Impact of Personal Information Protection Compliance Audits on Investment, Financing and IPO Projects

Author: FU, Peng QUAN, Jiahui

《个人信息保护合规审计管理办法》（“**《个保审计办法》**”）落实了个人信息保护合规审计（下文亦简称为“**审计**”）制度的具体要求。部分企业必须定期进行审计；主管机关在一定情况下，可要求部分企业进行审计。这一系列制度的落实，对投融资项目和上市项目的部分合规要求将产生重要影响，企业及参与项目的专业机构需要关注。

1、与个人信息保护合规审计有关的新义务

● 处理超过1000万人个人信息的处理者应当进行审计

《个保审计办法》规定，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审计。这成为此类处理者应当定期完成的义务。

实践中，大中型互联网企业、大部分金融机构、大量消费类企业的主营业务本身面向个人用户，容易收集大量个人的个人信息。企业如果处理的个人信息对应的人数超过1000万人，需要在《个保审计办法》于2025年5月1日施行后，至少每两年进行一次审计。

实践中，有的企业处理个人信息的数量接近1000万人，或者由于业务特性，个人信息处理所涉及的人数在短期内可能发生较大变化。此外，需要注意的是，有的企业对于不继续提供服务的用户，或者对于很长一段时间以前收集到、希望作为客户转化的销售线索，没有定期删除，持续存储，甚至持续进行日常使用等处理，前述用户数据及销售线索所涉及的个人信息均计入该企业的个人信息处理人数中，这容易使得企业处理个人信息涉及的人数合计达到较大数值。如前述企业个人信息处理活动所涉及的个人信息人数超过1000万人，则该等企业进行审计将成为一项法定的定期义务。

● 被相应政府部门要求进行审计的情况

相应的政府部门有权在如下三种情况下，要求企业进行审计：

（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。

实践中，**这三种情况往往伴生于其他网络安全、数据安全或个人信息安全事件。**例如，企业发生安全事件，达到监管规则要求的情况或者级别，需要向主管机关进行汇报，如主管机关认为这种事件构成上述三种情况之一，主管机关有权要求企业进行审计。

三种情况当中，“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”相对明确，但是上述（一）和（二）两种情况的边界相对不太明晰。这两种情况有可能随其他的执法事件或争议而相应产生。比如，在其他执法事件（甚至不一定是直接与个人信息保护有关的执法事件）当中，执法机关发现可能存在严重影响个人权益或者严重缺乏安全措施等情况，执法机关将展开调查。调查过程中，由于具体办案的执法机关本身的执法精力和资源可能有限，执法机关可能有更强动力要求处理者进行审计，有助于节

省执法资源，并有助于引入专业机构，从而更精准、完整地发现问题，督促和帮助处理者尽快完成整改。

此外值得注意的是，上述（一）和（二）可能与现有惯常进行的其他一些网络安全、数据安全执法构成实际的衔接或协同。例如，网安部门和网信部门时常在一些企业页面被恶意篡改或者一些企业发生安全事件的情况下，关注这些企业本身的网络安全和数据安全措施；这一执法关注缘由可能引发成因为严重缺乏安全措施，导致进一步促使执法机关考虑是否要求相应企业开展审计。

- **部分企业需要设立个人信息保护负责人来负责审计**

《个人信息保护法》仅笼统规定，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应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。《个保审计办法》首次在审计这一事项上，为设立个人信息保护负责人设定了明确的门槛，要求处理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审计工作。这是一项便捷及比较明确的规定，据此，处理100万人以上个人信息的企业应设立个人信息保护负责人。

此外，有的数据合规水位较高的企业，在《个保审计办法》颁布之前，已经设立了个人信息保护负责人，但是负责人权责职位中，可能没有明确规定负责人在审计方面的职责、权限、流程等。企业如果处理100万人以上个人信息，则需要注意在其个人信息保护负责人的内部制度中，明确关于审计的职责、权限、流程。

2、个人信息保护合规审计对投融资项目的影响

投融资项目中，融资方（即融资项目中的目标公司）一般很重视自身对投资人呈现的企业质量，其中包括合规程度，以尽量在企业风险程度方面向投资人呈现较佳的观感。投资人则关注融资方各方面是否存在不合规情况，由此产生的潜在风险（例如罚款，停业，整改等），以及对潜在风险的整改或者解决方案。

- **数据合规尽职调查中关注个人信息保护合规审计**

对于科技型企业，汽车、金融、医疗等行业企业或者处理个人信息量较大的其他类型的融资方，投资人可能会聘请顾问进行专项的数据合规尽职调查。此前的数据合规尽职调查中，由于审计的具体细节没有落地，所以关注程度较低，实际要求整改的依据相对有限，潜在风险相对可控。

目前，随着《个保审计办法》的颁布，审计的细节要求（包括义务主体、触发场景、审查范围等）以及没有依法进行审计的风险更为明晰。因此，投资人宜加强数据合规尽职调查中对于目标公司审计情况的关注。例如：

（1）如果目标公司处理超过1000万人的个人信息，则应关注是否在《个保审计办法》生效日后的两年内至少进行过一次审计。

（2）数据合规尽职调查往往会关注目标公司过往被通报、调查、处罚或者发生数据相关争议等的负面情况。对这些情况进行调查的过程中，需要与是否可能触发《个保审计办法》所规定的监管机构主动要求审计的情形结合考虑。例如，目标公司过往是否已经被主管机关关注甚至已经启动调查，是否已经发生过比较严重的个人信息泄露事件，是否发生过与个人信息保护有关的投诉、争议、诉讼或者舆情事件。这些事件可能引发监管机构对目标公司是否进行过、是否应当进行审计的关注。

（3）目标公司是否应当指定个人信息保护负责人，是否已经颁布制定了审计方面的内部管理制度和操作规程，或者已经指定的个人信息保护负责人的相应职权或职责范围中，是否有关于审计的内容。

- **交易文件应关注与个人信息保护审计有关的条款设计**

交易文件往往通过陈述与保证（representations and warranties）条款让目标公司明确目前的一些合规现状或事实情况，通过交割先决条件（condition precedent）条款来要求目标公司对真正重要的数据合规整改项在交割之前进行整改并达到一定状态，通过交割后承诺（post-closing covenant）条款来促使目标公司对其

他不太紧迫但需要整改的数据合规内容进行约定、要求完成整改，并通过违约（breach of contract）条款或者专门的赔偿（indemnity）条款来要求目标公司或者创始股东对某些数据合规瑕疵造成的损失进行赔偿。

在个人信息保护合规审计制度已经落地的情况下，**各方将关注是否以及在何种程度上，通过陈述保证条款，要求目标公司对现状进行确认。**例如，目标公司如果确认处理的个人信息涉及的人数不及1000万人并因此确定不属于根据《个保审计办法》需要进行定期审计的个人信息处理者，目标公司实际处理的个人信息所涉及人数这一客观状态在一个投资项目中可能难以得到确定性核实的，各方可以考虑协商，请目标公司对处理个人信息的人数不到法定数量从而不需要进行定期审计做出陈述与保证。例如，目标公司处理的个人信息涉及的人数远远不及100万人，从而不希望明确指定个人信息保护负责人并规定与审计的权责和流程。目标公司处理个人信息涉及的实际人数总数这一情况在投资项目中可能无法得到确定性核实，因此各方可能协商，由目标公司在陈述保证条款中，确认上述情况。

此外，**对于与审计有关的重大、核心事项，视交易节奏和各方对风险的判断，可能构成交割先决条件或者交割后的整改承诺。**例如，如果目标公司已经明确被主管机关要求进行审计，正在进行审计的过程中，如投资交易的交割没有特别紧急的时间表，投资人可能要求目标公司及时完成审计，并根据《个保审计办法》的要求，及时将审计报告报送给主管部门，并根据审计报告发现的问题及时整改，在整改完成后15个工作日内报送给主管部门，并进一步要求将上述任务的完成作为交割的先决条件。例如，如果目标公司处理个人信息涉及的人数超过了1000万人，但是尚未进行审计，各方可能要求目标公司在交割后、《个保审计办法》规定的时间内，及时完成审计。

另外，各方视交易中的具体风险情况，以及**视各方商业角度协商达成的风险分担安排，可能要求目标公司及创始股东对一些实质的审计不合规情况造成的损失进行赔偿。**例如已经被主管机关要求进行审计或已经被主管机关要求就审计发现问题进行整改但没有在要求的时间内完成审计、整改或整改后报告从而引发了处罚或其他负面后果，例如处理超过1000万人个人信息的目标公司没有按照规定的时间进行审计、整改或整改后报告而引发处罚或者其他负面后果。

3、个人信息保护合规审计要求对境内外上市项目的影响

个人信息保护合规审计制度作为将要明确落地的法定制度和义务，境内外上市中的发行人、保荐人和参与项目的其他专业机构需要关注这一制度对发行人合规性的要求和影响。

例如，对于处理超过1000万人个人信息的发行人，需要关注是否已经完成审计，或者至少将审计准备提上日程。从规则层面而言，《个保审计办法》于2025年5月1日起施行。所以此类发行人在2025年5月1日起的两年内，应当至少完成一次审计。当然，在未被主管部门要求进行审计的前提下，该等义务的具体实施时间，也可以结合上市项目的整体时间表综合考虑。一般而言，例如，在境外发行项目过程中的一些重要节点，比如港股上市项目的A1申报及香港联交所、香港证监会、中国证监会的反馈问询及答复期间，如果法定要求必须完成定期审计的截止时间未到，则对审计工作有所关注、一定程度上有推进合规义务落实的积极行为也是可以接受的。但如果根据项目时间表，在前述重要节点（特别是直接面对监管问询的重要节点）之前，法定必须进行定期审计的截止时间将要届满，则发行人有必要提前倒排时间，提早安排进行审计。

再如，如果发行人历史上发生过一些负面事件、争议或者被政府主管部门采取过监管行动（特别是例如已经发生过导致100万人以上个人信息或者10万人以上敏感个人信息泄露的安全事件），可能使得主管机构能够根据《个保审计办法》有抓手要求发行人进行审计的，则参与发行的各方应关注、论证此时是否可能需要发行人主动进行审计，以降低有关事件带来的潜在负面影响。

此外，对于处理个人信息涉及的人数达到100万人以上的发行人，需要设置个人信息保护负责人，并且将与审计有关的内容、流程写入负责人的权责范围。目前，大量境外上市项目中，数据合规顾问协助发行人进行数据合规整改时，在相当多的情况下会在内部制度层面要求或建议发行人设置个人信息保护负责人。后续，如发行人确属处理个人信息涉及的人数达到100万人以上的情况，应关注在个人信息保护负责人权责制度

中，加入审计的有关内容，并考虑进一步明确审计的管理制度和操作规程。

2025-02-18