君合研究简讯

JUNHE

2019 年 5 月 10 日

信息保护和网络安全法律热点问题

《互联网个人信息安全保护指南》正式出台

继 2018 年 11 月 30 日发布征求意见后，2019 年 4 月 10 日，公安部网络安全保卫局联合北京网络行业协会、公安部第三研究所共同研究制定的《互联网个人信息安全保护指南》（以下简称“**《指南》**”）正式发布。除了对《征求意见稿》原有的内容做了变动以外，指南还参考《网络安全法》（以下简称“**《网安法》**”）、GB/T35273-2017《信息技术安全个人信息安全规范》（以下简称“**《信安规范》**”）、GB/T22239《信息安全技术网络安全等级保护基本要求》（GB/T22239-2008《信息安全技术 信息系统安全等级保护基本要求》的修订中版本，目前仍在征求意见）增添了新的内容与要求，总结如下：

一、 适用范围

《指南》在第一节适用范围中明确“适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人”。上述表述说明除了传统意义上的互联网企业，其他领域的企业或个人，只要涉及到对于个人信息的控制与处理，均属于《指南》的适用范围。

从法律效力上看，《指南》并不属于有法律强制约束力的部门规章，其引言部分也说明“供互联网服务单位在个人信息保护工作中参考借鉴”。但是，由于目前《个人信息保护法》仍在全国人大立项制定过程之中，《指南》必然作为公安机关在实践之中执行《网安法》中涉及个人信息保护相关要求的重要参考。

二、 主要规定

《指南》从管理措施、人员设置、信息的收集使用、存储、共享、事件响应等多个方面全面的规定了企业对个人信息保护的实施要求，与《信安规范》等文件的内容有部分重合，也有突破、完善和更为严格之处。在此对其中的重要内容分析和总结如下：

(一) 安全保护义务

《指南》第 5.1 节要求“个人信息处理系统其安全技术措施应满足 GB/T 22239 相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务”。相较于《征求意见稿》中统一要求按照第三级等级保护的要求进行安全保护，《指南》并没有一刀切地要求个人信息持有者按照最高等级实行安全保护措施，而是基于企业自身的具体情况，按照所对应的等级开展安全保护。

(二) 组织管理体系

《指南》对管理机构以及管理人员均提出了要求。

1、 就管理机构而言，《指南》提出要授权专人负责个人信息的保护工作，并增设审计管理员的岗位；

2、 就管理人员方面，《指南》除了要求加强对个人信息管理人员在录用、离岗、教育培训等方面的管理，首次提出要定期考核管理人员对相关工作的基础知识、安全责任以及惩戒措施、法律法规等的理解，并记录存档考核记录；

3、 要求外部人员的访问，无论是通过物理或者网络渠道，均应先获得批准，并进行相应的限制和记录。

（三） 管理制度

在管理制度方面，《指南》对管理制度的内容、制定发布、执行落实与评审改进四个方面提出了要求。

1、 就管理制度内容而言，应包含个人信息保护的总体方针和安全策略等相关规章制度与文件、工作人员日常管理个人信息的操作流程以及个人信息管理制度体系，除此之外，还应制定个人信息安全事件应急预案；

2、 就制定发布而言，要明确专门的制度制定主体、制定程序、发布方式以及发布范围，对制定的制度进行论证和审定，并形成论证和评审记录；

3、 就制度执行落实方面，要对制度执行情况进行审批登记，要保存记录文件并定期汇报总结管理制度执行情况；

4、 就评审改进方面，要定期对安全管理制度进行评审并进行相应的修订，评审应形成记录，要及时更新管理制度的修订。

（四） 技术措施

《指南》从通用要求与拓展要求两方面对技术措施提出了要求，其中值得注意的点如下：

1、 就安全审计方面，《指南》提出安全审计要覆盖到每个用户、用户行为和安全事件；

2、 就身份鉴别方面，提出鉴别信息要定期更换并具有一定的复杂性，当确定信息被泄露后，应提供提示全部用户强制修改密码的功能，再验证确认用户后修改密码；

3、 就备份恢复方面，要求定期对备份数据进行恢复测试，保证数据可用性。

（五） 信息收集限制

《指南》对于个人信息持有者收集个人信息提出了更高的要求。例如，《指南》规定，不应收集与其提供的服务无关的个人信息，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息，

《指南》还规定，个人信息收集者“不应大规模收集或处理我国公民的种族、民族、政治观点、宗教信仰等敏感数据”。除此之外，《指南》中首次出现“个人生物识别信息应仅收集和使用摘要信息，避免收集其原始信息”的内容。例如信息持有者在收集脸部特征信息这种生物识别信息时，应仅收集脸部特征向量这种经过抽象化处理后得到的信息，而不能收集原始的脸部图像。

（六） 信息存储和应用及分享

《指南》对个人信息的存储、应用以及共享与转让等方面也提供了标准。

1、 就信息的保存方面，《指南》要求在存储的过程中要对信息通过安全加密等措施进行处理；应根据个人信息收集、使用的目的等作为依据对不用类型的个人信息设置不同的存储期限，并在超出时效后予以删除；除此之外，要对个人信息数据提供备份和恢复功能；

2、 就信息的应用方面，《指南》特别明确应用个人信息不得超出与个人信息主体签署的相关协议和规定，但经过处理无法识别特定个人且不能复原的个人信息除外；个人信息主体应有访问、修改、删除、纠正个人信息的权利；除此之外，《指南》要求应对个人信息的接触者设置相应的访问控制措施；

3、 就信息的共享与转让方面，《指南》提出个人信息原则上不得共享、转让。若要共享与转让个人信息，应进行个人信息安全影响评估。并对受让方的数据安全能力进行评估，确保受让方具备足够的数据安全能力。

4、 对于信息的存储，《指南》明确要求“在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定”。针对云服务，《指南》还专门提出要确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定。

（七） 用户画像

在第 6.3 c)一节中，《指南》对将个人信息用于用户画像的同意机制做出了规定：“完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利；如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据。”这是第一次出现以是否可能为用户带来法律后果为标准划分用户画像的同意机制。

（八） 应急处置

《指南》对于发生个人信息安全事件的应急处置提出了明确的要求，作为专章进行规定。从流程上来看，将应急处置划分为“应急机制与预案”、“处置与响应”两个部分，涵盖安全事件预防与处置的各个步骤。其中值得注意的是，对比《征求意见稿》中发生安全事件要向“有关主管部门”上报，《指南》第一次明确发生安全事件时应及时向公安机关报告。此外，《指南》还首次提出“应按《国家网络安全事件应急预案》等相关规定及时上报安全事件，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式”的要求。

三、 我们的观察

《指南》的出台为作为个人信息持有者的企业或个人提供了更为详细的个人信息保护的标准与规范，但同时要求也更高、更细节化，在实践之中将如何执行（例如数据本地化的规定），还有待于进一步观察。

董 潇 合伙人 电话：86 10 8519 1233 邮箱地址：dongx@junhe.com
袁 琼 律 师 电话：86 10 8553 7663 邮箱地址：yuanq@junhe.com
董俊杰 律 师 电话：86 10 8540 8722 邮箱地址：dongjj@junhe.com