数据合规专题

第二期

个人信息处理者的义务

（2024 年 10 月）

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等，不包括匿名化处理后的信息。

本期内容旨在通过案例进一步明确个人信息处理者的义务。

【案例简介】

薛祥飞在与浙江淘宝网络有限公司（下称**“淘宝公司”**）签订淘宝网络购物平台（下称**“淘宝平台”**）的注册协议并同意其隐私政策后，通过淘宝平台购买商品。为完成订单，淘宝公司收集、存储并与其他关联方共享薛祥飞该笔订单相关的个人信息，包括收件人姓名、收货地址、收货人联系电话、商品概括描述等。在商品签收前，薛祥飞接到境外来电，对方向其透露了与其在淘宝平台填写内容一致的订单信息，故薛祥飞认为淘宝公司泄漏了其个人信息，致使境外诈骗团伙多次致电实施电信诈骗，侵害了其个人信息权益和隐私权，遂诉至法院，请求判令淘宝公司赔礼道歉并赔偿损失。

法院经审理认为，淘宝公司能够证明其在本案中的个人信息处理

行为没有过错，且无证据证明薛祥飞个人信息的泄露与淘宝公司有关，故驳回薛祥飞的诉讼请求。主要理由包括：（1）淘宝公司能够证明其采取了个人信息保护必要合规措施，未违反关于个人信息处理者保护义务的规定，如：完成三级等保备案、制定内部个人信息保护规范、采取加密和限制使用等措施等；（2）淘宝公司能够证明个人信息处理行为具有合法性基础，未违反个人信息处理的规定，即：淘宝公司收集、保存、与第三方共享薛祥飞相关个人信息均取得其同意，且为履行合同之必需，未违反正当、必要处理原则；（3）淘宝公司能够证明其在处理具体信息上已尽到合理谨慎的安全保障注意义务，包括：设置内部风控管理体系防止信息泄露，采取信息去标识化、安全提示、下载管控、违规处罚等必要保护措施等。

【启示与建议】

上述案例中，淘宝公司胜诉的原因是严格履行了法律法规规定的个人信息处理者的义务，在各环节尽到了个人信息安全保护责任。

根据现行法律法规的规定，个人信息处理者负有以下义务：

1、一般个人信息处理者的义务

（1）根据个人信息处理目的和方式、个人信息种类及对个人权益的影响、可能存在的安全风险等，采取措施确保个人信息处理活动符合法律法规规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失，包括：制定内部管理制度和操作规程；对个人信息实行分类管

理；采取加密、去标识化[1]等安全技术措施；合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；制定并组织实施个人信息安全事件应急预案，以及法律法规规定的其他措施。

（2）定期对处理个人信息遵守法律法规的情况进行合规审计。

（3）符合法定情形的，应事前进行个人信息保护影响评估，并记录处理情况，法定情形包括：处理敏感个人信息[2]；利用个人信息进行自动化决策[3]；委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；向境外提供个人信息；其他对个人权益有重大影响的个人信息处理活动。

（4）发生或可能发生个人信息泄露、篡改、丢失的，应立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应包括：发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；个人信息处理者的联系方式。个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，可以不通知个人，但若履行个人信息保护职责的部门认为可能造成危害的，其有权要求个人信息处理者通知个人。

2、特殊个人信息处理者的义务

（1）处理个人信息达到国家网信部门规定数量的个人信息处理

[1] **去标识化**，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。
[2] **个人敏感信息**，是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。
[3] **自动化决策**，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

者，应指定个人信息保护负责人，监督个人信息处理活动及采取的保护措施，并公开个人信息保护负责人的联系方式，将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

（2）中华人民共和国境外的个人信息处理者，应在中华人民共和国境内设立专门机构或指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

（3）提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应按国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；对严重违反法律法规处理个人信息的平台内的产品或者服务提供者，停止向其提供服务；定期发布个人信息保护社会责任报告，接受社会监督。

（4）接受委托处理个人信息的受托人，应依法采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行法定义务。

上述义务是个人信息处理者的法定义务，是其在处理个人信息时应向权利主体承担的保护责任。个人信息处理者只有树立安全意识、建立合规体系、尽到安全义务，才能充分保障权利主体的个人信息权益，促进各行业及数字经济的平稳发展。

北京道商律师事务所

2024 年 10 月 27 日