数据合规专题

第十一期

数据使用的合规性要求

（2025年7月）

作为数据处理过程中的重要环节，数据的使用应同样遵循合法、正当原则。数据处理者应根据数据权利主体许可的使用目的、范围及方式等内容合法使用其授权的相关数据，并依法保障数据权利主体的知情权、决定权、修改权及删除权等合法权益。

通常情况下，数据处理者依据与数据权利主体的约定合法使用数据即可，但相较于其他数据权利主体而言，因个人信息主体具有广泛性及弱势性等特征，《中华人民共和国个人信息保护法》《信息安全技术 个人信息安全规范》（GB/T 35273-2020）等法律法规及相关标准对个人信息的使用作出如下具体规定：

一、个人信息访问控制

1、权限限制。对被授权访问个人信息的人员，个人信息处理者应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限。

2、操作审批。个人信息处理者须对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等重要操作。

3、角色分离。个人信息处理者须对安全管理人员、数据操作人

员、审计人员的角色进行分离设置。

4、超权限审批。确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息处理者内部设置的个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册。

5、权限被动触发。对个人敏感信息的访问、修改等操作行为，个人信息处理者可在控制角色权限的基础上，按照业务流程的需求触发操作授权。例如：当收到客户投诉，投诉处理人员才可访问该个人信息主体的相关信息。

二、个人信息的展示限制

个人信息处理者通过屏幕、纸质文书等界面展示个人信息的，可对需要展示的个人信息采取去标识化处理等措施，防止非授权人员及个人信息主体之外的其他人员未经授权获取个人信息，进而降低个人信息在展示环节的泄露风险。例如：加密处理快递面单上寄件人及收件人的姓名和联系方式，以及手机银行查询页面的银行卡号和余额信息等。

三、个人信息使用的目的限制

1、使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。

2、如收集的个人信息进行加工处理后所产生的信息，能够单独或与其他信息结合识别特定自然人身份或者反映特定自然人活动情

况的，应将其认定为个人信息，对其处理应遵循收集个人信息时获得的授权同意范围。若加工处理而产生的个人信息属于个人敏感信息的，对其处理则需符合对个人敏感信息的要求。

四、个人信息的加工及应用限制

个人信息处理者在使用个人信息时，还可能存在对个人信息进行分析、整合，生成衍生数据并再次使用的二次加工及应用行为。在此过程中，个人信息处理者除须做好上述工作外，还应注意以下事项：

（一）用户画像的使用限制

1、用户画像中对个人信息主体的特征描述，不应包含淫秽、色情、赌博、迷信、恐怖、暴力的内容，不应表达对民族、种族、宗教、残疾、疾病歧视的内容。

2、在业务运营或对外业务合作中使用用户画像的，不应侵害公民、法人和其他组织的合法权益；不应危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

3、除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确的身份指向性，避免精确定位到特定个人。例如：金融机构经个人信息主体授权后，为准确评价其个人信用状况，可使用直接用户画像，即直接使用特定自然人的个人信息所形成的该自然人的特征模型；若用于推送商业广告目的，则更适宜使用间接用

户画像，即使用来源于特定自然人以外的个人信息，如其所在群体的数据所形成的该自然人的特征模型，如“00后”、“自由职业者”等。

（二）个性化展示的使用

1、在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容，如标注“定向推送”、“猜你喜欢”以及将该推荐内容分页面展示等，并可建立个人信息主体对个性化展示所依赖个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

2、在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项。

3、在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项，且当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

（三）基于不同业务目的所收集个人信息的汇聚融合

当前，法律法规暂未明确汇聚融合的定义及应用场景，但结合数据共享及互联互通的发展现状，个人信息的汇聚融合可在一定程度上理解为将基于不同目的收集的个人数据综合汇总并加以融合。

由于个人信息汇聚融合过程中，可能存在部分去标识化的个人信

息在与其他信息关联后重新识别出特定个人，以及汇聚融合产生的信息出现偏差进而导致个人信息主体权益受损等风险。因此，在此场景下，个人信息处理者除应遵守“个人信息使用目的限制”项下的相关要求外，还应根据汇聚融合后个人信息的使用目的，开展个人信息安全影响评估，并采取有效的个人信息保护措施，保障个人信息主体的合法权益。

（四）信息系统自动决策机制的使用

个人信息处理者业务运营所使用的信息系统具备自动决策机制且能够对个人信息主体权益造成显著影响的（如自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应当符合下列要求：

1、在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

2、在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施；

3、向个人信息主体提供针对自动决策结果的投诉渠道,并支持对自动决策结果的人工复核。

此外，将于2025年10月1日起正式实施的《数据安全技术 基于个人信息的自动化决策安全要求》（GB/T 45392-2025），对自动化决策算法、特征生成、决策及典型场景等方面的安全要求作出了更为具体的规定，个人信息处理者可保持关注并参照执行。

北京道商律师事务所

2025 年 7 月【 】日