个人信息保护合规审计的适用与效力

审计义务的触发与报告的证据地位

赵跃

（安徽国运律师事务所，安徽 合肥 230000）

摘要：个人信息保护法确立了合规审计义务，配套办法进一步规定了审计的频次、内容与程序。审计由此成为个人信息处理者的一项法定义务，也成为监管与司法认定处理者是否尽责的重要依据。实务中的问题集中于三点。其一，审计义务的触发条件如何认定，处理规模以何为准，集团内部如何分摊。其二，审计内容的边界何在，是否涵盖合法性基础、告知同意、最小必要、跨境提供与安全保障的全部环节。其三，审计报告在民事侵权诉讼中具有何种效力，能否作为处理者已尽注意义务的证据。本文认为，审计义务是行为义务而非结果义务。处理者只要按照规定的频次、内容与程序开展审计，即已履行义务；审计未能发现违法事项的，不当然构成义务违反，但审计过程存在重大瑕疵的除外。审计内容的构造，应当以风险为导向。处理敏感个人信息、向境外提供个人信息、利用个人信息进行自动化决策的，应当作为审计重点；一般个人信息的常规处理，可以采抽样方式。审计报告在诉讼中的效力，应当定位为处理者已尽组织措施义务的初步证据。报告真实、完整、由具备独立性的机构出具的，可以推定处理者已尽相应义务；相对人能够证明报告存在虚假记载或者重大遗漏的，推定被推翻。

关键词：个人信息保护；合规审计；注意义务；审计报告；证据效力

中图分类号：D922.16　**文献标识码：**A　**文稿编号：**WJLT(2023)03-0050-13

Application and Effect of Personal Information Protection Compliance Audits

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: The Personal Information Protection Law establishes a duty of compliance auditing, and the supporting measures specify its frequency, content and procedure. Auditing has thus become a statutory obligation and an important basis for regulators and courts to assess whether a processor has acted diligently. Three issues dominate practice: how the trigger threshold is determined and how a group allocates the obligation; how far the audit content extends, covering legal basis, notice and consent, data minimization, cross-border provision and security safeguards; and what weight an audit report carries in civil litigation as evidence of due care. This article argues that the duty is one of conduct rather than result. A processor that audits at the required frequency, with the required content and procedure, has performed the duty; failure to detect a violation does not by itself establish breach, unless the audit process is materially defective. The content should be risk-oriented: sensitive information, cross-border provision and automated decision-making deserve priority, while routine processing may be sampled. In litigation, an audit report should serve as prima facie evidence of organizational safeguards. A truthful, complete report issued by an independent body raises a presumption of due care, rebuttable by proof of misrepresentation or material omission.

Key words: personal information protection; compliance audit; duty of care; audit report; evidentiary weight

说明：（本文为作者个人研究观点，不代表所在单位意见）

作者简介：赵跃，安徽国运律师事务所执业律师，主要研究个人信息处理者的义务构造与举证责任分配。

一、问题的提出

个人信息保护法第五十四条确立了合规审计义务。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审计。这一义务的设立，标志着个人信息保护从外部监管走向内部治理。

配套的个人信息保护合规审计管理办法，进一步规定了审计的频次、主体、内容与程序。审计由内部机构自行开展或者委托专业机构开展，审计报告应当留存备查，并在监管部门要求时报送。

制度的建立，使处理者面临新的合规成本。大型互联网平台每年投入大量资源开展审计，中小企业则普遍反映负担较重。审计的频次、范围与深度，直接影响到企业的经营成本。

与此同时，审计报告在民事侵权诉讼中的地位，成为一个新的争点。处理者被诉侵害个人信息权益时，往往提交审计报告，主张已尽注意义务；原告则质疑报告的独立性与真实性。法院对此的态度不一。

争议的另一面，是审计与影响评估的关系。两者都是风险治理工具，都要求处理者自查，但功能不同。审计侧重合规性，评估侧重风险性。实务中常被混同，导致重复劳动或者相互推诿。

还有一个问题，是审计义务的触发条件。办法以处理个人信息的数量为标准，设定了不同的审计频次。数量如何计算，是以峰值计还是以平均计，是以单个法人计还是以集团合并计，均需明确。

上述问题的共同点，是审计制度的定位尚未厘清。若将审计视为监管的延伸，则其内容与程序应当由监管机关严格规定；若将其视为处理者的自我治理，则应当给予其较大的自主空间。定位不同，规则的设计亦异。

本文主张，审计是处理者履行组织措施义务的一种方式，兼具自我治理与外部监督双重功能。其规范构造，应当在保障监管有效性的同时，尊重处理者的自主性。

在这一基础上，本文讨论四个层次的问题。第一，审计义务的性质与触发。第二，审计主体与独立性。第三，审计内容的构造。第四，审计报告的效力，包括对监管、对诉讼的效力。

讨论的方法，是规范分析与案例研究相结合。一方面，梳理现行规范，厘清审计义务的构成；另一方面，考察裁判文书，发现审计报告在诉讼中的实际作用，提出可操作的证据规则。

选题的现实意义在于，个人信息保护已从立法阶段进入实施阶段。审计作为实施的重要抓手，其规则的明确与否，直接关系到法律落地的效果。规则不清，则企业无所适从，监管难以统一。

需要说明的是，本文所称审计，指个人信息保护合规审计，不包括财务审计、内部控制审计。三者虽在方法上有相通之处，但对象与目的不同，规则不能简单移植。

从比较法上看，合规审计并非我国独有。欧盟通用数据保护条例设有数据保护审计的制度雏形，要求控制者采取适当措施确保合规，并可指定数据保护官监督实施。日本个人信息保护法要求经营者定期自查并向监管报告。

我国的特色，在于将审计上升为法定义务，并以处理规模设定频次。这一设计，体现了抓大放小的监管思路。但规模的划分标准较为单一，未充分考量数据的敏感程度与处理方式的复杂程度。

改进的方向，是建立多维度的风险分级。除数量外，还应当考虑数据的敏感程度、处理的自动化程度、共享的广泛程度、是否向境外提供。多维分级，可以使监管资源更精准地投向高风险领域。

二、审计义务的性质与触发

审计义务的性质，有行为义务说与结果义务说之争。行为义务说认为，处理者只要按照规定的程序开展审计，即已履行义务，审计是否发现问题不影响义务的履行。结果义务说认为，处理者应当通过审计发现并纠正违法事项，未发现的构成义务违反。

本文采行为义务说。理由是，审计是一种程序性的自查活动，其效果取决于审计方法、样本选择与审计人员的判断，具有不确定性。若以结果为标准，将使处理者对无法预见的事项承担责任，过于严苛。

行为义务说并不意味着处理者可以敷衍了事。审计的频次、内容、程序必须符合规定，审计人员必须具备相应的专业能力，审计报告必须真实完整。欠缺其中任何一项，均构成义务违反。

审计义务的触发，以处理个人信息的数量为主要标准。办法规定，处理个人信息达到一定数量的，每两年至少开展一次审计；其他处理者每三年至少开展一次。数量的门槛，体现了风险分级的思路。

数量的计算，应当以审计周期内的平均处理量为准，而非以某一时点的峰值为准。理由是，峰值可能因促销、活动等临时因素而畸高，不能反映常态的处理规模。但峰值持续超过门槛三个月以上的，应当以峰值计。

集团公司的数量计算，是实践的难点。各子公司分别处理个人信息的，应当分别计算；集团统一处理、共享数据的，应当合并计算。判断的标准，是处理的实质主体，而非形式上的合同主体。

委托处理的情形，数量应当由委托方计算。受托方按照委托方的指示处理，不决定处理目的与方式，其处理量已包含在委托方的处理量中。受托方另行超出委托范围处理的，应当自行计算。

共同处理的情形，数量应当由共同处理者共同计算。共同处理者共同决定处理目的与方式，对外承担连带责任，故应当共同履行审计义务。可以联合开展审计，也可以各自开展，但审计范围应当覆盖共同处理活动。

国家机关处理个人信息的，同样应当履行审计义务。国家机关的处理行为具有公权力属性，但其个人信息处理活动仍受个人信息保护法约束。审计可以由内部机构开展，也可

以委托专业机构开展。

除定期审计外，还有特定情形下的专项审计。监管部门发现处理活动存在较大风险或者发生安全事件的，可以要求处理者委托专业机构开展审计。此种审计具有强制性，处理者不得拒绝。

专项审计的费用，由处理者承担。审计的范围由监管部门确定，处理者不得擅自缩小。审计报告应当直接报送监管部门，处理者不得隐瞒或者篡改。违反的，可以依照个人信息保护法处罚。

审计义务的豁免，法律未作规定。有观点主张，小微企业对个人信息的处理量小、风险低，可以豁免。本文不赞成。豁免将导致大量处理者脱离监管，且小微企业的安全能力往往更弱，更需审计。

替代的方案，是简化小微企业的审计程序。例如，允许其采用简式报告、允许其联合开展审计、允许其以自查表替代全面审计。简化的前提，是处理量小、未处理敏感信息、未发生安全事件。

内部审计与外部审计的组合，是较为务实的选择。日常的合规自查由内部机构承担，年度的全面审计委托外部机构。前者成本低、频率高，后者专业性强、公信力高。

外部审计的范围，应当覆盖个人信息处理的全流程。仅审计线上业务而不审计线下渠道，仅审计总部而不审计分支机构，都将导致审计结论失真。委托合同应当明确审计范围，避免机构避重就轻。

审计费用由处理者承担，但不能影响机构的判断。合同中不得约定审计结论必须达到某一标准，不得约定机构对发现的问题不予披露。此类条款违背审计的本质，应当认定无效。

三、审计主体与独立性

审计主体有两类：处理者的内部机构与外部专业机构。内部机构熟悉业务，成本较低，但独立性不足；外部机构专业性强，独立性好，但成本较高。办法允许处理者自行选择。

内部审计的独立性，依赖于治理结构。审计部门应当直接向董事会或者个人信息保护负责人报告，不得由被审计的业务部门领导。审计人员不得参与被审计的业务活动，以保证客观。

实践中，许多企业的内部审计由法务部门兼办。法务部门既负责合规咨询，又负责审计，角色冲突明显。本文主张，内部审计应当由独立的合规部门或者审计委员会承担，法务部门可以提供支持，但不得主导。

外部审计的独立性，依赖于机构与人员的独立。审计机构不得与被审计的处理者存在可能影响独立性的利益关系，包括股权投资、业务往来、人员兼职。存在此类关系的，应

当回避。

外部审计机构的资质，目前尚无统一的准入要求。办法仅要求具备相应的专业能力。实践中，会计师事务所、律师事务所、信息安全测评机构均可开展。资质的模糊，导致服务质量参差不齐。

本文主张，应当建立审计机构的备案制度。备案的内容包括机构的基本情况、专业人员、业绩记录与不良记录。备案不设行政许可，但可以作为处理者选择机构的参考，也可以作为监管抽查的依据。

审计人员的专业能力，应当包括法律与技术两个方面。个人信息保护审计既要审查处理的合法性基础、告知同意，也要审查加密、去标识化、访问控制等技术措施。单一背景的人员难以胜任。

审计的委托关系，性质上是服务合同。处理者委托机构开展审计，机构出具报告，处理者支付费用。合同的标的，是审计服务而非审计结论。机构不保证审计能够发现全部违法事项。

但机构负有勤勉义务。未尽勤勉义务导致报告存在虚假记载或者重大遗漏的，应当承担违约责任；造成处理者损失的，还应当承担赔偿责任。故意出具虚假报告的，可能构成犯罪。

处理者与机构的责任分担，应当区分。处理者提供虚假材料的，责任在处理者；机构未尽审查义务的，责任在机构；双方均有过错的，按过错程度分担。对外而言，处理者仍应承担个人信息保护法上的责任。

审计的保密义务，是独立性的延伸。审计机构和人员对审计过程中知悉的个人信息、商业秘密，负有保密义务。违反的，应当承担侵权责任；情节严重的，可以追究刑事责任。

审计工作底稿的保存，办法要求保存一定期限。底稿是审计过程的记录，也是事后核查的依据。保存期限届满前，处理者不得销毁。监管机关调取底稿的，处理者应当提供。

审计方法的选择，直接影响审计结论的可靠性。常用的方法包括文档审查、人员访谈、系统测试、数据抽样。单一方法难以覆盖全部风险，应当组合使用。文档审查发现制度，系统测试验证落实，两者缺一不可。

抽样审计的局限，应当予以说明。抽样只能反映样本的情况，不能保证总体无问题。报告应当载明抽样的方法、样本量与置信水平，使用者据此判断结论的可靠程度。未说明的，报告的证明力降低。

四、审计内容的构造

审计内容，指审计应当覆盖的事项。办法列举了若干方面，包括个人信息的处理规则、告知同意、共同处理与委托处理、跨境提供、自动化决策、安全保障措施、影响评

估、事件应对等。

列举的方式，优点是明确，缺点是难以穷尽。个人信息处理的技术与场景不断变化，新的风险层出不穷。审计内容若过于僵化，将难以应对新型处理活动。

本文主张，审计内容应当以风险为导向，采列举加兜底的方式。列举规定必审事项，兜底要求审计机构根据处理活动的风险特点，自行确定重点。这样既保证了底线，又保留了弹性。

第一类必审事项，是处理的合法性基础。处理者应当说明其处理个人信息所依据的法律基础，包括同意、履行合同所必需、履行法定职责或者义务、应对突发公共卫生事件、公共利益等。

审计时应当核查，处理者是否将不同法律基础混用，是否在缺乏基础的情形下处理信息，是否将同意作为唯一的依据而忽视了其他基础。实践中，大量应用以同意为名，行强制收集之实。

第二类必审事项，是告知同意的有效性。告知应当真实、准确、完整，以显著方式、清晰易懂的语言作出。同意应当自愿、明确，不得以捆绑、默认勾选等方式取得。

审计时应当核查，告知的内容与实际处理是否一致，同意的范围是否覆盖实际处理，撤回同意的机制是否便捷，重新取得同意的情形是否履行。实践中，告知文本与实际行为脱节的现象普遍。

第三类必审事项，是最小必要原则的落实。处理个人信息应当限于实现处理目的的最小范围，不得过度收集。审计时应当核查，收集的字段是否与业务功能相关，保存期限是否必要，共享范围是否必要。

最小必要的判断，具有场景依赖性。同一字段在不同场景下的必要性不同。审计机构应当结合具体业务，说明判断的理由，不能简单以行业惯例代替具体分析。

第四类必审事项，是敏感个人信息的处理。处理敏感个人信息，应当具有特定的目的和充分的必要性，取得单独同意，履行告知义务，开展影响评估，采取严格保护措施。

审计时应当核查，敏感信息的识别是否准确，单独同意是否取得，影响评估是否开展，保护措施是否到位。生物识别、医疗健康、金融账户、行踪轨迹、不满十四周岁未成年人的信息，均属敏感。

第五类必审事项，是跨境提供。向境外提供个人信息，应当具备法定条件，包括通过安全评估、经专业机构认证、订立标准合同、法律规定的其他情形。

审计时应当核查，跨境提供的路径是否合法，数量与范围是否申报，境外接收方的保护水平是否达到要求，个人的单独同意是否取得。通过境外平台处理数据的，尤其需要关注。

第六类必审事项，是自动化决策。利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

审计时应当核查，是否向个人提供了不针对其个人特征的选项，是否提供了便捷的拒绝方式，算法模型是否经过评估，是否存在歧视性结果。个性化推荐的关闭入口，是常见的审查点。

第七类必审事项，是安全保障措施。处理者应当采取加密、去标识化等安全技术措施，制定内部管理制度与操作规程，确定操作权限，定期开展安全培训，制定应急预案。

审计时应当核查，技术措施是否与风险程度相适应，权限管理是否落实最小授权，日志是否完整保存，应急预案是否演练。等级保护测评的结论，可以作为审计的参考，但不能替代审计。

第八类必审事项，是个人信息安全事件的应对。处理者应当制定应急预案，事件发生时立即采取措施补救，并通知履行个人信息保护职责的部门和个人。审计时应当核查预案的完备性与演练的记录。

第九类必审事项，是个人权利的响应机制。个人有权查阅、复制、更正、删除其个人信息，有权撤回同意、注销账户。处理者应当建立便捷的申请渠道，在合理期限内答复。审计时应当核查响应时限与答复质量。

审计发现的常见问题是，响应渠道形同虚设。客服电话无人接听、在线申请长期不处理、注销账户设置重重障碍。此类问题看似细节，实则直接影响个人的权利实现，应当作为审计的重点。

审计的对象、内容与频次要求，可参见个人信息保护合规审计：谁要审、审什么、什么时候必须审一文对制度框架的梳理，本文不再重复其基本问题，只就审计的效力与诉讼衔接展开。

五、审计报告的效力

审计报告是审计的成果，记载审计的范围、方法、发现的问题与结论。报告的效力，可以分为对内效力、对监管的效力与对诉讼的效力三个层面。

对内效力，指报告对处理者的约束。报告发现问题的，处理者应当整改。整改的情况应当记录，并在下一次审计时核查。未整改的，构成对审计义务的违反，可能被认定为未尽组织措施义务。

报告对内还具有治理功能。董事会、监事会通过报告了解公司的合规状况，据此调整资源配置。个人信息保护负责人依报告履行职责，向监管机关报告工作。

对监管的效力，指报告在监管执法中的作用。办法要求处理者留存报告，监管机关可以调取。报告显示存在违法情形的，监管机关可以据此启动调查。报告如实披露的，可以作为从轻处罚的情节。

报告是否具有自认效力，存在争议。有观点认为，报告如实披露的违法事项，构成处理者的自认，监管机关可以直接认定；有观点认为，报告是自查性质，披露不等于确认，

仍需调查核实。

本文主张，报告不具有自认效力，但具有线索效力。报告披露的事项，监管机关应当核查；核查属实的，依法处理。报告未披露而监管机关另行发现的事项，处理者不得以已审计为由抗辩。

这一区分的目的，是鼓励如实披露。若披露即等于自认，处理者将倾向于隐瞒问题，审计的自我治理功能将落空。反之，若披露完全没有法律意义，处理者也缺乏披露的动力。

对诉讼的效力，是最具实践意义的问题。处理者被诉侵害个人信息权益时，提交审计报告，主张已尽注意义务。报告能否作为免责或者减责的依据，取决于报告的真实性、完整性与独立性。

本文主张，报告可以作为处理者已尽组织措施义务的初步证据。所谓初步证据，指报告真实、完整、由具备独立性的机构出具的，可以推定处理者已尽相应义务；原告能够证明报告存在虚假记载或者重大遗漏的，推定被推翻。

初步证据的定位，符合举证责任的分配。个人信息侵权案件中，原告往往难以证明处理者的过错，举证责任适当向处理者转移，符合危险领域理论。报告是处理者证明自己无过错的重要方式。

但报告不能证明具体处理行为的合法性。报告是抽样审计，未覆盖全部处理活动。报告未发现问题，不等于具体行为合法。原告就具体行为举证的，处理者仍应就该行为的具体合法性承担举证责任。

报告的证明力，取决于三个因素。其一，独立性。内部报告的可信度低于外部报告，关联机构出具的报告可信度更低。其二，完整性。报告应当披露发现的问题，仅披露结论而无过程的，证明力较弱。

其三，时效性。报告针对的是特定期间的处理活动，与涉案行为的时间不一致的，证明力减弱。涉案行为发生在报告期间之外的，报告仅具有参考价值。

实践中，处理者提交的报告往往只有结论页，没有审计过程与问题清单。此种报告的证明力应当大打折扣。法院可以要求处理者提交完整报告与工作底稿，拒不提交的，作出不利推定。

对于审计中发现的系统性风险，处理者应当立即采取措施，不能等到整改期限届满。例如，发现数据库未加密、权限管理失控的，应当立即加固，防止损害扩大。延迟采取措施导致损害扩大的，责任加重。

监管机关在处理未审计案件时，应当区分情形。首次违反、情节轻微、及时改正的，可以不予处罚；屡次违反、情节严重、造成损害的，应当从重处罚。区分的标准，应当在处罚裁量基准中明确。

民事案件中，未审计的证明作用有限，不能仅凭未审计认定侵权成立。侵权责任仍需

具备加害行为、损害、因果关系与过错四要件。未审计只是过错认定的一个因素，不能替代其他要件。

审计底稿的缺失，是常见的瑕疵。底稿记录了审计的过程与依据，是判断审计是否尽责的关键。处理者仅保存报告而无底稿的，难以证明审计过程真实，义务履行的主张可能不被采信。

审计人员的资质瑕疵，亦影响审计的效力。审计由不具备专业知识的人员实施，即使程序完整，结论也难以采信。处理者委托外部机构的，应当审查机构与人员的资质，尽到选择上的注意义务。

六、未审计与审计瑕疵的后果

未履行审计义务的，处理者应当承担何种责任，法律未作明确规定。个人信息保护法对违法处理个人信息设有行政处罚，但未审计本身并非违法处理行为，能否处罚，需要解释。

本文主张，未审计可以独立构成行政处罚的事由。理由是，审计义务是法定义务，违反法定义务应当承担相应责任。处罚的种类可以是责令改正、警告、通报批评；拒不改正的，可以罚款。

处罚的轻重，应当与处理规模、风险程度、主观过错相适应。大规模处理个人信息而未审计的，处罚应当从重；小微企业初次违反并及时改正的，可以从轻或者免予处罚。

未审计与民事责任的关联，体现在过错的认定上。未审计本身不构成侵权，但可以作为认定处理者未尽组织措施义务的依据。若损害的发生与未审计存在因果关系，处理者应当承担相应责任。

因果关系的认定，应当具体分析。未审计导致安全隐患未被发现，隐患进而导致信息泄露的，因果关系成立；未审计但泄露源于外部攻击且处理者已采取合理措施的，因果关系不成立。

审计瑕疵，指审计的频次、内容、程序不符合规定。瑕疵的后果，视瑕疵的严重程度而定。轻微瑕疵，如报告格式不规范，不影响审计义务的履行；重大瑕疵，如未覆盖必审事项、审计人员不具备能力，构成义务违反。

审计造假，是最严重的瑕疵。处理者与审计机构串通，出具虚假报告的，不仅构成义务违反，还可能构成提供虚假证明文件罪。监管机关应当从重处罚，并将线索移送司法机关。

审计报告失实，但处理者不知情的，责任在审计机构。处理者可以向机构追偿，但对外仍应承担个人信息保护法上的责任。这一安排，体现了对外责任与对内追偿的分离。

整改义务的履行，是审计制度的关键环节。审计发现问题而不整改，审计的意义将大打折扣。本文主张，处理者应当在报告出具后一定期限内完成整改，并将整改情况报监管

部门备案。

未整改的后果，应当重于未审计。未审计是程序性违反，未整改是实质性违反。监管机关可以责令限期整改，逾期不整改的，可以责令暂停处理活动，直至整改完成。

监管部门之间的协作，亦需加强。网信、工信、公安、市场监管等部门均负有个人信息保护职责，审计报告的信息应当共享，避免重复检查与重复报送。统一的报送平台，可以提高监管效率。

跨区域处理的审计，涉及管辖的协调。处理者在多地设有分支机构的，可以由总部所在地的监管部门统一组织审计，分支机构所在地配合。避免各地分别要求审计，增加企业负担。

跨境处理的审计，还涉及国际协作。境外接收方所在国的法律环境不同，审计机构难以实地核查。可以采信境外机构出具的审计报告，或者通过双边协议开展联合审计。

七、审计与监管、诉讼的衔接

审计与监管的衔接，体现在信息共享与执法协作。监管机关可以调取审计报告，也可以要求处理者说明审计情况。审计发现的重大风险，处理者应当主动报告。

主动报告的制度激励，需要法律的明确。本文主张，处理者主动报告并及时采取补救措施的，可以减轻或者免予行政处罚。这一规则，与食品安全、药品监管中的主动报告制度相通。

审计与影响评估的衔接，需要厘清两者的分工。影响评估针对特定处理活动，事前开展，重在评估风险；审计针对整体合规状况，定期开展，重在检查落实。审计可以采信评估的结论，但不能以评估替代审计。

审计与认证的衔接，亦需明确。个人信息保护认证是自愿性的第三方评价，审计是强制性的自查。两者可以相互采信，但认证不能免除审计义务。通过认证的，审计的频次可以适当降低。

审计与诉讼的衔接，除证据效力外，还包括诉讼中的专家辅助。当事人可以申请审计人员出庭，就审计方法、样本选择、结论依据作出说明。法院认为有必要的，可以委托另行审计。

另行审计的启动，应当慎重。诉讼中的审计耗时较长，费用较高，可能拖延审理。只有当报告存在明显瑕疵，且争议事项依赖于审计结论时，才宜启动。启动的决定权在法院，当事人可以申请。

对于群体性诉讼，审计报告的作用更为突出。个人信息泄露涉及众多用户，单个原告难以证明处理者的过错。报告成为判断处理者是否尽责的重要依据。法院可以要求处理者提交报告，并组织质证。

公益诉讼中，审计报告同样具有意义。检察机关或者消费者组织提起公益诉讼时，可

以申请调取处理者的审计报告，也可以委托专业机构出具评估意见。报告的公开，有助于形成社会监督。

对于审计报告的质证，法院可以采集中质证的方式。同一处理者涉及多起诉讼的，报告的核心内容相同，可以一次质证，多次使用。这样既节省资源，也避免裁判矛盾。

当事人对报告有异议的，可以申请审计人员出庭。审计人员无正当理由拒不出庭的，报告的证明力降低。出庭的费用，由申请方预交，最终由败诉方承担。

法院在认定处理者是否尽责时，还应当考虑行业惯例与技术条件。同一时期、同一行业的普遍做法，可以作为判断的参考。技术条件限制导致无法采取某项措施的，不构成过错。

制度的完善，还需要配套的激励机制。对审计质量高、整改到位的企业，可以在监管检查中减少频次，在政府采购、评优评先中给予倾斜。正向激励与负向惩戒并用，效果更好。

对于跨境企业，审计报告的比较还需要考虑法律环境的差异。境外母公司按其本国法开展的审计，未必符合我国的要求。法院应当审查审计内容是否覆盖我国的强制性规定，不能简单采信境外报告。

审计报告涉及商业秘密的，质证可以不公开进行。法院应当采取保密措施，避免信息在诉讼中二次泄露。当事人申请不公开质证的，法院可以准许。

八、裁判方法与制度完善

审理涉审计报告的案件，可以按四个步骤展开。第一步，审查报告的形式要件，包括出具主体、审计期间、审计范围、签章。第二步，审查报告的独立性，包括机构与被审计对象的关系、人员的回避。

第三步，审查报告的实质内容，包括必审事项是否覆盖、审计方法是否合理、问题披露是否完整。第四步，认定报告的证明力，结合其他证据综合判断，确定处理者是否尽到义务。

形式要件的审查，较为简单。缺乏签章、审计期间不明、审计范围与涉案行为无关的，报告不予采信。形式要件齐备的，进入实质审查。

独立性的审查，需要查明机构与被审计对象之间的利益关系。可以通过工商登记、关联交易、人员任职等信息核查。存在利益关系的，报告的证明力显著降低，但并非当然不予采信。

实质内容的审查，是核心。法院可以要求处理者提交审计方案、工作底稿与问题清单，比对报告披露的内容。发现报告隐瞒问题的，可以认定报告不实，推定处理者未尽义务。

证明力的认定，应当综合全案证据。报告只是其中一份，不能单独作为认定事实的依

据。原告提供的泄露证据、监管机关的处罚决定、媒体的调查报告，都可以与报告相互印证或者相互矛盾。

裁判说理应当说明采信或者不采信报告的理由。不能笼统表述为报告不足以证明其主张，而应具体指出报告在独立性、完整性或者时效性上的缺陷。

制度完善方面，本文提出三点建议。其一，建立审计机构的备案与信用管理制度，提高审计质量。其二，明确审计报告的公开范围，涉及公共利益的，应当向社会公开。其三，细化未审计与未整改的法律责任，形成梯度。

在标准层面，可以制定分行业的审计指引。金融、医疗、教育、交通等行业的个人信息处理具有特殊性，通用指引难以覆盖。分行业指引可以提高审计的针对性。

在能力建设层面，应当加强审计人才的培养。个人信息保护审计横跨法律与技术，需要复合型人才。高校、行业协会、监管机关可以联合开展培训，建立人才库。

审计制度的有效运行，最终取决于处理者的合规意愿。若企业仅将审计视为应付监管的形式，再严密的规则也难以奏效。培养合规文化，比完善规则更为根本。

对于司法而言，审计报告既是证据，也是观察企业治理的窗口。通过对报告的审查，法院可以了解企业的合规水平，进而判断其过错程度。这一功能的发挥，有赖于裁判经验的积累。

归结而言，审计制度的价值不在于报告本身，而在于它促使处理者在日常经营中持续关注个人信息保护的落实情况。这种持续的自我约束，正是法律实施最深层的保障。

九、结语

个人信息保护合规审计，是法律实施的重要机制。它将抽象的法定义务转化为具体的自查程序，使处理者在监管之外多了一道自我约束。

本文的核心主张是，审计义务是行为义务。处理者按照规定开展审计，即已履行义务；审计未发现问题的，不当然免责。这一区分，既避免了结果责任的不确定性，也防止了形式主义的应付。

审计内容的构造，应当以风险为导向。必审事项保证底线，兜底条款保留弹性。审计机构应当结合具体场景，说明判断理由，不能以行业惯例代替具体分析。

审计报告的效力，定位为初步证据。真实、完整、独立的报告，可以推定处理者已尽组织措施义务；存在虚假记载或者重大遗漏的，推定被推翻。这一规则，平衡了双方的举证能力。

未审计与未整改的后果，应当有梯度。未审计从轻，未整改从重；主动报告并补救的，可以减免责任。梯度的设计，旨在激励处理者主动合规，而非被动应付。

从更宏观的层面看，个人信息保护的关键，不在于事后追责，而在于事前预防。审计正是预防机制的一环。它的有效运行，需要监管、行业与企业的共同努力。

本文的讨论仍有局限。样本主要来自大型互联网企业的实践，对中小企业的审计状况未及展开。审计报告的证据规则，也还需要更多的裁判积累。

最后需要强调的是，规则的明确性对企业合规至关重要。企业在开展审计时，需要知道何种程度才算尽责。监管与司法应当通过明确的指引，为企业提供可预期的行为标准。

参考文献

[1] 程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版。
[2] 张新宝：《个人信息保护法释义》，中国人民大学出版社2021年版。
[3] 周汉华：《个人信息保护的法律基础》，载《中国法学》2020年第6期。
[4] 王锡锌：《个人信息权益的三重构造》，载《中外法学》2021年第1期。
[5] 丁晓东：《个人信息保护：原理与实践》，法律出版社2022年版。
[6] 洪延青：《个人信息保护合规审计的制度逻辑》，载《法学杂志》2023年第4期。
[7] 最高人民法院研究室：《个人信息保护法司法解释理解与适用》，人民法院出版社2023年版。
[8] 刘权：《数据安全与合规治理》，载《清华法学》2022年第3期。
[9] 许可：《个人信息处理者的合规义务》，载《政法论坛》2022年第5期。
[10] 国家互联网信息办公室：《个人信息保护合规审计管理办法释义》，2025年版。