附件：合规审计中重点审查事项

《参考要点》针对开展的个人信息处理活动列举了如下重点审查，为企业开展合规审计提供参考指引：

序号	审查维度	具体审查项			规定出处
1.	个人信息处理活动的合法性基础条件	1)	处理个人信息是否取得个人同意，该同意是否在个人信息主体充分知情的前提下自愿、明确作出		第 2 条
		2)	基于个人同意处理个人信息	个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，是否重新取得个人同意	
		3)		是否为个人提供便捷的撤回同意的方式	
		4)		是否对个人同意的操作进行记录	
		5)		是否存在以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务的情况；处理个人信息属于提供产品或者服务所必需的除外	
		6)	处理个人信息未取得个人同意，是否属于法律、行政法规规定不需取得个人同意的情形		
2.	个人信息处理规则	1)	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		第 3 条
		2)	是否以清单形式列明所收集的个人信息及其处理目的、方式、范围		
		3)	是否明确个人信息存储期限或者存储期限的确定方法、到期后的处理方式，以及确保存储期限为实现处理目的所必要的最短时间		
		4)	是否明确个人查阅、复制、加工、转移、更正、补充、删除、公开、限制处理个人信息以及注销账号、撤回同意的途径和方法		
		5)	向第三方提供个人信息的，是否明确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，是否取得个人的单独同意		
3.	告知义务的履行	1)	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		第 4 条
		2)	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		
		3)	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		
		4)	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		
		5)	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		
4.	与他人共同处理个人信息的情形	1)	是否约定各自的权利义务		第 5 条
		2)	各方采取的个人信息保护措施		
		3)	个人信息权益保护机制		
		4)	个人信息安全事件报告机制		

		5)	侵害个人信息权益造成损害的，各方应当承担的责任	
5.	委托处理	1)	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	第 6 条
		2)	个人信息处理者与受托人签订的合同，是否约定了委托处理的目的、期限、方式及个人信息的种类、受托人应当采取的技术措施和管理措施、双方的权利义务等	
		3)	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，以确保委托处理个人信息的活动符合法律规定	
		4)	受托人是否严格按照委托合同的约定处理个人信息，是否存在超出约定的处理目的、处理方式处理个人信息的情况	
		5)	当委托合同不生效、无效、被撤销或者终止时，受托人是否将个人信息返还个人信息处理者或者予以删除	
		6)	受托人是否存在转委托他人处理个人信息的情况，是否得到个人信息处理者的同意。	
6.	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	1)	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	第 7 条
		2)	接收方是否继续履行个人信息处理者的义务	
		3)	接收方变更原先处理目的、处理方式的，是否依照法律、行政法规有关规定重新取得个人同意	
7.	向其他个人信息处理者提供其处理的个人信息	1)	是否取得个人的单独同意	第 8 条
		2)	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	
		3)	接收方是否在双方约定的处理目的、处理方式和个人信息的种类等范围内处理个人信息	
		4)	变更处理目的、处理方式的，是否依照法律、行政法规规定重新取得个人同意	
		5)	是否事前进行个人信息保护影响评估	
8.	自动化决策的透明度和结果的公平性、公正性	1)	是否事前主动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	第 9 条
		2)	是否事前对算法模型进行安全评估，并按国家相关规定进行备案，以尽可能减少自动化决策算法模型存在的缺陷，当应用场景和主要功能发生变化时，是否对算法模型重新进行评估	
		3)	是否事前对算法模型进行科技伦理审查	
		4)	是否事前进行个人信息保护影响评估	
		5)	是否向用户提供保障机制，以便用户可以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，或要求个人信息处理者就应用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	
		6)	是否向用户提供删除或者修改用于自动化决策服务的针对其个人特征的用户标签功能	
		7)	是否采取必要措施对算法和参数模型进行保护	
		8)	是否对个人信息处理、标签管理、模型训练等自动化决策过程	

			中的人工操作进行记录，防范人为恶意操纵自动化决策信息和结果		
		9)	向个人进行信息推送、商业营销时，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		
		10)	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		
9.	公开处理的个人信息	1)	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		第 10 条
		2)	个人信息处理者公开个人信息前，是否进行了个人信息保护影响评估		
10.	在公共场所安装图像采集、个人身份识别设备	1)	应当重点对其安装图像采集、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	是否为维护公共安全所必需，是否存在为商业目的处理所采集信息的情况	第 11 条
		2)		是否设置了显著的提示标志	
		3)		若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	
11.	处理已公开个人信息	1)	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信息		第 12 条
		2)	利用已公开的个人信息从事网络暴力活动		
		3)	处理个人明确拒绝处理的已公开个人信息		
		4)	未取得个人同意处理已公开的个人信息对个人权益造成重大影响		
12.	处理敏感个人信息	1)	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的，是否事前取得个人的单独同意		第 13 条
		2)	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		
		3)	处理敏感个人信息的目的、方式是否合法、正当、必要		
		4)	敏感个人信息处理是否与提供商品或者服务、履行法定职责或者法定义务等特定的目的密切相关，是否以非必要不处理为原则		
		5)	是否在事前进行个人信息保护影响评估，并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		
		6)	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		
		7)	是否对处理敏感个人信息的过程进行了记录，以保障处理敏感个人信息流程合法合规		
13.	涉及处理不满十四周岁未成年人个人信息	1)	是否制定专门的未成年人个人信息处理规则		第 14 条
		2)	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、处理必要性及处理个人信息的种类、所采取的保护措施等		
		3)	是否存在强制要求未成年人或者其监护人同意非必要的个人信息处理的行为		

14.	向境外提供个人信息	1)	关键信息基础设施运营者和处理 100 万人以上个人信息的个人信息处理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	第 15 条
		2)	自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的个人信息处理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	
		3)	是否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的个人信息的情形，若有，是否经过中华人民共和国主管机关批准	
		4)	中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，是否按照其规定执行	
		5)	是否按照国家网信部门的规定，经专业机构进行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，或者符合法律、行政法规、国家网信部门规定的其他条件	
		6)	是否了解境外接收方所在国家或者地区的个人信息保护政策和网络安全环境对出境个人信息的影响	
		7)	是否存在违规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的情形	
15.	个人信息处理者对境外接收方采取监督措施的有效性	1)	是否了解和掌握境外接收方的情况，特别是接收方是否具备必要的个人信息保护能力	第 16 条
		2)	是否向境外接收方告知我国法律、行政法规对个人信息保护的要求，并要求境外接收方采取相应的保护措施	
		3)	是否采取签订协议、定期核查等方式，督促境外接收方切实履行个人信息保护义务	
16.	个人信息删除权保障情况	1)	个人信息处理目的已实现、无法实现或者为实现处理目的不再必要	第 17 条
		2)	停止提供产品或者服务，或者个人注销账号	
		3)	达到与个人约定的存储期限	
		4)	个人撤回同意	
		5)	因使用自动化采集技术等，无法避免采集到非必要个人信息或者未经同意的个人信息	
		6)	个人信息处理者违反法律、行政法规或者违反约定处理个人信息	
		7)	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，个人信息处理者应当停止除存储和采取必要的安全措施之外的处理	
17.	保障个人行使个人信息权益的权利	1)	是否建立个人行使权利的申请受理机制	第 18 条
		2)	是否向个人提供便捷的查阅、复制、转移、更正、补充、删除个人信息的方法	
		3)	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	
18.	响应个人申	1)	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	第 19 条

	请，对其个人信息处理规则进行解释说明		关于个人信息处理规则解释说明的要求	
		2)	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	
19.	个人信息处理者履行主体责任情况	1)	个人信息保护制度制定、组织架构、管理程序与处理个人信息的性质、规模、复杂程度、风险程度的适应性	第 20 条
		2)	个人信息保护职责分工是否合理、职责是否明确、报告关系是否清晰	
		3)	个人信息处理者为个人信息保护提供的人、财、物保障与企业业务规模、运营计划、个人信息合规风险管理的匹配性	
20.	个人信息处理者个人信息保护内部管理制度和操作规程	1)	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	第 21 条
		2)	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	
		3)	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，并采取有针对性的管理或者安全技术措施	
		4)	是否建立个人信息安全事件应急响应机制	
		5)	是否建立个人信息保护影响评估、合规审计制度	
		6)	是否建立畅通的个人信息保护投诉举报受理流程	
		7)	是否制定实施个人信息保护安全教育和培训计划	
		8)	是否建立个人信息保护负责人及相关人员履职评价制度	
		9)	是否建立针对个人信息处理相关人员的个人信息违规处置或者违规行为责任制度，并有效实施	
21.	评价个人信息处理者采取的技术措施的有效性	1)	是否参照有关国家标准或者技术要求，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	第 22 条
		2)	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	
		3)	采取的安全技术措施能否合理确定有关人员查阅、复制、传输等个人信息的操作权限，减少个人信息在处理过程中未经授权的访问和滥用风险	
22.	个人信息处理者教育培训计划的制定和实施情况	1)	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	第 23 条
		2)	培训内容、培训方式、培训对象、培训频率等能否满足个人信息保护需要	
		1)	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组织内个人信息处理相关部门与人员	
		2)	个人信息保护负责人是否有权提名个人信息保护团队负责人，并与其保持顺畅的沟通和联系	
		3)	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	
		4)	个人信息保护负责人是否有权对组织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	
		5)	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、联系方式等报送履行个人信息保护职责的部门	
23.	个人信息保护影响评估情况	1)	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通过个人信息保护影响评估	第 25 条
		2)	是否对个人处理活动的合法性、正当性和必要性进行了分析评估，是否存在过度收集个人信息的情况	
		3)	是否对限制个人自主决定权、引发差别性待遇、导致个人名誉受损或者遭受精神压力、造成人身财产受损等安全风险进行了分析评估	
		4)	是否对所采取的保护措施的合法性、有效性、适应性进行了分析评估	
		5)	个人信息保护影响评估报告和处理记录是否至少保存三年	
24.	个人信息安全事件应急预案的全面性、有效性、可执行性	1)	是否结合业务实际，对面临的个人信息安全风险作出了系统评估和预测	第 26 条
		2)	指导思想、基本策略，组织机构、人员，技术、物资保障及指挥处置程序、应急和支持措施等是否足以应对预测的风险	
		3)	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	
25.	个人信息处理者个人信息安全事件应急响应处置情况	1)	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	第 27 条
		2)	是否建立通报渠道，能否在事件发生后 72 小时内通知履行个人信息保护职责的部门和个人	
		3)	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	

《参考要点》规定**大型互联网平台运营者**[1]在进行合规审计时应当重点审查以下内容：

序号	审查维度		具体审查项	规定出处
1.	独立机构的独立性、履职能力、监督作用等	1)	评价独立机构对个人信息保护情况进行监督的独立性，重点审查外部成员与个人信息处理者及其主要股东是否存在可能妨碍其进行独立客观判断的关系	第 28 条
		2)	评价外部成员的履职能力，重点审查外部成员是否具备相应的专业知识、能力和经验，能否对个人信息处理者的个人信息保护情况进行监督、指导，发表客观公正的意见建议	
		3)	评价独立机构的监督作用，重点审查独立机构在个人信息处理者合规制度体系建设、平台规则制定、重大个人信息安全事件处置、督促企业履行社会责任等方面发挥的作用	
2.	大型互联网平台规则	1)	评价平台规则的合法合规性，是否存在与法律、行政法规相抵触的情况	第 29 条
		2)	评价平台规则的公平公正性，是否存在恶意竞争、影响消费者	

[1] 目前未有生效法律法规对于大型互联网平台运营者进行明确定义，《管理办法（征求意见稿）》及《参考要点》亦未对此数量做出明确规定，参考《网络数据安全管理条例（征求意见稿）》大型互联网平台运营者是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

			权益等违反公平竞争原则、诚实信用原则、公序良俗的内容	
		3)	评价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，是否对平台内经营者处理个人信息行为进行规范，平台内经营者的个人信息保护义务是否明确	
		4)	检查平台规则的执行情况，通过抽样等方式验证平台规则是否被有效执行	
3.	平台内产品或者服务提供者的个人信息处理活动的监督	1)	是否定期审核平台内产品或者服务提供者个人信息处理规则的合法性、合理性	第 30 条
		2)	是否定期对平台内产品或者服务提供者处理个人信息遵守法律、行政法规情况进行审核	
		3)	对于严重违反法律、行政法规处理个人信息的产品或者服务提供者，平台是否及时停止向其提供服务	
4.	个人信息保护社会责任报告的披露情况	1)	个人信息保护组织架构和内部管理情况	第 31 条
		2)	个人信息保护能力建设情况	
		3)	个人信息保护措施和成效	
		4)	个人行使权利的申请受理情况	
		5)	独立监督机构履职情况	
		6)	重大个人信息安全事件处理情况	

《参考要点》规定**处理个人信息达到国家网信部门规定数量的个人信息处理者**[2]应当指定**个人信息保护负责人**，对个人信息处理活动的合规性负责。合规审计时，应当重点审查下列事项：

序号	审查维度		具体审查项	规定出处
1.	个人信息保护负责人	1)	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	第 24 条
		2)	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组织内个人信息处理相关部门与人员	
		3)	个人信息保护负责人是否有权提名个人信息保护团队负责人，并与其保持顺畅的沟通和联系	
		4)	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	
		5)	个人信息保护负责人是否有权对组织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	
		6)	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、联系方式等报送履行个人信息保护职责的部门	

[2] 参考《个人信息安全规范》满足以下条件之一的组织，应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，负责个人信息安全工作：
1) 主要业务涉及个人信息处理，且从业人员规模大于 200 人；
2) 处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；
3) 处理超过 10 万人的个人敏感信息的。