合规视角下企业处理个人信息的风险检视及制度因应

陶 陶，余飞扬
（安徽大学，安徽 合肥 230039）

摘 要：个人信息保护法对企业的个人信息处理行为和用户个人信息保护提供了明确的法律指引，这也使得企业处理个人信息时面临更复杂的挑战和更多的法律风险，尤其表现在外部合规规范缺乏、用户个人信息生命周期管理和敏感信息不当利用等方面。基于此，要实现企业用户个人信息合规，须在平衡用户个人信息保护和合理利用价值基础上，国家和企业协同发力。一方面，健全合规指引体系、细化个人信息分级分类保护、建立合规激励机制；另一方面，完善“告知-同意”、最短存储时间和删除规则，制定风险评估和应急响应计划，加强技术防护。

关 键 词：企业合规；个人信息保护；“告知-同意”
中图分类号：D923.8 **文献标识码**：A **文章编号**：1671-2250(2023)04-0048-07
DOI:10.13777/j.cnki.issn1671-2250.2023.04.006

2022年中共中央、国务院发布了《关于构建数据基础制度更好发挥数据要素作用的意见》，其明确指出构建数据基础制度要以维护国家数据安全、保护个人信息和商业秘密为前提。企业建立有效合规机制，提升用户个人信息管理水平，是数字时代应有之义。有学者研究企业数据合规的困境和治理路径，将个人信息作为企业数据的内涵之一[1]。有学者研究个人信息保护的合规体系构建[2]。有学者关注在《中华人民共和国个人信息保护法》(以下简称《个保法》)下企业存取数据的风险及合规路径[3]。前述研究多立足于宏观视角讨论企业数据合规和个人信息保护合规，未涉及企业在具体实践中面临的个人信息合规挑战。文章拟立足于个人信息保护和合理利用的价值平衡，检视企业在处理个人信息中面临的法律风险，构建多层次的合规治理体系，以期对合规视角下企业处理个人信息的研究有所裨益。

1 用户个人信息合规的法理基础

1.1 合规内涵及规范依据

企业合规(compliance)是企业为有效防范、识别、应对可能发生的合规风险所建立的一整套公司治理体系[4]。其内涵有三方面：其一是企业经营治理须合乎规则；其二是避免因出现违法行为而承担法律责任；其三是建立外部激励机制[5]。合规风险是其最主要的应对客体。合规风险是企业经营不遵守法律规范，其行为进入法律课责范围[4]。个人信息合规风险亦为，企业违法违规处理个人信息，而致受到行政处罚，乃至被苛以刑事责任。部分学者将企业合规等同于企业刑事合规①，如此是对企业合规内涵的狭隘化理解，不利于合规制度建设。对企业而言，合规治理的依据不仅包括国家法律法规和法律解释，还包含企业自行颁布的规章制度、相关国际法律法规、商业惯例和伦理规范等。

学界过多讨论企业刑事合规，却忽视了民事合规的作用。受中国传统重刑轻民思想影响，时至今日，依赖刑法解决社会问题的做法仍然存在。对此，应充分发挥民法的前置法作用，充分发挥私法即民法在犯罪前端治理上的作用，将绝大部分失范和违法行为拦截在民事违法的范围以内，而不要进入刑法犯罪圈，

收稿日期：2023-03-28
基金项目：安徽省教育厅科学研究项目(YJS20210021)。
作者简介：陶陶(1997-)，男，安徽芜湖人，安徽大学法学院硕士研究生，研究方向：个人信息保护法。

以此实现良法善治之目标[6]。就个人信息合规而言，充分发挥民事法律的前置作用，规范个人信息权益保护，防微杜渐，将能演变成犯罪的风险提前扼杀在民法治理的前端。刑事法律理应保持谦抑性，刑事法律前移代替民事法律规范之位，可能会造成刑法适用过度化。可见，实现有效个人信息合规，应公私法融合，发挥《民法典》《个人信息保护法》在个人信息合规中的核心作用。

1.2　个人信息保护和合理利用的价值衡量

个人信息自决权为个人信息保护的对象，已在学界得到有力论证。其认为个人信息合规一般性要求应为现行法所确立的知情同意原则[2]。但《个保法》所规定的合法、正当、必要和诚信的处理原则，并不排斥个人信息处理者对个人信息经济价值的合理利用。故个人信息合规法理基础应为：在保护和合理利用的龃龉中，衡平个人和信息处理者所关切的利益和非对称的权利结构，以合理安置双方利益。

第一，保护个人信息的价值内涵为保护个人的人格尊严和信息自决权。个人作为目的性的存在，只有消除个人对“信息化形象”被他人操控的疑虑和恐慌，保持其信息化人格与其自身的一致性而不被扭曲，才能有自尊并受到他人尊重地生存与生活[7]。个人信息自决权的核心在于：个人信息的控制权为个人，即个人对与其相关的信息可以决定告知或隐瞒，并且可以决定是告知特定对象还是公开。所有的个人信息都是如此[8]。个人信息自决权与人格尊严密不可分，个人对自身信息的控制恰是为保护其人格自由发展。

第二，个人信息的合理利用价值内涵为经济价值。个人信息天然具有财产性基因，其能够满足商业需要且有可控性和稀缺性[9]。个人信息权益作为标表性人格利益，其经济价值的本质在于他人可通过授权处理内化于个人信息中的经济价值，且个人的人格权益并不会因该处理行为而受损[9]。如个人的健康信息、行踪信息、搜索记录等要素可以和个人发生剥离并存储在其他设备上，他人可在得到许可后实现对其占有和使用。

第三，个人信息保护和合理利用的价值平衡。在个人信息产生、处理、流通的链条上，用户实际处于弱势地位，若以经济价值优先，容易导致企业盲目追求个人信息数据所带来的利益，从而忽视用户的人格尊严和信息自决权，诱使用户的个人信息权利蒙受损害。个人信息保护中蕴含的人格尊严和数据主体控制权的价值更侧重于保护处于弱势方的用户。《个保法》通过规定个人信息的处理规则、跨境提供规则等，对个人信息处理者课以较重义务，从而增强个人的权利救济，实现有差别的平等。但《个保法》对用户个人信息的保护，并不意味着完全牺牲企业的利益。2022年，我国大数据产业规模增加到1.57万亿元，同比增长18%[10]。个人信息作为数字经济的重要生产要素，其流通、利用有助于企业精确定位市场需求，从需求倒逼供给，也有利于企业更好地对供给端进行升级改造。事实上，如果信息处理者对于任何信息进行任何处理都要花费不合理的成本来确定是否侵害他人的个人信息权益，或者允许信息主体频频打断信息的流通和传播，将严重影响信息产业的发展[11]。可见，在保护用户个人信息的前提下，对个人信息数据应是合理利用，任何片面做法都会打破二者之间的平衡，损害一方乃至双方利益。

2　企业用户个人信息合规的法律风险检视

合规制度引入我国时间较短，企业合规意识较为淡薄，用户个人信息保护长期缺失。随着立法对个人信息保护的重视，企业在处理用户个人信息时将面临更为复杂的法律风险。

2.1　外部合规规范缺乏

用户个人信息保护合规缺乏具体指引。《个保法》规定了个人信息处理者在个人信息生命周期管理中的义务，划定了个人和信息处理者之间的权利义务关系。但实际上，我国企业数量多，体量分层明显，分布行业广。中小型企业囿于资金、人员规模和收集场景，难以从《个保法》中得到有效的合规指引。相较于互联网企业，仍有许多企业收集个人信息的方式为线下面对面收集，对于这些个人信息的处理也亟待监管部门出台实施细则。《个保法》62条也提出网信部门要统筹协调制定个人信息保护的具体规则、标准。再如《旅游法》和《商业银行法》也规定了在旅游和金融方面收集的个人信息受到保护，但具体的监管和保护细则并未出台。如此不仅会使用户面临没有相应监管机构保护的窘境，还会导致缺乏监管的企业漠视用户个人信息保护。

2.2 用户个人信息生命周期管理风险

信息生命周期(Information Lifecycle)理论发端于信息资源管理领域。1985 年,霍顿(F. W. Horton)提出,信息是一种具有生命周期的资源,其由一系列逻辑上相关联的阶段或步骤组成。该阶段包括需求定义、收集、传递、处理、储存、传播、利用等[12]。个人信息生命周期正是上述理论的应用。在用户个人信息“收集—使用—存储—删除”的信息生命周期管理流程中仍存在合规风险。

2.2.1 违法收集用户个人信息

违法收集主要表现在非法收集和过度采集用户的个人信息。常见场景分别是向用户直接采集、向第三方采集、通过爬虫获得数据,核心风险是未贯彻“告知–同意”规则,未满足充分告知、自愿同意、明确授权、变更再次告知并征得同意、允许撤回同意等完整的规范要求[1]。2023 年 3 月 21 日,工信部发布了 55 款 APP(SDK)存在侵犯用户权益行为的通报②。主要涉及问题为企业违反正当性、合法性、必要性、透明性、最小化原则。如违规、超范围收集个人信息;APP 信息明示不到位;APP 强制、频繁、过度索取权限等。例如某案涉 APP 未显示隐私政策条款,未尽到告知义务,违法超范围收集大量非必要个人敏感信息,最终法院组织双方调解,要求案涉 APP 按照法律法规认真整改,否则其自愿支付 50 万违约金用于个人信息保护的公益支出③。

2.2.2 违法使用用户个人信息

违法使用主要表现为:其一,未经用户授权,擅自向第三方共享或出售个人信息、通过自动化决策向用户进行不可拒绝的个性化推送等。其二,同第三方关联用户个人信息,违反“告知–同意”规则,侵害用户知情权等个人信息权益。公民个人信息泄露,不仅会严重侵扰个人生活安宁,更有可能引发个人人身、财产权益受损。如杭州互联网法院审理的“吴某某诉某电商平台案”④,某电商平台未经用户同意将用户信息提供给第三方,给吴某某造成人格尊严等精神损害,亦终致其败诉并承担相应法律责任。

2.2.3 用户个人信息存储风险

用户个人信息存储法律风险在于:一是超出“为实现处理目的所必要的最短时间”;二是存储技术不当导致用户个人信息泄露。对第一种情况,《个保法》第 19 条规定的“所必要的最短时间”易产生争议,亟待细化。对第二种情况,其一为外部非法技术入侵。如使用非法计算机程序、网络钓鱼、恶意软件等窃取目标企业的用户信息。例如,蔚来汽车内部用户数据遭窃取被勒索 255 万美元等额比特币⑤。其二为内部合规不规范,员工违规泄露用户个人信息。如某通信公司员工将客户手机号及验证码出售给他人,以谋取个人利益⑥。未经匿名化和去标识化处理的用户个人信息包含大量有效信息。这些信息一旦泄露,用户个人隐私会被严重侵犯,用户人身、财产安全将遭受严重威胁。同时企业也将承受声誉和经济等多重损失。

2.2.4 用户个人信息删除未全面落实

个人无法请求删除与其相关的个人信息,其个人信息自决权亦为空中楼阁。为此,个人在符合法律规定或约定情形下,可请求信息处理者及时删除与其相关的个人信息[13]。《个保法》对个人信息删除的规定主要为五大删除情形(第 47 条)和逝者近亲属对逝者个人信息的删除(第 49 条)。笔者于 2023 年 4 月 10 日选取购物、社交、影视、分享、出行等领域内共十个 APP,对其当前生效隐私政策中有关个人信息删除的规定进行了整理(见表 1)。

根据表 1,可见在个人信息删除上主要存在三方面法律风险:第一,有部分 APP 在隐私政策中未设置个人撤回同意删除条款,不符合《个保法》第 47 条第 1 款第 3 项之规定。第二,对于逝者个人信息的删除,其中大量 APP 没有提及。逝者个人信息包含着人格和财产利益,若处理不当会侵犯逝者及其近亲属的人格权益。第三,关联第三方的个人信息删除,只有淘宝、拼多多和高德规定“尽可能通知”和“要求其及时删除”。个人信息处理者同第三方共享、委托和合作处理的用户个人信息,必须严格监督,若第三方侵害用户个人信息权益,个人信息处理者有承担连带责任的风险。除此之外,互联网企业能较为便捷地实现用户个人信息删除,但实践中,个人信息在诸多情形下面临删除难题,如用户在健身房、蛋糕店、咖啡店等店铺充值会员卡所留下的个人信息。

2.3　用户敏感信息不当利用风险

我国立法界定敏感个人信息采用“抽象概括+列举”模式，在该模式下企业应区分出敏感信息并对其特别保护。侵犯用户敏感信息，主要为采集超出必要性和最小化原则；误导欺骗用户，利用敏感信息牟利等。个人敏感信息泄露会给个人带来严重困扰，甚至诱发刑事犯罪。如北京某公司开发的APP违法采集儿童的面部识别特征、声音识别等个人敏感信息，通过自动化决策，将儿童短视频推送给目标用户。徐某某在浏览该APP所推送的视频后，利用视频中所含的儿童个人信息，在APP上和多名儿童进行联系，最终致使其中3名儿童被其猥亵侵犯。该公司的行为严重侵犯了儿童的个人信息权益，给儿童的人身安全造成极大威胁。余杭区人民检察院对该公司提起了民事公益诉讼⑦。

表1　十大APP隐私政策中个人信息删除权的规定

应用名称	个人撤回同意	逝者个人信息删除	关联第三方个人信息删除
淘宝	未规定	未直接提及	尽可能通知从我们处获得您的个人信息的主体，并要求其及时删除
京东	未规定	未提及	无规定
拼多多	未规定	未提及	尽可能通知从我们处获得您的个人信息的主体，并要求其及时删除
微信	未规定	联系客服	无规定
爱奇艺	有规定	未提及	无规定
抖音	未规定	有专门规定	无规定
百度APP	有规定	未提及	无规定
高德	未规定	未提及	尽可能通知从我们处获得您的个人信息的主体，并要求其及时删除
小红书	有规定	未提及	单独说明使用第三方服务受第三方隐私政策约束
知乎	有规定	联系客服	无规定

2.4　过错推定责任易导致企业举证不能

《个人信息保护法》第69条规定的个人信息处理者过错推定责任在价值取向上是为强化保护个人信息权益，但其实质基础在于处理者的处理行为引发的法定作为义务[14]。从实际观之，个人信息处理者和个人在举证能力上并不对称，举证证明个人信息处理者具有过错对个人而言存在障碍。欧盟《一般数据保护条例》(General Data Protection Regulation)第82条规定，数据的控制者和处理者都适用无过错责任，受害人在要求控制者或处理者承担责任时，无需证明其存在过错[15]。适用过错推定原则目的是加重信息处理者的举证义务，消弭信息处理者和个人之间不平等地位。这也意味着，企业要将个人信息合规落到实处，不能停于纸面、流于形式，否则将会面临举证不能的法律困境，以致承担举证不能的不利后果。如某房地产开发商未能举证证明其对陈某的个人信息尽到保护义务，因其举证不能，法院最终判决其侵犯陈某的个人信息权益，承担侵权责任⑧。

3　用户个人信息合规的实现路径

面对个人信息保护的复杂情形，传统的公私法分立模式显得力有不逮。用户个人信息保护不能基于法律调整的一元思维，需要寻找一个能使多元主体参与的全新保护模式。笔者以为，企业在个人信息保护中居于不可或缺的地位，个人信息保护需要国家和企业协同发力，在平衡保护和合理利用价值基础上，构建全方位、多层次、全过程、高效率的保护体系。

3.1　国家层面：健全合规指引体系、细化个人信息分级分类保护、建立合规激励机制

3.1.1　健全企业用户个人信息合规指引体系

首先，《个人信息保护法》《数据安全法》《网络安全法》确立了个人信息处理的基本原则和主要规则。其次，《旅游法》(第52条)《商业银行法》(第29条)规定在旅游经营和银行存贷款中要对用户的个人信息保密，但未规定监管主体、监管措施和泄露用户信息的法律责任。由此会导致保密条款的宣示意义大于实际意义。为此，应当在监管空白领域，逐步出台监管细则，以行政法规或部门规章形式，规定监管主体、审

查内容、监管措施和法律责任。最后,《个保法》62 条提出要制定个人信息保护的相应细则,针对小型处理者制定专门的个人信息保护规则。对于非平台和小型平台经营者,可以按类进行划分,出台针对化、具体化的个人信息收集范围和处理方式。可参考国资委发布的《中央企业合规管理办法》和“四部门”联合印发的《常见类型移动互联网应用程序必要个人信息范围规定》。

3.1.2 细化个人信息分类分级保护制度

个人信息分类分级具有重要的法益识别和风险防范功能[16]。当前,《个保法》将个人信息区分为一般信息和敏感信息,将非敏感信息笼统归为一般信息,做相同保护,不利于平衡保护和利用。为此,可对个人信息分类进一步细化,区分为强等级、中等级和弱等级,每个等级制定相应保护规则。强等级保护最为严格,其主要为用户最重要的敏感信息。企业不可随意采集和滥用,必须遵循合法、合理、必要、最小化原则,且要征得用户明示同意。在处理个人信息时,必须得到用户明确授权。中等级保护略弱于强等级,在处理中等级个人信息时,须履行“告知–同意”规则,在合法、合目的、必要、最小化原则下处理,用户享有《个保法》所规定的各项个人信息权益。弱等级的保护则兼顾企业对个人信息的合理利用。对于弱等级的用户个人信息,在收集、处理时可采用数据主体默示同意规则。但为防止企业滥用弱等级信息默示同意规则,可赋予数据主体抗辩权,即援引明示同意规则对抗企业对弱等级个人信息的滥用。

3.1.3 建立企业合规激励机制

个人信息的监管和治理本属于政府公共职责,但囿于执法资源短缺,难以实现全方位、无死角治理。为更好地实现个人信息保护,需鼓励企业在个人信息处理过程中进行合规治理。因此,可配套行政或刑事激励措施,激发企业合规内生动力。行政监管激励机制主要为:一是阻断行政处罚,作为减轻或免除行政处罚的事由;二是与行政机关达成和解协议,主动缴纳罚款,积极赔偿被害人或单位经济损失,约定在考验期内建立有效合规机制,并通过第三方评估,行政机关可据此对其作出从轻或减轻处罚的决定。行政合规激励措施在证券监管领域已有应用。

刑事合规激励主要为:涉案企业在公诉机关规定期间内完成合规整改,并通过第三方评估符合有效性标准,公诉机关可据此给予其不批准逮捕、不起诉、宽缓量刑建议等多种宽缓检察措施。目前司法实践中刑事激励机制主要有以下四个表现:其一,涉单位犯罪企业通过事后合规整改换取刑罚从宽待遇。其二,合规不起诉、合规从宽量刑建议等检察措施可同时惠及合规整改企业成员。其三,当企业内部人员涉嫌自然人犯罪(企业未涉嫌单位犯罪)时,事后合规整改是自然人获得从宽待遇的条件。其四,企业人员侵害本单位利益而构成纯自然人犯罪时,被害单位积极进行事后合规整改,检察机关对企业加害人进行从宽处理[17]。其中,刑事合规激励的受益主体范围、相对不起诉的适用条件和合规不起诉同刑事诉讼法的衔接仍需理论界和实务界深入探索。

需注意的是,在配套激励时,主办机关须确定企业是否将合规治理落到实处,对弄虚作假的企业,仍要严厉惩处,以此确立切实合规的正确导向。

3.2 企业层面:制定企业合规规章、落实个人信息保护具体规则

3.2.1 制定企业合规规章,切实落实合规制度

企业根据自身经营类型、市场定位、未来发展等,制定个性化用户个人信息合规规章制度。第一,发挥合规规章的约束作用,组织员工定期学习合规知识,明令禁止不合规行为,培育企业合规文化。第二,制定分级、授权访问机制,做到用户个人信息访问留痕,以防无权限的员工访问。第三,如前文所述,信息处理者承担过错推定责任,因此,企业在合规过程中,必须发挥“合规规章”的软法作用,认真贯彻落实,避免合规纸面化、形式化,进行定期或不定期检查。全面落实合规章程,做到合规全流程留痕,是切断企业责任和员工个人责任的关键。如“雀巢员工侵犯公民个人信息案”⑨,该案中雀巢公司证明已尽注意义务,将员工违法行为同企业行为分离,使其未陷入“单位犯罪”。

3.2.2 细化“告知–同意”规则

在前述工信部通报的 55 款 APP 里,有约 22%的 APP 存在 APP 信息明示不到位问题。“告知–同意”

完善思路如下：一是改进告知方式，企业在告知时应快捷地使用户知晓。二是完善告知内容。《个保法》规定告知的内容，应全部向用户告知，尤其是后续对用户信息利用所带来的不确定风险也应当一并告知用户[18]。三是针对不同等级个人信息，制定相应告知模式。用户个人敏感信息收集和处理的限制最为严格，针对敏感个人信息，应用显著标识告知用户，改变以往同质化的告知方式。在收集时要遵守合法、合目的、必要和最小化原则。如可在隐私政策中列举敏感信息收集种类并表明收集目的。四是要向用户提供更为便捷地撤回同意的选项。五是不得因用户不同意或撤回同意处理其个人信息而不提供产品或服务，亦不能因用户不同意提供非必要个人信息而拒绝用户使用产品的基本功能。

3.2.3　完善个人信息删除路径

删除权合规核心在于建立全链条用户数据删除机制。其一，要为用户提供方便快捷的删除选项和易懂的操作说明，同时告知用户删除的信息内容。其二，企业要在隐私政策中规定个人撤回同意可以请求删除。其三，对逝者的个人信息，企业应当在隐私政策中规定请求删除的主体、所需提供的材料、申请方式和受理期限等，尤需注意的是，该流程应简便可行，不可使权利主体陷入权利无法救济的窘境。其四，要实现全链条删除。用户不仅要能删除运营商或直接收集个人信息的企业所存储的信息，还要能删除存储在关联第三方上的个人信息。其五，要使用户有效删除信息，并提供删除的替代措施。用户删除信息原则上要做到彻底删除，若存在法律、行政法规规定的保存期限未届满，或技术上无法彻底删除的情形，应当停止存储，对已存储的个人信息进行访问和处理限制直至将备份清除或实现匿名化，并且要告知用户原因以及后续去标识化的处理手段、安全保障方式等。其六，对于没有应用软件的小微企业，如健身房、咖啡店等，应在出现《个保法》第47条情形时，主动删除用户个人信息。未主动删除时，当用户行使个人信息删除请求权，其应删除存储的用户信息。

3.2.4　细化最短存储时间规则

笔者认为个人信息存储时间规则的合规在于：第一，遵守法律法规规定的个人信息存储最短时间。例如《中华人民共和国电子商务法》要求商品和服务信息、交易信息保存时间自交易完成之日起不少于三年；《电信服务质量监督管理暂行办法》要求计费原始数据保存期限为5个月；《网络餐饮服务食品安全监督管理办法》要求网络订餐的订单信息保存时间不得少于6个月。第二，《个保法》要求最短存储时间为“实现处理目的所必要的最短时间”；《信息安全技术–个人信息安全规范》对个人信息处理者的要求为“实现个人信息主体授权使用的目的所必需的最短时间”。上述规范采用最小化原则即“所必要的最短时间”，皆未提供具体的最短时间判断标准。此处最小化原则给个人信息处理者提供依据自身情况处理的空间，但模糊表述较易产生诉争。对此，笔者以为，企业在个人信息存储最短时间上，应根据其所涉及业务特点，充分评估实现处理目的所要的最短时间，告知用户存储期限的判断依据或列举部分个人信息的使用期限，避免只在隐私政策中规定类似于“服务所需必要期限内”的笼统性条款。比如，淘宝网就在隐私政策中规定了存储期限的主要依据标准；爱奇艺则是采取列举部分个人信息存储期限加提供判断标准的模式⑩。

注释：

①如叶良芳教授在《刑事一体化视野下企业合规制度的本土化构建》一文中，默认企业合规即企业刑事合规。

②参见工信部通报！这55款APP(SDK)存在侵害用户权益行为 https://mp.weixin.qq.com/s/GAJqX0cNLu3KwWBkJ7KdWw，最后访问于2023年3月22日。

③参见杭州市互联网法院(2020)浙0192民初4252号。

④参见杭州互联网法院(2021)浙0192民初2929号。另参见杭州中院(2021)浙01民终12780号。

⑤《蔚来深陷用户数据“泄露门”！过度收集信息导致隐私难保护……》，载中国消费者报，https://mp.weixin.qq.com/s/UC27mWXinlcs_e4lRRr3Mg，最后访问于2023年3月22日。

⑥参见浙江省高级人民法院发布侵犯公民个人信息犯罪十大典型案例之九：台州市路桥区唐某侵犯公民个人信息案——通信公司员工利用营销之便出售他人手机号及验证码构成侵犯公民个人信息罪 https://www.pkulaw.com/pfnl/95b2ca8d4055fce1fc2ff9a67be6fb40b0a0debfd093fa55bdfb.html.

⑦参见检例第 141 号:浙江省杭州市余杭区人民检察院对北京某公司侵犯儿童个人信息权益提起民事公益诉讼。

⑧全省首例:株洲中院公开宣判一起房地产开发商侵犯购房人个人信息案 http://zzzy.hunancourt.gov.cn/article/detail/2022/12/id/7056031.shtml

⑨参见兰州市城关区人民法院(2016)甘 102 刑初 605 号刑事判决书。另参见兰州市中级人民法院(2017)甘 01 刑终 89 号刑事裁定书。

⑩参见《淘宝网隐私政策》第五章第一节和《爱奇艺隐私政策》第五章第一节。笔者于 2023 年 5 月 24 日最后访问其隐私政策。

参考文献:

[1]毛逸潇. 数据保护合规体系研究[J]. 国家检察官学院学报,2022(2):84-100.

[2]敬力嘉. 个人信息保护合规的体系构建[J]. 法学研究,2022(4):152-167.

[3]刘建华,张智翔. 个人信息保护法视角下企业存取数据的合规化管理[J]. 人民检察,2022(15):74.

[4]陈瑞华. 企业合规的基本问题[J]. 中国法律评论,2020(1):178-196.

[5]陈瑞华. 企业合规基本理论(第二版)[M]. 北京:法律出版社,2021:07-12.

[6]刘艳红. 民刑共治:中国式现代犯罪治理新模式[J]. 中国法学,2022(6):27-46.

[7]张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学,2015(3):38-59.

[8]杨芳. 个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体[J]. 比较法研究,2015(6):22-33.

[9]彭诚信. 论个人信息的双重法律属性[J]. 清华法学,2021(6):78-97.

[10]国家互联网信息办公室. 数字中国发展报告(2022 年)[EB/OL]. (2023-05-23)[2023-06-08]. http://www.cac.gov.cn/2023-05/22/c_1686402318492248.htm.

[11]黄薇. 中华人民共和国民法典人格权编解读[M]. 北京:中国法制出版社.2020:219.

[12]万里鹏. 信息生命周期研究范式及理论缺失[J]. 中国图书馆学报,2009(5):36-41.

[13]王利明. 论个人信息删除权[J]. 东方法学,2022(1):38-52.

[14]王道发. 个人信息处理者过错推定责任研究[J]. 中国法学,2022(5):103-121.

[15]杨立新. 侵害个人信息权益损害赔偿的规则与适用——《个人信息保护法》第 69 条的关键词释评[J]. 上海政法学院学报(法治论丛),2022(1):1-15.

[16]张勇. 敏感个人信息的公私法一体化保护[J]. 东方法学,2022(1):66-78.

[17]冀洋. 企业合规刑事激励的司法限度[J]. 比较法研究,2023(2):186-200.

[18]王俊,张雅婷,郭美婷,等. 个人信息保护法企业合规启示报告[J]. 网络信息法学研究,2021(2):114-165.

Risk Review and Institutional Response of Enterprises' Handling Personal Information from the Perspective of Compliance

TAO Tao, YU Feiyang

(Anhui University, Hefei Anhui 230039)

Abstract: The PIPL provides clear legal guidance for enterprises' personal information processing behavior and users' personal information protection, which also makes enterprises face more complex challenges and more legal risks when handling personal information, especially in the lack of external compliance norms, the management of users' personal information and the improper use of sensitive information. Based on this, in order to achieve compliance with the personal information of enterprise users, the state and enterprises must make concerted efforts on the basis of balancing the protection of users' personal information and the value of reasonable use. On the one hand, we should improve the compliance guidance system, refine the hierarchical and categorical protection of personal information, and establish a compliance incentive mechanism. On the other hand, we should improve the "inform-consent", minimum storage time and deletion rules, formulate risk assessment and emergency response plans as well as strengthen technical protection.

Key Words: corporate compliance; personal information protection; inform consent

(责任编辑:刘阳雄)