NEWSLETTER 数据合规

2019 第二期 /总第二期

数据合规时事速递

（双周刊）

北京市环球律师事务所

2019 年 4 月 30 日

目录

前 言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新监管动态、立法动态、合规前沿信息及相关案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息，以及数据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁
合伙人律师
直线： 86-10-6584-6768
总机： 86-10-6584-6688
邮箱： mengjie@glo.com.cn

一、近期监管动态

1. 四部门推进 App 违法违规收集使用个人信息专项治理[1]

治理进展

中央网信办、工信部、公安部、市场监管总局四部门指导成立的 App 违法违规收集使用个人信息专项治理工作组，成立以来所组织开展的 App 收集使用个人信息评估工作持续进行，并取得一些进展。目前，工作组接到公民举报信息超过 3480 条，涉及 1300 余款 App。工作组目前针对 30 款用户量大、问题严重的 App 发送了整改通知，要求其根据有关法律法规规范自身运营。

主要问题

被举报的 App 主要集中在金融借贷、社区社交、网上购物、短视频与直播、即时通讯等领域。举报信息所涉及的问题中，26%的 App 没有隐私条款或未在隐私条款中明确收集个人信息的目的、方式、范围；31%的 App 在申请打开收集个人信息相关权限时，未明确告知用户；20%的 App 收集与业务功能无关的个人信息，如金融借贷 App 收集用户通信录；19%的 App 未经用户同意，向他人提供设备 ID、应用程序列表等个人信息；13%的 App 强制索要与业务功能无关的权限，如计算器、手电筒、地理位置权限等。还有一些 App 存在不支持用户注销账户、更正或删除信息等问题。

治理措施

对于问题严重且用户量大的 App，工作组要求运营方认真整改、举一反三，及时纠正个人信息收集使用方面存在的问题，并限期向工作组反馈整改情况。逾期不改的，工作组将建议相关部门公开曝光，对情节严重的做出下架、停止服务等处理。

整治方向

针对当前 App 强制授权、过度索权、超范围收集个人信息等网民反映强烈的问题，将抓紧出台必要的管理规范和相关标准。对于问题严重且不及时整改的 App 运营方，将依法予以暂停相关业务、停业整顿、吊销相关业务许可证或吊销

[1] 《四部门抓紧推进 App 违法违规收集使用个人信息专项治理》，新华社。

营业执照等处罚。

2. 全国公安进一步深入开展“净网 2019”专项行动[2]

行动背景

为进一步深化打击整治网上违法犯罪乱象，努力建设高层次、高水平的平安网络，公安部自 1 月 22 日起在全国范围内组织开展“净网 2019”专项行动。专项行动开展以来，全国公安机关严打侵犯公民个人信息、黑客攻击破坏等违法犯罪，深入整治网络黑产、网络乱象，坚决夯实互联网企业安全主体责任，全力确保网络安全稳定。截至目前，共侦破各类涉网案件 10611 起，对 11058 人采取刑事强制措施。

行动进展

为有效清理违法犯罪信息传播源头，全国公安机关加大对违法犯罪信息多发高发部位的巡查力度，清理各类违法犯罪信息 150 万余条，关停违法违规网络帐号 16 万余个。同时，对部分不认真履行网络安全管理义务的互联网企业加大整治力度。各级公安机关办理各类行政案件 6099 起，关停网站或暂停服务 545 家，对违法信息突出的 225 家网站予以行政罚款处罚，依法约谈整改企业 4147 家，关停违法网络帐号、通信码号、支付帐号等 14 万余个。

此外，公安机关着力打击上游犯罪，加大力度对提供信息支撑、技术支撑和工具支撑的侵犯公民个人信息犯罪、黑客攻击破坏犯罪和非法制售“黑卡”犯罪进行严厉打击，抓获犯罪嫌疑人 1450 余名。

典型案例

（1）北京侦破网上贩卖艺人信息案

今年 2 月，北京德云社文化传播有限公司官方微博发布声明称，其旗下多名艺人住址、行程等信息被泄露。北京市公安局网安总队立即成立专案组开展侦查。2 月 28 日，专案组将犯罪嫌疑人郝某等 3 人抓获。经审查，3 人对贩卖艺人信息牟利的犯罪事实供认不讳。

（2）北京侦破非法控制摄像头案

今年 2 月，北京网安总队侦查发现，一款名为“蓝眼睛”的 APP 注册会员并充值后，能查看涉及多个国家和地区的智能摄像头 10 余万个。3 月，公安机关

[2] 《全国公安进一步深入开展“净网 2019”专项行动》，中国警察网。

在查明涉案人员真实身份及活动轨迹后，在广东深圳将该APP制作人巫某抓获。

（3）内江侦破侵犯公民个人信息案

今年2月，四川省内江市公安局网安支队打掉一个贩卖大学生裸贷信息的犯罪团伙，抓获犯罪嫌疑人10名，查获涉及百余人的女性大学生裸贷信息。经查，2018年6月以来，以贺某为首的违法犯罪团伙，在QQ群和微信群频繁发送贩卖裸贷信息的广告并进行贩卖。

（4）上海虹桥侦破组织考试作弊案

今年3月，上海市公安局虹桥分局民警侦查发现，一犯罪团伙通过事先招揽考生、物色替考人员，在春季高考过程中组织多名在校大学生进行替考作弊。对此，虹桥警方成立专案组开展侦查，打掉以刘某为主的11人替考作弊犯罪团伙。

（5）溧阳侦破“网络水军”案

今年4月，江苏省溧阳市公安机关接到一家企业报警，称发现歪曲事实、诽谤公司声誉的帖子，要求删帖时遭到刊登网站的“有偿删帖”要求。溧阳警方通过4个多月的侦查和调查取证，先后将涉案的14名“水军”抓获。经查，该团伙不到一年作案900余次，非法牟利104万元。

3. 一季度全国网信行政执法数据公布：约谈网站685家，警告网站248家[3]

执法背景

2019年1月，为解决网络生态问题频发、各类有害信息屡禁不止等问题，国家网信办启动为期6个月的网络生态治理专项行动。各级网信部门结合开展“清朗”等专项行动，会同有关部门依法查处网上违法信息和违法行为，严厉处置违法违规网站平台。

查处情况

据统计，全国网信系统依法约谈网站685家，警告网站248家，暂停更新网站125家，会同电信主管部门取消违法网站许可或备案、关闭违法网站2087家，移送司法机关相关案件线索286件。有关网站依照其用户服务协议关闭各类违法违规帐号群组8.9万余个。

[3] 《一季度全国网信行政执法工作取得新成效》，中网网信网。

有关部门依法关闭了大批游戏赌博网站、传播淫秽色情类信息的网站，并要求相关网站依照其用户服务协议关闭大批违法帐号，切实履行企业主体责任，维护网络信息传播秩序。

典型案例

针对部分公司传播低俗庸俗信息、破坏网上舆论生态等问题，国家网信办指导北京市网信办依法约谈相关负责人，责令其立即全面深入整改，整改期间暂停问题产品和频道更新一周；针对个别传播低俗庸俗信息、破坏网络生态的平台，北京市网信办依法约谈相关负责人，责令其全面深入整改，暂停相关频道的更新，并将违规帐号纳入黑名单。

4. 四部门启动“剑网 2019”专项行动[4]

行动简介

近日，上海市网信办约谈了部分新闻网站及 App 负责人，指出他们存在未获得互联网新闻信息服务资质，违规登载新闻信息，内容导向存在偏差，扰乱网络信息传播秩序的行为，责令其停止违法违规行为，开展全面深入整改，并依法做出罚款处罚。

4 月 26 日，国家版权局、国家互联网信息办公室、工业和信息化部、公安部四部门召开 2019 中国网络版权保护与发展大会，宣布启动打击网络侵权盗版“剑网 2019”专项行动。

“剑网 2019”专项行动将坚持以人民为中心的工作导向，高度关注权利人和群众反映强烈的网络侵权问题，不断加大版权执法监管力度，着力规范相关行业版权秩序，积极应对 5G、人工智能、区块链等新技术带来的挑战，不断提升版权管网治网能力，为庆祝新中国成立 70 周年营造良好的网络环境。

整治重点

此次专项行动从 4 月开始启动，将利用 6 个月的时间开展 5 项重点整治：**一是深化媒体融合发展版权专题保护。**严厉打击未经授权转载主流媒体新闻作品的侵权行为，严肃查处自媒体通过“标题党”、“洗稿”方式剽窃、篡改、删减主流媒体新闻作品的行为，依法取缔、关闭一批非法新闻网站（网站频道）及微博帐号、微信公众号、头条号、百家号等互联网用户公众帐号；**二是严格院线电影网**

[4] 《国家版权局等四部门启动“剑网 2019”专项行动》，国家版权局。

络版权专项整治。严厉打击影院偷拍盗录及通过网盘分享、微博微信、淘宝等渠道传播盗版影视作品的行为，着力规范点播影院、点播院线在放映、发行活动中的版权秩序，大力整治通过将服务器设在境外传播盗版影视作品的非法活动；**三是加强流媒体软硬件版权重点监管。**严厉打击 IPTV、OTT 及各类智能终端等流媒体硬件和各种流媒体软件、聚合类软件非法传播他人作品的行为，严厉打击通过电商平台销售各种破解版、越狱版 OTT 产品的行为；**四是规范图片市场版权保护运营秩序。**对图片公司假冒和虚假授权等侵权行为严格查处，大力推动图片公司在涉及版权的经营活动中违法违规行为的治理，使得企业更加合理地维护自己的权利，创造一个稳定有序的图片市场的版权秩序；**五是对网络关键领域版权治理成果进行巩固。**为了对网络影视、文学、动漫、音乐、应用商店、网盘等领域的治理成果进行巩固，应加强对有声读物、短视频、知识共享和网络直播等平台的监管。

官方点评

中央宣传部版权管理局有关的负责人表示，此次专项活动将重点查办突出的案件，全国的版权执法部门也要对行政处罚工作加大力度，尤其对社会危害性大，社会群众反响强烈的违法侵权的互联网应用，要严格调查处理，并提请相关部门采取吊销其电信业务经营许可证、停止为其提供网络接入服务以及注销其 ICP 备案等措施。对可能违反刑法构成犯罪的，应及时将案件移交给相应的公安部门进行处理；更有力的强化平台监管治理，监督各平台积极履行提供违法犯罪线索和配合相应机关调查的义务，网络服务提供商还应履行“通知—删除”的法定责任；加强对于各类典型案件的宣传力度，对不履行相关主体责任的互联网企业进行曝光。执法部门还应当鼓励社会公众加入对企业的监督，鼓励民众举报，并对提供有效线索的举报人进行奖励。

二、相关案例

1. 英国产妇及新生儿个人信息遭大规模泄露[5]

事件背景

Bounty 公司是一家英国母婴用品供应商，其日常商业模式是在国家卫生服务(NHS)医院中向怀孕女性及新生儿父母提供信息包以及婴儿礼品包。此案中，Bounty 公司在 10 个月内泄露了上千万条产妇及新生儿的高度敏感信息，包括出生日期、性别、姓名、地址、妊娠状态等。此类个人信息被重复售卖给不同买家，单条信息最高被重复出售 17 次。英国信息专员办公室调查总监史蒂夫·埃克尔斯利 (Steve Eckersley)表示，纵观 ICO 进行过的个人信息泄露相关调查，该信息泄露案为目前所经办案件中最为严重，影响最广的一次。

事件情况

经过长期调查，英国信息专员办公室依据英国 1998《信息保护法案》对 Bounty 公司处以了高达 400,000 欧的罚款。ICO 认为产妇数据分享并非 Bounty 商业模式下的主要业务，因此可以判定 Bounty 出于营利目的泄露个人信息。此外，由于 Bounty 从未告知顾客会将产妇个人信息传递给第三方的事实，即使顾客同意 Bounty 对第三方共享或传输信息，这些同意也属无效。

Bounty 公司不仅涉及信息泄露问题，其数据来源也存在问题。本次 ICO 调查暴露出 Bounty 公司与多达 79 家医院签订了有偿数据交易合同，向这些医院购买数据，其中不乏牛津大学医院 NHS 基金会等知名机构。据称，Bounty 公司的销售代表可以自由出入合作医疗机构，并向产妇发放个人信息采集表以及儿童福利相关的美国政府官方手册。

对此，英国健康和社会福利部发言人表示，国民健康服务基金会应当确保在其日常运营中始终将病人及其家庭的隐私和数据安全放在优先地位。

[5] 《英国产妇及新生儿个人信息遭大规模泄露》，英国金融时报周末杂志报道。

三、合规前沿

1.《全球百款互联网应用产品个人信息保护测评报告（2018）》在京正式发布[6]

发布背景

4 月 17 日，《全球百款互联网应用产品个人信息保护测评报告（2018）》（以下简称“报告”）在北京大学法学院报告厅对外公开发布。

北京大学互联网法律中心与北京大学粤港澳大湾区知识产权发展研究院联合完成并发布了此报告。北京大学互联网法律中心从 2014 年开始一直关注企业个人信息保护的相关问题，并前后发布了《互联网企业个人信息保护抽样测评报告》2014 版、2015 版和 2017 版。研究项目首席专家、北京大学法学院教授、北京大学粤港澳大湾区知识产权发展研究院执行院长张平女士介绍，相较于往年的报告，今年的报告在测评对象、测评领域及测评标准等方面都有所不同。

报告要点

此次测评共选取了 100 款国内外互联网的应用产品，根据报告内容显示，仅有 5 款 App 的个人信息保护政策总体水平达到了相对优秀的标准，有 35 款 App 表现良好，31 款 App 表现一般，还有 29 款 App 表现不佳。此次测评包含了 18 个领域，个人信息保护政策总体平均得分相对较高的主要集中在云储存类、浏览器类、出行导航类 App，而公益众筹类、航拍软件类、智能停车类 App 总体水平表现得最低，缺乏一个完整的个人信息保护政策。

此次报告对国内外的互联网应用产品的总体得分进行了对比分析，发现：在处理周期以及安全与维护机制方面，域外 App 的总体水平表现更好；而在政策形式和申诉反馈机制方面，域内 App 平均得分相对较高。

报告对比了最近四年的测评情况，发现越来越多的企业对个人信息保护给予了很高的重视并开始逐渐改进相关的保护政策，整体行业表现出在不断提升个人信息保护水平的良好趋势。在本年度的测评中，大多企业在个人信息保护合规上都有了很大改善。但在总体上，互联网企业在个人信息保护上仍有很多问题出现，尤其是涉及收集个人信息以及实现用户的知情同意权的方面，大多企业还有待改善。

[6] 《<全球百款互联网应用产品个人信息保护测评报告（2018）>在京正式发布》，中国新闻网。

合规方向

在经过测评分析后，报告对目前中国有关个人信息的立法和执法现状，以及个人信息保护的现实情况进行了分析。报告认为需要将未来和现在制定法律的相关标准进行统一，使法律体系保持周延一致；也需要统一行政执法，防止多头执法、运动式执法，使得个人信息保护的执法体系更加稳定和健全。除此之外，报告还呼吁社会多方都能参与到个人信息保护的进程中，国家机关要积极作为，企业要对个人信息保护制度不断完善以符合法律的规定，而学术研究机构、媒体等第三方机构则应当在个人信息保护进程中发挥更大的作用，共同构建一个完善的个人信息保护体系。

四、立法动态

1. 民法典人格权编二审稿提请审议——加强未成年人个人信息保护

审议情况

4 月 20 日，十三届全国人大常委会第十次会议召开，全国人大宪法和法律委员会就民法典人格权编草案修改情况进行了汇报。草案二审稿对肖像权、健康权、个人信息保护等方面进行了完善。

草案要点

相关法学教研机构和公众提出，我国应当加大对未成年人个人信息的保护力度，确保没有经过其监护人同意，企业不得收集和使用其个人信息。此外，对于国家机关及其工作人员在工作中知晓的个人信息，也建议增加其保密的义务。在经过相关机构讨论后，上述意见被采纳。因此，在新出台的草案第八百一十四条和第八百一十七条中增加了对此规定的相应条款，详情见下述相关法条内容。[7]

法条摘录

第六章　隐私权和个人信息保护

第八百一十一条　自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。

本法所称隐私是具有私密性的私人空间、私人活动和私人信息等。

第八百一十二条　除法律另有规定或者权利人同意外，任何组织或者个人不得实施下列行为：

（一）搜查、进入、窥视他人住宅等私人空间；

（二）拍摄、录制、公开、窥视、窃听他人的私人活动；

（三）拍摄、窥视他人身体的私密部位；

[7] 《民法典人格权编二审：增加对未成年人信息保护规定》，人民日报。

（四）获取、删除、公开、买卖他人的私人信息；

（五）以短信、电话、即时通讯工具、电子邮件、传单等方式侵扰他人的生活安宁；

（六）以其他方式侵害他人的隐私权。

第八百一十三条　自然人的个人信息受法律保护。

本法所称个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第八百一十四条　收集、使用自然人个人信息的，应当遵循合法、正当、必要原则，并应当符合下列条件：

（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；

（二）公开收集、使用信息的规则；

（三）明示收集、使用信息的目的、方式和范围；

（四）不违反法律、行政法规的规定和双方的约定。

第八百一十五条　自然人可以向信息持有者依法查阅、抄录或者复制其个人信息；发现信息有错误的，有权提出异议并要求及时采取更正等必要措施。

自然人发现信息持有者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求信息持有者及时删除其个人信息。

第八百一十六条　收集、使用或者公开自然人个人信息，有下列情形之一的，行为人不承担民事责任：

（一）在该自然人同意的范围内实施的行为；

（二）使用该自然人自行公开的或者其他已合法公开的信息，但是使用该信息侵害该自然人重大利益或者自然人明确拒绝他人使用的除外；

（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。

第八百一十七条　信息收集者、持有者不得泄露、篡改、毁损其收集、存储的个人信息；未经被收集者同意，不得向他人非法提供个人信息。但是经过处理无法识别特定个人且不能复原的除外。

信息收集者、持有者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、毁损、丢失。发生或者可能发生个人信息泄露、毁损、丢失的情况的，应当及时采取补救措施，依照规定告知被收集者并向有关主管部门报告。

第八百一十七条之一　国家机关及其工作人员对于履行职责过程中知悉的自然人隐私、个人信息，应当予以保密，不得泄露或者非法向他人提供。

2. 公安部网络安全保卫局、北京网络行业协会、公安部第三研究所联合发布《互联网个人信息安全保护指南》[8]

出台背景

为深入贯彻落实《网络安全法》、指导个人信息持有者建立健全公民个人信息安全保护管理制度并采取相关技术措施、有效防范侵犯公民个人信息的违法行为、保障网络数据安全和公民合法权益，在 2018 年 11 月 30 日公安部网络安全保护局发布的《互联网个人信息安全保护指引（征求意见稿）》基础上，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，会同北京网络行业协会和公安部第三研究所等单位，研究制定了《互联网个人信息安全保护指南》（以下简称“《指南》”），《指南》于 4 月 10 日发布。

适用范围

《指南》第 1 章明确了适用对象为“个人信息持有者”，即对个人信息进行控制和处理的组织或个人，正式发布的《指南》将征求意见稿中的“互联网企业”进一步明确为“通过互联网提供服务的企业”，并且包含其他“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”。也就是说，除了传统意义的互联网企业，金融、电信、交通、教育、医疗等行业也包含在内。存有大量公民个人信息的房产中介等企业，也应参考《指南》保护个人信息安全。

与其他法律的相关性

《网络安全法》特别加强和明确了个人信息保护方面的要求，《指南》的业务流程主要是按照《网络安全法》编制的，一些细化要求参考了推荐性国家标准 GB/T 35273—2017《信息安全技术 个人信息安全规范》。另外，根据《网络安全

[8] 《<互联网个人信息安全保护指南>解读》，计算机与网络安全。

法》，国家实行网络安全等级保护制度。《指南》的管理要求、技术要求和应急处置，都与《网络安全等级保护基本要求》(《信息系统安全等级保护基本要求》)的规定一致。以“保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”为目标，也是《网络安全法》的明确要求。另一方面，是否存在“窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息”等行为，也是《公安机关互联网安全监督检查规定（公安部令第 151 号)》的检查重点之一。

与等级保护定级的关系

《指南》并未将网络安全等级保护级别的要求明确为三级。《指南》规定“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，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。而根据征求意见稿，则“应按照 GB/T 22239—2008 7.1 第三级的物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复要求进行安全保护”。在《指南》正式发布后，具体按照《网络安全等级保护基本要求》的哪一级进行保护，需要经过等级保护定级备案后确定。这就意味着，根据影响国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的程度，如涉及个人信息的数量和类别达到一定规模，仍需按照三级甚至更高级别进行防护。

个人信息分级

《指南》中对于“个人信息”的定义借鉴了《网络安全法》当中的定义，与《个人信息安全规范》不同，《指南》并未对“个人敏感信息”进行定义。

匿名化

对于“匿名化”的问题，《指南》直接引用了《网络安全法》中“经过处理无法识别特定个人且不能复原”的定义。而在《个人信息安全规范》中，将“匿名化”定义为“通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。”

用户画像

互联网企业常常使用用户画像作为营销手段之一，其中，如何合法合规地使用个人信息则成为了企业最关注的问题。此次《指南》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”。

3. 简析《互联网个人信息安全保护指南》[9]

四月，公安部网络安全保卫局、北京网络行业协会及公安部第三研究所联合发布了《互联网个人信息安全保护指南》（以下简称“《指南》”）。该《指南》以去年公安部公布的《互联网个人信息安全保护指引（征求意见稿）》（以下简称“《征求意见稿》”）为基础，融合各界意见后最终定稿，是公安系统首个针对个人信息保护的指引性文件，代表了公安机关对个人信息保护工作的理解和态度。

《指南》的效力及适用范围

从效力来看，《指南》并非强制性法律规范。其引言部分说明，《指南》“供互联网服务单位在个人信息保护工作中参考借鉴”。因此，在个人信息保护实务中，企业仍应以现行法律、法规及其配套标准为主要合规标准，在合规方案的细节设计和落地实施中，参照《指南》内容加以完善。

《指南》在“范围”一章从两个维度阐释了其适用标准。一是场景标准，《指南》适用于“个人信息持有者”（对个人信息进行控制和处理的组织或个人）在“个人信息生命周期处理过程中”的“安全保护工作”；二是主体标准，即《指南》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。因此，《指南》并非仅仅针对“互联网公司”，如果传统企业，比如房地产中介或者食品公司，存有大量个人信息，也可以参考《指南》保护个人信息安全。

《指南》的框架及主要内容

从结构上看，《指南》使用“管理、技术、业务及应急”，将个人信息安全保护工作划分为四个部分。简而言之，《指南》所搭建的个人信息保护模型可以归纳为：

“在符合《GB/T 22239 信息安全技术 网络安全等级保护基本要求》（以下简称“《等级保护基本要求》”）相应等级要求的前提下，

（1） 以制度、机构和人员为维度，完善个人信息保护的管理机制；

（2） 在通信网络、区域边界及计算环境等方面，采用相应的技术手段保障个人信息的安全，并对云服务和物联网进行特定的保护；

（3） 在业务层面，注意对个人信息的收集、保存、应用、删除、委托处理、共享、转让及公开披露等环节中的保护；

[9] 《简析<互联网个人信息安全保护指南>》，吴迪。

（4） 建立合理的应急机制，如出现个人信息安全事件，应及时处置和响应。”

1. 管理机制

从管理制度上讲，《指南》建议企业制定个人信息保护的总体方针和安全策略、工作人员对个人信息日常管理的操作规程，建立个人信息管理制度体系以及个人信息安全事件应急预案。同时，完善制度的制定和发布流程，通过审批登记等方式加强制度的执行，并定期对安全管理制度进行评审。

从管理机构上讲，《指南》建议企业设置指导和管理个人信息保护的工作机构、由最高管理者或授权专人负责个人信息保护的工作、设置安全主管、安全管理各个方面的负责人，明确各机构和负责人的职业，以及合理配备和管理相应人员。

从管理人员上讲，《指南》比较细致地列举了关于人员的录用、离岗、考核、教育培训以及外部人员访问等方面的要求，比如录用中的背景调查、上岗时签署的保密协议、离岗后终止离岗人员的所有访问权限等。

2. 技术措施

《指南》并未沿用《征求意见稿》中，统一适用《等级保护基本要求》第三级的要求，而是更灵活地将企业安全技术的基线与企业本身情况相结合，建议“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，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。

《指南》在通用要求部分，从通信网络安全、区域边界安全、计算环境安全及应用和数据安全四个方面对企业的个人信息保护提出了基本的要求，比如在应用和数据安全中，《指南》建议企业应采取校验技术或密码技术，保证重要数据在传输和存储过程中的完整性，包括但不限于鉴别数据和个人信息。

需要注意的是，《指南》对云计算和物联网提出了更高的拓展要求，尤其是在云计算场景下，《指南》明确说明，个人信息原则上应当在中国境内存储，即“应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”。

3. 业务流程

大体来讲，《指南》与《GB/T 35273—2017 信息安全技术 个人信息安全规范》（以下简称“《个人信息安全规范》”）相应部分的框架比较相似。相较于《个人信息安全规范》，《指南》也增加了一些新要求。

其中，有两点需要企业额外注意。一是强调个人信息原则上不可以出境，即 6.2 条 a）款“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”；二是在一般情况下，使用用户画像进行营销推送活动的，尽管无需取得用户的事先授权，但要保证用户拒绝接受该服务的权利，即 6.3 条 c）款“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”。考虑到《个人信息安全规范》可能在近期更新，其他与个人信息保护相关的标准也在起草中，“数据出境”和“个性化展示”两个重要的合规方向，需要每一个涉及个人信息处理的企业重点关注。

此外，《指南》也进行了许多技术细节的规定，比如，在企业收集个人信息时，需要通过身份认证机制、加密以及安全检测和过滤等机制，保证个人信息收集过程中的安全性。

4. 应急处置

《指南》对个人信息安全事件的应急处置区分为应急机制、预案、处置和响应几个部分。与《个人信息安全规范》相比，《指南》强调了企业应建立网络安全风险评估和应急工作机制，以及应急预案应包含的内容，包括应急处理流程、事件上报流程等。《指南》对应急响应培训和应急演练的周期也提出了更严格的要求，即“至少每半年一次”。

结语

我们认为，虽然《指南》并非强制性法律规范，在某些方面也未提出更严格的要求（比如单独界定“个人敏感信息”及其保护规则），但《指南》体现出的特点可能会成为日后执法部门着重审查的合规要点，比如在安全技术上是否满足《指南》的基本要求，比如个人信息是否有跨境传输的情况。考虑到《指南》是继 App 违法违规收集使用个人信息专项治理工作组编制的《App 违法违规收集使用个人信息自评估指南》后，第一个关于个人信息保护的专项文件，我们建议企业要给与足够的重视。

中国首家律师事务所

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987