（2025 年 3 月）

目录

一、法规速递

《人脸识别技术应用安全管理办法》

发文机关：国家互联网信息办公室,公安部

发文时间：2025.03.13

生效时间：2025.06.01

第一条

为了规范应用人脸识别技术处理人脸信息活动，保护个人信息权益，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条

在中华人民共和国境内应用人脸识别技术处理人脸信息的活动，适用本办法。

在中华人民共和国境内为从事人脸识别技术研发、算法训练活动应用人脸识别技术处理人脸信息的，不适用本办法的规定。

第三条

应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行个人信息保护义务，承担社会责任，不得危害国家安全、损害公共利益、侵害个人合法权益。

第四条

应用人脸识别技术处理人脸信息，应当具有特定的目的和充分的必要性，采取对个人权

益影响最小的方式，并实施严格保护措施。

第五条

个人信息处理者应用人脸识别技术处理人脸信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）人脸信息的处理目的、处理方式，处理的人脸信息保存期限；

（三）处理人脸信息的必要性以及对个人权益的影响；

（四）个人依法行使权利的方式和程序；

（五）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

法律、行政法规规定可以不向个人告知的，从其规定。

处理残疾人、老年人人脸信息的，还应当符合国家有关无障碍环境建设的规定。

第六条

基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。法律、行政法规规定处理人脸信息应当取得个人书面同意的，从其规定。

基于个人同意处理人脸信息的，个人有权撤回同意，个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第七条

基于个人同意处理不满十四周岁未成年人人脸信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者应用人脸识别技术处理不满十四周岁未成年人人脸信息的，应当在存储、使用、转移、披露等方面制定专门的处理规则，依法保护未成年人个人信息安全。

第八条

除法律、行政法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。

除法律、行政法规另有规定外，人脸信息的保存期限不得超过实现处理目的所必需的最短时间。

第九条

个人信息处理者应用人脸识别技术处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。个人信息保护影响评估主要包括下列内容：

（一）人脸信息的处理目的、处理方式是否合法、正当、必要；

（二）对个人权益带来的影响，以及降低不利影响的措施是否有效；

（三）发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、出售、使用的风险以及可能造成的危害；

（四）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存 3 年。处理人脸信息的目的、方式发生变化，或者发生重大安全事件的，应当重新进行个人信息保护影响评估。

第十条

实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，应当提供其他合理、便捷的方式。

国家对应用人脸识别技术验证个人身份另有规定的，从其规定。

第十一条

应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道实施，减少人脸信息收集、存储，保护人脸信息安全。

第十二条

任何组织和个人不得以办理业务、提升服务质量等为由，误导、欺诈、胁迫个人接受人脸识别技术验证个人身份。

第十三条

在公共场所安装人脸识别设备，应当为维护公共安全所必需，依法合理确定人脸信息采集区域，并设置显著提示标识。

任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。

第十四条

人脸识别技术应用系统应当采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。涉及网络安全等级保护、关键信息基础设施的，应当按照国家有关规定履行网络安全等级保护、关键信息基础设施保护义务。

第十五条

个人信息处理者应当在应用人脸识别技术处理的人脸信息存储数量达到 10 万人之日起 30 个工作日内向所在地省级以上网信部门履行备案手续。申请备案应当提交下列材料：

（一）个人信息处理者的基本情况；

（二）人脸信息处理目的和处理方式；

（三）人脸信息存储数量和安全保护措施；

（四）人脸信息的处理规则和操作规程；

（五）个人信息保护影响评估报告。

备案信息发生实质性变更的，应当在变更之日起 30 个工作日内办理备案变更手续。终止应用人脸识别技术的，应当在终止之日起 30 个工作日内办理注销备案手续，并依法处理人脸信息。

第十六条

网信部门会同公安机关和其他履行个人信息保护职责的部门，建立健全信息共享和通报工作机制，协同开展相关工作。

网信部门、公安机关和其他履行个人信息保护职责的部门依法对应用人脸识别技术处理个人信息活动实施监督检查，个人信息处理者应当依法予以配合。

第十七条

任何组织、个人有权对违法应用人脸识别技术处理人脸信息的活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉人、举报人。

第十八条

违反本办法规定的，依照有关法律、行政法规的规定处理；构成犯罪的，依法追究刑事责任。

第十九条

本办法下列术语的含义：

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

（二）人脸信息，是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的面部特征生物识别信息，不包括匿名化处理后的信息。

（三）人脸识别技术，是指以人脸信息作为识别个体身份的个体生物特征识别技术。

（四）人脸识别设备，是指应用人脸识别技术识别个体身份的终端设备。

（五）验证个人身份，是指通过收集获得的人脸信息与信息系统存储的特定人脸信息进行“一对一”比对，确认和核对两者是否为同一人。

（六）辨识特定个人，是指通过收集获得的人脸信息与信息系统存储的特定范围内人脸信息进行“一对多”比对，发现和识别具有特定身份的个人。

第二十条 本办法自 2025 年 6 月 1 日起施行。

《中华人民共和国网络安全法（修正草案再次征求意见稿）》

发文机关：国家互联网信息办公室

发文时间：2025.03.28

生效时间：待定

一、将第五十九条修改为：“网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，由有关主管部门处二百万元以上一千万元以下罚款，并责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员处二十万元以上一百万元以下罚款。”

二、增加一条，作为第六十一条：“违反本法第二十三条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令改正或者停止违法行为，给予警告，没收违法产品和

违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。”

三、增加一条，作为第六十四条：“有本法第六十条第一项、第二项和第六十三条行为，造成本法第五十九条第三款规定的后果的，依照该款规定处罚。”

四、将第六十五条改为第六十七条，修改为：“关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、消除对国家安全的影响，并处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

五、将第六十八条、第六十九条第一项合并，作为第六十九条，修改为：“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、向有关主管部门报告的，或者违反本法第五十条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、通报批评，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。网络运营者有前款规定的违法行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前两款规定处罚。”

六、将第六十四条第一款、第六十六条、第七十条合并，作为第七十一条，修改为：“有

下列行为之一的，依照有关法律、行政法规的规定处理、处罚：（一）发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的；（二）违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的；（三）违反本法第三十七条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。”

七、增加一条，作为第七十二条：“网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。有关主管部门依据职责制定相应的行政处罚裁量基准，规范行使行政处罚裁量权。”

八、对部分条文作以下修改：（一）将第六十一条改为第六十二条、第六十二条改为第六十三条，将其中的“关闭网站”修改为“关闭网站或者应用程序”。（二）将第六十四条第二款改为第六十六条。此外，对条文序号作了相应调整。

关于《中华人民共和国网络安全法（修正草案再次征求意见稿）》的说明

党中央高度重视维护国家网络安全。习近平总书记多次作出重要指示，强调“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”。党的二十大和二十届三中全会对加强重点领域、新兴领域、涉外领域立法和增强立法系统性、整体性、协同性、时效性等作出了重要部署。为贯彻党中央决策部署，落实《十四届全国人大常委会立法规划》，适应网络安全新形势，我办会同相关部门起草了《中华人民共和国网络安全法（修正草案再次征求意见稿）》（以下简称《网络安全法（修正草案再次征求意见稿）》）。有关情况说明如下。

一、修改背景

《网络安全法》自2017年施行以来，为维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，提供了有力的法律保障。随着网络和信息技术日益融入社会生产生活，网络安全风险进一步凸显。2021年以来，《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）等网络安全相关立法相继制定实施，《中华人民共和国行政处罚法》（以下简称《行政处罚法》）修订出台，《网络安全法》需要适应形势加强与新出台法律的衔接协调，对相关法律责任制度作出科学优化，进一步保障网络安全。2023年9月，《十四届全国人大常委会立法规划》发布，明确将“网络安全法（修改）”列入了“第一类项目：条件比较成熟、任期内拟提请审议的法律草案”。2025年3月，《全国人民代表大会常务委员会工作报告》将修改网络安全法列入2025年的立法工作任务。修改工作启动以来，我办会同相关部门密切沟通，共同推进修改《网络安全法》工作，先后开展了调查研究、修正草案起草、征求中央和国家机关有关单位、面向社会公开征求意见等工作。在认真听取有关方面意见的基础上，形成了《网络安全法（修正草案再次征求意见稿）》。

二、修改思路

在《网络安全法（修正草案再次征求意见稿）》起草过程中，着重把握以下几点：**一是**坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平法治思想和习近平总书记关于网络强国的重要思想。**二是**坚持问题导向，重点强化网络安全法律责任，加大对违法行为处罚力度。**三是**坚持体系化衔接，加强与《数据安全法》《个人信息保护法》《行政处罚法》等相关法律有机衔接，在行政处罚的种类、范围、幅度等方面作出合理安排。**四是**坚持分类施策，科学设置网络运行安全、网络信息安全等不同类型违法行为的法律责任。

三、修改的主要内容

（一）关于网络运行安全的法律责任。

结合实践中危害网络安全后果的情况，增加造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的和造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的情形，并参照《数据安全法》调整了现行《网络安全法》第五十九条罚款幅度，增加相应处罚规定；新增销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的法律责任；明确关键信息基础设施运营者使用未经安全审查或者安全审查未通过的网络产品或者服务行为的处置处罚措施。

（二）关于网络信息安全的法律责任。

为防范新形势下网络信息内容安全风险对国家安全、政治安全带来的风险挑战，结合近年来网络信息内容执法实践，借鉴国外相关立法法律责任制度的新调整，完善现行《网络安全法》第六十八条、第六十九条针对的违法情形，调整未向有关主管部门报告和不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施情形的法律责任，明确对造成特别严重影响、特别严重后果的违法情形的处置处罚措施。

（三）关于个人信息和重要数据安全的法律责任。

鉴于《数据安全法》《个人信息保护法》等有关法律、行政法规对现行《网络安全法》第六十四条第一款、第六十六条涉及的个人信息和重要数据违法行为的处罚作出了新的专门规定，明确转致适用的规定。

（四）关于从轻、减轻或者不予行政处罚的情形。

统筹考虑《网络安全法》和《行政处罚法》的适用关系，专门新增一条衔接规定，明确网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依法从轻、减轻或者不予处罚；明确有关主管部门依据职责制定相应的行政处罚裁量基准。

《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》

发文机关：上海市互联网信息办公室

发文时间：2025.03.28

生效时间：待定

第一章 总则

第一条 目的和依据

为建立健全网络数据分类分级制度及重要数据目录管理机制，保障网络数据安全，促进网络数据开发利用，保护个人、组织的合法权益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《上海市数据条例》等法律法规要求，结合本市实际，制定本办法。

第二条 适用范围

本办法适用于在本市范围内开展的各行业、各领域的网络数据分类分级规则制定、网络数据分类分级实践、重要数据识别处理、网络数据安全保护体系建立等工作及其安全监管行为。

开展核心数据的网络数据处理活动，按照国家有关规定执行。

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

第三条 定义

本办法所称网络数据，是指通过网络处理和产生的各种电子数据。

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

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

公共数据，是指本市国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织，在履行公共管理和服务职责过程中收集和产生的数据。

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

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

第四条 管理原则

本市实行网络数据安全工作与业务工作协同管理，网络数据分类分级和重要数据目录管理应当结合网络数据所属行业领域特点，按照谁主管谁负责、属地管理的原则，坚持“谁收集谁负责、谁持有谁负责、谁使用谁负责”，统筹促进网络数据开发利用与保障网络数据安全。

第五条 部门职责

我市数据安全工作协调机制负责统筹协调网络数据安全重大事项和重要工作。

市网信部门负责统筹协调本市网络数据安全和相关监督管理工作，推进网络数据分类分级和重要数据目录管理。

市数据部门负责组织协调数据发展管理，推动公共数据资源开发利用，指导市大数据中心结合公共数据上链、数据开发利用等要求，推动各部门落实本市公共数据分类分级和重要公共数据目录管理。

本市各主管部门负责承担本行业、本领域网络数据安全监督管理职责，统筹本行业、本领域网络数据分类分级、重要数据目录确定、指导重要数据处理者履行安全保护责任等工作。

各部门对本部门工作中收集和产生的网络数据及网络数据安全负责，推进本部门数据分类分级和重要数据目录确定。

市公安机关、国家安全机关在各自职责范围内承担网络数据安全监管职责。

各区有关部门按照职责分工参照执行。

第二章　网络数据分类分级

第六条 网络数据分类分级原则

网络数据分类分级应当遵循国家有关规定，按照网络数据所属行业领域要求，依据科学实用、边界清晰、就高从严、点面结合、动态更新等原则进行。

如所属行业、领域没有主管部门认可的网络数据分类分级标准规范，或存在相关行业、领域规范未覆盖的网络数据类型，参照国家网络数据分类分级标准进行网络数据分类分级。

第七条 网络数据分类规则

网络数据分类应当根据网络数据管理和使用需求，结合网络数据所属行业领域已有的网络数据分类基础，灵活选择业务属性将网络数据逐级细化分类。

涉及法律法规有专门管理要求的网络数据类别（如个人信息、公共数据），应按照有关规定和标准进行识别和分类。

第八条 网络数据分级规则

网络数据分级应当根据网络数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将网络数据从高到低分为核心数据、重要数据、一般数据三个级别。

一般数据级别可根据本单位网络数据管理和使用需求进一步分级。公共数据、行业数据等有明确分级要求的从其规定。

当网络数据业务属性、重要程度和可能造成的危害程度变化时，应当对网络数据的级别进行动态更新。

第九条 网络数据分类分级流程

网络数据分类分级工作可以按照梳理网络数据资产、制定网络数据分类分级内部规则、实施网络数据分类、实施网络数据分级、形成网络数据资产清单、按有关程序上报重要数据目录等步骤开展。所属行业、领域有明确网络数据分类分级流程的从其规定。

第十条 网络数据分类分级保护

完成网络数据分类分级后，不同类别、级别的网络数据应当根据法律法规要求采取不同的保护措施，建立重要数据重点保护、一般数据全周期分级保护体系。

第三章 重要数据识别及目录管理

第十一条 重要数据识别依据

重要数据识别主要依据相关法律法规，行业、领域重要数据识别指南，数据分类分级相关国家标准等。各部门应当将相关重要数据识别依据报送至市网信部门。

第十二条 开展重要数据识别

网络数据处理者应当对所处理的数据情况进行盘点、梳理和分类分级，并判断其对国家安全、经济运行、社会稳定、公共健康和安全可能造成的影响，按照国家有关规定识别、申报重要数据。

各主管部门根据本行业、领域实际，审核申报情况，对确认为重要数据的，应当及时向网络数据处理者告知或者公开发布，同时将相关网络数据处理者纳入到重要数据处理者

名单。

第十三条 重要数据目录制定

各主管部门应当结合实际，按照下列方式之一组织开展本行业、领域重要数据目录制定工作：

（一）对照国家部委明确的本行业、领域重要数据目录，排摸掌握本行业、领域属地重要数据处理者底数及重要数据底数，形成我市本行业、领域重要数据目录；

（二）根据本行业、领域数据分类分级标准规范及重要数据识别规则或数据分类分级相关国家标准，组织本行业、领域数据处理者报送重要数据识别情况，形成我市本行业、领域重要数据目录；

（三）国家部委另行规定的重要数据目录制定方式。各部门应当结合实际，参照行业、领域重要数据目录制定方式，形成本部门重要数据目录。

第十四条 重要数据目录更新

各主管部门应当要求重要数据处理者在数据的业务属性、重要性和可能造成的危害程度发生变化时，重新开展重要数据识别，并上报变更情况。

各部门应当在本部门以及相关行业、领域数据重要程度和可能造成的危害程度变化、或重要数据处理者掌握数据发生变化时，更新本部门以及相关行业、领域重要数据目录。

第十五条 重要数据目录报告

各部门应当在重要数据目录制定完成或发生重大变化时，及时报告市网信部门。

第十六条 重要数据保护

重要数据处理者应当履行网络数据安全保护责任，明确网络数据安全负责人和网络数据安全管理机构，对重要数据进行重点保护。

重要数据处理者应当每年度对网络数据处理活动开展风险评估，并向主管部门报送风险评估报告，有关主管部门应当及时通报市网信部门、市公安部门。

各主管部门应当排摸掌握本行业、领域重要数据出境情况，涉及重要数据出境的，应当指导督促网络数据处理者通过市网信部门申报数据出境安全评估。

第四章 公共数据分类分级及开发利用

第十七条 公共数据分类分级

各部门在公共数据目录编制过程中，应当同步完成公共数据分类分级和重要公共数据识别，依托市大数据资源平台开展重要公共数据目录编制、上链工作。

公共数据中的重要数据目录，由各部门通过市大数据资源平台统一标记，并纳入本市公共数据统一管理。

第十八条 强化数据安全便捷共享

各部门应当按照相关规定，明确不同级别公共数据的共享应用场景、数据应用模式、共享方式，完善权限管理和审核机制，推动公共数据安全、便捷共享。

因数据分级需调整原有公共数据共享属性的，各部门应当提供依据，报市数据部门同意。

对于重要数据和较高级别的一般数据，各部门在确保安全可控的前提下，通过隐私计算、数据脱敏、匿名化等技术手段，可以依场景运用公共数据，充分促进数据要素流通利用。自然人、法人和非法人组织明确授权使用其公共数据的，应当按照授权依法提供。

第十九条 促进数据要素流通利用

纳入公共数据开放和授权运营范围的公共数据，应当优先完成数据分类分级和重要数据识别，保障公共数据资源安全开发利用。

第五章 监督考核

第二十条 监督检查

市网信部门定期会同数据管理等相关部门开展网络数据安全检查，形成检查结果并进行通报，督促网络数据处理者做好网络数据分类分级相关工作。

各主管部门对本行业、领域数据分类分级、重要数据保护行为进行监督，确保网络数据处理者能够依照规定识别申报重要数据，并加强重点保护。

第二十一条 绩效考核

市网信部门综合运用日常监督和评估结果，将各部门网络数据分类分级和重要数据目录管理工作纳入绩效考核。

第六章 附则

第二十二条 保障措施

各区、各部门应当加强组织领导、资金投入、人才队伍建设和法律法规宣传，合理保障网络数据分类分级、重要数据目录管理工作。

第二十三条 解释

本办法由市网信部门、市数据部门负责解释。

第二十四条 实施时间

本办法自 年 月 日起施行。

二、热点案例

中央网信办、工业和信息化部、公安部、市场监管总局关于开展 2025 年个人信息保护系列专项行动的公告

发布机关：国家互联网信息办公室

发布时间：2025.03.28

《中华人民共和国个人信息保护法》施行以来，中央网信办会同有关部门持续组织开展个人信息保护相关工作，建立健全工作机制，研究制定标准规范，依法依规查处各类违法违规行为，加强正面典型示范引领，督促指导个人信息处理者不断提升合规水平，取得了积极治理成效。2025 年，中央网信办将会同工业和信息化部、公安部、市场监管总局等部门，进一步深入治理常用服务产品和常见生活场景中存在的违法违规收集使用个人信息典型问题，切实维护人民群众在网络空间合法权益，着力提升人民群众满意度、获得感。相关部门将围绕以下重点问题开展系列专项行动：

1.App（含小程序、公众号、快应用）违法违规收集使用个人信息。

聚焦 App（含小程序、公众号、快应用）未提供个人信息收集使用规则，未按照个人信息收集使用规则处理个人信息，无相关功能或未使用相关功能时调用位置、媒体文件、通讯录、设备等非必要权限或收集非必要个人信息，未提供个人信息相关投诉渠道，未提供有效的更正删除个人信息及注销账号功能，提供个性化信息推送等功能但未提供便捷的拒绝方式，以及开屏等场景频繁“意外”跳转广告页面等问题开展治理。

2.SDK 违法违规收集使用个人信息。

聚焦 SDK 未提供个人信息收集使用规则，未按照个人信息收集使用规则或与 App 明确的规则处理个人信息，未使用 SDK 相关功能时调用位置、媒体文件、通讯录、设备等非必要权限或收集非必要个人信息，未提供个人信息相关投诉渠道，提供个性化信息推送等功能但未向 App 提供停止收集个人信息或关闭该功能的选项等问题开展治理。

3.智能终端违法违规收集使用个人信息。

聚焦智能手表、智能手环等穿戴产品，智能音箱、智能门锁、智能摄像头等家居产品，智能平板、智能学习机等学习终端，未提供个人信息收集使用规则，高频次、高精度、长时段超范围收集非必要个人信息，以及相关功能开启后需在后台持续收集个人信息或者需在云端计算和分析的，但未向用户进行显著提示等问题开展治理。

4.公共场所违法违规收集使用人脸识别信息。

聚焦交通运输、住宿旅游、教育培训、文化体育、物流商贸、休闲娱乐等公共场所使用人脸识别技术处理人脸信息，但未履行单独或书面告知同意等法律义务，未设置显著提示标识，未采取加密等严格保护措施，以及未依法开展个人信息保护影响评估等问题开展治理。

5.线下消费场景违法违规收集使用个人信息。

聚焦自动售卖、扫码点餐、出行乘车、入场停车、商超支付、扫码充电、房屋租赁等线下消费场景中，强制关注公众号、强制注册会员，强制收集非必要的手机号、生日、性别等信息，物业前台收集个人信息用于用户授权以外的目的，未经同意向第三方提供用户个人信息，以及上述场景中个人信息处理者未尽有效保护义务造成泄露等问题开展治理。

6.个人信息相关违法犯罪案件。

聚焦网络借贷、求职招聘、出行购票、教育、医疗、旅游住宿等领域个人信息违法犯罪活动，通过暗网电报等境外渠道以及境内渠道违规售卖公民个人信息，以及个人信息泄露或被攻击窃取等违法犯罪案件开展治理。

中央网信办、工业和信息化部、公安部、市场监管总局等有关部门将有序推进系列专项行动中的各项任务，集中治理各类典型违法违规问题，对拒不整改的依法从严处理；同时，有关部门将根据实际工作需要及时调整重点治理问题，确保专项行动取得实效，切实保护公民个人信息安全。

特此公告。

三、实务解读

1. 《网络安全法》2025 年修订的主要内容及趋势展望

供稿人：黄春林（上海市汇业律师事务所）、袁姜涛（上海市汇业律师事务所）、钱静雯（上海市汇业律师事务所）

2025 年 3 月 28 日，《网络安全法》2017 年 6 月 1 日实施后时隔八年，国家网信办会同相关部门再次起草了《中华人民共和国网络安全法（修正草案再次征求意见稿）》（下称“2025 修正草案”）并再次公开征求意见。在此之前，2022 年 09 月 14 日，国家网信办会同相关部门首次起草了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（下称“2022 稿”）并首次公开征求意见。2025 年 3 月，全国人大明确将修改《网络安全法》纳入本年度立法计划。预计，本次征求意见后，《网络安全法》修正立法进入最后的“直道冲刺”。

据悉，本次修订意在加强与相关法律之间的衔接协调，弥补相关法律责任漏洞，强化 CII 保护，细化责罚颗粒度，贯彻包容审慎原则，进一步增强《网络安全法》的科学性和导向性。

结合近期立法及执法情况，汇业律师事务所黄春林律师团队简要分析《网络安全法》2025 年修订的六大立法与执法趋势如下，仅供参考。

一、细化责罚颗粒度，提高执法活动科学性

《2022 稿》参照《个人信息保护法》第六十六条的立法技术，大量合并、归类和集

中了法律责任条款，意图提高执法活动灵活性。本次《2025 修正草案》秉持责罚相当的法治原则，进一步拆分、细化了相关罚则条款，明确违法行为与处罚力度的阶梯性，提高了执法活动的严肃性和科学性。

以违反《网络安全法》第二十一条规定（例如等保违法）为例，其违法行为和罚则对应关系如下：

违法行为	罚则
一般违法行为	责令改正，给予警告，可以处一万元以上五万元以下罚款
拒不改正的一般违法行为或者导致危害网络安全等后果的违法行为	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
造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的违法行为	处五十万元以上二百万元以下罚款……
	并对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款
造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的违法行为	处二百万元以上一千万元以下罚款……
	并对直接负责的主管人员处二十万元以上一百万元以下罚款

通过上表不难发现如下趋势：（1）对于“一般违法行为”的罚款处罚，并不再以“拒不改正”为前置要件，也就是说企业首次违法即可能面临罚款的处罚，但一般不追究个人责任；（2）违法行为不涉及 CII 的，罚金一般不会超过 200 万，但业务连续性的风险（例如停业整顿或关闭应用程序）仍然可能存在。

最后，《2025 修正草案》还首次明确，有关主管部门依据职责制定相应的行政处罚裁量基准，规范行使行政处罚裁量权，提高执法活动科学性。

二、法律责任转致适用个保法、数安法等，提高法律适用协调性

首先，本次《2025 修正草案》规定，下列三种违法行为转致适用个保法、数安法等法律、行政法规的规定，这样不仅增强了立法的协调性，理论罚款上限也从网安法的“100 万”同步升格为“5000 万”和“5%”：

（1）发布或传输违法信息内容的；

（2）侵害个人信息权益的；

（3）CIIO“在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的”。

值得注意的是，关于第（1）种违法行为，《2025 修正草案》删除了《2022 稿》旨在强化信息内容安全责任的“补丁条款”。彼时，《2022 稿》专门增加“补丁条款”，即 “法律、行政法规没有规定的”，处罚金额甚至顶格到“五千万元以下或者上一年度营业额百分之五以下”的“天花板”。当时，业界颇有争议，有人认为该条款违反“法不禁止即合法”的法治原则。此外，《网络安全法》将该类法律责任转致出去后，哪个“法律、行政法规”来承接，实践中还有待系列清朗行动检验。毕竟，之前关于信息内容安全违规的处罚，大多都是适用《网络安全法》，而其他规定了内容安全法律责任的“法律、行政法规”并不多见，即便有规定（例如《互联网信息服务管理办法》），相关责任也相对较“轻”。但无论如何，该条的调整，但愿本身就代表一种趋势吧。

此外，关于第（3）种违法行为，转致适用也可能会造成法律适用漏洞。因为，这里明确了重要数据相关的两种违法行为：“在境外存储重要数据”及“向境外提供重要数据”，但是《数据安全法》第四十六只规定了“向境外提供重要数据”的罚则，而没有“在境外存储重要数据”的罚则。关保条例和网数条款也找不到相关的罚则。唯一的

合理解释是：“在境外存储重要数据”逻辑上必然会导致“向境外提供重要数据”。但与其这样，不如这次一并修正到位。

三、信息内容安全监管调整思路，重点夯实平台治理责任

《2025 修正草案》在信息内容安全监管发力方向上作出调整，从原来的强化信息内容违法行为的直接打击处罚，调整为重点夯实平台的信息内容违规治理责任，加大对平台在违法信息内容治理不力的处罚力度。

如前所述，《2025 修正草案》直接删掉了直接打击违法信息内容的“补丁条款”。此外，《2025 修正草案》还删除了《2022 稿》中对违反《网络安全法》第四十八条第一款的信息内容直接违规内容的处罚条款。

作为本次修订的重头戏之一，相较于《网络安全法》，《2025 修正草案》强化了平台治理责任并加大了违规处罚力度。《2025 修正草案》明确，网络运营者有下列违法行为的，可以采取通报批评、停业整顿、关闭应用程序、对公司最高 1000 万元/个人最高 100 万元的罚款：

（1）网络平台对用户发布的法律、行政法规禁止发布或者传输的信息，未停止传输，未采取消除等处置措施，未保存有关记录，未向有关主管部门报告的；

（2）电子信息发送或应用软件下载服务平台知道其用户发送的电子信息、提供的应用软件含有法律、行政法规禁止发布或者传输的信息的，未停止提供服务，未采取消除等处置措施，未保存有关记录，未向有关主管部门报告的；

（3）其他网络运营者对法律、行政法规禁止发布或者传输的信息，不按照有关部门的要求停止传输，不采取消除等处置措施，不保存有关记录的。

四、坚持包容审慎导向，明确从轻、减轻处罚情形

《2025 修正草案》延续了《网络数据安全管理条例》为标志的包容审慎导向，适度调低了处罚力度，明确了从轻、减轻和不予处罚原则的适用。

首先，相较于《2022 稿》，《2025 修正草案》适度调低了部分违法行为的处罚上限，通篇最高处罚金额对齐《数据安全法》的“1000 万元”上限标准，大幅低于《2022 稿》及《个人信息保护法》的“5000 万”和“5%”上限标准。

其次，相较于《2022 稿》，《2025 修正草案》维持了《网络安全法》关于实名认证违法、网络安全检测认证违法等的较轻处罚力度。

再次，减少了“通报批评”的适用，删除了《2022 稿》中关于违反《网络安全法》第二十一条等一般违法行为（例如未开展等保、未制定制度等）适用“通报批评”的规则，适度降低了企业的被“舆论审判”的舆情风险。

最后，《2025 修正草案》还明确规定，网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。略有遗憾的是，本次没有将“尽职合规免责”和“勤勉合规减责”的正向激励机制纳入立法。

五、分类施策松中有紧，强化 CII 保护力度

《2025 修正草案》坚持分类施策原则，在包容审慎原则之外，强化了针对关键信息基础设施（CII）的违法打击力度。

《2025 修正草案》强调，因下列行为造成 CII 丧失局部或主要功能等严重危害网络安全后果的，对企业最高可以处以罚款 1000 万元，对直接负责的主管人员最高可以处以罚款 100 万元：

（1）违反《网络安全法》第二十一条规定的一般合规义务；

（2）网络安全事件应急预案、处理及报告违规，

（3）设置恶意程序；

（4）未及时对产品或服务存在安全风险采取补救措施；

（5）从事或帮助从事非法侵入、干扰网络活动，导致。

此外，《2025 修正草案》进一步完善了 CIIO 使用未经安全审查或者安全审查未通过的网络产品或者服务行为的处罚措施，从简单粗暴的“停止使用”改为“责令限期改正、消除对国家安全的影响”。

六、填补法律责任漏洞，强化关键产品和专用产品管理

《2025 修正草案》本次修订的另一大亮点之一，即首次从法律层面明确了销售或者提供违法违规的网络关键设备和网络安全专用产品的法律责任。根据《网络安全法》二十三条规定，网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。《2025 修正草案》明确，违反前述规定的，由有关主管部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。