以下几个特点：

a.互联网银行的股东主要为国内大型互联网巨头公司，通过背后的股东方的用户基础和导流优势加快其线上业务发展。

b. 借助技术手段实现业务创新，服务于线上用户。

c.运用互联网、大数据等优势，在服务模式、客户群体、风控制度等领域进行创新，为没有享受到传统银行完善金融服务的消费者和小微企业提供小额贷款服务。

d.在服务模式上不设物理网点，主要通过在线展业，绝大多数业务均通过在线申请、云端审批并迅速完成签约。

e.在风控制度上主要利用大数据、人工智能等技术手段和模型实现对个人的征信分析，绝大多数贷款产品都不需要抵押和担保。

而监管提示函提出的属地经营规则、严格管控异地授信的要求，和互联网银行与传统银行开展联合贷款业务所采用的线上贷款模式本身打破地域限制的互联网属性相冲突。虽然本函是针对辖内城商行、民营银行的互联网联合贷款业务进行的风险提示，与传统商业银行的互联网贷款业务以及互联网银行的线上业务并无直接联系，但不可否认的是，在此项监管要求下，互联网银行与传统银行的联合贷款业务发展可能会受到较大的限制。

结语

虽然浙江银保监局的该监管提示函仅针对本地域范围内的监管机构和商业银行，无论从发文主体、受众或者文件本身的效力上来看，都存在适用方面的局限

性，但结合去年年底一份网传版本的《商业银行互联网贷款管理暂行办法（征求意见稿）》（以下称“办法征求意见稿”）的内容，我们发现二者在监管态度和监管要求上存在异曲同工之处。因此，我们倾向于认为浙江此次监管提示函的下发，可能意味着监管并未放弃和放松对于银行互联网贷款业务的强势监管。无论对于传统银行、互联网银行或金融科技公司来说，都应当对这一强监管趋势加以重视，并作好应对准备。

第四节 银行开展电商业务的合规分析[178]

178.本文原标题为《银行跨界电商，可能遇到的法律合规问题有哪些?》，作者刘新宇、张功俐，网址：http://www.zhonglun.com/Content/2019/07-04/0848593115.html。

传统互联网电商平台在开展电商业务的同时，向商户、平台用户提供信用贷款、消费分期等金融服务已不鲜见。不过，银行作为传统金融机构之一，通过搭建电商平台的方式跨界开展电商业务，对于普通大众来说相对陌生。学界与业界关于银行开展电商业务的讨论、研究也较少。

SECTION 01 银行开展电商业务的概况

“银行电商平台”（或“银行系电商平台”）主要是指银行通过自运营或委托第三方公司代运营的方式，为电子商务交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务的电子商务平台。银行开展的电商业务是指通过银行电商平台销售商品、提供服务的经营行为。本文所讨论的银行开展的电商业务仅限于银行在网页端或移动端开辟出的独立“商城”板块，对于分散嵌入银行网页端和移动端的商铺优惠信息、线下营销活动不属于本文讨论的范围。

（一）银行电商平台与传统互联网电商平台业务的异同

异同点	相关内容
产品/服务总体内容基本一致，但是仍存在差异	• 银行电商平台提供的产品/服务与传统互联网电商平台基本一致。 • 银行设立的综合性电商平台在传统电商平台提供的产品和服务内容基础上，还增设了金融产品或服务板块，如销售基金产品、理财产品等。

异同点	相关内容
运营主体不同	• 银行电商平台主要依托银行内部业务部门，如网络金融部自运营或委托第三方代运营的方式。 • 传统互联网电商平台主要是电商公司自运营。
电商平台定位不同	• 银行开展电商业务的主要原因是增强客户粘性，获取客户真实交易数据。通过搭建电商平台，银行可以进一步开拓向客户提供金融服务的应用场景。 • 传统电商业务侧重突出电子商务主业，在突出主业的情况下提供金融服务或其他服务。
支付方式不同	• 银行电商平台多支持本行银行卡、银联支付，较少支持第三方支付。 • 传统互联网电商平台普遍支持多种支付方式，银联支付、第三方支付均使用频繁。

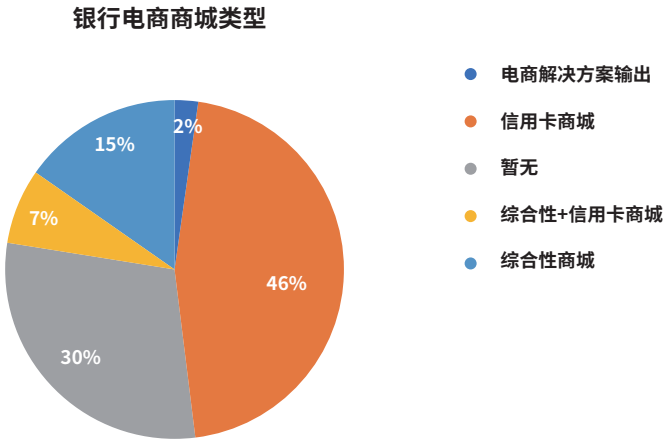
（二）银行开展电商业务的运营特点

我国目前有超过100家银行，笔者选取了附录所列54家银行作为研究样本进行分析。以下为初步统计结果：

1、银行开展电商业务搭建的商城类型

从是否已经开展电商业务角度看，54家银行中，38家银行已经开展电商业务，占比约70%；16家银行尚未开展电商业务，占比约为30%；

从已经开展电商业务的38家银行来看，8家银行通过设立综合性商城开展电商业务，25家银行通过设立信用卡商城(信用卡商城是指银行针对本行用户，特别是信用卡用户推出的积分兑换商城或信用卡分期商城。)开展电商业务，4家银行存在同时设立综合性商城和信用卡商城的情况。此外，1家银行在传统电子商务业务基础上，通过搭建电子商务平台，向外输出电子商务解决方案。具体比例如下图：



从检索情况来看，银行开展电商业务多通过建立综合性商城与信用卡商城方式进行。银行设立的综合性商城与信用卡商城的差异主要体现在以下几方面：

区别因素	综合性商城	信用卡商城
银行类型	• 国有商业银行、股份制银行	• 城商行
用户群体	• 无明确限制	• 一般仅针对本行用户
货物/服务	•产品类型丰富，服务内容多样，业务运营模式与传统互联网电商平台基本一致； •开辟金融财富板块，如工商银行“融e购提供金融产品、贵金属等具有银行特色的产品。	• 产品/服务选择空间少，内容较为单一
支付方式	• 支付渠道多样化 • 本行银行卡（借记卡、信用卡） • 银联支付 • 第三方支付，如微信支付	• 针对本行信用卡用户，一般不支持银联支付或第三方支付

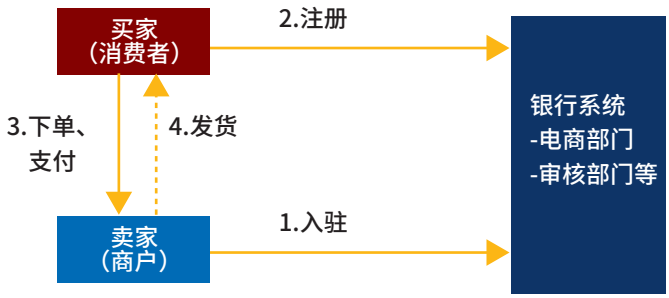
2、银行开展电商业务的运营主体

经检索发现，38家已开展电商业务的银行中，33家银行采用自运营模式，占比约87%，5家银行采用委托关联方或独立第三方进行代运营方式，占比约13%。两类运营模式的特征以及典型案例如下：

类别	特征及代表案例
自运营	• 银行本身作为银行电商平台的运营主体。 • 大部分银行采用自运营方式，如工商银行“融e购”，中国银行“聪明购”等。
代运营	• 以银行关联公司或独立第三方机构作为银行电商的运营主体。 • “民生商城”由北京民商智惠电子商务有限公司负责日常运营管理。

（三）银行开展电商业务的主要模式

银行开展电商业务的主要模式与传统互联网电商基本一致，从商户入驻、买家注册到最后产品/服务交付过程中，银行电商平台主要作为电子商务平台经营者，为交易双方/多方提供信息发布、交易撮合等服务，具体模式如下图：



银行电商基本业务模式

实践中，银行常常通过在电商业务各个环节引入金融增值服务来增强银行电商平台在吸引商户入驻、提升消费者粘性方面的竞争力。以下为银行电商业务各个环节涉及的主要法律文件及可能提供的金融增值服务内容：

流程描述	银行/银行电商所涉法律文件	银行电商平台提供的金融增值服务
①商户申请入驻，提交申请材料	•银行与商户签署《合作协议》或《商户入驻协议》等，明确商户入驻后的权利义务。 •银行与商户签署《交易结算服务协议》，确认由银行向商户提供交易结算服务。	•提供商户融资服务（如小额贷款、符合条件的供应链融资等）。 •提供移动端金融技术支持，提供商户的账务管理、订单管理等服务。 • 对商户存量资金提供银行理财服务。
②买家（消费者）通过身份证信息或银行卡信息注册	•买家注册时需要勾选/同意银行电商平台提供的包括但不限于如下协议： -《平台注册协议》 -《隐私条款》 -《用户授权书》	N/A
③买家通过银行电商平台向商户下单，从商户处购买商品/服务并支付货款/服务费	N/A N/A	对买家： •提供包括但不限于银行理财产品、贵金属等多样化的金融产品/服务。 • 提供消费分期服务。 对卖家： •提供应收账款融资服务/货物订单融资服务
④卖家向买家发货		• 提供保险服务渠道 -卖家：财产意外险/毁损险 -买家：运费险

SECTION 02

银行开展电商业务过程中主要法律问题探析

银行开展电商业务起步较晚，内部合规管理较传统互联网电商平台存在一定滞后性。电子商务业务领域的“根本大法”《电子商务法》的施行也对银行开展电商业务提出了新的要求。鉴于此，笔者基于对银行开展电商业务现状的检索，结合现行的法律法规，对银行开展电商业务相关的法律法规适用、资质申请、平台责任的认定及网络安全与数据保护等问题进行简要梳理。

（一）法律法规的适用

1、银行开展的电商业务与《电子商务法》的适用

银行通过搭建网络经营场所，给商家、消费者提供的包括信息发布、交易撮合等供电子商务交易双方或多方在境内独立开展交易活动的经营行为应适用《电子商务法》。首先，根据《电子商务法》第二条（《电子商务法》第二条第一款：中华人民共和国境内的电子商务活动，适用本法。本法所称电子商务，是指通过互联网等信息网络销售商品或者提供服务的经营活动。）关于法律适用范围的规定可知，《电子商务法》的基本适用范围是针对在中国境内开展的电子商务活动，并未对从事电子商务的主体进行限制。其次，根据《电子商务法》第九条（《电子商务法》第九条：本法所称电子商务经营者，是指通过互联网等信息网络从事销售商品或者提供服务的经营活动的自然人、法人和非法人组织，包括电子商务平台经营者、平台内经营者以及通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者。）关于电子商务经营者的分类，电子商务经营者可以划分为“电子商务平台经营者”，“平台内经营者”和“通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者”。根据本文第一部分关于银行开展电商业务的基本情况分析，银行开展的电商业务应属于在境内开展电子商务活动的电子商务平台经营者，其相关行为活动应适用《电子商务法》。

银行搭建的电商平台中涉及的“金融类产品和服务”不适用《电子商务法》。《电子商务法》第二条适用范围中有一条除外规定，即“法律、行政法规对销售商品或者提供服务有规定的，适用其规定。金融类产品和服务，利用信息网络提供新闻信息、音视频节目、出版以及文化产品等内容方面的服务，不适用本法”。从前述规定可知，《电子商务法》排除了“金融类产品和服务”以及“利用信息网络提供内容方面的服务”的适用，相关产品和服务将适用针对该领域的特别法。如银行通过其搭建的电商平台销售基金等金融产品将不适用《电子商务法》，而应遵照“金融类产品和服务”的相关法律法规进行规范。

2、银行开展电商业务可能涉及的常用法律法规

银行开展电商业务各环节涉及的常用法律法规汇总如下：

电商业务环节	具体业务问题	常用法律法规
电商平台的设立	•电商平台及其自营业务的资质申请问题，如是否需要取得增值电信业务牌照等 •电商平台隐私政策等网络安全与数据保护相关制度及文本建设	《电信条例》 《电信业务经营许可管理办法》 《网络安全法》 《电子商务法》
商户资质审查	•电商平台内经营者资质的审核，是否包含需要取得特殊许可/备案的业务 •提交申请的商户授权链是否完整	《互联网信息服务管理办法》 《出版物市场管理规定》 《网络食品经营监督管理办法》 《网络医疗器械经营监督管理办法》 《药品网络销售监督管理办法》（征求意见稿） 《电子商务法》
产品/服务的营销、推广	•产品/服务的广告宣传词是否涉及禁用词 •产品/服务标注的“原价”的判定 •产品/服务的广告宣传内容是否涉及商标、著作权侵权 •电商平台/商家的承诺保证是否优于法定规定	《广告法》 《广告法实施细则》 《价格法》 《商标法》 《著作权法》 《消费者权益保护法》 《电子商务法》
网络交易	•网络交易合同生效的判定、风险转移的规定 •产品/服务质量是否合格 •是否采用电子合同、是否进行电子签名	《网络交易管理办法》 《商标法》 《产品质量法》 《食品安全法》 《电子商务法》
物流配送	•风险转移时点的判定	《合同法》及相关司法解释 《电子商务法》
售后及纠纷解决	•电商平台/商家的承诺保证是否优于法定规定 •电商平台是否设有纠纷调解机制 •电商平台收到知识产权侵权通知后是否履行相应职责	《合同法》及相关司法解释 《侵权责任法》 《消费者权益保护法》 《电子商务法》

（二）业务开展所需的资质

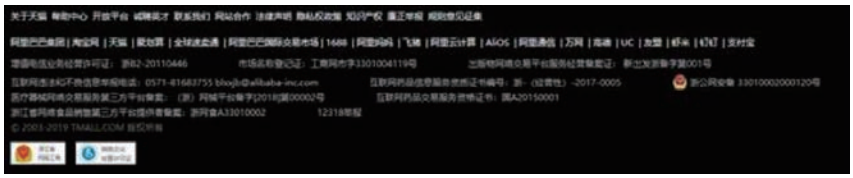
根据《电子商务法》第十二条，“电子商务经营者从事经营活动，依法需要取得相关行政许可的，应当依法取得行政许可”。公司设立后开展电子商务业务通常需要取得增值电信业务经营许可以及针对特定商品/服务的销售经营许可/备案两方面的资质。

1、增值电信业务经营许可

根据我国现行的电信相关法律法规，我国对于电信业务经营按照电信业务分类实行许可制度，经营电信业务需要依法取得相关电信业务经营许可证，其中，经营类电子商务应属于增值电信业务范围，应当取得相应的增值电信业务经营许可证。根据《电信条例》、《电信业务分类目录（2015年版）》等电信相关法律法规，结合上海、浙江、江苏等地通信管理局的反馈意见，经营商品类电子商务，如淘宝、京东等主要通过信息网络销售商品的电商平台通常被归入第二类增值电信业务“B21在线数据处理与交易处理业务”，而服务类电子商务，如58同城、携程等通过信息网络提供服务的电商平台通常被归入第二类增值电信业务“B25　信息服务业务”。除前述采用“销售产品”和“提供服务”的二分法对具体所属的增值电信业务进行区分以外，部分大型互联网电商平台持有的增值电信业务许可证同时包含“B21在线数据处理与交易处理业务”和“B25 信息服务业务”两类业务，如浙江淘宝网络有限公司持有的增值电信业务经营许可证（编号浙B2-20080224）的业务种类就包含B21和B25两类。

开展电商业务的银行目前在其电商平台网站底部披露的通常为银行的ICP备案编号，而非增值电信业务经营许可，银行电商平台可以考虑申请同时包含“B21在线数据处理与交易处理业务”和“B25　信息服务业务”两类业务种类的增值电信业务经营许可。鉴于现阶段银行开展电商业务主要通过信息网络以自营或商户入驻形式进行产品销售，根据现行法律法规和实务操作，银行开展电商业务应取得“B21在线数据处理与交易处理业务”的增值电信业务许可。考虑到银行后续可能继续在电商平台开拓服务市场，银行电商平台的运营主体可以选择申请同时包含“B21在线数据处理与交易处理业务”和“B25 信息服务业务”两类业务种类的增值电信业务许可，从而进一步丰富后续可开展业务的内容。同时，银行电商平台在申请增值电信经营许可时需要注意，2014年后“先照后证”的改革将增值电信业务许可明确为后置许可审批，根据笔者目前的检索，相关申请需要以营业执照中经营范围存在增值电信业务范围为前提，银行在申请相关证照时可能面临需要先修改经营范围的情形，具体时间和步骤需咨询主管的监管部门，以当地执行口径为准。

2、特定产品/服务的销售、经营许可/备案



除增值电信业务经营许可外，开展电商业务的平台还应针对其平台提供的特定产品/服务获取相应经营许可/备案。以天猫官网为例，天猫运营主体取得的资质许可除增值电信业务经营许可证外，还包括出版物网络交易平台服务经营备案证、互联网药品信息服务资质证书、医疗器械网络交易服务第三方平台备案、互联网药品交易服务资格证书、浙江省网络食品销售第三方平台提供者备案等。

从银行电商平台取得的相关资质许可情况看，目前只有少数银行对其取得的特殊销售、经营许可/备案进行公示，如中信银行“中信易家”在其银行电商平台网站底部对相关食品经营许可证（编号为JY11105050876919）进行列示。考虑到不少银行电商平台提供的产品类别包括食品、出版物、医疗保健品等，特定产品/服务的资质许可问题有待进一步规范。笔者梳理了以下几类较为常见的资质/许可的业务类型及相关法规基础：

业务内容	法律法规	资质/许可类型
出版物	《互联网信息服务管理办法》 《互联网文化管理暂行规定》	网络文化经营许可证
	《出版物市场管理规定》	出版物网络交易平台服务经营备案证
	《互联网视听节目服务管理规定》	信息网络传播视听节目许可证
	《网络出版服务管理规定》	网络出版服务许可证
医疗器械	《医疗器械网络销售监督管理办法》	医疗器械网络交易服务第三方平台备案
药品	《互联网药品交易服务审批暂行规定》 《关于实施<互联网药品交易服务审批暂行规定>有关问题的补充通知》	互联网药品交易服务资格证书
	《互联网药品信息服务管理办法》	互联网药品信息服务资质证书

（三）银行开展电商业务的责任承担

1、银行电商平台的法定义务

现阶段，银行开展电商业务过程中，较为常见的主体身份是“电子商务平台经营者”，为有效地降低银行电商平台因违反电商平台义务而引发相关责任承担的

风险，笔者根据《电子商务法》对银行电商平台在日常经营管理中应承担的相关义务进行如下梳理：

分类	职责内容	《电商法》条款序号
电子商务经营者在日常经营管理中应承担的一般性义务	应当依法办理市场主体登记	10
	依法履行纳税义务，并依法享受税收优惠	11
	依法需要取得相关行政许可的，应当依法取得行政许可	12
	销售的商品或者提供的服务应当符合保障人身、财产安全的要求和环境保护要求	13
	应当依法出具纸质发票或者电子发票等购货凭证或者服务单据	14
	持续公示营业执照信息、与其经营业务有关的行政许可信息、终止电子商务信息等并及时更新	15、16
	应当全面、真实、准确、及时地披露商品或者服务信息	17
	在展示特定化搜索结果的同时，应当向该消费者提供不针对其个人特征的选项	18
	以显著方式提示搭售商品或服务的行为	19
	应当按照约定向消费者交付商品/服务，并承担商品运输中的风险和责任	20
	不得对押金退还设置不合理条件	21
	不得滥用市场支配地位，排除、限制竞争	22
	应当遵守法律、行政法规有关个人信息保护的规定	23
	不得对用户信息查询、更正、删除以及用户注销设置不合理条件	24
	依法向有关主管部门提供电子商务数据信息	25
	依法从事跨境电子商务业务	26
电子商务平台经营者在日常经营管理中应承担的特殊义务	对申请进入平台的经营者进行核验、登记，建立登记档案，并定期核验更新	27
	依法向市场监管部门、税务部门报送平台内经营者信息，提示未办理相关登记的经营者依法办理工商、税务登记	28
	对未取得相关许可或不符合要求的产品应当依法采取必要的处置措施，并向有关主管部门报告	29
	应当采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动	30
	应当记录、保存平台上发布的商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年	31
	制定平台服务协议和交易规则，明确进入和退出平台、商品和服务质量保障、消费者权益保护、个人信息保护等方面的权利和义务	32
	应当在其首页显著位置持续公示平台服务协议和交易规则信息或者上述信息的链接标识	33
	修改平台服务协议和交易规则，应当在其首页显著位置公开征求意见	34
	不得对平台内经营者在平台内的交易进行不合理限制或者附加不合理条件，或者向平台内经营者收取不合理费用	35
	及时公示依据服务协议和交易规则对平台内商家的处理措施	36
	应当以显著方式区分标记自营业务和平台内经营者开展的业务	37
	资质审查及安全保障义务	38
	建立健全信用评价制度，公示信用评价规则	39

分类	职责内容	《电商法》条款序号
	不得删除消费者对其平台内销售的商品或者提供的服务的评价	39
	以多种方式向消费者显示商品或者服务的搜索结果；对于竞价排名的商品或者服务，应当显著标明“广告”	40
	应当建立知识产权保护规则	41
	应对侵犯知识产权的行为采取必要措施	42-45
	可以为经营者之间的电子商务提供仓储、物流、支付结算、交收等服务，不得采取集中竞价、做市商等集中交易方式进行交易，不得进行标准化合约交易	46

2、关于银行电商平台责任承担的常用条款

根据现行的电商法律法规，电商平台责任承担主要依据《电子商务法》中关于相关责任的承担条款，但在实践中，《电子商务法》并未完全涵盖电商平台可能承担的全部民事责任情形，部分关于电商平台的责任条款散见于其他法律法规，如《侵权责任法》、《消费者权益保护法》中关于网络经营者的责任条款。鉴于此，笔者根据银行电商平台不同行为的分类，就其责任承担原则及涉及的法律法规依据进行如下梳理：

行为分类	基本规则	法律法规依据
电商平台对其标记为自营业务需承担的民事责任——依法承担商品销售者或者服务提供者的民事责任	•由电商平台自身原因对消费者造成的损害后果承担侵权责任	《电子商务法》第37条 《侵权责任法》第36条、第41条、第43条 《消费者权益保护法》第44条
	•作为销售者，因其过错使产品存在缺陷，造成他人损害的，承担侵权责任	《侵权责任法》第42条
	•作为销售者，非因其过错造成损害的，受害人可以向生产者或销售者请求赔偿，销售者赔偿后，有权向生产者追偿（中间责任）	《侵权责任法》第43条
电商平台未采取必要措施和未尽审核或安全保障义务的民事责任	•未采取必要措施的连带责任： -知道或者应当知道平台内经营者销售的商品或者提供的服务不符合保障人身、财产安全的要求 -有其他侵害消费者合法权益行为，未采取必要措施的	《侵权责任法》第36条 《消费者权益保护法》第44条 《电子商务法》第38条
	•未尽审核和安全保障义务的相应责任： -对关系消费者生命健康的商品或者服务，电子商务平台经营者对平台内经营者的资质资格未尽到审核义务 -对消费者未尽到安全保障义务，造成消费者损害的	《电子商务法》第38条

行为分类	基本规则	法律法规依据
电商平台对侵害知识产权行为的处理	•电子商务平台经营者接到知识产权权利人发出的通知后（应包含构成侵权的初步证据），应当及时采取必要措施，并将该通知转送平台内经营者；未及时采取必要措施的，对损害的扩大部分与平台内经营者承担连带责任	《电子商务法》第42条 《侵权责任法》第36条
	•电子商务平台经营者知道或者应当知道平台内经营者侵犯知识产权的，应当采取删除、屏蔽、断开链接、终止交易和服务等必要措施；未采取必要措施的，与侵权人承担连带责任	《电子商务法》第45条 《侵权责任法》第36条 《消费者权益保护法》第44条
电商平台的先行赔付责任	•广告经营者、发布者发布虚假广告的，消费者可以请求行政主管部门予以惩处。广告经营者、发布者不能提供经营者的真实名称、地址和有效联系方式的，应当承担赔偿责任	《消费者权益保护法》第45条
	•发布虚假广告，欺骗、误导消费者，使购买商品或者接受服务的消费者的合法权益受到损害的，由广告主依法承担民事责任。广告经营者、广告发布者不能提供广告主的真实名称、地址和有效联系方式的，消费者可以要求广告经营者、广告发布者先行赔偿	《广告法》第56条
电商平台违反电子支付规则	•电子支付服务提供者提供电子支付服务不符合国家有关支付安全管理要求，造成用户损失的，应当承担赔偿责任	《电子商务法》第54条
	•未经授权的支付造成的损失，由电子支付服务提供者承担；电子支付服务提供者能够证明未经授权的支付是因用户的过错造成的，不承担责任 •电子支付服务提供者发现支付指令未经授权，或者收到用户支付指令未经授权的通知时，应当立即采取措施防止损失扩大。电子支付服务提供者未及时采取措施导致损失扩大的，对损失扩大部分承担责任	《电子商务法》第57条
电商平台毁损电子交易资料	•在电子商务争议处理中，电子商务经营者应当提供原始合同和交易记录。因电子商务经营者丢失、伪造、篡改、销毁、隐匿或者拒绝提供前述资料，致使人民法院、仲裁机构或者有关机关无法查明事实的，电子商务经营者应当承担相应的法律责任	《电子商务法》第62条

3、银行电商平台公布的免责条款的效力

银行电商平台公布的免责条款并不能完全保障银行在电子商务活动中免于承担相应责任。根据检索结果，大多数银行开展电商业务时都习惯在其电商平台网站的“法律声明”文本中，或在电商平台官网底部向消费者提示银行设立的电商平台在交易过程中是免责的。类似条款如“本银行卡商城所提供商品或服务信息均由第三方供应商提供，本行仅为相关信息提供链接和支付结算服务，对交易不作任何担保”。部分发布前述免责声明的银行电商平台，在其网站页面中还保留了“XX银行信誉保证　100%正品承诺”等构成单方允诺的宣传字眼。根据现行的法律法规，银行开展电商业务即使在其官网中进行免责声明或对消费者进行风险提示，也不能完全保证免责，具体责任承担还需结合实际情况进行判定。

银行设立的电商平台相较于传统互联网电商平台来说，起步时间晚，管理体系也有待完善，为防止因第三方供应商或商家的原因对消费者造成损害进而导致银行电商平台面临责任承担的风险，银行电商平台可以考虑从以下两方面对责任进行把控：一是可以通过完善内部审核体系、明确入驻商家与平台的责任承担等方式对风险进行控制；二是银行开展电商业务应妥善保存其履行电子商务平台经营者责任的相关记录，在特定情况下，可以作为减轻或免除其责任的依据。

（四）银行开展电商业务的网络安全与数据保护

1、电子商务平台经营者的网络安全与数据保护职责

根据监管部门近期发布的一系列法规文件，电子商务平台经营者在网络安全与数据保护，尤其是个人信息安全保护领域的职责不断加强。《电子商务法》将电子商务定义为“通过互联网等信息网络销售商品或者提供服务的经营活动”，根据其定义可知，电子商务与互联网、信息网络等具有天然联系，密不可分。《电子商务法》在电子商务领域基本延续了《网络安全法》中关于网络运行安全、网络信息安全的相关规定，一方面对电子商务经营者在网络安全领域的责任与义务进行明确，另一方面也突出强调了对电子商务消费者个人信息保护的重视。

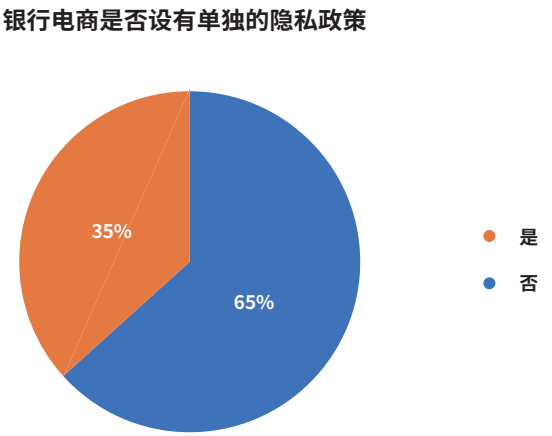
根据《电子商务法》、《网络安全法》等相关法律法规，电子商务平台经营者至少应从以下几方面着手进行网络安全与数据保护：

职责内容	法律法规
在展示特定化搜索结果的同时，应当向该消费者提供不针对其个人特征的选项	《电子商务法》第18条
不得对用户信息查询、更正、删除以及用户注销设置不合理条件	《电子商务法》第24条 《网络安全法》第43条
依法向有关主管部门提供电子商务数据信息	《电子商务法》第25条
对申请进入平台的经营者进行核验、登记，建立登记档案，并定期核验更新	《电子商务法》第27条
依法向市场监管部门、税务部门报送平台内经营者信息，提示未办理相关登记的经营	《电子商务法》第28条

职责内容	法律法规
者依法办理工商、税务登记	
应当采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动	《电子商务法》第30条 《网络安全法》第10条
应当记录、保存平台上发布的商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年	《电子商务法》第31条
不得删除消费者对其平台内销售的商品或者提供的服务的评价	《电子商务法》第39条
以多种方式向消费者显示商品或者服务的搜索结果；对于竞价排名的商品或者服务，应当显著标明“广告”	《电子商务法》第40条

除以上法律法规规定的职责外，今年4、5月份以来，网信办接连发布《App违法违规收集使用个人信息行为认定方法（征求意见稿）》、《网络安全审查办法（征求意见稿）》、《数据安全管理办法（征求意见稿）》、《儿童个人信息网络保护规定（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》等多部有关个人信息保护的文件，从隐私政策文本、网络运营者对网络安全与个人信息保护的职责，儿童个人信息网络保护等方面提出规范意见，推动了网络运营者的业务合规发展。银行运营的电商平台作为网络运营者之一，应密切关注并及时做好相应合规准备。

2、银行电商平台中个人信息保护制度建设亟待加强



相较于传统互联网电商平台对个人信息隐私保护的积极响应，银行电商平台对《隐私政策》的反映较为迟缓，根据笔者的检索，目前设有独立隐私权政策文本的银行电商平台比例约为35%。

工商银行“融e购”在隐私政策完善方面较为积极，其官网生效的版本为2018年10月21日制定并发布的，其中对于个人信息的收集、对外提供、保存、管理等方面都具有较为详细的规定。

不少银行电商还未对隐私政策给予充分的重视，部分银行电商目前没有发布单独的隐私政策，或存在已发布《隐私政策》，但颁布时间过早，条款简单，已不符合目前法律法规要求的情形。以下为某国有银行电商平台公布的隐私保密协议：


隐私保密协议

2012-12-25

1、我行收集您的相关信息，目的在于为您提供更优质的产品和服务。

2、我行将把以上相关信息用于保证您的资金安全、了解您的理财需求以及各项业务的开展。

3、我行设有严格的安全系统，未经允许的员工不得获取您的相关信息。

4、在法律规定的情况下，如司法机关、监管机构及其他相关机构需要，我行有可能提供您的相关信息。

5、我行可能会把您的相关信息提供给与我行联合提供业务的合作伙伴，该等合作伙伴仍需对您的相关信息进行保密。

6、我行将努力保证您相关信息的完整和准确，并为您变更信息提供便利。

从上述图片可以看出，该隐私保密条款发布时间为2012年12月25日，距今已经6年多，这期间《网络安全法》、《电子商务法》、《个人信息安全规范》、《互联网个人信息安全保护指南》等多部与个人信息保护密切相关的法律法规及规范性文件相继出台，目前若仅依靠图片版本的《隐私保密协议》显然已不符合业务发展的合规需求。

银行作为金融机构，对于数据安全、个人信息安全保护的意识普遍较为先进，依托于银行发展的银行电商平台更应充分发挥银行作为金融机构具有完善的数据管理制度的优势，加强对银行电商平台数据安全与个人信息安全的保护。

结语

银行电商平台在金融服务场景化的构建，业务模式创新等方面有其独特的发展特点。但是从本质上看，银行开展的电商业务在其发展过程中应遵循《电子商务法》等一系列调整电子商务业务的法律法规。从笔者初步检索情况来看，银行开展的电商业务在合规领域存在一定程度的滞后性，从业人员应密切关注电子商务领域的最新变化并结合其自身电子商务业务的发展特点积极做好合规安排。

附录：已检索的54家银行名单

序号	银行名称	序号	银行名称	序号	银行名称
1	工商银行	19	天津银行	37	郑州银行
2	农业银行	20	河北银行	38	重庆银行
3	中国银行	21	天津金城银行	39	成都银行
4	建设银行	22	上海华瑞银行	40	贵阳银行
5	交通银行	23	浙江网商银行	41	甘肃银行
6	中信银行	24	温州民商银行	42	大连银行
7	光大银行	25	重庆富民银行	43	厦门银行
8	华夏银行	26	哈尔滨银行	44	西安银行
9	民生银行	27	上海银行	45	九江银行
10	招商银行	28	江苏银行	46	中原银行
11	兴业银行	29	南京银行	47	江苏长江商业银行
12	广发银行	30	苏州银行	48	盛京银行
13	平安银行	31	杭州银行	49	浙商银行
14	上海浦东发展银行	32	温州银行	50	宁波东海银行
15	恒丰银行	33	宁波银行	51	宁波通商银行
16	渤海银行	34	徽商银行	52	厦门国际银行
17	中国邮政储蓄银行	35	江西银行	53	青岛银行
18	北京银行	36	赣州银行	54	深圳前海微众银行

第五节 跨境电商企业合规分析[179]

179. 本文原标题为《电商法元年面面观|新时期跨境电商企业合规要点图鉴》，作者陈际红、陈臧、薛泽涵，网址：http://www.zhonglun.com/content/2019/02-14/1603556501.html。

作为电子商务活动的重要组成部分，跨境电商进出口交易具备参与主体的多样性和贸易环境的复杂性，既考验跨境电商企业的合规管理工作，也对立法机关的监管法规与政策的制定提出挑战。对此，《电子商务法》于2019年1月1日正式生效，主要从跨境电商经营者守法要求，以及国家有关部门推进综合服务监管体系建设的角度入手，加强跨境电商行业规范顶层设计。在此框架下，为有序引导跨境电商零售进出口业务发展，海关总署等有关部门在2018年底陆续发布一系列针对性法规政策，对新时期跨境电商企业的合规工作提出新的具体要求。

SECTION 01

跨境电商新规都有哪些

这批于2018年底发布、于2019年1月1日起生效的跨境电商监管法规政策（见表1，以下统称“跨境电商新规”或者“新规”），旨在从税收政策、企业管理、信用管理等多方面加强对跨境电商企业的监管。

序号	法规名称	发布部门
1	《关于跨境电子商务零售进出口商品有关监管事宜的公告》（海关总署公告2018年第194号）（“《194号》”）	海关总署
2	《关于完善跨境电子商务零售进口监管有关工作的通知》（商财发【2018】486号）（“《486号》”）	商务部、国家发展和改革委员会、财政部、海关总署、国家税务总局、国家市场监督管理总局
3	《关于完善跨境电子商务零售进口税收政策的通知》（财关税【2018】49号）（“《49号》”）	财政部、海关总署、国家税务总局
4	《关于实时获取跨境电子商务平台企业支付相关原始数据有关事宜的公告》（海关总署公告2018年第165号）（“《165号》”）	海关总署
5	《关于调整跨境电商零售进口商品清单的公告》（财政部公告2018年第157号）（“《157号》”）	财政部、国家发展和改革委员会、工业和信息化部、生态环境部、农业农村部、商务部、中国人民银行、海关总署、国家税务总局,国家市场监督管理总局、国家药品监督管理局、国家密码管理局、国家濒危物种进出口管理办公室
6	《关于公布<海关认证企业标准>的公告》（海关总署公告2018年第177号）（“《177号》”）	海关总署

表1：跨境电子商务零售进出口相关法规

相较于以往覆盖面较小、过渡政策频发的立法特点，本次新规由不同监管层面的法规政策组合，以初步完整的监管体系呈现，监管重点明确且力度加大，将迫使参与跨境电商的各类企业高度重视企业的全面合规工作。

SECTION 02

新规是否适用于所有跨境电商交易场景

然而，并非所有的跨境电商交易行为均会纳入上述新规的监管范围。

从消费行为看，上述新规仅适用于“跨境电商零售进出口”。依据《486号》规定，受新规约束的“跨境电子商务零售进口”是指中国境内消费者通过跨境电商第三方平台经营者自境外购买商品，并通过“网购保税进口”（海关监管方式代码1210）或“直购进口”（海关监管方式代码9610）运递进境的消费行为。

从商品要求看，仅在商品满足以下条件时，方能纳入跨境电商零售进口的适用范围：

A. 属于《跨境电子商务零售进口商品清单（2018年版）》（“《2018版清单》”）内、限于个人自用并满足跨境电商零售进口税收政策规定的条件；且

B. 通过与海关联网的电子商务交易平台交易，能够实现交易、支付、物流电子信息“三单”比对；或

C. 未通过与海关联网的电子商务交易平台交易，但进出境快件运营人、邮政企业能够接受相关电商企业、支付企业的委托，承诺承担相应法律责任，向海关传输交易、支付等电子信息。

即：仅在商品满足上述“A+B”或者“A+C”条件时，才会落入跨境电商新规适用范围。基于上述要求，若商品不在《2018版清单》范围内或者超出个人自用范围的，或是企业无法自行传输或者委托进出境快件运营人、邮政企业向海关传输交易、支付、物流“三单”信息的进口销售行为，均不适用跨境监管新规，同样也无法享受跨境电商零售进口商品的特殊税收优惠政策。

SECTION 03

新规下跨境电商企业应重点关注的合规要求有哪些

纵览跨境电商新规，可以看到新规在合规层面呈现出“一对方向，两种模式，四类主体，九大要点”的鲜明特点。

“一对方向”：新规同时囊括了对跨境电商进口、出口这对方向的监管要求。

“两种模式”：新规规定目前企业参与跨境电商零售进口交易主要适用“网购保税进口”及“直购进口”两种监管模式。

“四类主体”：新规同时对于跨境电商企业、跨境电商平台、境内服务商、消费者等参与跨境电商零售进出口的四种主体提出要求。

“九大要点”：新规从企业管理、通关管理、税收管理、数据管理、信用管理、平台管理、场所管理、检疫、查验和物流管理、退货管理等九个方面对跨境电商企业提出全面合规要求。

（一）企业管理

1.注册登记

新规对于参与跨境电商零售进出口的各类企业均提出了明确的注册（信息）登记的要求，甚至将要求主体从境内电商平台企业扩展到境外电商企业。具体要求为：

参与跨境电商零售进口的境内跨境电商企业（包括物流、支付等），均需办理工商登记 + 在所在地海关办理注册登记。

参与进口的境外跨境电商企业同样需要注册登记，但需通过境内代理人在该代理人所在地海关办理注册登记。

参与出口的境内跨境电商企业（包括物流等）应在所在地海关办理信息登记。如需报关，应在海关办理注册登记。

2.资质要求

新规对于参与跨境电商零售进出口业务的境内服务的资质提出了明确的要求，具体包括：

物流企业	应获得国家邮政管理部门颁发的《快递业务经营许可证》。直购进口模式下，物流企业应为邮政企业或者已向海关办理代理报关登记手续的进出境快件运营人。
支付企业	为银行机构的，应具备银保监会或者原银监会颁发的《金融许可证》。
	为非银行支付机构的，应具备中国人民银行颁发的《支付业务许可证》，支付业务范围应当包括“互联网支付”。

对此，企业若自身作为物流、支付企业的，应关注是否具备相应的资质要求；若自身作为跨境电商企业（电商平台企业）的，应关注合作的物流、支付企业是否具备相应的资质。

（二）通关管理

1. 商品首次进口许可批件、注册或备案要求

新规对于明确列入《2018版清单》并采取直购进口或者网购保税进口的商品，按照个人自用进境物品监管，不执行有关商品首次进口许可批件、注册或者备案要求。同时，对于化妆品、婴幼儿配方奶粉、医疗器械、特殊食品（包括保健食品、特

殊医学用途配方食品等）等特殊商品，无论是采用网购保税进口模式还是直购进口模式，均延续之前的过渡监管政策，不执行首次进口许可批件、注册或备案要求。

对此，我们建议企业需根据商品类别，确认是否落入《2018版清单》，由此进一步确定商品首次进口许可的证件、注册或者备案要求。

2.数据传输

新规对于进出口申报前参与跨境电商进出口零售的相关企业向海关传输电子信息的方式、内容等提出明确要求。

进口申报前，跨境电子商务平台企业或跨境电子商务企业境内代理人、支付企业、物流企业应当分别通过国际贸易“单一窗口”或跨境电子商务通关服务平台向海关传输交易、支付、物流等电子信息（应施加电子签名），并对数据真实性承担相应责任。

直购进口模式下，邮政企业、进出境快件运营人可以接受跨境电子商务平台企业或跨境电子商务企业境内代理人、支付企业的委托，在承诺承担相应法律责任的前提下，向海关传输交易、支付等电子信息（应施加电子签名）。

出口申报前，跨境电子商务企业或其代理人、物流企业应当分别通过国际贸易“单一窗口”或跨境电子商务通关服务平台向海关传输交易、收款、物流等电子信息（应施加电子签名），并对数据真实性承担相应法律责任。

企业应认识到，与海关之间数据传输，是进出口通关管理必不可少的工作流程。对此，企业应做好数据安全传输保障。同时，跨境电商平台应在消费者下单前告知消费者，其个人信息（交易信息等）基于法律法规及海关监管要求，需要共享至海关。

3.报关要求

对于进口，跨境电商企业（境内代理人）或委托的报关企业需填写《中华人民共和国海关跨境电子商务零售进出口商品申报清单》（“《申报清单》”）+采取“清单核放”方式办理报关手续。

对于出口，一般情况下，跨境电子商务企业或其代理人应提交《申报清单》，采取“清单核放、汇总申报”方式办理报关手续。而在跨境电子商务综合试验区内符合条件的跨境电子商务零售商品出口，可采取“清单核放、汇总统计”方式办理报关手续。对此，我们建议跨境电商企业或其代理人除了提交《申报清单》外，应关注是否处于跨境电商综合试验区，由此决定是采取“清单核放、汇总申报”还是“清单核放、汇总统计”方式办理报关手续。

4.汇总申报

新规要求跨境电商企业或其代理人在办理零售出口后，应当于每月15日前，将上月结关的《申报清单》依据清单表头同一收发货人、同一运输方式、同一生产

销售单位、同一运抵国、同一出境关别，以及清单表体同一最终目的国、同一10位海关商品编码、同一币制的规则进行归并，汇总形成《中华人民共和国海关出口货物报关单》向海关申报。

（三）税收管理

此次新规中的税收政策重点明确了办税时间及交易限值。其中，作为跨境电商零售进口商品在关税、进口环节增值税和消费税的代收代缴义务人，在海关注册登记的跨境电商平台企业、物流企业或申报企业应当依法向海关提交足额有效的税款担保。海关放行后30日内未发生退货或修撤单的，代收代缴义务人在放行后第31日至第45日内向海关办理纳税手续。

交易限值及应纳税款的关系如下表所示：

交易限值	单次交易限值由人民币2000元提高至5000元。
	年度交易限值由人民币20000元提高至26000元。
	对跨境电商零售进口清单内商品实行限额内零关税、进口环节增值税和消费税按法定应纳税额70%。
位于上下限值区间	完税价格超过5000元单次交易限值但低于26000元年度交易限值，且订单下仅一件商品时，可以自跨境电商零售渠道进口，按照货物税率全额征收关税和进口环节增值税、消费税，交易额计入年度交易总额。 但年度交易总额超过年度交易限值的，应按一般贸易管理。

对此，我们建议跨境电商企业应对每笔订单以及定期对阶段订单进行关注、监控和统计，关注应纳税额的变化。如超出交易限额对消费者消费金额将产生影响的，应提前告知消费者相关细节。

（四）数据管理

除上述“通关管理”中提到的数据传输要求外，在日常监管过程中，参与跨境电商零售进出口的各类企业均需与海关共享相关业务数据，具体义务要求为：

跨境电商平台企业	应向海关实时传输施加电子签名的跨境电商零售进口交易电子数据（相关原始数据，包括订单号、商品名称、交易金额、币制、收款人相关信息、商品展示链接地址、支付交易流水号、验核机构、交易成功时间以及海关认为必要的其他数据）。
支付、物流企业	应如实向监管部门实时传输施加电子签名的跨境电商零售进口支付、物流电子信息。
报关企业	接受跨境电商企业委托向海关申报清单。
物流企业	应向海关开放物流实时跟踪信息共享接口。

涉嫌走私或违反海关监管规定的跨境电商企业、平台、境内服务器	应配合海关调查，开放交易生产数据（ERP数据）或原始记录数据。

此外，随着《网络安全法》及配套的个人信息保护相关法律法规的相继出台与深化落实，个人信息保护问题得到各界的充分关注，新规同样在此对企业提出管理红线：

第一，海关对违反本通知规定参与制造或传输虚假“三单”信息、为二次销售提供便利、未尽责审核订购人身份信息真实性等，导致出现个人身份信息或年度购买额度被盗用、进行二次销售及其他违反海关监管规定情况的企业依法进行处罚。

第二，对利用其他公民身份信息非法从事跨境电商零售进口业务的，海关按走私违规处理，并按违法利用公民信息的有关法律规定移交相关部门处理。

对此，我们建议跨境电商企业应充分重视交易过程中所收集的个人信息的合法、合理、按约定使用，并做好个人信息保护。

（五）信用管理

新规在原有的《海关企业新用管理办法》的基础上进一步丰富了信用管理的标准，并建立起信用评级、公示与惩戒制度。参与跨境电子商务零售进出口业务并在海关注册登记的企业，纳入海关信用管理。

海关将重点关注企业在内部控制（组织机构、进出口业务、内部审计、信息系统）、财务状况、守法规范（守法状态、进出口业务规范、海关管理要求、外部信用）、贸易安全（场所安全、进入安全、人员安全、商业伙伴安全、货物安全、集装箱安全、运输工具安全、危机管理）等层面的表现，并据此进行信用评级。

海关根据信用等级（分为认证企业、一般信用企业和失信企业等三个等级。认证企业分为高级认证企业和一般认证企业）实施差异化的通关管理措施，包括：

对认定为诚信企业的，依法实施通关便利。

对认定为失信企业的，依法实施严格监管措施

高级认证企业信息和失信企业信息共享至全国信用信息共享平台，通过“信用中国”网站和国家企业信用信息公示系统向社会公示，并依照有关规定实施联合激励与联合惩戒。

考虑到公示与惩戒手段将对企业的外在声誉及商业开发产生实质性影响，我们提醒企业需充分重视信用管理，按照新规要求推进合规自评与自我完善整改工作。

（六）平台管理

《电子商务法》就电商平台应当承担的平台管理责任义务进行了细致的规定，跨境电商新规基于这些基本要求，结合跨境电商实务的具体行为规范，对跨境电商平台企业提出更为详尽明确的操作要求。为满足新规要求，提升合规水平，我们建议企业应当做好以下设置/制度建设工作：

在商品订购网页或页面其他醒目位置向消费者提供风险告知书，获取其确认同意后方可下单购买。风险告知书中应明确包括：1）商品相关标准及技术规范，提醒消费者注意与国标的差别并自行承担相关风险；2）配备商品中文电子标签；3）提醒消费者购买的境外商品仅限自用而不得再次销售。

建立平台内交易规则及平台管理制度。对平台内入驻企业的主体身份真实性进行审核，与其签署协议并明确责任义务，公示主体身份信息和消费者评价、投诉信息。

分区块、频道，或者用明显标识对跨境电商和国内电商企业/产品进行划分。

为消费者提供纠纷处理和维权通道。

在网站醒目位置及时发布商品风险监测信息、监管部门发布的预警信息等。

建立防止跨境电商零售进口商品虚假交易及二次销售的风险控制体系。

及时关闭平台内禁止以跨境电商零售进口形式入境商品的展示及交易页面，并将有关情况报送相关部门。

（七）场所管理

新规对于网购保税进口模式的开展均有明确的区域限制，其仅能在海关特殊监管区域或保税物流中心（B型）内开展。同时，针对业务实践中出现的部分跨境电商企业为了解决保税区内体验店经营困境而将部分的体验店设置在远离海关保税区的中心城区，以满足顾客线下自提网购保税商品的需求的情形，新规明确提出原则上不允许这类“网购保税+线下自提”模式在海关特殊监管区域外开展。

同时，对于监管作业场所，跨境电商监管作业场所经营人或者仓储企业应按照海关要求建立计算机系统并按要求交换电子数据。

（八）检疫、查验和物流管理

新规提出，网购保税进口业务在一线入区时以报关单方式进行申报。跨境电子商务零售进出口商品可采用“跨境电商”模式进行转关。其中，跨境电子商务综合试验区所在地海关可将转关商品品名以总运单形式录入“跨境电子商务商品一批”，并需随附转关商品详细电子清单。以“网购保税进口”（监管方式代码1210）海关监管方式进境的商品，不得转入适用“网购保税进口A”（监管方式代码1239）的

城市继续开展跨境电子商务零售进口业务。但网购保税进口商品可在同一区域（中心）内的企业间进行流转。

值得注意的是，新规并未明确提及之前针对部分特殊商品作为进口前置条件的检疫、查验要求。在此情形下，我们理解仍旧沿袭原有的安排。以化妆品为例，新规实施后，化妆品未经动物试验的，仍无法通过跨境电商平台在境内进行销售。

（九）退货管理

新规对于跨境电商进出口模式下办理退货手续做出了明确规定。

在跨境电子商务零售进口模式下，允许跨境电子商务企业境内代理人或其委托的报关企业申请退货，退回的商品应当符合二次销售要求并在海关放行之日起30日内以原状运抵原监管作业场所，相应税款不予征收，并调整个人年度交易累计金额。

对超过保质期或有效期、商品或包装损毁、不符合我国有关监管政策等不适合境内销售的跨境电子商务零售进口商品，以及海关责令退运的跨境电子商务零售进口商品，按照有关规定退运出境或销毁。

在跨境电子商务零售出口模式下，退回的商品按照有关规定办理有关手续。

对此，我们建议跨境电商企业如需办理退货，应根据进出口模式要求，针对不同商品情况，响应上述不同的处理要求。

结语

实现跨境电子商务有序管理与规范运行，是我国推进新业态新模式发展的重要举措。跨境电商新规在这一时代趋势与战略要求的背景下应运而生，彰显了国家对于推进跨境电商零售进出口行业积极健康发展的决心与智慧。对此，跨境电商企业需切实关注新规中提及的合规要点，并做好评估合规工作，共同参与我国跨境电商行业规范治理工作。

第六节 酒店行业数据合规分析[180]

自欧盟《通用数据保护条例》（“GDPR”）生效以来，共有约68起公开的处罚案例。[181]近日，英国信息监管局（Information Commissioner’s Office，简称“ICO”）发出了两份声明，拟对B航空公司[182]和M国际酒店集团[183]开出1.83亿英镑和9920万英镑的巨额罚单。两份处罚都还没有生效，ICO还需要在考虑拟受处罚公司的陈

180.本文原标题为《从某国际酒店集团违反GDPR被罚看酒店行业数据治理》，作者周洋、孟宪石、吕皓，网址：http://www.zhonglun.com/Content/2019/09-02/1438095330.html。
181.参见 http://www.enforcementtracker.com/
182.参见ICO官网相关声明 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
183.参见ICO官网相关声明 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

述以及涉及的欧盟其他成员国数据保护机构[184]的意见后作出最终处罚决定。如这两份处罚最终落实，将成为GDPR生效以来金额最高的罚款。

M国际酒店集团是总部位于美国马里兰州的全球最大的国际酒店管理公司之一。本次ICO拟对M国际酒店集团处罚是关于M国际酒店集团于2018年11月通知ICO的网络安全事件，即全球约3.39亿条客户记录，其中包括欧洲经济区（EEA）31个国家的3000万条居民个人信息，700万英国居民个人信息被泄露。据查，该网络安全事件是由于M国际酒店集团旗下S酒店管理系统被黑客攻击导致的数据漏洞，该漏洞自2014年便已存在。M国际酒店集团在2016年收购了S酒店集团，但在2018年才发现此漏洞。ICO认为M国际酒店集团在收购S酒店集团时未作充分的尽职调查，并且在保证酒店系统安全方面，也未采取更多的保护措施。

184.GDPR第51条规定，每个成员国应当建立一个或多个独立公共机构，负责监管GDPR的实施。根据GDPR第56.1条和第60.1条的规定，数据控制者或处理者的主要营业机构或唯一营业机构所在地的监管机构应充当领导性监管机构。领导性监管机构应和其他相关监管机构进行合作，努力达成共识。

185.参见欧洲数据保护委员会官网相关内容https://edpb.europa.eu-/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

186.GDPR共有99条正文条款（Article）和173条引注（Recital）。引注条款虽不是正文，但是对正文条款的背景交代和具体阐释。

187.参见GDPR第23条引注。

SECTION 01

中国本地酒店也可能受GDPR管辖

是否只有这种在欧盟有分支机构的国际连锁酒店才受GDPR管辖呢？答案是否定的，中国本地酒店也可能受到GDPR管辖。GDPR的地域管辖跟传统的地域管辖不同，不限于在欧盟境内有法律实体的机构。根据GDPR第3条对“地域范围”的规定，GDPR不仅适用于“在欧盟境内设立的数据控制者或处理者对个人数据的处理”，对于未设立在欧盟境内的数据控制者或处理者，只要其“为欧盟境内的数据主体提供商品或服务（不论此项商品或服务是否要求数据主体支付对价）”，或者“对发生在欧盟境内的数据主体的活动进行监控”，便也受到GDPR管辖。

对“欧盟境内的数据主体”的判断只需考虑数据主体（在被提供商品服务或被监控行为的时候）的位置是否在欧盟境内，而与国籍、住所等法律地位无关。[185]所以，如果欧盟成员国的游客来到中国，未在网上预订而直接走进某家本地酒店登记入住，即便他/她持有欧盟成员国护照，其个人信息也不当然受GDPR管辖。

如何理解“为欧盟境内的数据主体提供商品或服务”和“监控”两种情形的含义，可以参考GDPR的引注（Recital）[186]以及欧洲数据保护委员会（European Data Protection Board）发布的《关于GDPR地域管辖的指引-公众版本》。是否属于“为欧盟境内的数据主体提供商品或服务”可以通过确定数据控制者或处理者是否明显以欧盟成员国的数据主体为目标客户（targeting）来判断。确定这种意图的考虑因素比如，是否使用欧盟成员国使用的语言或货币，以使欧盟的数据主体有订购货物和服务的可能；是否有提及在欧盟境内的客户/用户。[187]比如，一家在欧盟没有任何分支机构的中国本土酒店，可能因为经常接待欧洲游客，若酒店的官网有欧

盟成员国的语言版本或可以用欧盟成员国的货币网上支付，这种情况很可能被认为是以欧盟成员国的数据主体为目标客户，从而需要受GDPR管辖。

至于是否构成“对发生在欧盟境内的数据主体的活动进行监控”，可以通过确定数据主体是否被网络追踪，包括对自然人进行分析处理，特别是为了做出与他/她有关的决策，或是对他/她的个人偏好、行为和态度进行分析或预测。[188]比如，一家本土酒店为了未来市场拓展或商业统计分析需要，在网上收集、处理了欧盟境内自然人的个人数据，对其存档并进行大数据分析，则有可能构成该条中的“监控”，从而受到GDPR管辖。

因此，按照GDPR的地域管辖规定，即便在欧盟境内没有任何实体设立和人员派驻的中国本地酒店，也有可能会受其管辖，也需重视GDPR合规工作。

188.参见GDPR第24条引注。
189.参见GDPR第4条定义条款。
190.参见GDPR第26条引注。
191.参见http://www.enforcementtracker.com/。

SECTION 02

酒店行业的数据治理

由于酒店行业涉及大量的客户信息收集和处理，其数据治理尤为重要，特别是跨国酒店集团，还涉及到数据出境问题，个人数据保护工作更加复杂。就设立于中国境内的酒店（无论跨国酒店集团还是中国本地酒店）而言，中国相关法律法规和GDPR的合规问题都需要同时考虑。

（一）酒店住客的哪些信息受到保护

酒店行业从业者首先需要考虑的是酒店住客的哪些数据受到GDPR或中国法规的保护，从而需要特别注意。

1.GDPR项下要求

GDPR保护的是个人数据，这里的“个人数据”指的是[189]任何已识别或可识别的自然人（即“数据主体”）相关的信息。一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而被识别。基于该定义，酒店预定信息、支付信息中的能识别到住客的数据，比如姓名、身份证或护照号码、住址、电话号码、银行卡信息、社会身份等能够单独凭此识别到个人的信息，肯定是受GDPR保护的。但是，其他不能单独凭借以识别到个人的信息，比如住客的消费习惯，也受GDPR保护吗？

这个问题可以从GDPR的引注部分[190]以及过往的执法案例[191]中得到答案。在GDPR语境下，能够识别到个人的信息的含义非常广泛，不仅包括本身可以识别到个人的信息，还包括和其他信息结合能够识别到个人的信息；不仅是数据控制者

192.参见GDPR第9条和第51条引注。
193.参见《网络安全法》第76条。
194.参见《信息安全技术 个人信息安全规范》附录B。

能够识别到个人，让其他人识别到个人的信息也算。这里“能够识别”不仅是普通人可识别，还包括利用处理数据当时可获得的合理的技术手段能够识别的。比如，酒店收集到的住客的职业信息，虽然大概率不能单独地识别到住客个人，但与其他APP上的信息（比如定位）结合并使用技术手段，则很有可能能够识别到个人。根据已有的GDPR的执法案例，电子邮箱、登录信息、预定/交易详情、职业、病历记录等都属于受GDPR保护的个人信息。

另外，GDPR还对“特殊类型个人数据的处理”作了特别规定[192]。对于一些敏感信息（对其处理将会对个人基本权利和自由产生重大风险的），具体来讲，即显示种族、政治观念、宗教或哲学信仰、工会成员的个人数据、基因数据、生物性识别数据、以及和个人健康、性生活或性取向相关的数据，GDPR禁止对这些数据进行处理。当然，也有例外规定，比如数据主体明确同意基于特定目的而授权处理或者处理这些数据对于数据控制者履行责任是必要的。鉴于此，酒店最好不要收集关于住客的以上列举的信息，即便为了给住客提供餐饮或满足客户特殊需要，一定要在收集这些特殊类型的信息前告知住客目的并单独取得住客的明确同意。

2.中国法项下要求

在中国法项下，需要注意酒店住客的“个人信息”和“个人敏感信息”的收集使用问题。中国法项下“个人信息”[193]的内涵和GDPR类似，都是包括了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。关于个人信息的示例，可以参考《信息安全技术-个人信息安全规范》附录A。根据其中的示例，酒店行业从业者需注意，除了我们常识中的个人基本身份信息属于受到保护的信息外，有一些也同样受保护的信息可能较难想到，比如住客的家庭关系、婚姻状况、宗教信仰、性取向、生理特征、职业、工作单位、网站浏览记录、位置信息等都属于受保护的个人信息。另外，由于有“与其他信息结合”这点，中国法项下个人信息的含义范围也是很广的，酒店住客的预定信息、支付信息、消费习惯等都需要谨慎处理，遵守中国法项下对个人信息的保护规定。

“个人敏感信息”是指[194]个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇的个人信息。通常情况下，14岁以下（含）儿童的个人信息和自然人的隐私信息属于个人敏感信息。关于个人敏感信息的示例，可以参考《信息安全技术个人信息安全规范》附录B，其中对个人敏感信息有更加严格的保护规定，需特别注意。

（二）酒店住客享有哪些权利？

明确了住客受保护的个人数据的范围，我们来看看住客对这些个人数据拥有哪些权利，也即酒店数据管理者负有哪些义务。

1.GDPR项下要求

在GDPR项下，我们主要关注数据主体权利及数据出境的相关规定。

GDPR项下有关数据主体权利的条款主要集中在第三章，和酒店行业较为相关的比如知情权[195]、访问权[196]、更正权[197]、删除权/被遗忘权[198]、数据可携权[199]。对这些权利，酒店数据管理者需要将GDPR的具体规定体现在其网络运营中，比如在隐私政策、会员守则、用户协议、技术操作中加以体现。其中最新和讨论最多的是被遗忘权和数据可携权。

“被遗忘权”赋予根据数据主体要求数据控制者删除其个人信息的权利，即便个人数据已被公开，数据主体也可要求数据控制者采取合理措施删除。对于中国境内的酒店来说，遵守该规定可能有些难度。因为根据《治安管理处罚法》等法律法规，酒店是被要求收集住客身份信息并直接联网记录到公安系统上的。关于这项权利在中国语境下能落实到何种程度有待实践考验。

“数据可携权”是指数据主体有权要求以一种结构化的、通用的、机器可读的形式复制他们的个人数据。数据主体也可以选择将他们的数据传输给其他数据控制者。酒店的数据管理者需要确保酒店的系统能够履行上述业务，保证住客的上述数据权利，比如为保证住客的数据可携权，酒店必须有可以保存住客元数据的系统，以便在住客请求时可以向其提供通用的、机器可读的数据，如果仅提供扫描文件/pdf格式，可能难以达到要求。

这些GDPR赋予数据主体的权利，给了住客极大的自主决定其个人信息的自由，在一定条件下，他们可以要求酒店删除其存储多年的住客的个人信息（删除权/被遗忘权），甚至可以要求酒店将住户的个人信息传输给其竞争对手（数据可携权）。除了上述因住客在GDPR项下享有的权利给酒店带来的义务外，酒店数据控制/处理者，还负有其他义务，如个人数据泄露时的通知义务，即在个人数据发生泄露的情况下，数据控制者应当在72小时以内报告监管机构，如可能给数据主体的权利、自由带来较高风险的，应当及时告知数据主体。

此外，对于国际连锁酒店来说，数据出境是绕不开的话题。对于跨境数据传输，GDPR的原则是当个人数据从欧盟转移到第三国时，GDPR所规定对欧盟境内自然人的数据保护水平不应降低（也包括从第三国转移到另一第三国）。[200]所以，GDPR的跨境数据传输要求和中国的企业也息息相关。不仅欧盟居民个人数据从欧盟向其他国家或地区传输要遵守GDPR跨境传输规则，从中国向其他非欧盟国家传输数据也可能需要遵守GDPR的相关规则。比如，中国的M酒店向其美国总部传输住客或员工数据。落实上述跨境传输原则的方式有两种：一是作出“充分保护水平”的认定（adequate level of protection decision）；二是“适当保障措施”（appropriate safeguards）。

195. 参见GDPR第13条，第14条。
196.参见GDPR第15条。
197.参见GDPR第16条。
198.参见GDPR第17条。
199.参见GDPR第20条。
200.参见GDPR第101条引注。

"充分保护水平"是指欧盟委员会作出认定，认为相关的国家/地区等对个人数据具有充分保护，只要在这份欧盟委员会列出的"白名单"中，就可以将欧盟境内个人的数据传输过去，不受任何额外的限制。到目前为止，在这份"白名单"上的有：安道尔、阿根廷、加拿大（商业机构）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭和美国（仅限于隐私盾框架/Privacy Shield Framework ）[201]。这里"隐私盾框架"[202]指的是规范欧盟和美国之间出于商业目的的个人数据交换的机制。其主要目的是向美国的公司提供可靠的机制，以便其接受从欧盟传输至美国的个人数据。美国的公司要受惠于隐私盾框架，必须遵守美国商务部（Department of Commerce）发布的隐私盾规则（Privacy Shield Principles）。想加入隐私盾的公司需要向美国商务部（通过隐私盾官网）自我认证，并公开承诺遵守隐私盾框架规则。虽然加入隐私盾框架是自愿的，但一旦加入，其违反承诺将会有法律后果。由于中国尚未在"白名单"中，涉及从欧盟传输到中国的个人数据无法依赖该"重组保护水平"认定规定得以合规传输。

"适当的保障措施"是指如果数据出境接收方不在上述被认定为有充分保护水平的"白名单"内，则控制者或处理者只有提供"适当的保障措施"才能将个人数据转移到该国。结合中国的法律实践，这样区分可能更便于理解："适当的保障措施"可以按照是否需要监管机构个案批准分为两大类：即（i）不需要监管机构提供任何具体授权的适当保障措施和（ii）需要监管机构提供具体授权的适当保障措施。

第一大类是不需要欧盟成员国数据保护监管机构的个案批准的适当保障措施，例如，经监管机构批准的"有约束力的公司内部规则"（Binding Corporate Rules）、欧盟委员会制定的"标准数据保护条款"（Standard Contractual Clause）、"行为准则"（Code of Conduct）、"认证机制"（certification mechanism）等。[203]

" 有约束力的公司内部规则" 是指在欧盟内欧盟境内成立的跨国公司数据传输的内部规则，它允许跨国公司将同一集团内部的个人数据在国际上转移到没有提供适当保护水平的国家。这些公司内部规则需提交给欧盟内欧盟境内有权的数据保护机构批准。[204]这项跨境合规传输规则，对于国际酒店集团来说是值得尝试的，集团订立公司内部规则，提交欧盟数据保护机构审批，通过后集团内部从欧盟到其他国家的传输就不再受额外限制了，对集团内部管理会方便很多。

"标准数据保护条款"是指欧洲委员会制定标准合同条款，为国际传输的数据提供保护。到目前为止，欧洲委员会已经发布了两套适用于从欧盟的数据控制者传输到其他地区的数据控制者（controller）的标准数据保护条款，以及一套适用于从欧盟的数据控制者传输到其他地区的数据处理者（processor）的标准数据保护条款。[205]这些标准合同条款对于有跨境传输要求的国际酒店集团来说很有实用价值，集团内部酒店之间以及酒店和第三方预定系统、在线旅行社之间的数据传

201.参见欧盟委员会官网相关内容 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en。
202.参加欧盟委员会官网相关内容 https://www.privacyshield.gov/Program-Overview
203.参见GDPR第46条。
204.参见欧盟委员会官网相关内容 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en。
205.参见欧盟委员会官网相关内容 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en。

输可以考虑参照该标准条款。

“行为准则”是指协会以及其它代表某类控制者或处理者的实体为了对适用GDPR进行细化，可以针对特定行业起草行为准则，其中就包括涉及将个人数据转移到第三国的行为准则[206]。一个特定于行业的规范可以使国家机构、利益集团、企业等都受益。经欧盟委员批准的行为准则是数据控制者或处理者证明其符合GDPR的重要手段之一。欧盟数据保护委员会负责核查所有登记的已生效行为准则，并以恰当的方式使得公众能够获取。目前我们尚未看到有中国的酒店行业协会颁布有关GDPR跨境传输的行业准则。

“认证机制”是指欧盟委员会鼓励建立数据保护认证机制、数据保护印章和标记，以证明数据控制者和处理者的操作符合GDPR。认证须经有权监管机构认可的认证机构颁发。颁发给控制者或处理者的认证的有效期最长是三年。欧盟数据保护委员会负责核查所有已登记的认证机制、数据保护印章和标记。不过，获得这个认证并不能减轻控制者或处理者遵循GDPR的义务，但是确实可以使公众能够快速判断相关产品和服务的数据保护水平，从而提高对品牌的信任。GDPR要求该类认证机构必须满足一定的资质，受到有权监管机构认可[207]。认可度较高的比如TrustArc的 GDPR Validation[208]。

第二大类是需要欧盟成员国数据保护监管机构提供具体授权（即需要监管机构的个案批准）的适当的保障措施，和酒店行业有关的是酒店数据控制者或处理者与数据接收者之间的合同条款，这种保证措施是需要数据保护监管机构个案审批才能实施跨境传输的[209]。

如果酒店不符合上述“充分保护认定”或“适当的保障措施”，要想跨境传输数据，只有满足特定减损条件才能进行。所谓减损条件，可以理解为在特定情形下，对跨境传输规则降低要求。比如，数据主体已被明确告知跨境传输不存在充分保护或适当的保障措施，预期的数据传输存在风险，但数据主体仍然明确表示同意该数据转移的；或者，转移对于履行数据主体与控制者之间的合同，或者履行数据主体在签订合同前所提出要求是必要的；或者，转移对于实现公共利益是必要的等情形下[210]。

此外，对于既不存在充分保护认定或适当的保障措施，也不符合上述减损条件，数据跨境传输在以下例外情形下可以进行：转移是非重复性的，仅关乎很小一部分数据主体的权利，对于实现控制者的正当利益是必要的，且该正当利益不会被数据主体的权利对于中国本地酒店来说，可能涉及到欧盟境内住客[211]的数据较为有限，该例外情形可能适用。不过，在根据该条做跨境传输前，需要通知监管机构和数据主体[212]。

206.参见GDPR第40条，第41条。
207.参见GDPR第42条，第43条，第100条引言引注。
208.参见 https://www.trustarc.com/products/gdpr-validation/
209.参见GDPR第46.3条。
210.参见GDPR第49条。
211.注意上文对“欧盟境内的数据主体”的判断。
212.参见GDPR第49.1条，第113条引注。

213.参见《消费者权益保护法》第29条。
214.参见《电子商务法》第24条，第25条。
215.参见《网络安全法》第四章。

2.中国法项下要求

中国法项下，也有很多酒店数据管理者应当注意的数据主体的权利、酒店数据管理者的义务以及跨境传输的要求，我们比照GDPR中规定的相关权利和义务来分析。

在法律层面关于酒店住客个人信息保护的法律主要是《网络安全法》，《电子商务法》和《消费者权益保护法》。《消费者权益保护法》中关于消费者个人数据权利的保护其实只有一条，主要规定了经营者在收集、使用消费者个人信息时，应当遵循的原则；消费者对收集、使用信息的知情权、同意权；经营者不得泄露消费者个人信息的义务这几个方面[213]。《电子商务法》明确了电子商务经营者需要保证用户信息查询、更正、删除以及用户注销的权利，但依照法律、行政法规的规定要求电子商务经营者保存或提交有关主管部门的，电子商务经营者应当保存或提交。[214]《网络安全法》从收集、使用个人信息的原则，个人信息主体的知情权、同意权、信息删除权、更正权，防止信息泄露和及时告知主管机关的义务等方面做了更为详细的规定[215]。

中国法律下的这些权利和义务和GDPR中的有类似的地方，但细节规定也有不同。例如个人信息主体的“删除权”，在中国法律下，只有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，才有权要求网络运营者删除其个人信息。而在GDPR项下数据主体有更大的删除权，比如如果酒店为了市场营销目的处理住客数据，数据主体可以无条件要求数据管理方删除其数据。再比如，对信息泄露及时告知主管机关的义务，GDPR要求数据控制者在知悉泄露后72小时内报告监管机构，《网络安全法》同样要求告知有关主管部门，但未明确告知的具体时限。

值得一提的是，《网络安全法》对“关键信息基础设施”的运营者规定了额外的安全保护义务，比如，需要设置专门的安全管理机构和安全管理负责人，自行或者委托第三方对其网络的安全性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监管部门，对重要系统和数据库进行容灾备份等。酒店行业的信息系统是否属于关键信息基础设施呢？

《网络安全法》对关键信息基础设施的描述是“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”。根据这个规定，普通的酒店应该不属于关键信息基础设施，具体判断需要参照相关配套文件。中国国家网信办2016年发布的《关键信息基础设施网络安全检查操作指南》对关键信息基础设施的判断确定了三个步骤，一是判定属于关键信息基础设施的关键业务，二是确定支撑该业务的信息系统，三是依据业务对信息系统的依赖程

度和考虑信息系统发生安全事故后可能造成的损失，判定关键信息基础设施。酒店行业并未出现在第一步的关键业务判定列表中，所以一般认为酒店行业不属于关键信息基础设施。但是，第三步的损失量化判定过程中有提到一旦发生网络安全事故，可能造成100万人个人信息泄露的信息系统应被认定为关键信息基础设施。因此，大型的酒店集团（比如M酒店，在开篇所述事故中导致了全球约3.39亿条客户信息被泄露）不排除被认定为关键信息基础设施的可能性。

除了法律层面的规定外，对于酒店行业的数据管理者来说，《个人信息安全规范》是做好中国法项下合规工作需要关注的重要文件。其中，对个人信息安全基本原则、个人信息的收集、保存、使用、委托处理、共享、转让、公开披露、个人信息安全事件的处置、个人信息及个人敏感信息的定义和示例、隐私政策模板等都给出了详尽的指引。《个人信息安全规范》不是法律法规，它的法律地位是“推荐性国家标准”。但是，由于《个人信息安全规范》具有很强的实践性，是国家保证《网络安全法》等法律法规真正落地实施的重要方式，也是相关政府主管部门对个人信息处理活动进行监督、管理和评估时的重要参考依据。而且，根据《国务院办公厅关于印发国家标准化体系建设发展规划（2016-2020年）的通知》，我国标准体系建设的目标之一是“强制性标准守底线、推荐性标准保基本、企业标准强质量的作用充分发挥”。作为推荐性标准，《个人信息安全规范》应该被视为企业普遍适用的实践指南。

关于个人信息出境，中国国家网信办于2019年6月发布了《个人信息出境安全评估办法（征求意见稿）》，其中规定个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估[216]。如果该征求意见稿生效，将大大增加境内企业数据出境的难度。报经监管机构进行安全评估的要求将扩大到所有网络运营者，而非以往仅限于关键信息基础设施运营者[217]。这样的规定虽然没有强制要求酒店数据管理者这样的网络运营者将个人数据存储于境内，但是因为出境前需要做个案评估审批，事实上给数据出境增加了极大的难度。

（三）酒店行业数据治理的责任划分

上文较为详细地分析了酒店行业需注意的有关数据保护（包括数据出境）方面GDPR和中国法项下的主要规定，那么一旦上面这些规定的合规工作没有做好，酒店行业数据保护的责任人是谁呢（酒店管理公司，酒店业主，第三方平台）？我们仍然从GDPR和中国法两个视角来看。

1、GDPR项下要求

想要厘清GDPR项下酒店数据保护的责任主体，我们首先需要分清几个概念：数据控制者、共同控制者、处理者[218]。这三个概念在GDPR正文条款中都有定义，但

216.参见《个人信息出境安全评估办法（征求意见稿）》第3条。
217.参见《网络安全法》第37条，《个人信息和重要数据出境安全评估办法（征求意见稿）》第9条，《信息安全技术 数据出境安全评估指南（征求意见稿）》第4.2.6条。
218.参见GDPR第4条，第26条。

欧盟委员会官网上对其的解释更为简明。

“数据控制者”确定处理个人数据的目的和方法，因此，如果一个企业决定“为什么”和“如何”处理个人数据的，那么它就是数据控制者。当企业与一个或多个组织共同决定“为什么”和“如何”处理个人数据时，这些企业/组织就是“共同控制者”。共同控制者之间的内部关系由双方约定安排，但对数据主体承担共同的、连带的责任。“数据处理者”仅在控制者的委托下处理个人数据，数据处理者通常是企业外部的第三方技术公司。数据处理者对控制者的职责需在合同中加以规定，例如，合同必须明确在合同终止后个人数据该怎么处置。处理者的典型活动是提供IT解决方案，包括云存储。[219]需要特别说明的是，当不止一个控制者或处理者，或控制者与处理者同时涉及到同一项数据保护违规处理时，每个控制者或处理者都应当对损失负有连带责任，以便保证对数据主体的有效赔偿。[220]

酒店住客的预定通常会分为以下几个渠道：(1) 最常见的是从酒店管理公司的官网直接预定，通常价格是最低的，但是酒店管理公司对每个预定要向酒店业主收取一定的费用；(2) 通过第三方酒店预定系统进行预定，比如全球分销系统/GDS（Global Distribution System），通过GDS预订的，GDS会对每个预定向酒店收取一定的费用；(3) 通过在线旅行社/OTA（Online Travel Agency）预定，比如携程会对每个预定向酒店收取一定费用；(4) 酒店住客直接到店入住，在酒店前台办理入住。除了预定系统的数据需要管理，酒店财务系统也会存有大量住客的信息。对于酒店住客数据的存储大致有两种模式：一种是数据储存在酒店本地的服务器系统内，一旦管理合同终止，业主仍留有存储器里的住客信息。另一种是纯云端存储，所有住客数据都第一时间上传到酒店管理公司或其委托的第三方的云端服务器中，一旦管理合同终止，所有数据都被酒店管理公司所掌握，业主可能几乎没有数据留存。

结合上述酒店行业的常见数据运作模式，我们认为，在酒店管理公司明显掌握数据控制权，比如预定是从酒店管理公司网站或从管理公司委托的第三方预定系统，且数据也是由管理者控制（如存储于其自身或委托的第三方的云端服务器上），则酒店管理公司可以被认为是数据控制者。这种情况下，酒店业主是否属于共同数据控制者，要具体看其是否能和酒店管理公司共同决定“为什么”和“如何”处理住客的个人数据。这种情况下，可能就要看在酒店管理合同中对于数据的收集和使用是如何约定了：(1) 如果管理合同中明确酒店业主不能收集、使用、处理、存储酒店住客的个人数据，则业主不应是数据的控制方，一旦发生数据安全方面的责任，责任应完全由管理公司承担。如果发生数据安全事件，数据主体可以向酒店管理公司或者第三方系统供应商追责，管理者和第三方之间的内部责任划分由他们之间的合同决定。(2) 如果酒店管理合同约定，业主可以和酒店管理者共同掌

219.参见 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en。
220.参见GDPR第82.4条。

握住客数据，决定住客的数据收集和使用问题，则酒店管理者、酒店业主会被视为共同数据控制者。这样的话，一旦发生安全事件，数据主体则可以向酒店管理者，酒店业主，或者第三方系统供应商追责。酒店管理者和酒店业主作为数据共同控制者内部的责任划分由其之间的合同决定。这种情况下，也应当在酒店管理者和酒店业主之间的合同中根据他们对于住客数据的实际控制能力，明确约定责任划分。

221.参见《网络安全法》第76条。
222.参见《电子商务法》第9条。
223.参见《个人信息安全规范》第3.4条，第8.6条。

2、中国法项下要求

要厘清中国法项下酒店数据保护的责任主体，我们也需要分清几个概念：网络运营者、电子商务经营者、个人信息控制者、共同个人信息控制者。

“网络运营者”是《网络安全法》中的概念，指的是网络的所有者、管理者和网络服务提供者。[221]据此，判断酒店管理者和酒店业主谁是《网络安全法》项下的数据安全责任主体，就是看谁拥有和管理酒店系统的数据的主体。

“电子商务经营者”是《电子商务法》中的概念，是指通过信息网络从事销售商品或者提供服务的自然人和组织，包括电子商务平台经营者、平台内经营者以及通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者。[222]考虑到现在很多酒店都有自己的网站预定渠道，这些酒店应当属于通过自建网站提供服务的电子商务经营者。酒店管理公司还是酒店业主是电子商务经营者，要看该提供预定服务的自建网站是谁拥有的，通常情况下对于国际酒店管理品牌该网站系统都是管理公司所拥有并运营。

“个人信息控制者”和“共同个人信息控制者”都是《个人信息安全规范》中的概念，“个人信息控制者”是指有权决定个人信息的处理目的、方式等的组织或个人。和GDPR类似，《个人信息安全规范》中也有共同个人信息控制者这个概念。虽然没有具体定义，但是规定了当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务。据此，如果酒店业主可以和酒店管理者共同决定住客个人信息处理的目的和方式，则酒店业主属于共同个人信息控制者，住客也可以向其主张数据安全损害赔偿，不过业主方可以在与酒店管理者的合同中约定内部的责任划分。由于《个人信息安全规范》中没有数据处理者的概念，在示例中将第三方技术工具提供商（例如网站经营者与在其网页或应用程序中部署统计分析工具的第三方插件）也算为共同个人信息控制者。据此，酒店管理者或业主使用的第三方系统也有可能被算作共同个人信息控制者。[223]

结语

224.参见《个人信息安全规范》第10.2条。

考虑到上述复杂的数据安全合规要求以及潜在的合规责任，酒店行业的数据管理者最好早做打算。

梳理酒店的个人数据保护现状。由于酒店行业属于个人数据密集行业，我们建议做好个人信息安全影响的评估梳理工作。《个人信息安全规范》中也提到，个人信息控制者应“建立个人信息安全影响评估制度，定期（至少每年一次）开展个人信息安全影响评估”[224]对于大型连锁酒店，很可能会落入GDPR要求设置专门的数据保护官职位的范围，对应着中国法项下要求的设立专职的个人信息保护负责人和个人信息保护工作机构。

重视隐私政策、会员协议以及其他与住客之间的协议，以及酒店与供应商、第三方数据处理机构的协议，注意对其中有关个人数据收集、处理等内容。收集最小必要的住客信息，对照GDPR的要求，用清晰、明确、易于理解的方式表述。

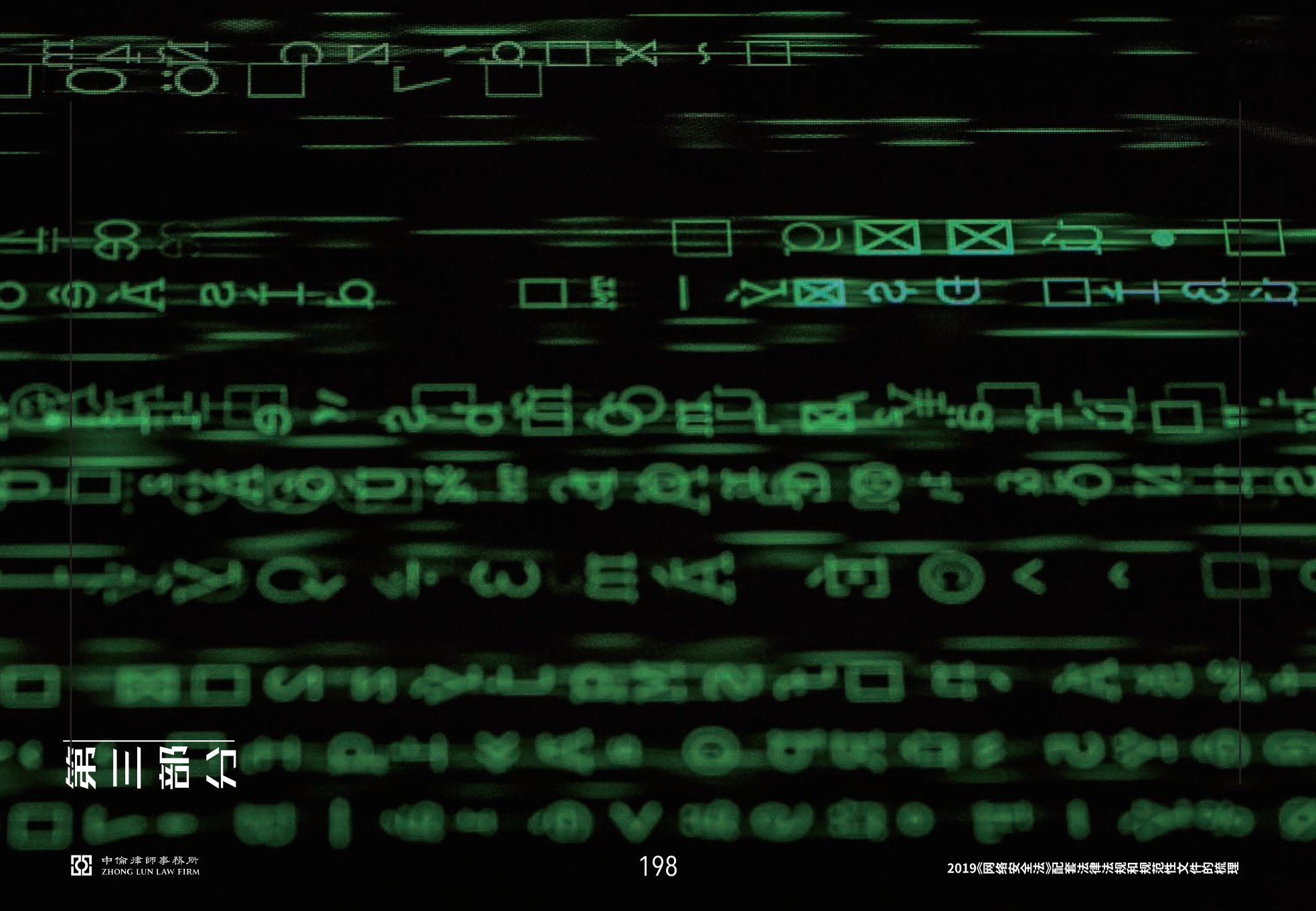
在酒店业主和酒店管理方之间的合同中明确约定住客数据收集和处理的义务方和责任方。

查验和升级酒店的信息技术系统，保障酒店的技术手段可以实现住客在GDPR项下的权利。

建立完善数据泄露报告制度及应急预案。对于个人数据的泄露，GDPR规定了向监管机构报告，并根据可能造成的风险程度向数据主体进行通报，否则将受到惩处，因此需要企业采取了合理的技术性、组织性的风险控制措施。

按照网络安全等级保护制度的要求，履行安全保护义务。大型连锁酒店的信息系统保存着海量的客户数据，需按照《网络安全法》的要求建立对数据的保护策略，建议按照《信息安全技术网络安全等级保护基本要求》标准三级防护要求实施数据保护。

数据安全尽职调查的必要性。随着GDPR和中国法律对个人信息保护的重视和执法力度的加大，在酒店行业的并购交易中，并购方对标的公司数据治理方面的合规尽调应被提到越来越重要的位置。正如ICO在对M国际酒店集团的处罚中的态度，并购方对其收购的标的公司中的个人数据的保护负有责任。这就要求并购方在并购交易的过程中做好充分的数据合规尽职调查，并据此在并购交易中建立适当的责任机制，且为收购后的数据合规管理打好基础，设计好制度。



第三部分

3

2019《网络安全法》配套法律法规和规范性文件的梳理

于2017年6月1日正式生效的《中华人民共和国网络安全法》，作为我国网络空间安全管理的基本法律，对网络运营者的网络运行安全、网络信息安全提出了若干制度性管理要求，重点包括网络信息内容管理制度、网络安全等级保护制度、关键信息基础设施的安全保护制度、个人信息和重要数据保护制度、网络产品和服务管理制度、网络安全事件管理制度等。

为保障上述制度的有效实施，一方面，以国家互联网信息办公室（以下简称“中央网信办”）为主的多个监管部门制定了多项配套法规，进一步细化和明确了各项制度的具体要求、相关主体的职责以及监管部门的监管方式；另一方面，全国信息安全标准化技术委员会（以下简称“信安标委”）同时制定并公开了一系列以信息安全技术为主的重要标准（包括征求意见稿），为网络运营者和监管部门提供了非常具有操作性的合规指引。与此同时，工业和信息化部（以下简称“工信部”）以及公安部也在自己的职权范围内，制定了相应的规定或规范性文件；国家质量监督检验检疫总局、国家食品药品监管总局、国家宗教事务局等部门针对各自领域内的数据制定了具体的规范、标准和规定。

整体而言，2019年，新发布的生效法规及尚处于征求意见稿阶段的法规草案数量较大。有以下几个特点：

在规范对象上，新发布规范对于上述各大网安制度均有涉及，并集中于网络产品和服务管理、网络安全事件管理等制度；移动智能终端、云计算、电子政务移动办公系统、移动互联网应用服务器等领域均出台了专门的安全技术标准。

在制定主体机构方面，信安标委作为信息技术领域标准的主要制定部门，加快了制定相关标准的进程，发布了大量的标准规范；工信部针对工业互联网建设、公共互联网安全等领域出台了相应的规范文件。中央网信办、公安部分别针对互联网信息内容管理、网络安全等级保护等主题发布了生效规范。

具体到细分制度层面：

在互联网信息内容管理制度方面，中央网信办、教育部等部门已经针对互联网信息内容制定了专门的管理规定，并提出了相关指导意见，以期全方位多层次地保障互联网信息内容的安全和可控性。

在网络安全等级保护制度方面，国家市场监督管理总局、国家标准化管理委员会发布《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》、《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》、《GB/T 25070-2019信息安全技术 网络安全等级保护安全设计技术要求》三个网络安全领域的国家标准，共同构筑新时代的网络安全等级保护制度，标志着等保2.0的正式到来。

在个人信息保护制度方面，其核心内容主要包括个人信息收集和使用过程中的安全规范以及个人信息和重要数据出境时的安全评估制度。2019年4月10日，公

安部制定发布了《互联网个人信息安全保护指南》，中央网信办在2019年6月13日制定发布了《个人信息出境安全评估办法（征求意见稿）》，以加强对个人信息的保护。此外，针对儿童个人信息保护问题，中央网信办还制定颁布了《儿童个人信息网络保护规定》，以加强对儿童个人信息的保护。

在网络安全管理制度方面，2019年5月24日，中央网信办会同国家发展和改革委员会等12部局联合起草并发布《网络安全审查办法（征求意见稿）》，对2017年国家网信办发布的《网络产品和服务安全审查办法（试行）》在适用范围、适用原则、审查内容和审查程序等诸多方面均有较大幅度的变更。中央网信办于2019年5月28日发布《数据安全管理办法（征求意见稿）》[225]，向社会公开征求意见，在继承《网络安全法》原则性规定的基础上，着重规范了网络运营者对于个人信息和重要数据的安全管理义务。2019年6月18日，工信部发布了《网络安全漏洞管理规定（征求意见稿）》，以求进一步加强网络安全漏洞管理。

在密码管理方面，2019年10月26日，第十三届全国人民代表大会常务委员会第十四次会议审议通过并公布了《中华人民共和国密码法》，该法将于2020年1月1日起施行，将对商用密码产品的管理及使用、境内外主体采购密码产品行为等产生深远影响。

为方便企业快速把握目前以《网络安全法》及其配套法规为核心的网络安全及数据合规保护的立法体系，同时感知2019年以来国内本领域的最新立法动向，我们将提供如下整理材料，供各界参考：

附件一：《网络安全法》相关法律和规范性法律文件汇总

附件二：2019年各主要部门在网络安全及数据保护合规领域的立法成果汇总。

225.《数据安全管理办法（征求意见稿）》原文请见 http://www.moj.gov.cn/news/content/2019-05/28/zlk_235861.html

附件一:《网络安全法》及其配套法律法规和规范性文件汇总

序号	文件名称	发布机构	生效时间	法律状态
1.基本法律和国家战略				
1.1	《国家安全法》	全国人大常委会	2015-7-1	现行有效
1.2	《网络安全法》	全国人大常委会	2017-6-1	现行有效
1.3	《全国人民代表大会常务委员会关于加强网络信息保护的决定》	全国人大常委会	2012-12-28	现行有效
1.4	《国家网络空间安全战略》	国家互联网信息办公室	2016-12-27	现行有效
1.5	《网络空间国际合作战略》	外交部、国家互联网信息办公室	2017-3-1	现行有效
2.互联网信息内容管理制度				
2.1	《互联网信息服务管理办法(2011修订)》	国务院	2011-1-8	现行有效
2.2	《即时通信工具公众信息服务发展暂行规定》	国家互联网信息办公室	2014-8-7	现行有效
2.3	《互联网危险物品信息发布管理规定》	公安部、国家互联网信息办公室、工业和信息化部、环境保护部、国家工商行政管理总局、国家安全生产监督管理总局	2015-3-1	现行有效
2.4	《互联网信息内容管理行政执法程序规定》	国家互联网信息办公室	2017-6-1	现行有效
2.5	《互联新闻信息服务管理规定》	国家互联网信息办公室	2017-6-1	现行有效
2.6	《互联网新闻信息服务许可管理实施细则》	国家互联网信息办公室	2017-6-1	现行有效
2.7	《互联网跟帖评论服务管理规定》	国家互联网信息办公室	2017-10-1	现行有效
2.8	《互联网论坛社区服务管理规定》	国家互联网信息办公室	2017-10-1	现行有效
2.9	《互联网群组信息服务管理规定》	国家互联网信息办公室	2017-10-8	现行有效
2.10	《互联网用户公众账号信息服务管理规定》	国家互联网信息办公室	2017-10-8	现行有效
2.11	《互联网新闻信息服务新技术新应用安全评估管理规定》	国家互联网信息办公室	2017-12-1	现行有效
2.12	《互联网新闻信息服务单位内容管理从业人员管理办法》	国家互联网信息办公室	2017-12-1	现行有效
2.13	《微博客信息服务管理规定》	国家互联网信息办公室	2018-3-20	现行有效
2.14	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》	国家互联网信息办公室	2018-11-30	现行有效
2.15	《互联网宗教信息服务管理办法(征求意见稿)》	国家宗教事务局	N/A	正式版未发布,未生效

序号	文件名称	发布机构	生效时间	法律状态
2.16	《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》	国家互联网信息办公室	N/A	正式版未发布，未生效
2.17	《网络生态治理规定（征求意见稿）》	国家互联网信息办公室	N/A	正式版未发布，未生效
2.18	《网络安全威胁信息发布管理办法（征求意见稿）》	国家互联网信息办公室	N/A	正式版未发布，未生效
2.19	《网络音视频信息服务管理规定》	国家互联网信息办公室	2020-1-1	已发布，未生效
3.网络安全等级保护制度				
3.1	《网络安全等级保护条例（征求意稿）》	公安部	N/A	正式版未发布，未生效
3.2	《网络安全等级保护测评机构管理办法》	公安部	2018-3-23	现行有效
3.3	《信息安全技术 网络安全等级保护定级指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
3.4	《信息安全技术 网络安全等级保护实施指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
3.5	《信息安全技术 网络安全等级保护测评过程指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
3.6	《GB／T 36627-2018信息安全技术 网络安全等级保护测试评估技术指南》	全国信息安全标准化技术委员会	2019-4-1	现行有效
3.7	《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》	全国信息安全标准化技术委员会	2019-12-1	现行有效
3.8	《GB/T 25070-2019信息安全技术 网络安全等级保护设计技术要求》	全国信息安全标准化技术委员会	2019-12-1	现行有效
3.9	《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》	全国信息安全标准化技术委员会	2019-12-1	现行有效
4.键信息基础设施安全保护制度				
4.1	《关键信息基础设施安全保护条例（征求意见稿）》	国家互联网信息办公室	N/A	正式版未发布，未生效
4.2	《国家网络安全检查操作指南》	中央网络安全和信息化领导小组办公室、网络安全协调局	2016-6-1	现行有效
4.3	《信息安全技术 关键信息基础设施安全检查评估指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
4.4	《信息安全技术 关键信息基础设施安全保障评价指标体系（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效

序号	文件名称	发布机构	生效时间	法律状态
4.5	《信息安全技术 关键信息基础设施网络安全保护要求(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
4.6	《信息安全技术关键信息基础设施安全控制措施(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.个人信息和重要数据保护制度				
5.1	《GB/T 35273-2017信息安全技术 个人信息安全规范》	全国信息安全标准化技术委员会	2018-5-1	现行有效
5.2	《信息安全技术 个人信息安全规范(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.3	《GB/T 34978-2017 信息安全技术移动智能终端个人信息保护技术要求》	全国信息安全标准化技术委员会	2018-5-1	现行有效
5.4	《信息安全技术 公共及商用服务信息系统个人信息保护指南》	工业和信息化部	2013-2-1	现行有效
5.5	《个人信息出境安全评估办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
5.6	《信息安全技术 数据出境安全评估指南(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.7	《信息安全技术 个人信息去标识化指南(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.8	《信息安全技术 个人信息安全影响评估指南(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.9	《互联网个人信息安全保护指南》	公安部	2019-4-10	现行有效
5.10	《信息安全技术 数据交易服务安全要求(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.11	《信息安全技术 信息安全风险评估规范》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.12	《数据安全管理办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
5.13	《App违法违规收集使用个人信息自评估指南》	App专项治理工作组	2019-3-1	现行有效
5.14	《网络安全实践指南-移动互联网应用业务功能个人信息收集必要性规范》	全国信息安全标准化技术委员会	2019-5-1	现行有效
5.15	《儿童个人信息网络保护规定》	国家互联网信息办公室	2019-10-1	现行有效
5.16	《信息安全技术 个人信息安全工程指南(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
5.17	《App违法违规收集使用个人信息行为认定方法(征求意见稿)》	App专项治理工作组	N/A	正式版未发布,未生效

序号	文件名称	发布机构	生效时间	法律状态
	《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（草案）》	国家市场监督管理总局；中国国家标准化管理委员会	N/A	正式版未发布，未生效
6.产品和服务管理制度				
6.1	《网络产品和服务安全审查办法（试行）》	国家互联网信息办公室	2017-6-1	现行有效
6.2	《关于发布<网络关键设备和网络安全专用产品目录（第一批）>的公告》	工业和信息化部；公安部；国家认证认可监督管理委员会；国家互联网信息办公室	2017-6-1	现行有效
6.3	《移动智能终端应用软件预置和分发管理暂行规定》	工业和信息化部	2017-7-1	现行有效
6.4	《GB/T 34942-2017 信息安全技术 云计算服务安全能力评估方法》	全国信息安全标准化技术委员会	2018-5-1	现行有效
6.5	《GBT 35278-2017信息安全技术移动终端安全保护技术要求》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.6	《GB/T 34975-2017信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法》	全国信息安全标准化技术委员会	2018-5-1	现行有效
6.7	《GB/T 34976-2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法》	全国信息安全标准化技术委员会	2018-5-1	现行有效
6.8	《GB/T 34977-2017信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法》	全国信息安全标准化技术委员会	2018-5-1	现行有效
6.9	《GB/T 35274-2017信息安全技术 大数据服务安全能力要求》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.10	《GB/T 35279-2017信息安全技术 云计算安全参考架构》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.11	《GB/T 35281-2017 信息安全技术 移动互联网应用服务器安全技术要求》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.12	《关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）的公告》	国家认监委 工业和信息化部 公安部 国家互联网信息办公室	2018-3-15	现行有效
6.13	《关于网络关键设备和网络安全专用产品安全认证实施要求的公告》	国家认监委 国家互联网信息办公室	2018-5-30	现行有效
6.14	《网络关键设备和网络安全专用产品安全认证实施规则》	国家认监委	2018-6-27	现行有效
6.15	《信息安全技术 网络产品和服务安全通用要求（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效

序号	文件名称	发布机构	生效时间	法律状态
6.16	《GB/T 35280-2017信息安全技术 信息技术产品安全检测机构条件和行为准则》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.17	《信息安全技术 网络安全专用产品类别与代码(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
6.18	《信息安全技术 工业控制系统产品信息安全通用评估准则》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
6.19	《信息安全技术 智能音视频采集设备应用安全要求(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
6.20	《GB/T 35282-2017 信息安全技术 电子政务移动办公系统安全技术规范》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.21	《GB/T 35287-2017 信息安全技术 网站可信标识技术指南》	全国信息安全标准化技术委员会	2018-7-1	现行有效
6.22	《信息安全技术 工业互联网平台安全要求及评估规范(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
6.23	《移动互联网应用程序(APP)安全认证实施细则》	国家认证认可监督管理委员会	2019-3-15	现行有效
6.24	《GB/T 36630-2018信息安全技术 信息技术产品安全可控评价指标(第1-5部分)》	全国信息安全标准化技术委员会	2019-4-1	现行有效
6.25	《网络安全审查办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
6.26	《网络关键设备和网络安全专用产品相关国家标准要求(第二版征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
6.27	《网络交易监督管理办法(征求意见稿)》	国家市场监督管理总局	N/A	正式版未发布,未生效
7.网络安全事件管理制度				
7.1	《国家网络安全事件应急预案》	中央网络安全和信息化领导小组办公室	2017-1-10	现行有效
7.2	《工业控制系统信息安全事件应急管理工作指南》	工业和信息化部	2017-5-31	现行有效
7.3	《公共互联网网络安全突发事件应急预案》	工业和信息化部	2017-11-14	现行有效
7.4	《公共互联网网络安全威胁监测与处置办法》	工业和信息化部	2018-1-1	现行有效
7.5	《GB/T 20985.1-2017信息技术安全技术 信息安全事件管理 第1部分:事件管理原理》	全国信息安全标准化技术委员会	2018-7-1	现行有效

序号	文件名称	发布机构	生效时间	法律状态
7.6	《GB/T 29246-2017信息技术 安全技术 信息安全管理体系 概述和词汇》	全国信息安全标准化技术委员会	2018-7-1	现行有效
7.7	《公安机关互联网安全监督检查规定》	公安部	2018-11-1	现行有效
7.8	《信息安全技术 网络攻击定义及描述规范(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
7.9	《信息安全技术 网络安全事件应急演练通用指南(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
7.10	《信息安全技术 网络安全威胁信息表达模型(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
7.11	《信息安全技术 信息安全风险评估规范》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
7.12	《网络安全漏洞管理规定(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效

附件二:2019年各主要部门在网络安全及数据保护合规领域的立法成果汇总

发布日期	文件名称	发布机构	生效时间	法律状态
全国人民代表大会常务委员会				
2019-10-26	《中华人民共和国密码法》	全国人民代表大会常务委员会	2010-01-01	尚未生效
工业和信息化部				
2019-11-21	《国家车联网产业标准体系建设指南(车辆智能管理)(征求意见稿)》	工业和信息化部	N/A	正式版未发布,未生效
2019-09-27	《关于促进网络安全产业发展的指导意见(征求意见稿)》	工业和信息化部	N/A	正式版未发布,未生效
2019-09-04	《工业大数据发展指导意见(征求意见稿)》	工业和信息化部	N/A	正式版未发布,未生效
2019-07-02	《云计算服务安全评估办法》	国家互联网信息办公室; 国家发展和改革委员会; 工业和信息化部; 财政部	2019-09-01	现行有效
2019-06-04	《网络关键设备安全检测实施办法(征求意见稿)》	工业和信息化部	N/A	正式版未发布,未生效
2019-04-15	《关于加强工业互联网安全工作的指导意见(征求意见稿)》	工业和信息化部	N/A	正式版未发布,未生效
2019-04-15	《基于LTE的车联网无线通信技术 安全认证技术要求》	工业和信息化部	N/A	正式版未发布,未生效
2019-01-25	《工业互联网综合标准化体系建设指南》	工业和信息化部; 国家标准化管理委员会	2019-01-25	现行有效

发布日期	文件名称	发布机构	生效时间	法律状态
公安部				
2019-04-10	《互联网个人信息安全保护指南》	公安部	2019-04-10	现行有效
国家互联网信息办公室				
2019-11-20	《网络安全威胁信息发布管理办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-11-18	《网络音视频信息服务管理规定》	国家互联网信息办公室; 文化和旅游部; 国家广播电视总局	2020-01-01	尚未生效
2019-09-10	《网络生态治理规定(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-08-12	《儿童个人信息网络保护规定》	国家互联网信息办公室	2019-10-01	现行有效
2019-07-22	《互联网信息服务严重失信主体信用信息管理办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-06-18	《网络安全漏洞管理规定(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-06-13	《个人信息出境安全评估办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-05-28	《数据安全管理办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-05-21	《网络安全审查办法(征求意见稿)》	国家互联网信息办公室	N/A	正式版未发布,未生效
2019-01-10	《区块链信息服务管理规定》	国家互联网信息办公室	2019-02-15	现行有效
全国信息安全标准化技术委员会				
2019-10-22	《信息安全技术 个人信息安全规范(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
2019-08-21	《全国信息安全标准化技术委员会<网络安全标准实践指南>管理办法(暂行)》	全国信息安全标准化技术委员会	2019-08-21	现行有效
2019-08-14	《网络关键设备和网络安全专用产品相关国家标准要求(第二版征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
2019-08-08	《信息安全技术 移动互联网应用(App)收集个人信息基本规范(草案)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
2019-06-25	《信息安全技术 安全处理器技术规范(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效
2019-06-25	《信息安全技术 信息系统密码应用基本要求(征求意见稿)》	全国信息安全标准化技术委员会	N/A	正式版未发布,未生效

发布日期	文件名称	发布机构	生效时间	法律状态
2019-06-25	《信息安全技术 生物特征识别信息的保护要求（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
2019-06-25	《信息安全技术 工业互联网平台安全要求及评估规范（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
2019-06-25	《信息安全技术 个人信息安全工程指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
2019-06-01	《网络安全实践指南-移动互联网应用基本业务功能必要信息规范》	全国信息安全标准化技术委员会	2019-06-01	现行有效
国家市场监督管理总局、国家标准化管理委员会				
2019-10-24	《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（草案）》	国家市场监督管理总局、国家标准化管理委员会	N/A	正式版未发布，未生效
2019-05-15	《国家标准化管理委员会、国家能源局关于加强能源互联网标准化工作的指导意见》	国家标准化管理委员会；国家能源局	2019-05-15	现行有效
2019-05-13	《GB/T 22239-2019信息安全技术　网络安全等级保护基本要求》	国家市场监督管理总局、国家标准化管理委员会	2019-12-01	现行有效
2019-05-13	《GB/T 28448-2019信息安全技术　网络安全等级保护测评要求》	国家市场监督管理总局、国家标准化管理委员会	2019-12-01	现行有效
2019-05-13	《GB/T 25070-2019信息安全技术　网络安全等级保护安全设计技术要求》	国家市场监督管理总局、国家标准化管理委员会	2019-12-01	现行有效
2019-04-30	《网络交易监督管理办法（征求意见稿）》	国家市场监督管理总局	N/A	正式版未发布，未生效
中国人民银行				
2019-03-28	《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》	中国人民银行	2019-03-28	现行有效
其他部门				
2019-11-11	《教育移动互联网应用程序备案管理办法》	教育部	2019-11-11	现行有效
2019-11-08	《数字化城市管理信息系统智能井盖基础信息（征求意见稿）》	住建部	N/A	正式版未发布，未生效
2019-08-17	《国家医疗保障局关于完善“互联网+”医疗服务价格和医保支付政策的指导意见》	国家医疗保障局	2019-08-17	现行有效

发布日期	文件名称	发布机构	生效时间	法律状态
2019-08-01	《国务院办公厅关于促进平台经济规范健康发展的指导意见》	国务院办公厅	2019-08-01	现行有效
2019-06-26	《关于规范快递与电子商务数据互联共享的指导意见》	国家邮政局、商务部	2019-06-26	现行有效
2019-06-06	《互联网道路运输便民政务服务系统业务办理工作指南（试行）》	交通运输部	2019-12-31	尚未生效
2019-06-05	《网络工程设计标准》	住房和城乡建设部	2019-10-01	现行有效
2019-05-05	《App违法违规收集使用个人信息行为认定方法（征求意见稿）》	App专项治理工作组	N/A	正式版未发布，未生效
2019-03-24	《互联网上网服务营业场所管理条例（2019年修订）》	国务院	2019-03-24	现行有效
2019-03-15	《移动互联网应用程序（App）安全认证实施细则》	国家认证认可监督管理委员会	2019-03-15	现行有效
2019-03-01	《App违法违规收集使用个人信息自评估指南》	App专项治理工作组	2019-03-01	现行有效

欢迎联系以下合伙人

陈际红
合伙人
知识产权部
北京办公室
+861059572003
chenjihong@zhonglun.com

刘新宇
合伙人
金融部
上海办公室
+862160613700
jeffreyliu@zhonglun.com

周洋
合伙人
公司二部
上海办公室
+862160613658
zhouyang@zhonglun.com

孟宪石
合伙人
房地产和基础设施部
北京办公室
+8610 5957 2159
mengxianshi@zhonglun.com

编委

龚乐凡

张炯

编辑

韩璐

刁远

李付雷

薛泽涵

中伦研究院出品