个人信息处理合规审计制度的意义、目标与功能

文/陈 炎

个人信息处理合规审计是指个人信息处理合规审计机构及人员，对个人信息处理者的个人信息处理活动或个人信息处理制度体系是否遵循法律法规、国家标准等规范，加以监督、鉴证、评价、建议的过程。《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）在第一章第一条开宗明义地规定了立法目的及立法依据：为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。为了建立多层次的个人信息保护合规体系，《个人信息保护法》明确提出了个人信息处理者开展个人信息保护合规审计的要求。第五十四条规定，“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。”第六十四条规定，“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。”

承接《个人信息保护法》的立法宗旨，个人信息处理者的合规审计是个人信息处理者的义务之一，有利于实现个人信息保护之目的，即强化个人信息权益保护与规范个人信息处理活动，并能够为预测、决策、责任追究提供依据。

开展个人信息处理合规审计的意义

从制度安排上看，《个人信息保护法》第四章、第五章分别规定了个人在个人信息处理活动中的权利、个人信息处理者的义务。至此，个人信息保护至关重要的权利义务配置体系得以构建。诚如法谚有云：没有无权利的义务，也没有无义务的权利。《个人信息保护法》第五章个人信息处理者的义务体系中，第五十一条、第五十二条及第五十三分别规定了个人信息处理者的基本义务、指定个人信息保护负责人及设立专门机构等。值得重视的是，第五十四条把个人信息处理者的合规审计义务作为个人信息处理者义务体系中的一项特殊义务单独加以规定，非并入第五十一条所列具体措施项下，更加凸显了其重要性和意义。

（一）强化个人信息权益保护

从个人信息处理合规审计与个人信息权益的关系来看，开展个人信息处理合规审计有助于强化个人信息权益保护。个人信息权之性质乃私权利，其保护的法益乃私法益，其主体乃

自然人，若依客体物论则客体乃个人信息，若依客体行为论则客体为个人信息处理行为，个人信息权之内容乃对个人人格、身份等信息予以支配的权利义务关系。个人信息权不仅存在于个人与个人之间，而且存在于国家与个人之间；个人信息权存于国家与个人之间不影响其私权性，国家处理个人信息也必须依法进行，负有保护个人信息的义务。例如，《个人信息保护法》第三十五条规定，“国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。”此条规定不难理解：原则上，国家机关处理个人信息需履行告知义务以取得个人同意，而例外情形下才免除该告知义务。另外，值得阐明的是，国家与私人之间的法律关系为公法关系，而私人与私人之间的法律关系为私法关系，这是依据主体形式论所作的公私划分。在此基础上经过关系形式论修正后可得知，国家与私人之间纯粹建立在“意思自治”基础上的平等法律关系则为私法关系。至此，个人信息权的私权属性以及个人信息保护法的私法属性已不言自明。

阐明个人信息权益之性质、主体、客体及内容，有助于理解个人信息处理合规审计对该权益的强化保护意义。正如前文述及：个人信息处理行为乃个人信息权之客体，而对权利客体加以监督势必能够强化权益之保护，即开展个人信息处理合规审计监督势必强化个人信息权益保护。这是个人信息权益结构本身所包含的义理。

（二）规范个人信息处理活动

“受托责任是一种普遍的经济关系，也是一种普遍的、动态的社会关系。”依据审计学原理，受托责任是审计产生的客观基础。依循此理可推知，受托责任中的受托信息责任是个人信息处理合规审计的客观基础。基于受托责任关系，个人信息处理者对个人所提供的个人信息予以处理，而由于信息不对称等问题，个人为避免或减少由此带来的损失，对个人信息处理者之个人信息处理活动产生了监督需要，个人信息处理的合规审计正是满足该监督需要的核心方法之一。由此可得，个人信息处理活动需要相应的合规审计监督来加以规范。

个人信息处理合规审计通过鉴证个人信息处理活动与个人信息处理法律法规、国家标准等规范的一致程度，能够切实规范个人信息处理活动，查证、纠正个人信息处理中的不合规行为，避免带来个人信息上的财产、精神损害后果。

（三）为预测、决策、责任追究提供依据

个人是个人信息处理合规审计报告潜在使用者之一。个人选择是否同意将个人信息交付个人信息处理者加以处理时，产生了对个人信息处理者所声明的个人信息处理政策或指引，乃至个人信息处理者个人信息处理合规性的信任风险，基于个人信息处理是否合规的怀疑，信任风险产生了个人信息处理合规审计的需求。

个人信息处理合规审计如何优化预测、决策？个人信息处理合规审计优化相关者的预测、决策的主要方面依赖于审计报告的制作、披露与应用，而次要方面包括但不限于审计过程中的沟通等。个人信息处理合规审计报告应当包括但不限于以下要素：标题、接收者、审计意见、形成审计意见的基础、个人信息处理者的责任、个人信息处理合规审计机构及人员的责任、其他需要报告的事项、签名盖章及报告日期。对预测、决策尤为重要的当属个人信

息处理合规审计报告中审计意见与形成审计意见的基础：当审计意见呈现消极表述时，审计报告接收者依据形成审计意见的基础找寻消极审计意见的原因，从而判断、分析个人信息处理合规制度体系所存在的问题，以及制定解决个人信息处理合规问题的方案。

一旦个人信息处理违反法律法规、国家标准、行业准则等，个人信息处理者则应承担相应的法律法规责任。在个人信息处理者内部，一旦个人信息处理主要负责人或分管负责人未能履行相应的合规控制义务，而产生个人信息处理不合规风险或损失，那么个人信息处理主要负责人或分管负责人应当承担相应的法律法规责任。个人信息处理合规审计报告能够作为责任追究的依据，从而提高履行个人信息保护职责的部门，以及个人信息处理者的责任追究准确性、时效性、公正性，从而避免追责的主观恣意。

当然，不仅个人信息处理合规审计报告能够为责任追究提供助力，而且审计工作底稿能够佐证审计报告的真实性、独立性、专业性。然而，从现实角度来看，由于审计工作底稿具有保密性且归属于审计机构及人员，往往不会像审计报告那样进行公开披露。一旦个人信息处理合规审计机构或人员因审计工作而面临法律法规责任追究时，完备的审计工作底稿能够有利于审计方规避法律法规风险或者有助于理清审计方的责任。

个人信息处理合规审计的目标

美国会计学会审计概念委员会在 1973 年发布的《审计基本概念说明》中对审计所下的定义为，审计是为了鉴证有关经济行为和经济事项的声明与既定标准之间的一致程度，而客观地收集和评定有关证据，并将其结果传达给有关使用者的系统过程。在此定义中，可以看到审计的直接目标是对被鉴证和评价事项发表意见——确保按照既定标准实施经济行为和汇报经济事项，而其根本目标在于保证经济活动的真实性、合法性和效益性。

因此，个人信息处理合规审计既有对传统审计目标的承续，又在此基础上有所发展。概括地说，个人信息处理合规审计的直接目标在于确保按照法定原则和方式处理个人信息，其根本目标在于确保个人信息的真实性、准确性和完整性。

（一）确保个人信息的真实性、准确性和完整性

个人信息处理合规审计的根本目标是确保个人信息的真实性、准确性和完整性。换言之，个人信息处理合规审计的根本目标是保证个人信息的真实与质量。个人信息处理合规审计的根本目标可由其根本性质和根本意义佐证。

从根本性质上讲，审计作为一种信息鉴证服务，意为信息的可信度提供保证。可以看到，个人信息处理合规审计的根本目标与其审计本身的根本性质高度契合——二者都是以保证信息的真实可靠为落脚点，从而证明其根本目标是归于个人信息的真实、准确和完整。

从权益保护上看，如果被处理的个人信息是错误、模糊或缺漏的，就很容易由此对信息主体的个人权益造成负面影响或危害。个人信息可以重建自然人的某种状态或某种特性并产生相应的法律效果，故而个人信息的真实、准确和完整至关重要。个人信息是个人信息保护的基本单元，保证个人信息的真实与质量，必然有助于保护个人信息权益，这也符合《个人信息保护法》中以质量原则为代表的诸原则。

从上述个人信息合规审计意义上讲，个人信息处理合规审计的根本意义在于保护个人信息权益。由此可以看到，个人信息处理合规审计的根本目标与其根本意义高度契合——个人信息的真实、准确与完整有利于保护个人信息权益。

（二）确保按照法定原则和方式处理个人信息

个人信息处理合规审计的直接目标是确保个人信息处理者按照法定原则和方式处理个人信息。依据《个人信息保护法》第五条、第六条、第七条、第八条、第九条，处理个人信息需要遵循的法定原则包括：合法、正当、必要与诚信原则；目的限制原则；公开透明原则；质量原则；责任原则与安全原则。依据《个人信息保护法》第四条第二款，个人信息的处理方式包括:个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

确保个人信息处理者按照法定原则和方式处理个人信息的有效方法即个人信息处理的合规审计，这一审计监督手段诞生于两权分离所带来的委托风险：个人信息处理权与个人信息所有权的分离，即创造了第三方施加审计监督的审计需要——以合规审计手段对个人信息处理法定原则和方式的遵守情况予以监督。从现实的角度分析，个人信息处理者往往占据信息优势地位，其对个人信息有着现实控制力，个人信息主体往往处于信息弱势地位，为了制衡与削弱个人信息处理者在个人信息占有与控制上的“相对特权”。作为第三方的个人信息处理合规审计机构和人员适时介入与前两者建立不同的权利义务关系，一方面使得个人信息处理者与个人信息主体处于相对信息均势地位，另一方面凸显了个人信息处理合规审计机构和人员不可或缺的独立性。

从审查形式上看，个人信息处理的合规审计即审计机构及审计人员以其专业判断、专业经验、专业知识，确定个人信息处理是否遵循法定原则：确定个人信息处理是否符合个人信息的法定方式。如此审计的目的，在于控制不合规风险，确保个人信息处理的法定原则与法定方式得以遵循。

个人信息处理合规审计的功能

个人信息处理合规审计制度的内在实质体现于监督与鉴证功能，其外在形式体现于评价与建议功能。从现实角度来看，一方面，个人信息处理者基于增强其个人信息处理合规性的可信度的鉴证需要，而履行个人信息处理合规审计义务。另一方面，个人信息处理合规审计有助于个人信息主体及履行个人信息保护职责的部门有效监督个人信息处理者。至此，监督与鉴证功能相辅相成，成为个人信息处理合规审计制度的“支柱性”功能。进一步分析，鉴证成果的表达自然生成评价功能，监督成果的表达自然生成建议功能，因而评价与建议功能体现为监督与鉴证功能的外化表达形式。

（一）监督与鉴证功能

个人信息处理合规审计的实质功能是监督个人信息处理并且鉴证此二者的一致程度：个人信息处理行为与既定法律法规、标准、准则等规范的一致程度。性质决定功能，审计性质决定审计功能：监督与鉴证功能。依据审计学原理可知，自审计受托责任确立之始，所有权人对经营权人的监督、鉴证之意就“蕴藏”于审计之中。上述原理同样适用于个人信息处理合规审计。个人信息处理权与所有权相分离，所有权人为检验处理权人所传递的个人信息处理情况真实性，自然需要专业人员对个人信

息处理情况的真实性、准确性、完整性予以监督、鉴证。

个人信息处理合规审计的实质功能之一即监督功能。个人信息处理合规审计的监督功能体现于审计机构及审计人员对个人信息处理的真实情况予以动态监察，以确保个人信息处理的合规性。个人信息合规审计的监督功能主要着眼于监督个人信息处理的过程。监督功能在于检验、确保个人信息处理过程的可信度。通过个人信息处理合规审计，明确个人信息处理的真实状况，清晰划分合规与不合规的个人信息处理活动，从而肯定合规的个人信息处理活动，营造合规的个人信息处理软环境。

个人信息处理合规审计的实质功能之二即鉴证功能。鉴证作为一种保证，鉴证服务是保证服务的重要组成部分。个人信息处理合规审计的鉴证功能体现于：审计机构及审计人员对个人信息处理的事实情况予以静态验证，以增强个人信息处理合规性的可信度。审计鉴证功能主要着眼于鉴证个人信息处理的结果。鉴证功能在于增强个人信息处理合规性的可信度。例如，在财务审计中，“已审计的财务报表由于审计报告的鉴证作用会增强其可信性，”从而使得委托人或公众对已审计的报告文件更加信赖。

（二）评价与建议功能

个人信息处理合规审计的形式功能是评价个人信息处理者的个人信息处理现状并提出建议。个人信息处理合规审计的形式功能之一即评价功能。个人信息处理合规审计的评价功能体现于：审计机构及审计人员依据既定的个人信息处理合规审计标准，对个人信息处理制度及个人信息处理现状与其符合程度予以评定，从而准确清晰地认知现有个人信息处理制度的不足，为其个人信息处理制度的完善提供基础支撑。评价功能主要着眼于测评现有的个人信息处理制度及个人信息处理现状。根据审计理论，以财务报表为例，审计意见的内容需要呈现财务报表的两个方面：一是财务报表是否按照使用的会计准则和相关会计制度的规定编制；二是财务报表是否在所有重大方面公允反映了被审计单位的财务状况、经营成果和现金流量。因此，个人信息处理合规审计的审计意见亦当呈现个人信息处理的两个方面：一是个人信息处理是否按照法律法规和相关的个人信息处理制度开展；二是个人信息处理是否在所有重大方面保护了个人信息所有人的个人信息权益。由于个人信息合规审计意见必须呈现对个人信息处理制度及现状的分析、判断，个人信息处理合规审计报告中的审计意见正是审计评价功能得以发挥的直接成果展现。在个人信息处理合规审计报告中所呈现的审计证据体现评价的客观性，而审计报告中所呈现的专业判断体现评价的主观性，故而评价功能兼有主观性与客观性，此二者构成评价功能的两大核心特性。

个人信息处理合规审计的形式功能之二即建议功能。个人信息处理合规审计的建议功能即“建言献策”功能。个人信息处理合规审计的建议功能体现于：审计机构及审计人员依据个人信息处理法律法规和相关制度，针对个人信息处理合规制度的不足，以构建完善的个人信息处理制度为目的而提出改进方案。个人信息处理合规审计的建议功能主要着眼于完善现有的个人信息处理制度。有价值的建议注重合理性和实践性。例如，在财务审计实务中，审计师一般会向公司管理层与治理层出具管理建议书，其内容往往涉及审计师所发现的企

业中与财务报表相关的内控制度的一些缺陷并提出建议。

个人信息保护的核心在于对个人信息处理活动的规范，个人信息处理活动的规范有赖于个人信息处理者建立健全完善的个人信息处理合规制度体系，而监督、鉴证与评价个人信息处理合规制度体系以及对个人信息处理合规制度体系提出建议，都离不开个人信息处理合规审计制度功能的发挥。确保个人信息的真实性、准确性和完整性，并且确保按照法定原则和方式处理个人信息，是个人信息处理合规审计的目标。强化个人信息权益保护、规范个人信息处理活动并为预测、决策、责任追究提供依据，是个人信息处理合规审计的意义所在。

（责任编辑：曹伟）

作者单位系西北政法大学法治学院

个人信息处理合规有关规范作重点列举

规范种类	规范名称
法律	《个人信息保护法》《审计法》《数据安全法》《民法典》《未成年人保护法》《电子商务法》《消费者权益保护法》《网络安全法》
行政法规	《关键信息基础设施安全保护条例》
部门规章	《儿童个人信息网络保护规定》
规范性文件	《常见类型移动互联网应用程序必要个人信息范围规定》 《App 违法违规收集使用个人信息行为认定方法》 《关于开展 APP 侵害用户权益专项整治工作的通知》 《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》 《关于开展信息通信服务感知提升行动的通知》
司法解释	《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》 《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》 《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》
国家标准	《信息安全技术个人信息安全规范》(GB/T35273-2020) 《信息安全技术个人信息安全影响评估指南》（GB/T 39335-2020）

说明：个人信息保护合规审计的审计依据为我国个人信息保护相关现行有效的法律、行政法规。有关部门已发布的法律法规征求意见稿和国家标准亦可作为参考。建议重点关注的审计依据：医疗、金融、汽车等不同行业主管监管部门亦会制定相关行业监管规则，企业开展合规审计过程中，应对行业监管规则中要求的个人信息保护义务进行核实和遵从。（来源：《关于推进个人信息保护合规审计的若干建议》）