2020 年 3 月 30 日

“摇钱树”还是“烫手山芋”——企业应如何处理个人敏感信息

在新冠疫情防控持续向好的态势下，作为加快复工复产的重要抓手，加快 5G 网络、数据中心、人工智能等新基础设施建设再次成为全国上下的焦点。“新基建”的升级将促进万物互联和大数据经济发展，而作为大数据经济的“血液”及“石油”，自然人的交易记录、健康生理、生物识别、行踪轨迹等个人敏感信息，对经济社会转型发展的重要性不言而喻。但相关法律法规对个人敏感信息的保护及违法处罚作出严格规定，给企业经营管理中的个人敏感信息处理行为设定了一条无形的“高压线”。对企业而言，个人敏感信息既有可能是“摇钱树”，又有可能是“烫手山芋”。本文拟梳理有关个人敏感信息保护的特殊规则，以期对企业合法处理个人敏感信息提供参考。

一、主要法域下的个人敏感信息界定

鉴于个人敏感信息的特殊性和重要性，个人信息的主要执法法域均对个人敏感信息作出了规定。在欧盟法下，《一般数据保护条例》（简称“**GDPR**”）第 9 条规定了“个人敏感信息”范围，涉及以下一种或一种以上类别的个人数据，包括种族或民族背景、政治观念、宗教或哲学信仰、工会成员身份、能够识别特定个人的生物识别数据、以及与自然人健康、性生活或性取向有关的数据。而日本的《个人信息保护法》将个人敏感信息称为“需要注意的个人信息”，是指政令（相当于行政法规）规定的、为避免造成不公正的歧视、偏见和其他不利情况而就其处理需要特别注意的信息，例如种族、信仰、社会身份、病历、犯罪经历、因犯罪而被害的事实及其他方面个人信息。

根据 2020 年 3 月 6 日发布的新版《信息安全技术 个人信息安全规范》（GB/T 35273—2020、以下简称“**《安全规范》**”），我国的个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。虽然《安全规范》仅是推荐性国家标准，并非强制性标准，但已经成为相关政府监管部门执法的重要依据，也是企业个人信息合规要求的重要指南。

《安全规范》还列举了以下个人敏感信息的参考类型：

个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等

个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

对比欧盟、日本等域外法，可以看出我国对个人敏感信息的界定借鉴了 GDPR 的立法思路。但在保护对象的范围方面, GDPR 主要面向对种族、信仰、性别取向等可能导致伦理方面受歧视性待遇的信息，中国除了保护个人免受名誉、精神、歧视性待遇外，还保护人身、财产免受损害。日本的规定比较折中，既防止歧视对待、偏见，也注意到了其他不利情况。从界定范围来看，中国规定的个人敏感信息范围比 GDPR、日本广泛。

二、个人敏感信息的特别处理规则

对于个人敏感信息的保护，除了适用个人信息安全的基本原则（权责一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与）以及关于一般个人信息的处理规则之外，还应注意《安全规范》以及其他行业法规规定中的特殊保护要求。

1、 “明示同意”原则

对于企业等个人信息控制者收集、处理个人敏感信息的行为，《安全规范》规定了应事先获得个人信息主体（用户）的“明示同意”原则。《安全规范》规定的“同意”方式包括“授权同意”、“明示同意”等，其中对“明示同意”的要求更高。

“明示同意”是指，个人信息主体（比如 APP 用户）通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。肯定性动作包括用户主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”、主动填写。

值得注意的是，实务中存在通过隐性方式获得用户“默示”同意的做法（包括仅展示预先勾选的“同意”、“下一步”等唯一选项，引导用户直接做出同意；强制捆绑、一次性获得用户关于收集其多种类型个人信息的综合同意），不能满足上述获取个人敏感信息的“明示同意”要求，存在违规风险。

2、 处理个人敏感信息的特别规则

《安全规范》除规定了一般个人信息的处理规则之外，还着重强调了对个人敏感信息的特别处理要求。

（1）收集、存储与传输

企业在通过手机 APP 等收集个人敏感信息前，应征得个人信息主体的明示同意；传输和存储个人敏感信息，应采用加密等安全措施（采用密码技术时应遵循密码管理相关国家标准）。

（2）共享、转让

企业在向第三方共享及转让其控制的个人敏感信息前，应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先取得个人信息主体的明示同意。

（3）访问控制

企业对个人敏感信息的访问、修改等操作行为，应在对角色权限控制的基础上，按照业务流程的需

求触发操作授权。例如，不是主动访问，而是当收到用户投诉时，投诉处理人员才可访问该个人信息主体的相关信息。

(4) 内部机构设置、人员管理及安全事件处置

处理超过 10 万人的个人敏感信息的企业，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作；对于从事个人信息处理岗位上的相关人员，企业应当与其签署保密协议，并对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等，防止出现个人敏感信息违法行为；万一企业发生个人敏感信息泄露事件时，应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。

3、 对个人生物识别信息的加重保护

由于基因、指纹、面部等个人生物识别信息具有不可逆性，无法通过常规的变更密码等方式修改弥补，一旦发生安全事件，将给个人带来严重损害，对此《安全规范》专门列出了应当遵守的加重保护要求。

(1) 收集环节：单独告知、明示同意

企业在收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，征得个人信息主体的明示同意；

(2) 原则上禁止存储

企业原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：a）仅存储个人生物识别信息的摘要信息；b） 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；c）在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像；企业确需存储个人生物识别信息的，应当与个人身份信息分开存储。

(3) 禁止共享、转让、公开披露

企业原则上不应共享或转让、公开披露个人生物识别信息，确需共享和转让的，仍应当单独向用户告知目的、信息类型等内容，并征得个人信息主体的明示同意。

4、 特殊行业的专门规则

除上述对于个人敏感信息的共通保护规则外，在与儿童保护、医疗资源、金融信息等有关的特殊行业，还存在专门的保护规则，从事该等领域的企业需满足该等领域的特殊合规要求。

- 《儿童个人信息网络保护规定》对 14 周岁以下的儿童个人信息进行特殊监管，在收集、使用、转移、共享、存储、披露、删除等全生命周期的各个环节保护儿童个人信息；
- 《人类遗传资源管理条例》、《国家健康医疗大数据标准、安全和服务管理办法（试行）》《健康医疗信息安全指南(征求意见稿)》，则对个人健康生理信息、医疗数据、人类遗传资源材料及人类遗传资源信息等的收集、使用、共享等做出特别规定。
- 全国金融标准化技术委员会于 2020 年 2 月 20 日公布的《个人金融信息保护技术规范》，将《安全规范》的规定落实到个人金融信息保护的各个环节。

5、 与 GDPR、日本处理规则的比较

如第一部分所述，欧盟 GDPR 规定的个人敏感信息范围比我国的范围窄，但是在个人敏感信息的处理方面，GDPR 原则上不允许处理个人敏感信息，规制要求更加严格。而日本的《个人信息保护法》，则规定处理个人敏感信息必须事先取得用户的同意，与中国规定类似；但是日本对于一般个人信息的收

集及使用，没有明确要求取得用户的事先“同意”，仅以限制滥用为原则，比中国的个人信息保护规则宽松。

我们注意到实践中很多跨国公司的在华投资企业，由于接受境外母公司的全球统一管理，往往简单地复制粘贴该境外母公司的个人信息保护制度或者直接适用母公司的制度，考虑到各法域存在明显的监管差异，这种做法可能存在中国法下的个人信息合规风险，建议企业依据中国法梳理其个人信息保护相关制度。

三、 侵害个人敏感信息的法律责任及执法动向

对侵害个人敏感信息的违法行为，主要包括处理个人信息时未履行保护义务、未依法保护网络安全等，根据《网络安全法》关于侵害个人信息的相关规定，将受到责令改正、罚款、停业整顿或者吊销营业执照等行政处罚。

特别需要注意的是，刑法对于个人敏感信息予以高度保护，即使从一般角度来看侵犯的敏感信息数量较少，也有可能被追究刑事责任。比如，根据最高法、最高检《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第五条，非法获取、出售或者提供“行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的”或者“住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的”，即达到刑事立案的追诉标准。此外，从事金融、电信、交通、教育、医疗等行业的工作人员如果将履行职责或者提供服务过程中获得的个人敏感信息出售或者非法提供给他人的，将会受到“从重处罚”。

我们注意到，近期发生了“连锁酒店 5 亿条个人信息（包括用户身份证、入住酒店的行踪、消费记录等）泄露”、“保险公司员工销售 1000 万条用户信息营利”、“医疗机构未经许可向境外传输人类遗传资源”等涉及个人敏感信息的重大违法案件，再次引起全社会对保护个人敏感信息的关注。相关政府监管部门在依法打击的同时，针对企业利用 APP 处理个人信息等多次发动联合检查。我们建议企业及时制定并完善个人信息保护制度，根据最新规范的要求设置相应的个人信息保护部门或负责人员，健全企业内部网络安全建设，以不断满足强化“新基建”大形势下充分利用“个人敏感信息”的合规要求。

杨锦文　合伙人　电话：86 10 8553 7608　邮箱地址：yangjw@junhe.com
高　健　电话：86 10 8519 1359　邮箱地址：gaojian@junhe.com