艾华迪集团 AVISTA GROUP

艾华迪洞察

《个人信息保护合规审计管理办法（征求意见稿）》合规审计讨论

引言

2023年8月3日，为指导、规范个人信息保护合规审计活动，根据《中华人民共和国个人信息保护法》（以下称《个人信息保护法》）当中有关要求，国家互联网信息办公室起草并发布了《个人信息保护合规审计管理办法（征求意见稿）》（以下简称《管理办法》）及配套的《个人信息保护合规审计参考要点》（以下简称《参考要点》），并公开征求公众意见。

《管理办法》及《参考要点》旨在通过明确个人信息保护合规审计的具体要求、形式等内容，以期进一步完善国内个人信息保护相关的法规监管及企业内部合规体系。

本司选取《管理办法》和《参考要点》中的精要部分进行说明，从内部监控角度提供进一步的解读，以协助个人信息处理企业能更好地理解个人信息保护合规要求。

©AVISTA Group. All rights reserved

个人信息保护合规审计是什么？

《管理办法》第三条定义了个人信息保护合规审计为 “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”。

个人信息处理者应当明确区分个人信息类型为一般个人信息及敏感个人信息。《管理办法》中描述的一般个人信息及敏感个人信息包括如下：

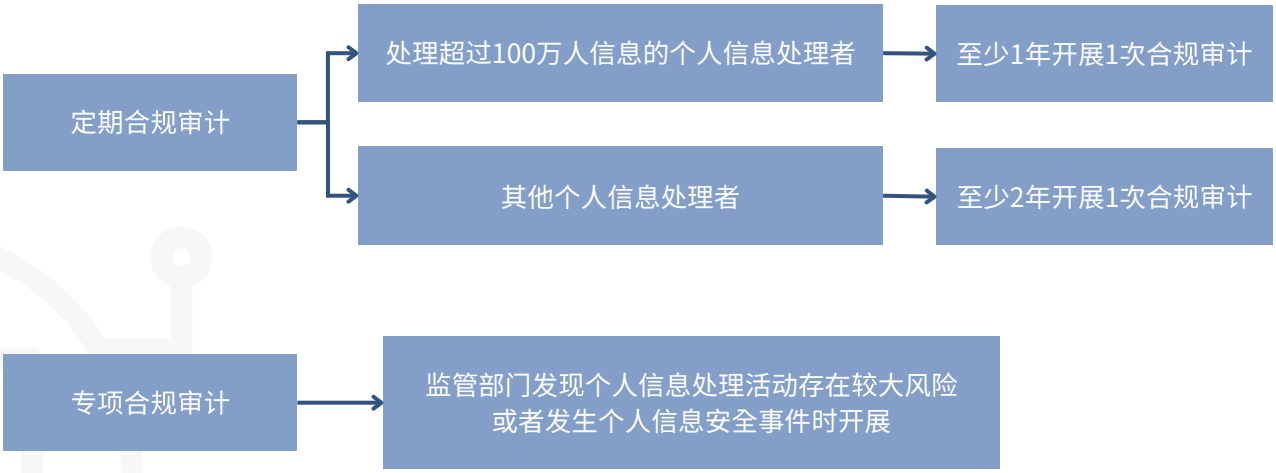
一般个人信息	个人基本资料、一般身份信息、网络身份标识信息、个人教育工作信息、个人通信信息、联系人信息、个人上网记录、个人常用设备信息、个人位置信息、其他信息
敏感个人信息	生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹以及不满十四周岁的未成年人的个人信息

为什么要做个人信息保护合规审计？

《个人信息保护法》第五十四条及第六十四条要求个人信息处理者必须进行 “定期合规审计”及/或“专项合规审计”。如企业未有按该法规要求进行合规审计，将依照《个人信息保护法》第六十六条，被处以没收违法所得、暂停营业、罚款及吊销营业资质等处罚。

个人信息保护合规审计的启动条件是？

参照《管理办法》第四条及第六条，《个人信息保护法》规定的“定期合规审计”及“专项合规审计”的启动条件为：



©AVISTA Group. All rights reserved

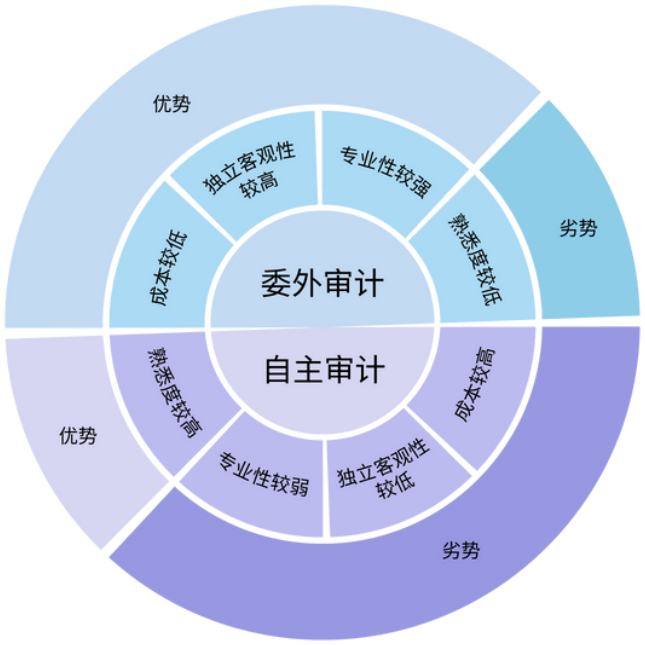
个人信息保护合规审计可以由谁执行？

1）审计工作主体

《管理办法》第十三条提及将建立《个人信息保护合规审计专业机构推荐目录》，鼓励个人信息处理者优先选择推荐目录中的专业机构开展个人信息保护合规审计。《管理办法》第五条及第七条亦针对执行工作的主体进行了说明，即：

合规审计类型	工作主体
定期合规审计	本组织内部机构 或 外部专业机构
专项合规审计	外部专业机构

2）审计方式比较



3）专业机构说明

结合《管理办法》及《参考要点》，为确保合规审计的独立性和客观性，专业机构连续为同一审计对象开展个人信息保护合规审计不得超过三年。此外，专业机构应当诚信正直，公正客观地作出合规审计职业判断。

©AVISTA Group. All rights reserved

个人信息保护应该关注哪些重点？

1）不同行业的个人信息保护相关内部监控系统关注重点

- **金融信贷行业**

关注重点	详情
实名数据收集及使用	1. 企业收集申请人的身份识别及联系信息、资产交易及消费明细等敏感信息时是否已获得申请人的明确同意。 2. 企业是否存在过度收集用户信息的情况。
安全技术措施	1. 企业采取了哪些安全措施来保护个人数据的机密性和完整性，数据传输和存储是否使用了加密技术以确保其安全。 2. 是否有防止未经授权访问的控制措施。
通讯信息安全	1. 企业在通过短信、邮件及电话进行信贷催收时是否存在非法使用个人信息的情况。 2. 企业是否保护申请人信息免受网络攻击及电信诈骗等威胁。
应急响应机制	1. 企业是否建立完善的应急机制能及时有效地应对个人信息安全事件。

©AVISTA Group. All rights reserved

- **互联网平台行业**

关注重点	详情
注册与用户数据收集	1. 互联网平台通常要求用户注册账户，涉及个人信息的收集。企业是否明确告知用户数据收集的目的和方式并获得了用户的同意。
数据存储和跨境传输	1. 如需进行境外上市及进行跨境数据传输，企业是否已按法规获得足够的政府备案授权。 2. 是否采取了必要安全措施来保护个人信息数据在存储及跨境传输时的安全性。
交易数据和支付信息	1. 企业是否对用户的支付信息和交易数据采取了足够的安全措施。 2. 平台处理相关数据是否合规，以避免滥用或不当使用。
个性化推荐及广告	1. 当平台会根据用户的社会关系、浏览偏好及操作习惯等个人信息进行个性化推荐和广告时，平台是否透明地告知用户此类行为，并获得用户的同意。 2. 用户是否有自由选择是否接受个性化推荐的权利。
个人信息保护影响评估	1. 企业是否进行了个人信息保护影响评估，以确定数据处理活动可能对用户权益的影响，并采取相应的措施来降低这些影响。
社会责任报告	1. 企业是否定期发布社会责任报告，向持份者透明披露个人信息保护情况。

- **百货零售行业**

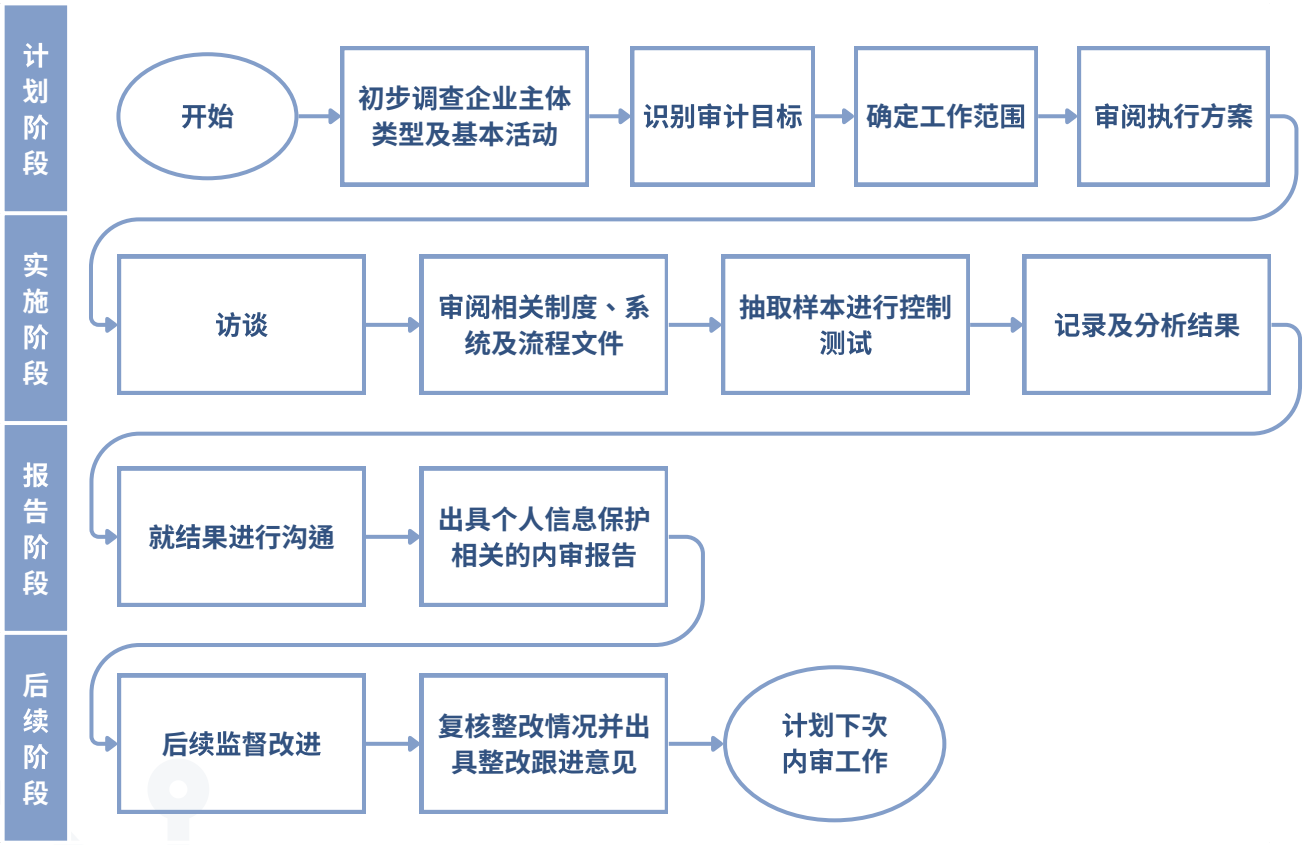
关注重点	详情
消费者会员信息收集	1. 企业在收集消费者会员信息时是否充分履行告知义务。 2. 是否对收集的个人信息进行加密处理使未授权员工无法提取。
第三方合作和数据共享	1. 当企业于运输配送、会员管理、扫码支付等第三方平台安排分享数据活动前，有否在分享数据协议中明确个人信息数据共享的方式及监督措施。
合规教育和培训	1. 企业是否为员工提供合规培训，以提高员工的个人信息保护意识和能力。

©AVISTA Group. All rights reserved

2）重点的规章制度及程序

《管理办法》及《参考要点》当中描述了大量对于个人信息保护相关内部监控系统的要求。参考本司过往内审工作之经验，本司认为《管理办法》及《参考要点》当中与个人信息保护工作相关的重点制度及程序包括：

一般企业应如何审阅个人信息保护相关内部监控系统的有效性？



©AVISTA Group. All rights reserved

总结

中国内地对于个人信息保护的要求越加清晰及严格。于2023年8月发布的《管理办法》更为个人信息保护合规审计提供了明确的指导要求。企业必须意识到个人信息保护相关的内部监控系统重要性，积极识别个人信息保护相关合规风险，以应付日益严格的法规要求。

联络我们

彭颂邦
特许金融分析师，
资深会计师(香港)，
资深会计师(澳洲)，
皇家特许测量师学会专业会员，
皇家特许测量师学会注册估价师

首席合伙人
vincent.pang@avaval.com
+852 3702 7388
+86 138 1023 8603

詹金强
会计师

风险管理咨询主管
derek.chim@avaval.com
+852 3702 7312
+86 189 3866 2083

艾华迪集团（「艾华迪」）是一家行业领先的独立专业咨询机构，专注于为企业提供各类估值、风险管理咨询、环境、社会及管治 (ESG) 咨询、企业咨询和房地产咨询服务。我们为国际评估准则理事会（IVSC）的企业会员。

艾华迪的足迹遍布亚太地区，分别在香港、上海、北京及深圳设有办公室。我们致力于充分利用本土和海外工作网络的完美结合，以及业务单位产生的协同效应，通过提供高质量的服务，为客户提供解决复杂商业难题的最优方案。

艾华迪的服务团队由100多名专业顾问组成，具有各类国际认可的专业资格，并清楚了解监管机构的标准和财务报表的披露要求。我们的管理团队和项目成员背景相当多元化，分别来自于国际知名的评估机构、咨询公司及会计师事务所，持有进行专业咨询工作的各类资质，如特许金融分析师 (CFA)、会计师 (CPA)、资产评估师 (CPV)、金融风险管理师 (FRM)、皇家特许测量师学会专业会员 (MRICS) 等。

艾华迪网站　Facebook　LinkedIn　微信

©AVISTA Group. All rights reserved