解答《个人信息保护法》的重要合规实务问题

本文首发于《商法》问答信箱 作者：顾正平 向文磊

中国首部专门针对个人信息保护和规范的综合性法律，《个人信息保护法》(下称《个保法》)，于 2021 年 8 月 20 日正式出台，并将于 2021 年 11 月 1 日生效。

由于此前个人信息保护领域已有大量法规规定和行业标准等规范性文件，已初步形成完整的监管体系，对于企业合规落地的难度稍低于《数据安全法》(下称《数安法》)。同时，由于监管部门已经积累了丰富的执法经验，对于企业合规而言，紧迫性、重要性是不言而喻的。《个保法》的出台进一步完善和提升了中国个人信息保护制度，同时也为企业提供了更系统也更严格的个人信息保护规则指引。本问答旨在为相关企业在开展《个保法》合规实践时经常遇到的关键问题提供有益思路与借鉴参考。

Q：如何判断是否构成个人信息？

答：判断是否构成个人信息，应重点考虑识别的可能性。实践中，认定直接标识符(如身份证号、医保卡号、银行卡号、住址)和具有识别特定个人可能性的间接标识符(如车牌号、智能终端设备的位置、订单编号、浏览记录)均构成个人信息。

去标识化技术(如隐私计算)并不是排除个人信息保护监管的避风港。《个保法》仅明确了匿名数据不构成个人信息，而经去标识化处理的个人信息仍可能构成《个保法》所规制的个人信息。另外，聚合类数据是否适用个人信息保护的相关规定也应结合具体的业务场景进行判断，如是否已通过知情同意等措施确保数据处理具有合法基础。

个人信息还可能与《数安法》项下重要数据的范围重叠。比如在汽车数据领域，车辆运行的轨迹数据如果涉及主体超过 10 万人的个人信息，就会既构成重要数据，也是个人信息或敏感个人信息。

Q ：个人信息处理的合法性基础有哪些？

答：(1) 告知同意仍然是处理个人信息最核心的合法性基础。实践中，即使具备数据处理的其他适用合法性基础，如履行合同或人力资源管理之必需，告知同意仍然是企业得以最大限度处理个人信息的关键原则。

(2) 履行合同之必需在实践中的应用场景也较为常见，但监管所认可的范围可能有限。例如在电商服务中，虽然消费者的订单记录、住址等对于履行买卖合同、物流管理等是必需的个人信息，但若相关企业希望针对该等个人信息进行自动化决策、数据共享等行为，则仍需要进一步征得消费者的同意。

(3) 人力资源管理之必需的场景并不意味着企业在任何情况下均可以未取得个人同意即处理其个人信息。例如，通过人脸识别进行考勤或核验员工病假时，由于面部识别信息、个人健康或疾病信息构成敏感个人信息，因此不能豁免个人同意，而应优先取得单独同意。我们建议企业在人力资源管理工作中结合个人信息的类型、收集目的、用途等评估处理方式。

Q ：如何认定敏感个人信息？授权规则如何实现？

答：(1) 针对敏感个人信息的行业性专项执法将成为未来触发《个保法》巨额罚则的核心监管场景之一。

(2) 敏感个人信息通常包括生物识别、医疗健康、金融账户、行踪轨迹及未成年人信息等。须注意的是，上述类型项下的不同信息的敏感程度不同。

(4) 处理敏感个人信息应当取得个人的单独同意，具体实现方式应结合行业特性、业务类型、技术可操作性等因素进行判断、选择。

Q： 个人信息是否可以跨境提供？

答：(1) 对于关键信息基础设施运营者(CIIO)而言，其个人信息处理量达到网信部门规定的数量，即须履行本地化部署的义务。确需出境的，须通过网信部门的安全评估。

(2) 非 CIIO 企业的个人信息跨境提供方面，只要企业能够完成个人信息保护的专业认定或采用中国版 SCC(标准合同)，即可合规地向境外提供个人信息。但是，非 CIIO 企业向境外提供敏感个人信息或跨境的数据量达到一定级别，则会触发安全评估、安全审查申报等义务。有必要强调的是，目前执法部门对于“跨境”的认定通常采用广义标准，即包括境外实体通过云端接口访问境内实体的数据等情况。

Q：违反《个保法》会导致什么法律后果？

答：第六十六条规定，违反《个保法》的规定处理个人信息的，由相应主管部门责令改正、责令暂停或终止服务、没收违法所得；针对拒不改正的，采取“双罚制”，即对企业(100 万元以下)和直接责任人员(10 万元以下)并处罚款。针对情节严重的违法行为，第 66 条进一步规定由执法部门责令改正，并处五千万元以下或者上一年度营业额 5%以下罚款，同时还可责令暂停业务或停业整顿及吊销相关业务许可等。

须注意的是，相关违法行为还可能同时触发《数安法》《银行业监督管理法》《生物安全法》《出口管制法》《人类遗传资源管理条例》等相关法律法规的罚则。