DOI:10.19641/j.cnki.42-1290/f.2023.20.012

个人信息保护合规审计制度建设思考

胡耘通（博士生导师）

【摘要】伴随着数字经济的迅猛发展，个人信息作为当前一项重要的数据资源，亟需给予充分关注和重点保护。为了落实《个人信息保护法》的相关条款内容，国家互联网信息办公室发布的《个人信息保护合规审计管理办法（征求意见稿）》将填补立法空白，开创新的审计实践。但其仍需要在扩充合规审计的评价依据、增加法律责任条款设置、消除民事法律关系行政倾向、明确审计结果的具体意见形式、强化审计结果的公布与运用等方面予以完善，以真正发挥规范和保障个人信息保护合规审计良好运行之应有功效。

【关键词】评价依据；责任条款；民事法律关系；审计结果

【中图分类号】F239　　【文献标识码】A　　【文章编号】1004-0994(2023)20-0088-4

伴随着数字经济的迅猛发展、数字社会的积极建立，数据逐渐成为一种新型生产要素，数据安全也越发重要，而个人信息的数据保护已然成为整个数据安全体系的核心和基础。在持续推进数字中国建设的战略背景之下，《个人信息保护法》首次以法律形式明确了个人信息保护合规审计，具有非常重大的现实意义（陈智敏，2022）。但奇安信行业安全研究中心等单位联合发布的《中国政企机构数据安全风险分析报告》显示，个人信息数据被泄露的案件最多，2022年3～9月，全国约有868.8亿条个人信息数据被泄露，相当于平均每人有62条个人信息数据被以各种方式盗取、泄露，个人信息的数据安全保障情况堪忧。为回应现实的紧迫情势，我国近年来陆续颁布《数据安全法》《个人信息保护法》等专门法律法规，为数据安全以及合规管理工作的依法开展提供了法定依据。与此同时，合规审计也成为一种新型的数据（信息）安全治理手段。《个人信息保护法》第54、64条分别明确了个人信息处理的自主审计及监管要求审计①；《网络数据安全管理条例（征求意见稿）》第53、58条分别明确了年度审计及国家建立数据安全审计制度②。可见，在全面依法治国背景下，数据（信息）安全合规审计制度的建立完善是良法善治的必然要求。未来，个人信息保护合规审计将是一项常态化、持续性的制度工作。2023年8月，《个人信息保护合规审计管理办法（征求意见稿）》（简称《征求意见稿》）具体落实了《个人信息保护法》第54、64条关于个人信息保护合规审计的条款，为合规审计工作制定了具体的执行规则，将填补自《个人信息保护法》规定合规审计机制以来相关下位规范的空白。

一、《征求意见稿》的积极意义

《个人信息保护法》自2021年11月施行以来，针对个人信息保护的监管力度不断加大，公民个人的信息保护意识也显著提升，滥用个人信息、侵犯个人信息权益等问题得到较大改善。《征求意见稿》从立法目的、审计定义、审计对象、审计机构、审计启动、审计时限、独立性要求等方面进行了全面的规范，并发布了《合规审计参考要点》，为实际工作提供了操作指南。而加强个人信息保护，除强化法治宣传以厘清个人在信息处理活动中的权利、明确个人信息处理者的义务外，合规审计不失为一件防范和控制个人信息处理风险的“利器”。《征求意见稿》发布的目的就在于通过合规审计“提高个人信息处理活动合规水平，保护个人信息权益”。美国会计学家梅格斯曾言，我们正生活在一个履行受托责任的伟大时期。受托责任不仅是一种普遍的经济关系，更是一种非静止的社会活动关系。基于受

【基金项目】重庆市社会科学规划项目（项目编号：2022NDYB18）；重庆市教委人文社会科学研究项目（项目编号：23SKSZ009）；重庆市研究生教育教学改革研究项目（项目编号：YJG223046）；重庆市高等教育教学改革研究项目（项目编号：233134）；黑龙江省哲学社会科学研究规划项目（项目编号：19FXB036）

【作者单位】西南政法大学法务会计与财税合规研究中心，重庆 401120

托责任关系，个人信息处理者处理个人信息，但源于信息非对称等矛盾，个人为避免或减少由此带来的损害，会对个人信息处理活动产生监督需求，合规审计恰是对个人信息处理活动监督需求的回应方式之一。个人信息保护合规审计通过审查、评价个人信息处理活动与法律法规、国家规定等相关标准的一致程度，揭示个人信息处理者的不合规或者违规情形，并按照相关规定予以披露、问责。由此不仅能提高个人信息处理活动的质量和保障水平，而且有助于减轻个人信息权益上的损害（陈炎，2022）。目前，个人信息保护合规审计仅处于探索阶段，个人信息处理者对合规性、审计流程的理解判断不一。总体而言，合规审计不仅是个人信息处理者实施自我治理、自我监督的必要工具，也是监管部门监督个人信息处理者行为的重要方式。本质上，个人信息保护合规审计被视为对个人信息处理者针对个人信息处理、保护情形的功能性“体检”，对个人信息处理者开展合规审计、建立多层次的个人信息保护体系、提升个人信息保护能力具有显著效果。

二、扩充合规审计的评价依据

评价依据是合规审计工作的前提，要想通过合规审计工作得出适当的结论意见，就必须遵循科学、合理的评价依据。《征求意见稿》第3条指出，“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”。该条规定除明确合规审计定义外，还提出了审查和评价的依据——“法律、行政法规”。《个人信息保护法》第51条要求“个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定……”；第54条指出，“个人信息处理者应当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”。可见《个人信息保护法》仅明确了个人信息处理活动遵守、符合“法律、行政法规”的要求，但《征求意见稿》的审计评价依据是否限于“法律、行政法规”，评价标准的范围是否较窄？值得进一步考量。

与此近似，《审计法》第3条规定“审计机关依据有关财政收支、财务收支的法律、法规和国家其他有关规定进行审计评价”；《中国注册会计师审计准则第150号——对财务报表形成审计意见和出具审计报告》第11条明确指出“注册会计师应当就财务报表是否在所有重大方面按照适用的财务报告编制基础的规定编制并实现公允反映形成审计意见”，此处的“财务报告编制基础”就是评价依据。“法律、行政法规”是否能够涵盖所有个人信息处理活动的全部标准？换句话说，其他法规或者国家规定是否会对个人信息处理活动进行规定？例如，《儿童个人信息网络保护规定》属于部门规章，当涉及儿童个人信息处理活动时，审计评价是否需要遵循？另外，《信息安全技术 个人信息安全规范》（GB/T 35273-2020）、《信息安全技术 个人信息安全影响评估指南》（GB/T 39335-2020）等国家标准，是否属于合规审计的评价依据？实际上，随着数据信息保护的纵深发展，医疗、金融、汽车等不同行业的监管部门亦会制定相关准则，合规审计也应当遵从行业准则中设置的关于个人信息保护义务、责任方面的标准规定。按照循序渐进的原理，地方性法规、地方规章及其他国家规定应当成为审计评价依据。因此，建议将《审计法》第3条修改为“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、法规和国家其他有关规定的情况进行审查和评价的监督活动”。当然，国家其他规定还应当涵盖行业标准、地方标准等，具体适用于某个行业、某个区域的个人信息保护合规审计工作。

三、增加法律责任条款设置

法律责任是保障法律规范有效落实的重要环节。《征求意见稿》仅在第15条明确规定，“违反本办法规定的，依据《个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任”。但《个人信息保护法》也缺乏相关主体的法律责任条款，包括专业机构以及个人信息处理者的某些违法行为，均没有设置法律责任条款。以专业机构为例，《征求意见稿》第14条明确了其从事合规审计活动中应当履行的义务，但未规定对应的法律责任条款，如果专业机构不能“诚信正直、公正客观地作出合规审计职业判断”，应如何承担法律责任？如果专业机构“有出具虚假、失实报告等违规行为的”，仅是“永久禁止列入个人信息保护合规审计专业机构推荐目录”，则法律责任与违法行为并不匹配。此外，《征求意见稿》第8条明确规定个人信息处理者“应当保证专业机构能够正常行使下列权限……”，如果个人信息处理者违反该规定、出现不提供或者协助查阅相关文件或资料的情况，应如何追究相应的法律责任，也缺乏规定。再如，《征求意见稿》第7条指出，“个人信息处理者按照履行个人信息保护职责的部门要求开展个人信息保护合规审计的，应当在收到通知后尽快按照要求选定专业机构进行个人信息保护合规审计”。这里的“尽快”含义并不明确，且对于没有“尽快”

进行合规审计的行为，也缺乏针对个人信息处理者的违法责任条款。

“没有无权利的义务，也没有无义务的权利”。基于权利义务相一致的基本理念，针对专业机构以及个人信息处理者的违法行为，笔者建议增补相应的法律责任条款。例如，如果个人信息处理者违反《征求意见稿》第7、8条规定，不能尽快进行合规审计的、不能保证专业机构正常行使权限的，履行个人信息保护职责的部门（简称“监管部门”）应当“责令改正，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款”。如果专业机构违反《征求意见稿》第14条规定，出现不能“诚信正直、公正客观地作出合规审计职业判断”“转包委托第三方开展个人信息保护合规审计”等情形，监管部门应当“责令改正，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款”。当然，如果专业机构有出具虚假、失实报告等行为并构成犯罪的，则追究相应的刑事法律责任。

四、消除民事法律关系行政倾向

无论是自主实施审计，还是监管要求审计，个人信息处理者与专业机构之间均是基于合同而建立的民事法律关系，应当首先符合民事法律关系的基本特征——平等性、自主性等，但现有规定带有行政倾向。例如，《征求意见稿》第9条规定，“个人信息处理者按照履行个人信息保护职责部门要求委托专业机构开展个人信息保护合规审计的，应当在90个工作日内完成个人信息保护合规审计；情况复杂的，报经履行个人信息保护职责的部门批准后可适当延长”。针对“情况复杂的”，延长合规审计期限，需要经过监管部门批准。换句话说，基于个人信息处理者与专业机构之间被审计与审计的民事法律关系，延长审计期限需要监管部门的“批准”，原本应当由民事法律关系的双方当事人自主变更的“审计期限”，改为“批准”变更，即行政权力介入民事法律关系的运行，使民事法律关系的平等性、自主性受到影响。再如，《征求意见稿》第11条规定，“个人信息处理者按照履行个人信息保护职责的部门要求委托专业机构开展个人信息保护合规审计的，应当按照专业机构给出的整改建议进行整改，经专业机构复核后将整改情况报送履行个人信息保护职责的部门”。该条款“整改”带有强制性，即“应当按照……整改建议”整改，并将整改情况报监管部门。专业机构的审计意见、整改建议原本属于民事法律关系的内容，一般也属于双方自愿协商的结果，只属于约定条款，并非法定的权利义务内容，不具备强制性，显然“应当……整改”的要求，带有强制性的行政色彩，突破了当事人之间的民事法律关系属性。

专业机构的合规审计与审计机关的国家审计并不相同，后者带有行政执法的属性，审计机关的审计结果包括整改建议均具有具体行政行为的典型特点——强制性，且会追究不整改的法律责任[③]。归根结底，专业机构的合规审计本质上仍属于民事法律行为，不应具备法律上的强制性。因此，建议将《征求意见稿》第9条修改为“个人信息处理者按照履行个人信息保护职责部门要求委托专业机构开展个人信息保护合规审计的，应当在90个工作日内完成个人信息保护合规审计；情况复杂的，经个人信息处理者、专业机构协商延长不超过30个工作日”；将第11条修改为“个人信息处理者按照履行个人信息保护职责的部门要求委托专业机构开展个人信息保护合规审计的，履行个人信息保护职责的部门审核专业机构的审计报告，要求个人信息处理者进行整改。专业机构复核整改情况，报送履行个人信息保护职责的部门。拒不整改或者整改不到位的，由履行个人信息保护职责的部门追究相应的法律责任”。可见，监管部门在履行审核专业机构审计报告的职责之后，再依照相应的职权向个人信息处理者下达整改建议，由单纯的民事法律关系变更为监管部门与个人信息处理者之间的行政法律关系，不仅增强了整改建议的权威性，而且能确保民事法律关系与行政法律关系相互独立，剥离了民事法律关系的行政倾向。

五、明确审计结果的具体意见形式

《征求意见稿》第10条指出，“个人信息处理者按照履行个人信息保护职责部门要求委托专业机构开展个人信息保护合规审计的，应当按照本办法要求组织实施个人信息保护合规审计，在实施必要合规审计程序后，及时将专业机构出具的个人信息保护合规审计报告报送履行个人信息保护职责的部门。个人信息保护合规审计报告应当由合规审计负责人、专业机构负责人签字并加盖专业机构公章”。该条款明确了审计报告生效的形式要求，即“签字”+“公章”。但关于审计结果的实质规定显然是匮乏和薄弱的，就本质而言，个人信息保护合规审计属于一项审查、评价的监督活动，既然涉及审查、评价，就需要出具相应的审计结果报告，个人信息处理是合规还是不合规，抑或是部分合规、部分不合规等。虽然审计不是一项完全的保证，但至少能够给予相应的意见和建议，否则相应“整改”规

定也无从谈起。

与国家审计的行政执法性质不同，专业机构作为民事法律主体，其审计行为更应当符合民事法律活动的特征。因此，专业机构应当参照《中国注册会计师审计准则第1501号——对财务报表形成审计意见和出具审计报告》相关规定④出具审计结果，专业机构应当就个人信息处理活动是否遵守法律法规、国家相关规定的情况形成审计结果，具体包括：无保留意见——能够遵守法律法规、国家相关规定；非无保留意见——视遵守或者违反法律法规、国家相关规定的情况或者无法获得审计证据的情况以及严重程度，分别发表保留意见、否定意见或无法表示意见。

六、强化审计结果的公布与运用

在要求委托专业机构开展的个人信息保护合规审计中，监管部门只要求“在实施必要合规审计程序后，及时将专业机构出具的个人信息保护合规审计报告报送”（《征求意见稿》第10条）。该项规定中，一方面并未明确是否要公布该审计结果，另一方面也没有明确“报送”之后如何运用该审计结果。实际上，《个人信息保护法》第61条要求履行个人信息保护职责的部门“组织对应用程序等个人信息保护情况进行测评，并公布测评结果”。可见，公布审计结果不仅属于监管部门履行职责的一种方式，而且有利于增强社会公众监督。此外，《征求意见稿》第11条规定，“个人信息处理者按照履行个人信息保护职责的部门要求委托专业机构开展个人信息保护合规审计的，应当按照专业机构给出的整改建议进行整改，经专业机构复核后将整改情况报送履行个人信息保护职责的部门”。此处“整改”被过度赋予了行政属性，其原本属于民事主体之间的自主行为。事实上，“整改”应当由监管部门做出明确规定，而非专业机构的权力职责范围。另外，对相关人员进行追责属于合规审计结果的运用问题，也需要进一步明确和细化。

基于此，建议将《征求意见稿》第10条修改为“个人信息处理者按照履行个人信息保护职责部门要求委托专业机构开展个人信息保护合规审计的，个人信息处理者应当及时将审计报告报送履行个人信息保护职责的部门。履行个人信息保护职责的部门在符合相关保密规定的情形下，向社会公开审计结果”。这一方面可将审计结果对外公开，以有效接受社会监督，另一方面也能够发挥警示与教育作用（贾丹等，2022）。并且，监管部门应当依据审计结果对个人信息处理者及相关人员给予相应的处理处罚措施，包括纳入诚信建设体系等，以提高个人信息保护的社会认可度和接受度，同时提高个人信息处理者及相关人员的违法成本。

七、其他需要完善的内容

《征求意见稿》作为一项创新型立法，还有部分条文值得商榷完善。例如，第7条指出，“个人信息处理者按照履行个人信息保护职责的部门要求开展个人信息保护合规审计的，应当在收到通知后尽快按照要求选定专业机构进行个人信息保护合规审计”。此处应当明确“尽快”的涵义，建议修改为“10个工作日”。再如，第14条指出，“专业机构在履行个人信息保护合规审计职责时不得恶意干扰个人信息处理者的正常经营活动”。此处“恶意”作为主观意愿，在实践中难以判断，建议删除“恶意”二字。

总体来说，《征求意见稿》具有极显著的开拓意识和时代特色，回应了全面依法治国以及数据信息保护的基本诉求。如果期望发挥应有的作用，应当进一步坚持开门立法、科学立法的基本原则，多方吸纳各种有益意见和建议，进而完善《征求意见稿》的基本内容，从而发挥其在个人信息保护领域的应有功能。

【注　释】

①《个人信息保护法》第54条规定，“个人信息处理者应当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64条规定，“履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患”。

②《网络数据安全管理条例（征求意见稿）》第53条规定“大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况等进行年度审计，并披露审计结果”。第58条规定，“国家建立数据安全审计制度。数据处理者应当委托数据安全审计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”。

③《审计法》第52条指出，“审计结果以及整改情况应当作为考核、任免、奖惩领导干部和制定政策、完善制度的重要参考；拒不整改或者整改时弄虚作假的，依法追究法律责任”。

④《中国注册会计师审计准则第1501号——对财务报表形成审计意见和出具审计报告》第11条规定，“注册会计师应当就财务报表是否在所有重大方面按照适用的财务报告编制基础的规定编制并实现公允反映形成审计意见”；第17条规定，“如果认为财务报表在所有重大方面按照适用的财务报告编制基础的规定编制并实现公允反映，注册会计师应当发表无保留意见”。

【主要参考文献】

陈炎.个人信息处理合规审计制度的意义、目标与功能[J].审计观察，2022(12)：12~17.

陈智敏.个人信息保护合规审计系统构建研究[J].审计观察，2022(12)：18~22.

贾丹，张誉馨，王姗.我国个人信息保护合规审计制度的路径探讨[J].工业信息安全，2022(4)：17~22

（责任编辑·校对：李小艳　黄艳晶）