附件 1

小型个人信息处理者个人信息保护合规审计自查表

序号	合规审计事项	合规情况自查	不合规及整改情况说明
1	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。	□合规　□不合规　□不适用	
2	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。	□合规　□不合规　□不适用	

3	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。	□合规 □不合规 □不适用	
4	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。	□合规 □不合规 □不适用	
5	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。	□合规 □不合规 □不适用	
6	个人信息处理者存在因合并、重组、分立、	□合规 □不合规 □不适用	

	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。		
7	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。	□合规 □不合规 □不适用	
8	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	□合规 □不合规 □不适用	

	和结果公平、公正的事项。		
9	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。	□合规 □不合规 □不适用	
10	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。	□合规 □不合规 □不适用	
11	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。	□合规 □不合规 □不适用	
12	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	□合规 □不合规 □不适用	

	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。		
13	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。	□合规　□不合规　□不适用	
14	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	□合规　□不合规　□不适用	

	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。		
15	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	□合规　□不合规　□不适用	

	措施之外的处理。		
16	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。	□合规 □不合规 □不适用	
17	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。	□合规 □不合规 □不适用	
18	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	□合规 □不合规 □不适用	

	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。		
19	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。	□合规 □不合规 □不适用	
20	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。	□合规 □不合规 □不适用	
21	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：	□合规 □不合规 □不适用	

	（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。		
22	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。	□合规　□不合规　□不适用	
23	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，	□合规　□不合规　□不适用	

	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。		
24	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。	□合规 □不合规 □不适用	

附件 2

小型个人信息处理者个人信息保护影响评估表

序号	影响评估情形	影响评估内容	影响评估结论	备注
1	处理敏感个人信息	个人信息的处理目的、处理方式等是否合法、正当、必要	□是 □否 □不适用	
		对个人权益的影响及安全风险	□无影响 □有影响 □不适用	
		所采取的保护措施是否合法、有效并与风险程度相适应	□是 □否 □不适用	
2	利用个人信息进行自动化决策	个人信息的处理目的、处理方式等是否合法、正当、必要	□是 □否 □不适用	
		对个人权益的影响及安全风险	□无影响 □有影响 □不适用	
		所采取的保护措施是否合法、有效并与风险程度相适应	□是 □否 □不适用	
3	委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息	个人信息的处理目的、处理方式等是否合法、正当、必要	□是 □否 □不适用	
		对个人权益的影响及安全风险	□无影响 □有影响 □不适用	
		所采取的保护措施是否合法、有效并与风险程度相适应	□是 □否 □不适用	
4	向境外提供个人信息	个人信息的处理目的、处理方式等是否合法、正当、必要	□是 □否 □不适用	

		对个人权益的影响及安全风险	□无影响 □有影响 □不适用	
		所采取的保护措施是否合法、有效并与风险程度相适应	□是 □否 □不适用	
5	其他对个人权益有重大影响的个人信息处理活动	个人信息的处理目的、处理方式等是否合法、正当、必要	□是 □否 □不适用	
		对个人权益的影响及安全风险	□无影响 □有影响 □不适用	
		所采取的保护措施是否合法、有效并与风险程度相适应	□是 □否 □不适用	