（2025 年 2 月）

目录

一、法规速递

《个人信息保护合规审计管理办法》

发文机关：国家互联网信息办公室

发文时间：2025.02.14

生效时间：2025.05.01

第一条 为了规范个人信息保护合规审计活动，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，制定本办法。

第二条 在中华人民共和国境内开展个人信息保护合规审计，适用本办法。

本办法所称个人信息保护合规审计，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。

第三条 个人信息处理者自行开展个人信息保护合规审计的，应当由个人信息处理者内部机构或者委托专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第四条 处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。

第五条 个人信息处理者有以下情形之一的，国家网信部门和其他履行个人信息

保护职责的部门（以下统称为保护部门），可以要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计：

（一）发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；

（二）个人信息处理活动可能侵害众多个人的权益的；

（三）发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的。

对同一个人信息安全事件或者风险，不得重复要求个人信息处理者委托专业机构开展个人信息保护合规审计。

第六条 个人信息处理者自行开展或者按照保护部门要求委托专业机构开展个人信息保护合规审计的，应当参照本办法附件《个人信息保护合规审计指引》。

第七条 专业机构应当具备开展个人信息保护合规审计的能力，有与服务相适应的审计人员、场所、设施和资金等。

鼓励相关专业机构通过认证。专业机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。

第八条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当为专业机构正常开展个人信息保护合规审计工作提供必要支持，并承担审计费用。

第九条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求选定专业机构，在限定时间内完成个人信息保护合规审计；情况复杂的，报保护部门批准后，可以适当延长。

第十条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，在完成合规审计后，应当将专业机构出具的个人信息保护合规审计报告报送保护部门。

个人信息保护合规审计报告应当由专业机构主要负责人、合规审计负责人签字并加盖专业机构公章。

第十一条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求对合规审计中发现的问题进行整改。在整改完成后 15 个工作日内，向保护部门报送整改情况报告。

第十二条 处理 100 万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。

提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督。

第十三条 专业机构在从事个人信息保护合规审计活动时，应当遵守法律法规，诚信正直，公正客观地作出合规审计职业判断，对在履行个人信息保护合规审计职责中获得的个人信息、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，在合规审计工作结束后及时删除相关信息。

第十四条 专业机构不得转委托其他机构开展个人信息保护合规审计。

第十五条 同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计。

第十六条 保护部门对个人信息处理者开展个人信息保护合规审计情况进行监督检查。

第十七条 任何组织、个人有权对个人信息保护合规审计中的违法活动向保护部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

第十八条 个人信息处理者、专业机构违反本办法规定的，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。

第十九条 对国家机关和法律、法规授权的具有管理公共事务职能的组织的个人信息保护合规审计，不适用本办法。

第二十条 本办法自 2025 年 5 月 1 日起施行。

附件：个人信息保护合规审计指引

一、本指引根据《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、行政法规制定。

二、对个人信息处理活动的合法性基础进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，是否取得个人同意，该同意是否由个人在充分知情的前提下自愿、明确作出；

（二）基于个人同意处理个人信息的，个人信息的处理目的、处理方式、处理的个人信息种类发生变更的，是否重新取得个人同意；

（三）基于个人同意处理个人信息的，是否依照法律、行政法规取得个人单独同意

或者书面同意；

（四）处理个人信息未取得个人同意的，是否属于法律、行政法规规定不需要取得个人同意的情形。

三、对个人信息处理规则进行合规审计的，应当重点审查下列事项：

（一）是否真实、准确、完整地告知个人信息处理者的名称或者姓名和联系方式；

（二）是否以清单等便于查看的形式列明所收集的个人信息及其处理方式和种类；

（三）是否与处理目的直接相关，采取对个人权益影响最小的方式；

（四）是否明确个人信息保存期限或者保存期限的确定方法、到期后的处理方式，以及确定保存期限为实现处理目的所必要的最短时间；

（五）是否明确个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的途径和方法。

四、对个人信息处理者履行告知个人信息处理规则义务进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理规则；

（二）告知文本的大小、字体和颜色是否便于个人完整阅读告知事项；

（三）线下告知是否通过标注、说明等多种方式向个人履行告知义务；

（四）在线告知是否提供文本信息或者通过适当方式向个人履行告知义务；

（五）个人信息处理规则发生变更的，是否将变更内容及时告知个人；

（六）处理个人信息不需要告知的，是否属于法律、行政法规规定应当保密或者不需要告知的情形。

五、对个人信息处理者与其他个人信息处理者共同处理个人信息进行合规审计的，应当重点审查下列事项：

（一）是否约定各自的权利义务；

（二）个人信息权益保护机制；

（三）个人信息安全事件报告机制；

（四）其他法律、行政法规规定需要约定的权利和义务。

六、对个人信息处理者委托处理个人信息进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者在委托处理个人信息前，是否开展个人信息保护影响评估；

（二）个人信息处理者与受托人签订的合同，是否与受托人约定了委托处理的目的、期限、方式、个人信息的种类、保护措施以及双方的权利义务等；

（三）个人信息处理者是否采取定期检查等方式，对受托人的个人信息处理活动进行监督。

七、个人信息处理者存在因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息情形的，应当重点审查个人信息处理者是否向个人告知接收方的名称或者姓名和联系方式。

八、对个人信息处理者向其他个人信息处理者提供其处理的个人信息进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，是否取得个人的单独同意；

（二）是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，法律、行政法规规定应当保密或者不需要告知的除外；

（三）是否事前进行个人信息保护影响评估。

九、对个人信息处理者利用自动化决策处理个人信息进行合规审计的，应当重点审查下列事项：

（一）自动化决策的透明度，以及自动化决策的结果是否公平、公正；

（二）是否事前告知个人自动化决策处理个人信息的种类及可能带来的影响；

（三）是否事前进行个人信息保护影响评估；

（四）是否向用户提供保障机制，以便个人通过便捷方式拒绝通过自动化决策方式作出对个人权益有重大影响的决定，并要求个人信息处理者就通过自动化决策方式作出对用户个人权益有重大影响的决定予以说明；

（五）向个人进行信息推送、商业营销的，是否同时提供不针对个人特征的选项，或者提供便捷的拒绝自动化决策服务的方式；

（六）是否采取了有效措施，防止自动化决策根据消费者的偏好、交易习惯等对个人在交易条件上实行不合理的差别待遇；

（七）其他可能影响自动化决策的透明度和结果公平、公正的事项。

十、对个人信息处理者基于个人同意公开个人信息进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者公开其处理的个人信息前是否取得个人单独同意，该授权是否真实、有效，是否存在违背个人意愿将个人信息予以公开的情况；

（二）个人信息处理者公开个人信息前，是否进行个人信息保护影响评估。

十一、个人信息处理者在公共场所安装图像收集、个人身份识别设备的，应当重点对其安装图像收集、个人信息身份识别设备的合法性及所收集个人信息的用途进行审查。审查内容包括但不限于：

（一）是否为维护公共安全所必需，是否为商业目的处理所收集的个人信息；

（二）是否设置了显著的提示标识；

（三）个人信息处理者所收集的个人图像、身份识别信息用于维护公共安全以外用途的，是否取得个人单独同意。

十二、对个人信息处理者处理已公开的个人信息进行合规审计的，应当重点审查个人信息处理者是否存在下列违法违规行为：

（一）向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；

（二）利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；

（三）处理个人明确拒绝处理的已公开个人信息；

（四）对个人权益有重大影响，未取得个人同意；

（五）收集、留存或处理已公开个人信息的规模、时间或使用目的超出合理范围。

十三、对个人信息处理者处理敏感个人信息进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息，是否事前取得个人的单独同意；

（二）基于个人同意处理个人信息的，处理不满十四周岁未成年人的个人信息，是否事前取得未成年人的父母或者其他监护人的同意；

（三）处理敏感个人信息的目的、方式、范围是否合法、正当、必要；

（四）是否在事前进行个人信息保护影响评估；

（五）是否向个人告知处理敏感个人信息的必要性以及对个人权益的影响，法律、行政法规规定应当保密或者不需要告知的除外；

（六）法律、行政法规规定应当取得书面同意的，是否取得书面同意；

（七）是否遵守法律、行政法规对处理敏感个人信息的限制性规定。

十四、对个人信息处理者处理不满十四周岁未成年人个人信息进行合规审计的，应当重点审查下列事项：

（一）是否制定专门的个人信息处理规则；

（二）是否向未成年人及其监护人告知未成年人个人信息的处理目的、处理方式、处理必要性，以及处理个人信息的种类、所采取的保护措施等，法律、行政法规规定不需要告知的除外；

（三）基于个人同意处理个人信息，是否存在强制要求未成年人或者其监护人同意处理非必要个人信息的行为。

十五、对个人信息处理者向境外提供个人信息进行合规审计的，应当重点审查下列事项：

（一）关键信息基础设施运营者向境外提供个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定；

（二）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定；

（三）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息的，是否按照国家网信部门的规定，经个人信息保护认证或者按照国家网信部门制定的标准合同与境外接收方签订合同并向所在地省级网信部门备案，或者符合法律、行政法规、国家网信部门规定的其他条件；

（四）存在向外国司法或者执法机构提供存储于中华人民共和国境内个人信息情形的，是否经过中华人民共和国主管机关批准；

（五）是否向被列入限制或者禁止个人信息提供清单的组织和个人提供个人信息。

十六、对个人信息删除权保障情况进行合规审计的，应当重点审查下列事项：

（一）个人信息处理目的是否已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者是否停止提供产品或者服务，或者个人是否已注销账号；

（三）保存期限是否已届满；

（四）个人是否撤回同意；

（五）个人信息处理者是否违反法律、行政法规或者违反约定处理个人信息；

（六）应当删除个人信息，但法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者是否停止除存储和采取必要的安全措施之外的处理。

十七、对个人信息处理者保障个人在个人信息处理活动中的权利情况进行合规审计的，应当重点审查下列事项：

（一）是否建立便捷的个人行使权利的申请受理机制和处理机制；

（二）是否及时响应个人行使权利的申请，是否及时、完整、准确告知处理意见或者执行结果；

（三）拒绝个人行使权利请求的，是否向个人说明理由。

十八、个人信息处理者应当响应个人申请，对其个人信息处理规则进行解释说明，合规审计时应当重点对下列内容进行评价：

（一）个人信息处理者是否提供便捷的方式和途径，接受、处理个人关于个人信息处理规则解释说明的要求；

（二）接到个人的要求后，个人信息处理者是否在合理的时间内，使用通俗易懂的语言对其个人信息处理规则作出解释说明。

十九、个人信息处理者应当依照法律、行政法规的规定制定内部管理制度和操作规程，明确组织架构、岗位职责，建立工作流程、完善内控制度，保障个人信息处理合规与安全。合规审计时，应当重点对个人信息处理者个人信息保护内部管理制度和操作规程进行审查，包括但不限于：

（一）个人信息保护工作的方针、目标、原则是否符合法律、行政法规规定；

（二）个人信息保护组织架构、人员配备、行为规范、管理责任是否与应当履行的个人信息保护责任相适应；

（三）是否根据个人信息的种类、来源、敏感程度、用途等，对个人信息进行分类；

（四）是否建立个人信息安全事件应急响应机制；

（五）是否建立个人信息保护影响评估制度、合规审计制度；

（六）是否建立畅通的个人信息保护投诉举报受理流程；

（七）是否合理制定个人信息处理操作权限；

（八）是否制定实施个人信息保护安全教育和培训计划；

（九）是否建立个人信息保护负责人及相关人员履职评价制度；

（十）是否建立个人信息违法处理责任制度；

（十一）法律、行政法规规定的其他事项。

二十、个人信息处理者应当采取与所处理个人信息规模、类型相适应的安全技术措施，并对个人信息处理者采取的技术措施的有效性进行评价，评价内容包括但不限于：

（一）是否采取相应安全技术措施实现个人信息的保密性、完整性、可用性；

（二）是否采取加密、去标识化等安全技术措施，确保在不借助额外信息的情况下，消除或者降低个人信息的可识别性；

（三）采取的安全技术措施能否合理确定有关人员查阅、复制、传输个人信息等的操作权限，减少个人信息在处理过程中未经授权的访问和滥用风险。

二十一、对个人信息处理者教育培训计划的制定和实施情况进行合规审计时，应当重点对下列事项进行评价：

（一）是否按计划对管理人员、技术人员、操作人员、全员开展相应的安全教育和培训，是否对相应人员的个人信息保护意识和技能进行考核；

（二）培训内容、方式、对象、频率等能否满足个人信息保护需要。

二十二、对个人信息处理者指定的个人信息保护负责人履职情况进行合规审计的，应当重点审查下列事项：

（一）个人信息保护负责人是否具有相关的工作经历和专业知识，熟悉个人信息保护相关法律、行政法规；

（二）个人信息保护负责人是否具有明确清晰的职责，是否被赋予充分的权限协调个人信息处理者内部相关部门与人员；

（三）个人信息保护负责人在个人信息处理重大事项决策前是否有权提出相关意见和建议；

（四）个人信息保护负责人是否有权对个人信息处理者内部个人信息处理的不合规

操作进行制止和采取必要的纠正措施；

（五）个人信息处理者是否公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送保护部门。

二十三、对个人信息处理者开展个人信息保护影响评估情况进行合规审计时，应当重点对影响评估开展情况和评估内容进行审查：

（一）是否依照法律、行政法规的规定，在进行对个人权益具有重大影响的个人信息处理活动前进行个人信息保护影响评估；

（二）是否对个人信息的处理目的、处理方式等进行合法、正当、必要评估；

（三）是否对个人权益的影响及安全风险进行评估；

（四）是否对所采取的保护措施的合法性、有效性，以及与风险程度的适应性进行评估。

二十四、个人信息处理者应当制定个人信息安全事件应急预案。合规审计时，应当对应急预案的全面性、有效性、可执行性作出评价，包括但不限于下列内容：

（一）是否结合业务实际，对面临的个人信息安全风险作出系统评估和预测；

（二）总体要求、基本策略，组织机构、人员，技术、物资保障，指挥处置程序，应急和支持措施等是否足以应对预测的风险；

（三）是否对相关人员进行应急预案培训，定期对应急预案进行演练。

二十五、对个人信息处理者个人信息安全事件应急响应处置情况进行合规审计的，应当重点审查下列事项：

（一）是否按照应急预案、操作规程及时查明个人信息安全事件的影响、范围和可能造成的危害，分析、确定事件发生的原因，提出防止危害扩大的措施方案；

（二）是否建立通报渠道，在安全事件发生后按照相关规定及时通知保护部门和个人；

（三）是否采取相应措施将个人信息安全事件可能造成的损失和可能产生的危害风

险降低到最小。

二十六、对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制定的平台规则进行合规审计的，应当重点审查下列事项：

（一）平台规则是否与法律、行政法规相抵触；

（二）平台规则个人信息保护条款的有效性，是否合理界定了平台、平台内产品或者服务提供者的个人信息保护权利和义务；

（三）平台规则的执行情况，是否通过抽样等方式验证平台规则被有效执行。

二十七、对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发布的个人信息保护社会责任报告进行合规审计的，应当重点审查社会责任报告披露下列内容的情况：

（一）个人信息保护组织架构和内部管理情况；

（二）个人信息保护能力建设情况；

（三）个人信息保护措施和成效；

（四）个人行使权利的申请受理情况；

（五）独立监督机构履职情况；

（六）重大个人信息安全事件处理情况；

（七）促进个人信息保护社会共治的科普宣传、公益活动情况；

（八）法律、行政法规规定的其他事项。

《公共安全视频图像信息系统管理条例》

发文机关：国务院

发文时间：2025.02.10

生效时间：2025.04.01

第一条　为了规范公共安全视频图像信息系统管理，维护公共安全，保护个人隐私和个人信息权益，根据有关法律，制定本条例。

第二条　本条例所称公共安全视频图像信息系统（以下简称公共安全视频系统），是指通过在公共场所安装图像采集设备及相关设施，对涉及公共安全的区域进行视频图像信息收集、传输、显示、存储的系统。

第三条　公共安全视频系统管理工作坚持中国共产党的领导，贯彻党和国家路线方针政策和决策部署。

建设、使用公共安全视频系统，应当遵守法律法规，坚持统筹规划、合理适度、标准引领、安全可控，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第四条　国家鼓励和支持视频图像领域的技术创新与发展，建立和完善相关标准体系，支持有关行业组织依法加强行业自律，提高公共安全保障能力和个人信息保护水平。

第五条　国务院公安部门负责全国公共安全视频系统建设、使用的指导和监督管理工作。国务院其他有关部门在各自职责范围内负责公共安全视频系统建设、使用的相关管理工作。

县级以上地方人民政府公安机关负责本行政区域内公共安全视频系统建设、使用的指导和监督管理工作。县级以上地方人民政府其他有关部门在各自职责范围内负责公共安全视频系统建设、使用的相关管理工作。

第六条　县级以上地方人民政府应当加强对公共安全视频系统建设的统筹规划，充分利用现有资源，避免重复建设。

第七条　城乡主要路段、行政区域道路边界、桥梁、隧道、地下通道、广场、治安

保卫重点单位周边区域等公共场所的公共安全视频系统，由县级以上地方人民政府按照建设规划组织有关部门建设，纳入公共基础设施管理，建设、维护经费列入本级政府预算。

下列公共场所涉及公共安全区域的公共安全视频系统，由对相应场所负有经营管理责任的单位按照相关标准建设，安装图像采集设备的重点部位由县级以上地方人民政府各有关部门按照职责分工指导确定：

（一）商贸中心、会展中心、旅游景区、文化体育娱乐场所、教育机构、医疗机构、政务服务大厅、公园、公共停车场等人员聚集场所；

（二）出境入境口岸（通道）、机场、港口客运站、通航建筑物、铁路客运站、汽车客运站、城市轨道交通站等交通枢纽；

（三）客运列车、营运载客汽车、城市轨道交通车辆、客运船舶等大中型公共交通工具；

（四）高速公路、普通国省干线的服务区。

在前两款规定的场所、区域内安装图像采集设备及相关设施，应当为维护公共安全所必需，除前两款规定的政府有关部门、负有经营管理责任的单位（以下统称公共安全视频系统管理单位）外，其他任何单位或者个人不得安装。

第八条　禁止在公共场所的下列区域、部位安装图像采集设备及相关设施：

（一）旅馆、饭店、宾馆、招待所、民宿等经营接待食宿场所的客房或者包间内部；

（二）学生宿舍的房间内部，或者单位为内部人员提供住宿、休息服务的房间内部；

（三）公共的浴室、卫生间、更衣室、哺乳室、试衣间的内部；

（四）安装图像采集设备后能够拍摄、窥视、窃听他人隐私的其他区域、部位。

对上述区域、部位负有经营管理责任的单位或者个人，应当加强日常管理和检查，发现在前款所列区域、部位安装图像采集设备及相关设施的，应当立即报告所在地公安机关处理。

第九条　在本条例第七条规定之外的其他公共场所安装图像采集设备及相关设施，

应当为维护公共安全所必需，仅限于对该场所负有安全防范义务的单位或者个人安装，其他任何单位或者个人不得安装。

依照前款规定安装图像采集设备及相关设施的，应当遵守本条例除第十一条、第十四条、第十五条、第十六条第二款、第十七条规定的强制性要求之外的其他各项规定。

第十条　依照本条例安装图像采集设备及相关设施，位于军事禁区、军事管理区以及国家机关等涉密单位周边的，应当事先征得相关涉密单位的同意。

第十一条　公共安全视频系统管理单位应当按照相关标准建设公共安全视频系统，开展设计、施工、检验、验收等工作，并依法保存、管理相关档案资料。

第十二条　公共安全视频系统采用的产品、服务应当符合国家标准的强制性要求。产品、服务的提供者不得设置恶意程序；发现其产品、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。

第十三条　公共安全视频系统管理单位应当按照维护公共安全所必需、注重保护个人隐私和个人信息权益的要求，合理确定图像采集设备的安装位置、角度和采集范围，并设置显著的提示标识。未设置显著提示标识的，由公安机关责令改正。

第十四条　公共安全视频系统管理单位应当在系统投入使用之日起 30 日内，将单位基本情况、公共安全视频系统建设位置、图像采集设备数量及类型、视频图像信息存储期限等基本信息，向所在地县级人民政府公安机关备案。本条例施行前已经启用的，应当在本条例施行之日起 90 日内备案。公共安全视频系统备案事项发生变化的，应当及时办理备案变更。

公共安全视频系统管理单位应当对备案信息的真实性负责。

公安机关应当加强信息化建设，为公共安全视频系统管理单位办理备案提供便利，能够通过部门间信息共享获得的备案信息，不要求当事人提供。

第十五条　公共安全视频系统管理单位应当履行系统运行安全管理职责，履行网络安全、数据安全和个人信息保护义务，建立健全管理制度，完善防攻击、防入侵、防病毒、防篡改、防泄露等安全技术措施，定期维护设备设施，保障系统连续、稳定、安全运行，确保视频图像信息的原始完整。

公共安全视频系统管理单位委托他人运营的，应当通过签订安全保密协议等方式，约定前款规定的网络安全、数据安全和个人信息保护义务并监督受托方履行。

第十六条　公共安全视频系统管理单位使用视频图像信息，应当遵守法律法规，依法保护国家秘密、商业秘密、个人隐私和个人信息，不得滥用、泄露。

公共安全视频系统管理单位应当采取下列措施，防止滥用、泄露视频图像信息：

（一）建立系统监看、管理等重要岗位人员的入职审查、保密教育、岗位培训等管理制度；

（二）采取授权管理、访问控制等技术措施，严格规范内部人员对视频图像信息的查阅、处理；

（三）建立信息调用登记制度，如实记录查阅、调取视频图像信息的事由、内容及调用人员的单位、姓名等信息；

（四）其他防止滥用、泄露视频图像信息的措施。

第十七条　公共安全视频系统收集的视频图像信息应当保存不少于30日；30日后，对已经实现处理目的的视频图像信息，应当予以删除。法律、行政法规对视频图像信息保存期限另有规定的，从其规定。

第十八条　为公共安全视频系统提供网络传输服务的电信业务经营者，应当加强对视频图像信息传输的安全管理，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，维护数据的完整性、保密性和可用性。

第十九条　接受委托承担公共安全视频系统设计、施工、检验、验收、维护等工作的单位及其工作人员，应当对接触到的视频图像信息和相关档案资料予以保密，不得用于与受托工作无关的活动，不得擅自留存、加工、泄露或者向他人提供。

第二十条　国家机关为履行执法办案、处置突发事件等法定职责，查阅、调取公共安全视频系统收集的视频图像信息，应当依照法律、行政法规规定的权限、程序进行，并严格遵守保密规定，不得超出履行法定职责所必需的范围和限度。

第二十一条　为了保护自然人的生命健康、财产安全，经公共安全视频系统管理单位同意，本人、近亲属或者其他负有监护、看护、代管责任的人可以查阅关联的视频图像信息；对获悉的涉及公共安全、个人隐私和个人信息的视频图像信息，不得非法对外提供或者公开传播。

第二十二条　公共安全视频系统收集的视频图像信息被依法用于公开传播，可能损害个人、组织合法权益的，应当对涉及的人脸、机动车号牌等敏感个人信息，以及法人、非法人组织的名称、营业执照等信息采取严格保护措施。

第二十三条　任何单位或者个人不得实施下列行为：

（一）违反法律法规规定，对外提供或者公开传播公共安全视频系统收集的视频图像信息；

（二）擅自改动、迁移、拆除依据本条例第七条规定安装的图像采集设备及相关设施，或者以喷涂、遮挡等方式妨碍其正常运行；

（三）非法侵入、控制公共安全视频系统；

（四）非法获取公共安全视频系统中的数据；

（五）非法删除、隐匿、修改、增加公共安全视频系统中的数据或者应用程序；

（六）其他妨碍公共安全视频系统正常运行，危害网络安全、数据安全、个人信息

安全的行为。

第二十四条　公安机关对公共安全视频系统的建设、使用情况实施监督检查，有关单位或者个人应当予以协助、配合。

有关单位或者个人发现有违反本条例第七条第三款、第八条第一款、第九条第一款规定安装图像采集设备及相关设施的，可以向公安机关举报。公安机关应当依法及时处理。

第二十五条　公安机关应当严格执行内部监督制度，对其工作人员履行公共安全视频系统建设、使用职责情况进行监督。

公安机关及其工作人员在履行公共安全视频系统建设、使用、监督管理职责过程中，有违反本条例规定，或者其他滥用职权、玩忽职守、徇私舞弊行为的，任何单位或者个人有权检举、控告。

第二十六条　违反本条例第七条第三款、第九条第一款规定安装图像采集设备及相关设施的，由公安机关责令限期改正，并删除所收集的视频图像信息；拒不改正的，没收相关设备设施，对违法个人并处 5000 元以下罚款，对违法单位并处 2 万元以下罚款，对其直接负责的主管人员和其他直接责任人员处 5000 元以下罚款。

第二十七条　违反本条例第八条第一款规定安装图像采集设备及相关设施的，由公安机关没收相关设备设施，删除所收集的视频图像信息，对违法个人并处 5000 元以上 1 万元以下罚款，对违法单位并处 1 万元以上 2 万元以下罚款，对其直接负责的主管人员和其他直接责任人员处 5000 元以上 1 万元以下罚款；偷窥、偷拍、窃听他人隐私，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

对相应区域、部位负有经营管理责任的单位或者个人未履行本条例第八条第二款规

定的日常管理和检查义务的，由公安机关责令改正；拒不改正或者造成严重后果的，对违法个人处 5000 元以上 1 万元以下罚款，对违法单位处 1 万元以上 2 万元以下罚款，对其直接负责的主管人员和其他直接责任人员处 5000 元以上 1 万元以下罚款，并通报有关主管部门根据情节轻重责令暂停相关业务或者停业整顿、吊销相关业务许可或者吊销营业执照。

第二十八条　未依照本条例第十条规定征得相关涉密单位同意安装图像采集设备及相关设施的，由公安机关没收相关设备设施，删除所收集的视频图像信息，对违法个人并处 5000 元以上 1 万元以下罚款，对违法单位并处 1 万元以上 2 万元以下罚款，对其直接负责的主管人员和其他直接责任人员处 5000 元以上 1 万元以下罚款；非法获取国家秘密、军事秘密的，依照有关法律的规定给予处罚；构成犯罪的，依法追究刑事责任。

第二十九条　未依照本条例第十四条规定备案或者提供虚假备案信息的，由公安机关责令限期改正；拒不改正的，处 1 万元以下罚款。

第三十条　违反本条例第二十三条第二项规定擅自改动、迁移、拆除图像采集设备及相关设施的，由公安机关责令改正，给予警告；拒不改正或者造成严重后果的，对违法个人处 5000 元以下罚款，对违法单位处 5000 元以上 1 万元以下罚款，对其直接负责的主管人员和其他直接责任人员处 5000 元以下罚款。

第三十一条　违反本条例规定，未履行网络安全、数据安全和个人信息保护义务，或者非法对外提供、公开传播视频图像信息的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》的规定给予处罚；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第三十二条　公安机关及其工作人员在履行公共安全视频系统建设、使用、监督管

理职责过程中，违反本条例规定，或者有其他滥用职权、玩忽职守、徇私舞弊行为的，由上级公安机关或者有关主管部门责令改正，对负有责任的领导人员和直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

其他国家机关及其工作人员在履行公共安全视频系统建设、使用、相关管理职责过程中，违反本条例规定，或者在依照本条例第二十条规定查阅、调取视频图像信息过程中，有滥用职权、玩忽职守、徇私舞弊行为的，由其上级机关或者有关主管部门责令改正，对负有责任的领导人员和直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

第三十三条　在非公共场所安装图像采集设备及相关设施，不得危害公共安全或者侵犯他人的合法权益，对收集到的涉及公共安全、个人隐私和个人信息的视频图像信息，不得非法对外提供或者公开传播。

违反前款规定的，依照本条例第三十一条规定给予处罚。

第三十四条　本条例自 2025 年 4 月 1 日起施行。

二、热点案例

国家网信办依法集中查处一批侵害个人信息权益的违法违规 App

发布机关：国家互联网信息办公室

发布时间：2025.02.19

近期，针对广大人民群众反映强烈的 App 未公开收集使用规则、未按法律规定提供删除或更正个人信息功能等问题，国家网信办依据《个人信息保护法》《网络数据安全管理条例》《App 违法违规收集使用个人信息行为认定方法》等法律法规，依法依规查处“开个密室馆”等 82 款违法违规 App（含小程序）。

经查，“开个密室馆”等 4 款 App 存在未公开收集使用规则问题，违反《个人信息保护法》等法律法规，依法依规予以下架处置；“动态壁纸帝”等 78 款 App 存在未按法律规定提供删除或更正个人信息功能问题，违反《个人信息保护法》等法律法规，依法依规责令限期 1 个月完成整改，逾期未完成整改的，依法依规予以下架处置。

国家网信办相关负责人表示，将依法强化个人信息保护领域监督管理，坚决维护人民群众个人信息权益，不断提升网络空间法治化水平。

三、实务解读

1. 《公共安全视频图像信息系统管理条例》对企业部署 CCTV 的合规影响

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 2 月 10 日，国务院正式发布《公共安全视频图像信息系统管理条例》（以下简称“CCTV 条例”），全文三十四条，将于 2025 年 4 月 1 日开始实施。在此之前，公安部于 2016 年、2024 年先后两次公开征求意见。相较于征求意见稿，正式稿适度减轻了一般经营场所部署 CCTV 的合规责任，适度放宽了厉害关系人查看关联 CCTV 片段的限制条件，理清了条例与《个人信息保护法》等的规范边界。在此之前，广东、北京、重庆、江苏等地已经先后发布了公共 CCTV 监管相关的地方性规范。

结合近期立法、监管及司法实践，并参考类似项目经验，就 CCTV 条例对企业在经营场所部署 CCTV 的合规影响，我们解读如下，仅供参考。

一、设备类型

根据相关法律法规和监管实践，CCTV 条例规定的视频图像信息系统主要包括两类：

（1）仅具有图像采集功能的传统监控设备及其系统；

（2）具有个人身份识别的图像采集设备及其系统。

二、场所范围

（一）应当部署 CCTV 的场所

编号	场所类型	实例	主体
一类场所	公共安全场所	城乡主要路段、行政区域道路边界、地下通道、广场等； 治安保卫重点单位周边区域，例如金融、新闻机构等。	法定主体或者负有经营管理责任的单位
二类场所	人员聚集场所	商贸、会展中心，文体娱乐场所，停车场，医疗机构等； 交通枢纽、大中型公共交通工具、主干道沿线等；等	

（二）可以部署 CCTV 的场所

编号	场所类型	实例	条件
三类场所	经营性公共场所	商场、超市、餐厅、宾馆、厂区、园区、办公楼等的出入口、主要通道、大厅等	（1）非封闭的公共经营场所； （2）为维护公共安全所必需； （3）安装主体仅为对该场所负有安全防范义务的单位； （4）符合最小化原则；等等
四类场所	非公共场所	私人住宅周边	（1）不得危害公共安全或者侵犯他人的合法权益； （2）不得非法对外提供或者公开传播。

根据 CCTV 条例，企业违反前述规定拒不改正的，由公安机关没收相关设备设施，删除所收集的视频图像信息，对单位处 2 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 5 千元以下罚款。

（三）禁止部署 CCTV 的场所

根据 CCTV 条例及《人脸识别技术应用安全管理规定（试行）（征求意见稿）》等

规定，下列可能侵害他人隐私的区域、部位不得安装 CCTV：

（1）第三类场所的封闭式私人空间，例如用户具有隐私期待的客房、包房、单间、VIP 独立休息区、主管独立办公室、胶囊区、电话间等；

（2）第三类场所的敏感、隐私部位，例如浴室、卫生间、育婴室、更衣室、试衣间、化妆间等的内部区域；

（3）学生宿舍、单位住宿或休息场所的内部空间；

（4）能够拍摄、窥视、窃听他人隐私的其他区域、部位，以及可能造成歧视性、身心不适或隐私焦虑的其他部位，例如怼脸监控、定向拍摄等；等等。

根据 CCTV 条例，企业违反前述禁止规定的，由公安机关没收相关设备设施，删除所收集的视频图像信息，对单位处 1 万元以上 2 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 5 千元以上 1 万元以下罚款。

三、设备、安装及数据规范

根据 CCTV 条例及相关立法要求：

（1）部署的相关设备应当符合相关标准的强制性检测、评估要求，相关系统必须符合网络安全等级保护等要求，其他符合《公安视频图像信息系统安全技术要求》《信息安全技术 人脸识别数据安全要求》等标准。

（2）部署时应当合理确定安装位置、角度，确保精度和采集范围的最小必要。

（3）设置显著的提示标识，并参照《信息安全技术 个人信息处理中告知和同意的实施指南》等内容落实告知同意责任。

（4）第一、二类场所部署的 CCTV 的数据留存日期为 30 日，第三类场所的留存日期建议不得超过 30 日；留存日期期满后，应当对删除数据或者匿名化。

（5）收集的图像类个人信息，只能用于维护公共安全的目的，不得用于基于个人信息的热区分析、客流统计、熟客识别其他目的；取得个人单独同意的除外。

四、备案管理

根据 CCTV 条例，第一、二类场所部署的新增 CCTV 应当在系统启用前 30 日内向公安机关办理备案，存量 CCTV 应当在 90 日内补办备案；备案情况发生变化的应当办理变更备案。在国家层面，第三类场所部署的 CCTV 暂无强制公安备案的要求。

此外，根据《人脸识别技术应用安全管理规定（试行）（征求意见稿）》规定，在公共场所使用人脸识别技术，或者存储超过 1 万人人脸信息的人脸识别技术使用者，应当在 30 个工作日内向所属地市级以上网信部门备案。

五、调取、查看及传播规范

1. 官方调取

根据 CCTV 条例及《个人信息保护法》等规定，国家机关因履行执法办案、处置突发事件等法定职责，查看、调取公共视频系统收集的视频图像信息，应当依照法律、行政法规规定的权限和程序进行，并履行告知义务，法律另有规定除外。

对于调取程序规定，例如北京、广东、无锡、武汉等地明确规定，工作人员不少于两人；出示工作证件；出示公安机关的批准文件或者所在单位出具的证明文件；履行登记手续；等等。

2. 个人查看

为了更大程度保障人民群众的生命及财产安全，相较于征求意见稿，正式稿适度放宽了适用条件。CCTV 条例首次明确，满足下列所有条件的，个人可以查看关联的视频图像信息：

（1）前提必须为了保护自然人生命健康、财产安全，例如儿童走失、传染溯源、财物丢失等；

（2）申请人严格限定是利害关系人，即本人、近亲属或者其他负有照管责任的人；

（3）坚持最小必要原则，只能查看（不含复制、传播等）与之关联的片段信息；

（4）经 CCTV 管理单位同意；等等。

3. 公开传播

根据 CCTV 条例及《个人信息保护法》等规定，视频图像信息被用于新闻报道、舆论监督、回应热点等公开传播用途时，必须满足如下条件：

（1）经数据主体同意（个人单独同意）；

（2）对敏感个人信息及敏感数据采取严格的保护性措施，例如去标识化；等等。

此外，通过上述渠道对外提供视频图像信息的，应当如实记录提供的事由、内容及接收方人员的单位、姓名等信息。

六、其他合规治理要求

企业在部署 CCTV，以及在开展收集、提供、公开视频图像信息的数据处理活动时，还应当满足的合规治理要求包括但不限于：

（1）根据《个人信息保护法》、《网络数据安全管理条例》等规定，依法开展个人信息保护影响评估或数据安全影响评估；

（2）依法加强对供应商资质审查，依法签署协议，并监督供应商履行网络安全、数据安全和个人信息保护义务；

（3）发生系统安全事件或漏洞风险时，应当立即采取处置、补救等措施，按照规定及时履行报告、通知等义务；

（4）建立系统监看、管理等重要岗位人员的入职审查、保密教育、岗位培训等管理制度；

（5）采取授权管理、访问控制等技术措施，严格规范内部人员对视频图像信息

的处理；

（6）建立信息调用登记制度；等等。

其中，以上（4）、（5）、（6）三项，第一、二类场所主体强制适用，第三、四类场所主体可以比照开展合规建设。