（2025 年 9 月）

目录

一、法规速递

《国家网络安全事件报告管理办法》

发文机关：国家互联网信息办公室

发布时间：2025.09.11

生效时间：2025.11.01

第一条 为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，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》、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者，在发生网络安全事件时，应当按照本办法的规定进行报告。

第三条 国家网信部门负责统筹协调全国网络安全事件报告管理工作。省级网信部门负责统筹协调本行政区域内网络安全事件报告管理工作。

第四条 网络运营者在发现或获知涉及本单位的网络安全事件时，应当按照《网络安全事件分级指南》（见附件）进行研判，属于较大以上网络安全事件的，按以下程序报告：

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过 1 小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过 2 小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过 4 小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时，并同时向同级有关部门通报。

本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告。

涉嫌违法犯罪的，网络运营者应当及时向公安机关报案。

第五条 网络运营者应当以合同等形式要求为其提供网络安全、系统运维等服务的组织或个人，及时向其报告监测发现的网络安全事件，并协助其按照本办法规定报告网络安全事件。

第六条 鼓励社会组织和个人报告所获悉的较大以上网络安全事件。

第七条 报告网络安全事件时，应当包括下列内容：

（一）涉事单位名称及涉事系统或设施基本情况；

（二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等；

（三）事态发展趋势及可能造成的进一步影响和危害；

（四）网络安全事件原因初步分析意见；

（五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等；

（六）拟进一步采取的应对措施以及请求支援事项；

（七）网络安全事件现场保护情况；

（八）其他应当报告的情况。

对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。

网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。

第八条 网络安全事件处置工作结束后，网络运营者应当于 30 日内对相关事件发生原因、应急处置措施、造成的危害、责任追究、完善整改情况、教训等进行全面分析总结，形成事件处置总结报告按照原渠道上报。

第九条 网信部门建设 12387 网络安全事件报告热线电话和网站、邮箱、传真等方式，统一接收网络安全事件报告。

第十条 网络运营者未按照本办法规定报告网络安全事件的，有关主管部门按照有关法律、行政法规的规定进行处罚。

因网络运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对网络运营者及有关责任人依法从重处罚。

承担网络安全事件报告的部门未按照本办法规定报告网络安全事件的，依据有关法

律、行政法规和网络安全工作责任制追究相关单位和人员责任。

第十一条 发生网络安全事件时，网络运营者已采取合理必要的防护措施，按照应急预案进行处置、有效降低网络安全事件影响和危害，并按照本办法规定及时报告的，可视情从轻或不予追究相关单位和人员责任。

第十二条 本办法所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

本办法所指网络运营者是指网络的所有者、管理者和网络服务提供者。

本办法所指《网络安全事件分级指南》参照《信息安全技术 网络安全事件分类分级指南》国家标准（GB/T 20986-2023）制定，以有限枚举的方式给出相关事件的分级定量指标。

第十三条 涉及国家秘密的网络安全事件报告，按照有关部门规定执行。

第十四条 本办法自 2025 年 11 月 1 日起施行。

附件

网络安全事件分级指南

一、特别重大网络安全事件

符合下列情形之一的，为特别重大网络安全事件：

1.重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

2.核心数据、重要数据、海量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为特别重大网络安全事件：

1.省级以上党政机关门户网站、中央重点新闻网站因攻击、故障，导致 24 小时以上不能访问。

2.关键信息基础设施整体中断运行 6 小时以上或主要功能中断运行 24 小时以上。

3.影响一个或多个省级行政区 50%以上人口，或者 1000 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.核心数据、重要数据泄露或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

5.泄露 1 亿人以上公民个人信息。

6.省级以上党政机关门户网站、中央重点新闻网站、超大型网络平台等被攻击篡改，导致违法有害信息特大范围传播。以下情况之一，可认定为“特大范围”：

（1）在主页上出现并持续 6 小时以上，或在其他页面出现并持续 24 小时以上；

（2）通过社交平台转发 10 万次以上；

（3）浏览或点击次数 100 万以上；

（4）省级以上网信部门、公安机关认定为是“特大范围传播”的。

7.造成 1 亿元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

二、重大网络安全事件

符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

1.重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

2.核心数据、重要数据、大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为重大网络安全事件：

1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 6 小时以上不能访问。

2.关键信息基础设施整体中断运行 1 小时以上或主要功能中断运行 3 小时以上。

3.影响一个或多个地市级行政区 50%以上人口，或者 100 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等的工作、生活。

4.核心数据、重要数据泄露或被窃取、篡改、仿冒，对国家安全和社会稳定构成严重威胁。

5.泄露 1000 万人以上公民个人信息。

6.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站，大型以上网络平台等被攻击篡改，导致违法有害信息大范围传播。以下情况之一，可认定为“大范围”：

（1）在主页上出现并持续 2 小时以上，或在其他页面出现并持续 12 小时以上；

（2）通过社交平台转发 1 万次以上；

（3）浏览或点击次数 10 万以上；

（4）省级以上网信部门、公安机关认定为是“大范围传播”的。

7.造成 2000 万元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

三、较大网络安全事件

符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

1.重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，

业务处理能力受到影响。

2.重要数据、较大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为较大网络安全事件：

1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 2 小时以上不能访问。

2.关键信息基础设施整体中断运行 10 分钟以上或主要功能中断运行 30 分钟以上。

3.影响一个或多个地市级行政区 30%以上人口，或者 10 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.重要数据泄露或被窃取，对国家安全和社会稳定构成较严重威胁。

5.泄露 100 万人以上公民个人信息。

6.党政机关、企事业单位门户网站，重点新闻网站，网络平台等被攻击篡改，导致违法有害信息较大范围传播。以下情况之一，可认定为“较大范围”：

（1）在主页上出现并持续 30 分钟以上，或在其他页面出现并持续 2 小时以上；

（2）通过社交平台转发 1000 次以上；

（3）浏览或点击次数 1 万以上；

（4）省级以上网信部门、公安机关认定为是“较大范围传播”的。

7.造成 500 万元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

四、一般网络安全事件

除上述网络安全事件外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》

发文机关：国家互联网信息办公室

发布时间：2025.09.12

生效时间：待定

第一条 为指导规范大型网络平台设立、运行个人信息保护监督委员会，对个人信息保护情况进行监督，促进大型网络平台个人信息保护合规水平提升，保护个人信息权益，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规和国家有关规定，制定本规定。

第二条 中华人民共和国境内提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者（以下称为大型网络平台服务提供者）设立、运行个人信息保护监督委员会，适用本规定。

本规定所称个人信息保护监督委员会，是指由大型网络平台服务提供者成立的，主要由外部成员组成的，对大型网络平台个人信息保护情况进行监督的独立机构。

本规定所称个人信息保护监督委员会外部成员（以下称为外部成员），是指具备个人信息保护专业知识和技能，不在受聘大型网络平台担任除监督委员会成员外的其他职务的人员。

国家网信部门会同国务院公安部门等有关部门依照有关法律法规规定，制定发布大型网络平台清单。

第三条 个人信息保护监督委员会（以下称为监督委员会）成员人数应与大型网络平台业务规模、用户数量等相匹配，一般不得少于 7 人，外部成员占比不低于三分之二。

第四条 外部成员应当保持身份和履行职责的独立性，受聘期间不得具有下列情形：

（一）本人或者其直系亲属在受聘大型网络平台服务提供者或者其子公司、分公司、控制企业任职；

（二）直接或间接持有受聘大型网络平台服务提供者已发行股份百分之一以上，或者是受聘大型网络平台服务提供者前十名股东中的自然人股东及其直系亲属；

（三）本人或者其直系亲属在直接或间接持有受聘大型网络平台服务提供者已发行股份百分之五以上的股东单位或者在受聘大型网络平台服务提供者前五名股东单位任职；

（四）为受聘大型网络平台服务提供者或者其子公司、分公司、控股企业提供财务、法律、咨询、审计等专业服务的人员；

（五）其他可能影响外部成员独立性的情形。

第五条 担任监督委员会外部成员应当符合下列条件：

（一）符合本规定第四条规定的独立性要求；

（二）具备履行职责的专业素质，熟悉个人信息保护、数据安全相关法律法规、国家标准等，从事个人信息保护相关工作不少于 3 年；

（三）具备良好的声誉，能够客观公正、独立廉洁地履行职责；

（四）具有正常履行职责的身体条件、工作时间等；

（五）具有良好的个人品德，不存在违法犯罪、重大失信等不良记录；

（六）法律、行政法规规定的其他条件。

第六条 大型网络平台服务提供者组织提名外部成员时，应当充分了解被提名人职业、学历、职称、工作经历、兼职情况、有无违法犯罪和重大失信记录等，并对其符合独立性和担任外部成员的其他条件提出意见。被提名人应当就其符合独立性和担任外部成员的其他条件作出说明。被提名人同时受聘的大型网络平台不得超过三家。

外部成员聘任决定应当由大型网络平台服务提供者董事会等决策机构或其授权的董事长、执行董事等高级管理人员作出。

第七条 大型网络平台服务提供者可以按照国家规定，结合专兼职的工作内容和工作时长、工作量等情况给予外部成员与其承担职责相适应的报酬。报酬的标准由董事会等决策机构批准，并在大型网络平台服务提供者个人信息保护社会责任报告中披露。个人信息保护社会责任报告应当每年公开发布，并且便于查阅和保存。

除上述报酬外，外部成员不得从大型网络平台服务提供者及其持股百分之五以上股东、控股股东、实际控制人或者有利害关系的单位和人员取得其他利益。

第八条 监督委员会内部成员（以下称为内部成员）由大型网络平台服务提供者董

事会等决策机构或其授权的董事长、执行董事等高级管理人员决定。

第九条 监督委员会设主任一名，由外部成员担任，经监督委员会全体成员选举产生，负责监督委员会工作。

监督委员会设秘书一名，可由内部成员担任，负责处理监督委员会的会议筹备、文件管理、组织联络等综合性事务。

第十条 监督委员会成员在同一大型网络平台任期为三年，任期届满，可以连任，连任不得超过两届。

监督委员会成员在任期届满前可以提出辞任。监督委员会成员辞任应当提前 30 个工作日向大型网络平台服务提供者董事会等决策机构或其授权的董事长、执行董事等高级管理人员提交书面辞任报告。

第十一条 监督委员会成员应当勤勉尽责，有下列情形之一的，由董事会等决策机构或其授权的董事长、执行董事等高级管理人员作出解聘决定：

（一）外部成员不再符合本规定第五条规定的条件；

（二）连续三次未出席监督委员会会议或者连续两次未出席监督委员会定期会议；

（三）不适合担任监督委员会成员的其他情况。

大型网络平台服务提供者解聘监督委员会成员的，应当允许被解聘监督委员会成员提出异议说明，并将解聘原因、异议说明及异议说明答复等情况及时报送所在地省级网信部门。

监督委员会成员在任职期内辞任或被解聘等，导致监督委员会成员少于 7 人或外部成员占比低于三分之二的，大型网络平台应当在 30 个工作日内补任相关人员；若辞任或被解聘成员为监督委员会主任，应当及时选举产生新的主任；若辞任或被解聘成员为监督委员会秘书，应当及时任命新的秘书；在补任完成前，个人信息保护监督委员会应当继续履行相应职责。

第十二条 大型网络平台服务提供者应当根据本规定，制定监督委员会规则，面向社会公开征求意见不少于 15 日，根据公开征求意见情况修改完善后，报经董事会等决策机构批准。监督委员会规则一般应当载明下列事项：

（一）监督委员会的组成、成员任期和任免程序；

（二）监督委员会职责及监督事项；

（三）监督委员会成员职责；

（四）监督委员会主任的选举和职责；

（五）监督委员会秘书的产生和职责；

（六）监督委员会会议的召开、通知、表决、监督意见形成和记录；

（七）监督委员会运行机制、经费保障；

（八）需要明确的其他事项。

第十三条 监督委员会重点对大型网络平台下列事项进行监督：

（一）个人信息保护合规制度体系建设情况；

（二）平台或产品个人信息保护规则制修订情况；

（三）敏感个人信息保护情况；

（四）个人信息保护影响评估开展情况；

（五）个人信息保护合规审计开展情况；

（六）落实监管机构提出的整改要求情况；

（七）个人信息安全事件处理情况；

（八）个人行使个人信息权益保障情况；

（九）向境外提供个人信息合规情况；

（十）个人信息保护社会责任履行及报告发布情况；

（十一）个人信息保护负责人履行职责情况；

（十二）利用个人信息进行自动化决策等情况；

（十三）与个人信息保护相关的其他重大事项；

（十四）法律、行政法规规定的其他监督事项。

监督委员会应当建立与大型网络平台用户常态化沟通机制，听取用户意见建议，回应用户关切。

第十四条 监督委员会成员履行下列职责：

（一）出席监督委员会会议，对审议监督事项发表意见，对需表决事项进行表决；

（二）了解大型网络平台个人信息保护情况，可就有关问题进行询问，并要求答复；

（三）可列席大型网络平台个人信息保护工作有关会议；

（四）听取大型网络平台用户的个人信息保护意见；

（五）向监督委员会报告大型网络平台个人信息处理活动相关风险和问题；

（六）法律、行政法规规定的其他职责。

第十五条 监督委员会应当至少每三个月召开一次定期会议，就大型网络平台个人信息保护监督事项进行审议，并作出监督意见。

主任或者三分之一以上成员提议，可召开临时会议，审议大型网络平台个人信息保护相关事项。

第十六条 监督委员会会议有过半数成员出席方可举行。秘书应当于会议召开 15 日前将会议的时间、地点、议题等事项通知全体成员，同时提供完备的会议资料。

主任或者三分之一以上成员认为会议筹备不充分的，可要求延期召开会议或者延期审议事项，秘书应当对会议延期情况进行记录。

第十七条 监督委员会成员应当按时出席监督委员会会议。确有原因不能出席的，应当对会议事项提出明确的书面意见。

第十八条 监督委员会应当就会议审议事项进行充分讨论，监督委员会成员应当客观地发表独立意见，监督委员会秘书应当完整准确记录会议情况，形成会议记录和决议记录，出席会议的成员应当核实记录内容并签署意见。

监督意见应当取得全体成员三分之二以上同意。监督委员会应当及时将监督意见通知大型网络平台服务提供者。

第十九条 大型网络平台服务提供者应当自收到监督意见之日起 10 个工作日内处理监督委员会作出的监督意见，确有理由不予处理的，应当答复监督委员会。监督委员会认为答复理由不成立的，可以向所在地省级网信部门报告。

第二十条 监督委员会成员在履行职责过程中发现大型网络平台个人信息处理活动存在风险或违法违规收集处理个人信息等问题的，应当向监督委员会和大型网络平台服务提供者提出书面建议。监督委员会和大型网络平台服务提供者未处理的，或成员对处理结果有异议的，成员应当向所在地省级网信部门报告。

第二十一条 监督委员会及其成员在履行职责过程中，不得干预大型网络平台正常

运营，对在履行职责过程中知悉的个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供。

第二十二条 监督委员会及其成员履行职责过程中，大型网络平台服务提供者有关组织、人员应当积极配合，不得恶意拒绝、阻碍或者隐瞒，不得干预其独立履行职责。

第二十三条 大型网络平台服务提供者应当为监督委员会及其成员提供履行职责所需的工作条件和协助，做好相关对接工作。个人信息保护负责人应当每三个月向监督委员会报告大型网络平台个人信息保护有关情况。

第二十四条 大型网络平台服务提供者应当及时向社会公开监督委员会规则、成员信息等。

已设立监督委员会的大型网络平台，不再满足本规定第二条相关条件，向所在地省级网信部门报告有关情况后，可以撤销监督委员会。

第二十五条 大型网络平台服务提供者应当在监督委员会成立、变更之日起 30 个工作日内，向所在地省级网信部门报送监督委员会规则、成员名单等信息。

监督委员会应当每年向所在地省级网信部门报送履行职责情况报告。

省级网信部门每年向国家网信部门报送大型网络平台个人信息保护监督委员会相关工作情况。

第二十六条 国家网信部门会同国务院有关部门建立健全信息共享和通报工作机制，对全国大型网络平台落实本规定要求的情况进行监督检查。

省级网信部门负责统筹协调本行政区域内大型网络平台落实本规定要求的监督管理工作。

第二十七条 监督委员会履行职责不到位，导致大型网络平台出现重大个人信息安全事件的，或严重违反个人信息保护相关法律法规的，省级以上网信部门应当要求大型网络平台服务提供者解散监督委员会，重新成立监督委员会。

第二十八条 任何组织和个人有权对大型网络平台服务提供者、监督委员会及其成员的违法违规活动向省级以上履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当在 15 个工作日内依法处理，并将处理结果告知投诉、举报人。

第二十九条 大型网络平台服务提供者违反本规定的，依照《中华人民共和国个人

信息保护法》、《网络数据安全管理条例》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。

第三十条 本规定由国家网信部门负责解释。

第三十一条 本规定自 年 月 日起施行。

《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》

发文机关：国家互联网信息办公室

发布时间：2025.09.16

生效时间：待定

第一章 总则

第一条 为科学认定未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者范围，根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》《未成年人网络保护条例》等法律法规规定，制定本办法。

第二条 认定工作坚持依法依规、公平公正、实事求是的原则，充分保障未成年人合法权益，综合平衡相关网络平台和相关方合法权益，发挥各方力量强化未成年人网络保护。

第三条 认定工作由国家网信部门负责统筹协调，国家新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、市场监督管理、广播电视等有关部门依据各自职责共同参与，并指导设立认定咨询委员会承担具体工作。

第四条 认定工作应避免影响网络平台服务提供者的正常生产经营活动。网络平台服务提供者应当配合认定机构的认定工作。

第五条 认定工作原则上应当公开进行。认定工作涉及的国家秘密、商业秘密、个人隐私等应当依法予以保密。

第二章 认定标准

第六条 符合以下情形之一的，应当认定为未成年人用户数量巨大的网络平台服务提供者：

（一）该网络平台提供的产品或者服务专门以未成年人为服务对象，注册用户在1000万以上或者月活跃用户在100万以上。

（二）该网络平台提供的产品或者服务的对象不局限于未成年人的，未成年人注册用户数量在1000万以上或者月活跃未成年人用户在100万以上。

第七条 认定对未成年人群体具有显著影响的网络平台服务提供者，应当综合考虑以下因素：

（一）该网络平台下载量、注册用户数量、月活跃用户数量规模较大，或网络产品的销售额、交易量等较大；

（二）该网络平台未成年人登录频次、使用时长、喜爱程度、消费金额等指标较高；

（三）该网络平台涵盖大量涉及或面向未成年人的信息内容；

（四）该网络平台在 3 年内存在较多涉未成年人突出情况，违法违规问题较为突出，受到社会广泛关注；

（五）该网络平台在相关垂直领域排名靠前；

（六）其他对未成年人群体具有显著影响的因素。

第三章 程序启动

第八条 国家网信部门会同有关部门按照认定流程，研究启动认定工作。

认定工作原则上每3年开展一次，也可在网络平台出现用户数量激增、对未成年人影响显著提升、社会广泛关注等情形时视情启动。

第九条 认定咨询委员会根据认定标准与实际情况，提出纳入认定工作的网络平台服务提供者建议名单，经国家网信部门会同有关部门审定后，通知相关网络平台服务提供者开展自评估工作。

第十条 网络平台服务提供者应当按照认定标准，全面准确评估对未成年人的影响，并在收到通知后 20 个工作日内提交自评估报告。

第十一条 网络平台服务提供者对所提交的自评估报告及材料完整性、真实性负责，不得具有误导性，并根据要求提供必要解释说明等补充材料。

第四章 论证与决定

第十二条 认定工作应当通过座谈会、听证会、实地走访等多种形式听取各方意见建议。

认定名单征求意见稿向社会公开征求意见。公开征求意见的期限一般为 30 日。

第十三条 认定咨询委员会根据意见征求情况，拟定认定名单建议稿。

第十四条 国家网信部门会同有关部门根据认定标准，综合研究确定最终认定名单并向社会公布。

第十五条 网络平台服务提供者对认定结果存在异议的，可在 15 个工作日内，向认定咨询委员会提交书面异议申请及相关证明材料，详细说明异议理由。

第五章 认定调整

第十六条 国家网信部门会同有关部门对认定结论的实施效果进行跟踪监测。

已认定的网络平台服务提供者认为自身已持续 6 个月不符合认定标准的，可以提交变更认定结论申请以及证明材料。

国家网信部门会同有关部门按照本办法前述规定的有关程序，做出启动认定或者驳回决定。

第十七条 国家网信部门会同有关部门可根据认定工作开展情况，按程序适时优化调整认定标准，并提前进行公示。

第六章 附则

第十八条 本办法所称网络平台服务提供者涵盖各类网络产品和服务提供者、智能终端产品制造者和销售者以及互联网新技术新应用新产品提供者等。

第十九条 本办法自公布之日起施行。

二、热点案例

公安网安部门依法对某人工智能服务科技有限公司予以行政处罚

发布机关：国家网络安全通报中心

发布时间：2025.09.15

公安网安部门在“护网—2025”专项工作中发现，某主营业务为对外提供人工智能模型训练基础数据（算料）的科技有限公司，在处理人脸等生物识别类敏感个人信息前，未按《个人信息保护法》有关规定进行个人信息保护影响评估。属地公安机关依据《个人信息保护法》规定，对该公司依法予以行政处罚，并责令整改。

安全提示：合法合规的人工智能训练数据是高水平大模型研发的基石。提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络和数据安全风险。产业链相关企业要以案为鉴，遵守《网络安全法》《个人信息保护法》《数据安全法》，切实履行网络安全、数据安全和信息安全责任义务，在采集公民个人信息时及时征得采集对象同意，对外交付数据前开展个人信息保护影响评估及数据出境安全评估，以更高水平的训练数据安全保障人工智能产业高质量发展。

近期网络安全、数据安全、个人信息保护相关执法典型案例

发布机关：国家互联网信息办公室

发布时间：2025.09.16

近段时间以来，全国网信系统认真贯彻落实《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规，持续加大网络安全、数据安全、个人信息保护相关执法工作力度，各地网信部门依法查处一批涉网页篡改、数据泄露、违法违规处理个人信息、新技术新应用未经评估上线等违法违规案件。现将典型案例发布如下。

1.广东某科技股份有限公司网页篡改案。

网信部门工作发现，该企业用于业务审批等的办公协作平台登录页面被篡改为违法有害内容。经查，该企业涉事系统存在任意文件上传漏洞，遭受勒索软件攻击，该企业当天发现后仅重装系统，未修复系统漏洞。其后，攻击者利用该漏洞上传远程控制木马，将登录页面篡改为违法有害内容。该企业未依法履行网络安全保护义务，未采取必要技术措施保障网络安全，未及时修复系统漏洞，造成网页篡改后果，违反《网络安全法》相关规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

2.新疆某互联网科技有限公司网页篡改案。

网信部门工作发现，该企业门户网站及开发运维的 8 个网站子页面被篡改为涉赌违法信息。经查，该企业上述网站存在安全缺陷和漏洞，相关网页源代码 php 文件被恶意篡改，出现涉赌违法信息。事件发生时，网站管理员休假不在岗，网站处于无人管理状态。该企业作为网络产品、服务提供者，未及时发现其开发的网站存在安全缺陷和漏洞，未立即采取补救措施，未按照规定及时告知用户并向主管部门报告，违反《网络安全法》相关规定，属地网信办已依法责令其改正，并予以警告处罚。

3.山东某医学检验有限公司数据泄露案。

网信部门工作发现，该企业某系统相关数据被搜索引擎爬虫爬取。经查，涉事系统开启

目录浏览功能，存在目录遍历和未授权访问漏洞，未正确配置防火墙入侵防护策略，未按照规定留存相关网络日志。相关搜索引擎爬虫通过遍历请求爬取了网站组织架构和文件，导致系统相关数据泄露。该企业未依法履行网络安全、数据安全保护义务，涉事系统未依法留存相关网络日志，未采取技术措施和其他必要措施保障数据安全，造成数据泄露后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

4.浙江某科技股份有限公司数据被窃取案。

网信部门工作发现，该企业 FTP 系统相关数据被窃取。经查，该企业为方便共享、打印系统文件，将涉事系统设置为允许匿名访问，并设置云服务器安全组规则不生效，长期存在未授权访问漏洞，导致涉事系统相关数据被窃取。该企业未依法履行网络安全、数据安全保护义务，涉事系统未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

5.重庆某科技公司数据被窃取案。

网信部门工作发现，该企业用于汽车租赁服务的“OA 信息系统”相关数据被窃取。经查，该企业涉事系统 3306 端口开放 MySQL 数据库服务，未设置用户密码，存在弱口令漏洞，导致涉事系统相关数据被先后窃取 159 次。该企业未依法履行网络安全、数据安全保护义务，涉事系统未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

6.广东某保险代理有限公司数据被窃取案。

网信部门工作发现，该企业提供保险代理服务的后台系统相关数据被窃取。经查，该企业涉事系统存在越权遍历访问漏洞，攻击者可通过遍历 URL ID 的方式批量获取数据，且该企业购买的云防火墙服务已过期，未按照规定留存相关网络日志，导致涉事系统相关数据被窃取。该企业未依法履行网络安全、数据安全保护义务，涉事系统未依法留存相关网络日志，未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

7.湖南某科技股份有限公司数据存在泄露安全风险案。

网信部门工作发现，该企业内网数据库相关数据存在泄露安全风险。经查，该企业内网数据库存在未授权访问漏洞和弱口令漏洞，某软件研发工程师为工作便利，将合作项目中掌握的大量用户数据拷贝至企业内网数据库，并打开企业内网的公共互联网访问端口，导致内网数据库相关数据暴露在互联网上。该企业未依法履行网络安全、数据安全保护义务，未建立网络安全和数据安全管理制度，涉事系统未采取技术措施和其他必要措施保障数据安全，存在数据泄露安全风险，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

8.北京某科技有限公司运营的 App 超范围收集个人信息案。

网信部门工作发现，该企业运营的 App 违反必要原则，收集与其提供的服务无关的个人信息。经查，该企业开发的 App 在用户未使用任何功能情况下，后台运行时收集上传用户应用程序安装、卸载信息。用户使用上传 AI 头像等功能时，调用非必要存储权限。相关行为超出了实现个人信息处理目的最小必要范围，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规。属地网信办已依法责令其改正，并予以警告、罚款处罚。

9.上海某科技有限公司违法违规收集人脸信息案。

网信部门工作发现，该企业运营的自动售货机存在违法违规收集人脸信息等问题。经查，该企业运营的自动售货机在用户支付环节存在未经同意收集人脸信息等问题，同时该企业存在未建立个人信息保护影响评估制度、相关系统存在 SQL 注入高危漏洞等问题，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告处罚。

10.浙江某科技有限责任公司运营的 App 提供深度合成服务未按规定进行安全评估案。

网信部门工作发现，该企业运营的 App 提供 AI 换脸服务未按规定进行安全评估。经查，该企业运营的 App 是一款深度合成类服务产品，提供视频换脸、图片换脸、照片舞动配音等图片处理功能，用户可对上传图片、视频中的人物进行换脸，但未按规定落实安全评估要求，相关深度合成内容也未作显著标识，存在较大安全风险，违反《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》《互联网信息服务算法推荐管理规定》《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》等规定。网信部门已依法责令移动应用程序分发平台依规依约对该 App 予以下架处置。国家网信办有关负责人表示，网络空间已经成为人们生产生活的新空间，让互联网在法治轨道上健康运行是全社会的共同责任。网信部门将认真贯彻习近平新时代中国特色社会主义思想，特别是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，深入推进依法治网，依法查处相关违法违规行为，切实维护国家网络安全、数据安全，保护人民群众合法权益。

三、实务解读

1. 个人信息保护负责人（PIPO）信息报送及官方审核的十大实务问题

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）

为了落实《个人信息保护法》等要求，国家网信办发布了《关于开展个人信息保护负责人信息报送工作的公告》（下称“报送公告”），明确处理 100 万人以上个人信息的个人信息处理者，应当在 2025 年 8 月 29 日前，向属地网信部门完成个人信息保护负责人（PIPO）情况及个人信息处理相关情况的信息报送。截至目前，绝大多数企业已经通过系统递交了报送信息，部分企业已经收到了审核通过的结果。

根据相关法律法规、政策口径及近期行业报送实践，我们针对 PIPO 报送的十大实务问题简要解读如下，仅供相关组织参考。

一、PIPO 有哪些法定职责？

1. 法律层面

（1）《个人信息保护法》明确规定：PIPO 负责对个人信息处理活动及采取的保护措施进行监督。《个人信息保护合规审计管理办法》及《审计指引》则对职责作了进一步细化，包括但不限于：负责企业个人信息保护合规审计工作；在个人信息处理重大事项决策前，有权提出意见和建议；对内部不合规的个人信息处理操作，有权制止并采取必要的纠正措施；等等。

（2）特殊情形：涉及儿童个人信息处理的，PIPO 应当依据《儿童个人信息网络保护规定》第 15 条，审批工作人员访问儿童个人信息的需求。当个人信息处理量超过 1000 万人时，PIPO 还需承担《网络数据安全保护条例》第 30 条所规定的相关职责，例如牵头管理机构工作，以及向有关主管部门报告网络数据安全情况，等等。

2. 国标层面

参考《信息安全技术 个人信息安全规范》第 11.1 条，PIPO 还应履行以下职责：

（1）全面统筹实施企业内部个人信息保护工作，对保护工作负直接责任；
（2）组织制定并推动落实个人信息保护工作计划；
（3）制定、签发、实施并定期更新个人信息保护政策和相关规程；
（4）建立、维护和更新个人信息清单（包括类型、数量、来源、接收方等）及访问授权策略；
（5）开展个人信息保护影响评估，提出改进建议并督促整改；
（6）组织开展个人信息安全培训；
（7）在产品或服务上线前进行检测，避免出现未披露的个人信息收集、使用或共享行为；
（8）公布投诉举报渠道，并及时处理相关投诉举报；
（9）与监管部门保持沟通，及时通报和报告个人信息保护及事件处置情况；等等。

二、PIPO 与其他职位有什么不一样？

1. 监管报送

根据《个人信息保护法》第 52 条及《关于开展个人信息保护负责人信息报送工作的公告》，个人信息处理量超过 100 万的企业需向监管部门报送 PIPO 信息。其他类似岗位（如《网络安全法》下的网络安全负责人、《数据安全法》下的数据安全负责人）目前尚无向监管部门的强制报送要求。

2. 信息公开

根据《个人信息保护法》第 52 条等规定，企业需要依法公开 PIPO 的联系方式。其他类似岗位（如 IT 负责人、安全负责人、人事负责人等）目前尚无信息公开的法律强制要求。

3. 个人责任大小

《个人信息保护法》第 66 条等规定，PIPO 一旦被认定为直接负责的主管人员的，个人可能面临最高 100 万元罚款，以及在一定期限内禁止担任相关企业的董监高及 PIPO。相比之下，网络安全负责人面临的最高罚款为 10 万元，且目前无禁业处罚等规定。

三、PIPO 个人有什么法律风险吗？

根据《个人信息保护法》第 66 条、《网络数据安全管理条例》第 56 条、《治安管理处罚法》《刑法》等规定，PIPO 个人可能承担以下显性法律风险：

罚款风险	作为主管人员或直接责任人员，可能因违法行为被处以最高 100 万元罚款
禁业风险	可能在一定期限内被禁止担任 PIPO、董事、监事或高级管理人员
刑事风险	作为主管人员或直接责任人员，可能因违法行为处以行政拘留甚至承担刑事责任的风险。

四、企业应当为 PIPO 提供哪些任职保障？

如前所述，PIPO 负责对企业的个人信息处理活动以及采取的保护措施等进行监督，负责个人信息处理者的个人信息保护合规审计工作。因此，企业应当为 PIPO 履职

提供相应保障。

具体应提供的任职保障，我们理解应包括但不限于如下：

1. 职级要求：
如前所述，PIPO 承担监督职责，并负责审计工作。参考《网络数据安全管理条例》对于网络数据安全负责人的要求，网络数据安全负责人由网络数据处理者管理层成员担任；参考《数据安全技术 敏感个人信息处理安全要求》，其中明确 PIPO 由处理者管理层成员担任。因此，PIPO 的级别建议不低于助理总监级别，从而保障其能独立行使监督权并负责审计活动，等等。

2. 资源支持：
参考《信息安全技术 个人信息安全规范》的规定，企业应为个人信息安全工作提供人力、物力、财力保障等，应为 PIPO 提供必要的资源。

我们理解企业的资源支持应包括但不限于如下：

（1）人力方面：企业应根据个人信息处理规模以及复杂程度，为 PIPO 配备必要的团队成员，从而支撑其工作。参考主流行业实践，处理个人信息超过 1000 万（或敏感个人信息超过 100 万）的企业，一般至少配备 3 人的专职团队。
（2）财力方面：企业应提供充足的财务预算，用于 PIPO 开展合规审计、教育培训、获取外部法律和技术支撑等。
（3）其他方面：企业应为 PIPO 履行职责提供必需的技术工具、系统权限，例如相关的数据访问权限、文档查阅权等等。

五、行业实践中一般如何保障 PIPO 个人权益？

参考目前行业实践情况，可从如下角度保障 PIPO 个人权益：

（1）为 PIPO 购买职业责任保险：
参考部分外资企业实践，例如为 PIPO 购买相关责任保险，并确保相关保险条款可以覆盖责任事件中的救济性成本。

目前，部分集团总部已购买类似保险，建议进一步确认集团总部所购买的类似保险中的被保险人是否涵盖中国 PIPO。

（2）与 PIPO 签署补偿协议：
参考部分外资企业实践，考虑到 PIPO 与企业其他职位不一样且个人责任巨大（详见本文第二、三部分），同时鉴于目前主流的责任保险可能暂时无法全面覆盖 PIPO 的个人经济性责任，因此我们建议企业与 PIPO 签订《PIPO 履职保障与自愿补偿协议》，为 PIPO 勤勉履职行为（非故意或严重违反企业规章制度行为）而产生的责任提供补偿。

六、行业实践中一般由谁担任 PIPO？

目前行业实践中，一般由以下几类人员担任 PIPO：（1）企业已设立专门的个人信息或隐私保护机构的，通常由该机构负责人担任；（2）法务或合规部门的负责人；（3）信息技术或安全部门的负责人；（4）少数情况下，也可能由业务负责人乃至由企业主要负责人担任。

我们建议企业采取（1）、（2）两类做法。目前，中国 PIPO 还是偏合规管理方向，PIPO 相关履职活动高度依赖于对中国法律法规的理解和适用，例如企业开展个人信息保护合规审计工作，需要牵头的 PIPO 对法律法规要求、审计要点和合规尺度进行准确把控。因此，任命具有法律专业知识背景的负责人担任 PIPO，更符合设立

该岗位的制度初衷，这也是目前较为常见的行业实践。

七、PIPO 与各业务/系统个人信息保护负责人是什么关系？

两者的关系可从以下几个角度区分理解：

（1）就法律性质而言，PIPO 是根据法律规定任命并报送的负责人，属于法定岗位；各业务/系统个人信息保护负责人并非是法定岗位，仅为满足 PIPO 信息报送的监管政策要求；

（2）就职责范围而言，企业的个人信息保护全面工作，仍由 PIPO 根据相关法律规定及岗位职责总体负责；各业务/系统个人信息保护负责人主要负责各自领域内的个保合规执行和落地等工作；

（3）就法律责任而言，各业务/系统个人信息保护负责人的法律责任并不会因报送而额外增加。根据《网信部门行政处罚裁量权基准适用规定》第 13 条的要求，相关责任人员的具体责任会根据具体相关责任人员的履职行为、主观过错等因素综合考量。

此外，我们建议企业以不同人选分别任命 PIPO 与各业务/系统个人信息保护负责人。因为，《个人信息保护负责人信息报送系统填报说明（第一版）》的填报说明明确要求企业分别填写各业务/系统个人信息保护负责人及其职位、电话及邮箱等内容，且填报示例内容均不同于 PIPO 的填报示例内容。因此，PIPO 与各业务/系统个人信息保护负责人为不同人选符合监管本意或期待。此外，分任制逻辑更符合企业个人信息保护合规工作实际，有利于推动各业务领域有效落实个人信息保护合规要求。参照已经通过备案的报送案例，分任制并未受到网信部门挑战，仅少数地区网信部门可能要求企业简要补充说明二者关系。

八、如何填报 PIPO 报送的业务/系统信息？

参照已经通过备案的报送案例，建议企业以“业务/场景”为维度申报，而不是以“系统”为维度申报。

以“业务/场景”为维度申报，符合“抓主要矛盾”的原则，有利于现行个保负责人信息报送制度的监管落地，符合现阶段为企业合规减负的大背景。报送个人信息保护负责人的姓名、联系方式等，是《个人信息保护法》第 52 条规定的法律义务；报送前述信息以外的其他信息（例如个人信息处理场景及数量等信息），并非《个人信息保护法》明确规定的法定义务，暂无直接对应的罚则。

在进行申报场景筛选时，我们建议企业坚持“重点突出、场景一致性、主体不遗漏”的原则，具体包括：

（1）企业的主营业务相关的场景（例如车联网、临床试验、电商场景、会员关系管理场景等）；
（2）对外的 2C 业务场景，涉及数据量较大的（例如 10 万+）；
（3）之前已经披露过的场景，例如数据出境申报、隐私政策披露等已披露的；
（4）覆盖不同类型主体（例如客户/用户、会员、医生/研究者/讲者、患者/受试者、车主/驾驶人、员工/候选人、供应商/经销商联系人等）；等。

九、PIPO 报送程序还有哪些实务问题？

参照已经通过备案的报送案例，PIPO 报送的具体审核单位为属地的直辖市下辖区/地市级网信部门，目前不同属地网信办的审核进度、审核口径等稍有不同。

首轮申报的企业目前收到的补正主要是形式层面，例如格式不一致（不得调整表格列宽）、信息填报不完整（《个人信息负责人信息报送表》漏填少填等）、缺少证

明材料（部分属地网信办要求提供 PIPO 的劳动合同），材料不完整（部分属地网信办要求 PIPO 任命书需由法代签字）等。

若“审核状态”显示为“退回完善”的，企业应当在 10 个工作日内补充完善材料。逾期未补充完善材料的，视为主动终止本次信息报送程序。

十、企业未按时办理 PIPO 报送有什么法律责任？

根据网信办发布的《关于开展个人信息保护负责人信息报送工作的公告》，未履行信息报送手续的，依照有关法律法规规章的规定处理，具体包括《个人信息保护法》第 66 条的规定相应的法律责任（责令改正、给予警告、罚款等）。

执法实践中的具体罚则，监管部门会依据《网信部门行政处罚裁量权基准适用规定》等，对违法行为的事实、当事人主观过错等因素进行综合评估与裁量。