XXXXXX 有限公司审核案例

推荐机构：广州赛宝认证中心服务有限公司
认证领域：隐私安全管理体系审核
审核时间：2023 年 5 月 29 日—5 月 31 日
审核人员：刘敏（组长/组员）

一、案例背景

此案例为 2023 年对“XXX 有限公司”的隐私安全管理体系（PMIS）的审核发现, XXX 公司通过官网电子商城为客户提供一站式产品采购（销售）服务，在 2023 年国家对隐私安全高度重视且不断有企业被处罚的大背景下，我们在审核过程中重点关注了企业对合规要求的满足情况。

二、审核过程及发现

基于上述背景介绍，审核过程中审核员以合规为主线结合标准条款要求，对业务开展过程中涉及隐私处理的各项活动以及可能产生合规风险的各业务环节进行了充分了解。在交流过程中发现相关人员并不了解“个保法”的一些重要法规要求，重点加强了对隐私处理相关岗位人员的访谈。在访谈中发现公司在实际业务开展中并没有向客户提供个人信息处理撤回的相关机制。再进一步登陆公司电子商城进行实操验证，发现用户注册时提供的隐私政策声明中确实也没有定义“用户如何撤回同意”的相关说明。同步查看线下制度化的《隐私保护政策》，发现策略中对此项要求确实也没有明确定义。

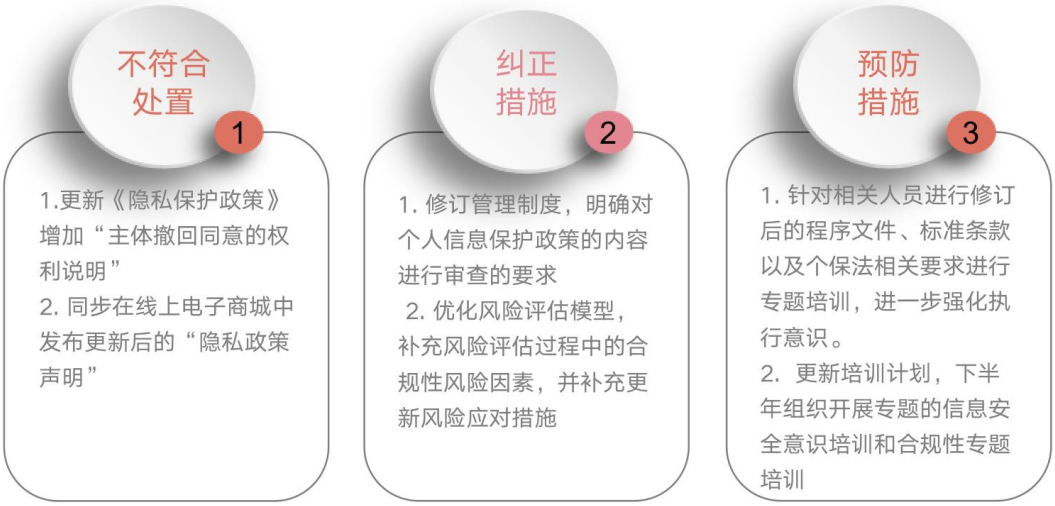
在审核过程中,开出以下不符合项：“查 XXX 公司电子商城平台的《隐私政策声明》中未包含“PII 主体如何撤回同意的信息”的相关内容，不符合 ISO/IEC27701:2019 标准 7.3.4 条款的相关要求（此不符合项除了不满足标准要求外，也不满足“中华人民国和国个人信息保护法” 第二章第十五条“基于个人同意处理个人信息的，个人有权撤回其同意，个人信息处理者应当提供便捷的撤回同意的方式。”的法规要求）

审核员与客户沟通并解释了相关合规风险后，公司管理层高度重视和认可，欣然接受不符合项。

三、纠正预防

企业在后续的整改过程中，分析不符合的原因涉及这几个方面，首先隐私处理团队对合规要求了解不够，本身就不清楚这项要求，当前定义的有关个人信息处理的程序中也缺少隐私政策内容完整性进行检查确认的机制；此外，风险评估团队也没有意识到相关合规方面的风险，没有意识到一旦风险发生，可能给公司带来的巨大损失。

不符合整改和处置包含以下方面



四、客户收益

通过审核员对标准要求和合规要求的讲解，客户管理层对此次发现的问题高度重视，同时在后续的举一反三自查过程中发现一些其他的个人信息处理的合规风险，基于风险评估结果，组织重新梳理了当前的隐私安全管理制度，并在公司范围内组织了广泛的合规性的相关培训。

通过审核员的现场交流和行业案例分享，客户充分意识到了合规问题可能给公司带来的不仅仅是简单的经济处罚，更多的是企业声誉和客户信心的损失。一旦发生，未来对业务会产生巨大影响。帮助客户提升风控意识，在业务发展的同时能更好的守护安全底线。