

2021
NO. 09



数据合规资讯月报
Data Compliance Monthly Newsletter

天达共和律师事务所

East & Concord Partners

摘要

尊敬的各位客户、同仁：

欢迎参阅天达共和律师事务所数据合规团队为您呈现的《数据合规资讯月报》2021 年第九期，本期月报主要包括：

- **立法动态**

介绍 2021 年 8 月 26 日至 2021 年 9 月 25 日期间及前后境内外数据保护立法动态，并针对部分立法动态提供简要评论。

- **执法聚焦**

介绍 2021 年 8 月 26 日至 2021 年 9 月 25 日期间及前后境内外部分典型执法案例，并针对部分执法活动提供简要评论。

- **行业新闻**

精选 2021 年 8 月 26 日至 2021 年 9 月 25 日期间及前后互联网及相关行业与网络安全和数据保护有关的新闻资讯。

- **热点评述**

2021 年 8 月 20 日，《中华人民共和国个人信息保护法》（以下称“《个保法》”）通过并发布，将于 2021 年 11 月 1 日起正式生效。《个保法》是我国第一部关于个人信息保护的专门性基本法律，本期热点评述我们将通过对《个保法》重点问题的解读，理清法律脉络，希望为企业研究合规对策提供借鉴。

目 录

摘 要	1
目 录	2
立 法 动 态	3
➢ 境内立法	3
➢ 境外立法	6
执 法 聚 焦	8
➢ 境内执法	8
➢ 境外执法	10
行 业 新 闻	11
➢ 境内新闻	11
➢ 境外新闻	13
热 点 评 述	14

立法动态

境内立法

- 8月27日，为了规范互联网信息服务算法推荐活动，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进互联网信息服务健康发展，国家互联网信息办公室（“国家网信办”）起草了《互联网信息服务算法推荐管理规定（征求意见稿）》（以下称《算法管理规定》），并向社会公开征求意见。

（http://www.moj.gov.cn/pub/sfbgw/lfyjzj/lflfyjzj/202108/t20210827_436209.html）

简析：《个保法》中专条对于个人信息处理者利用个人信息进行自动化决策的处理活动进行了规定，明确要求保证决策的透明度和结果公平、公正等。虽然自动化决策并非算法的唯一应用，自动化决策依据的数据也非仅限于个人信息，但是算法作为自动化决策以及人工智能技术的基础且核心要素，对于“算法公正”的管理要求早就引起社会普遍关注。本次《算法管理规定》征求意见稿针对的适用范围广泛，几乎涵盖所有算法类型和服务领域，显示了监管层对于网络安全和数据保护的管理向技术层面深化的倾向。其中针对算法推荐服务提供者提出的一系列管理合规要求，分类分级管理及对应的备案等管理要求，都值得相关企业高度重视。9月29日，国家网信办、中央宣传部、教育部、科学技术部、工业和信息化部（“工信部”）、公安部、文化和旅游部、国家市场监督管理总局（“市场监管总局”）、国家广播电视总局等九部委制定了《关于加强互联网信息服务算法综合治理的指导意见》，明确提出计划利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。算法管理将成为下一个监管重点领域。

- 8月29日，深圳市召开第七届人民代表大会常务委员会第三次会议，《深圳经济特区数字经济产业促进条例（草案）》（“《条例（草案）》”）提请会议审议，以进一步优化数字经济产业发展环境。《条例（草案）》提出要依法设立数据交易场所，探索开展数据跨境流通交易。《条例（草案）》明确，要率先建立数据生产要素会计核算制度，建立数字知识产权快速预审机制，将优质数字产品纳入深圳手信名录。

（http://www.sz.gov.cn/cn/xxgk/zfxxgj/zwdt/content/post_9093276.html）

简析：继今年7月6日正式发布《深圳经济特区数据条例》之后，深圳市在大数据立法上再发力，意图进一步优化数字经济产业发展环境。继通过《深圳经济特区数据条例》确立数据的财产权，借以解决数据交易中确权问题的基础上，《条例（草案）》又在全国首次提出探索建立数据生产要素会计核算制度，希望借此突破数据交易中数据定价的难题。《条例（草案）》还明确规定依法设立数据交易场所，制定交易制度规则和行业标准，探索开展数据跨境流通交易、数据资产证券化等交易模式创新。深圳在数据要素市场的立法中已经先行先试迈出了重要的步伐。

- 9月1日，《上海市促进城市数字化转型的若干政策措施》（“《若干政策措施》”）正式生效，成为上海市数字化转型制度体系的重要组成部分。《若干政策措施》提出，到2025年，推动上海数字经济核心产业增加值进一步提高，着力形成上海城市数字化

转型的制度框架体系。同时，着力强化目标引领、制度供给、精准服务、统筹推进，聚焦经济、生活、治理重点领域高频急难问题，立足于全方位激发各类主体的转型活力和动力。

（http://www.gov.cn/xinwen/2021-09/02/content_5634970.htm）

简析：上海作为我国经济中心，在城市数字化转型的浪潮中当然不能甘居人后。本次《若干政策措施》提出全面激发经济数字化创新活力、全面提升生活数字化服务能力、全面提高治理数字化管理效能、数字化转型建设多元化参与、系统全面的数字化转型保障5方面共27项政策制度和保障措施。《若干政策措施》中诸多亮点值得关注，例如推进国企数字化转型“一把手”负责制，探索“首席数字官”制度等。

- 9月3日，中国证券监督管理委员会（“证监会”）发布《证券期货业网络安全等级保护基本要求》、《证券期货业网络安全等级保护测评要求》2项金融行业标准（“两项标准”），自公布之日起正式施行。

（http://www.csrc.gov.cn/pub/newsite/zjhxwfb/xwdd/202109/t20210903_404764.html）

简析：自《网络安全法》明确建立网络安全等级保护制度之后，《数据安全法》再次强调了网络安全等级保护制度对于企业履行数据安全保护义务的基础作用。各行业监督管理部门在制定本行业数据分类分级规则和重要数据具体目录的同时，也在明确本行业网络安全等级保护的具体要求。本次的两项标准对证券期货业进一步落实好网络安全等级保护工作相关要求具有非常重要的意义。两项标准分别规定了证券期货业网络安全等级保护的总体要求，以及第一级到第四级等级保护对象的安全通用要求和安全扩展要求，适用于证券期货业分等级的非涉密对象的安全建设和监督管理；以及证券期货业网络安全等级保护的等级测评方法、第一级到第四级的网络安全等级保护对象的测评要求、整体测评以及测评结论，明确适用于证券期货业安全测评服务机构、等级保护对象的运营使用单位及行业主管部门对证券期货业等级保护对象的安全状况进行安全测评，也可供网络安全职能部门进行证券期货业网络安全等级保护监督检查时参考使用。

- 9月13日，为贯彻落实《中华人民共和国网络安全法》《网络产品安全漏洞管理规定》，规范网络产品安全漏洞收集平台备案管理，工信部起草了《网络产品安全漏洞收集平台备案管理办法（征求意见稿）》，并公示听取社会各界意见。

（https://www.miit.gov.cn/gzcy/yjzj/art/2021/art_50884c2ec2864fdf9205510562ecaf9b.html）

- 9月15日，工信部发布《关于加强车联网网络安全和数据安全工作的通知》（“《通知》”），以健全完善车联网安全保障体系，加强车联网网络安全和数据安全管理工作。《通知》指出要落实安全主体责任，全面加强安全保护，加强智能网联汽车安全防护，加强车联网网络安全防护，加强车联网服务平台安全防护，加强数据安全保护，健全车联网安全标准体系。

（http://www.gov.cn/zhengce/zhengceku/2021-09/16/content_5637709.htm）

简析：汽车关系百姓出行，随着车联网技术和应用的发展，汽车数据以及网络通信技术与汽车、电子、道路交通运输等领域深度融合的车联网越来越成为监督管理的重要领域。《通知》以智能网联汽车生产企业、车联网服务平台运营企业、基础电信运营企业等相关企业为管理对象，对于网络安全和数据安全提出了基本要求和具体措施。其中涉及强

化数据出境安全管理，明确了在车联网数据的出境管理中，由所在省（区、市）通信管理局、工业和信息化主管部门进行安全评估的报备工作等内容，值得重点关注。

- 9月15日，国家网信办发布了《关于进一步压实网站平台信息内容管理主体责任的意见》（“《意见》”），旨在充分发挥网站平台信息内容管理第一责任人作用，引导推动网站平台准确把握主体责任，明确工作规范，健全管理制度，完善运行规则，切实防范化解各种风险隐患，积极营造清朗网络空间。国家网信办有关负责人指出，出台《意见》的主要目的，是为了聚焦各类网络乱象，着力破解网站平台履行信息内容管理主体责任存在的认识偏差、管理失范、能力不足、效果不彰等突出问题，指导督促网站平台补短板、强弱项、提水平，确保网站平台始终坚持正确的政治方向、舆论导向和价值取向。

（http://www.cac.gov.cn/2021-09/15/c_1633296789845827.htm）

简析：网络平台的信息内容生态管理仍将是监管的重点领域。

- 9月22日，中国银行保险监督管理委员会发布了《商业银行监管评级办法》（“《办法》”），将“数据治理”纳入商业银行监管评级要素。《办法》的发布和实施进一步完善了商业银行监管规则，为加强商业银行非现场监管、发挥监管评级的重要作用提供了制度保障，有利于合理分配监管资源、增强监管能力，有利于引导银行完善风险防控、筑牢全面风险管理体系，有利于完善金融风险预警和处置机制，守住不发生系统性金融风险底线，维护金融稳定和国家金融安全。

（<http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=1008577&itemId=915&generaltype=0>）

➤ 境外立法

✧ 英国

- 9月2日，英国《适龄设计规范》（Age appropriate design code, “AADC”）生效，在线服务提供者在使用儿童数据时需要遵循15个标准，以确保他们履行数据保护法规定的义务，保护儿童的在线数据。基于欧盟《通用数据保护条例》（GDPR），AADC主要对在线服务情景下的儿童数据保护设立了具体标准。英国信息委员办公室（Information Commissioner’s Office, “ICO”）网站相关信息介绍，如果某在线服务网站很可能被18岁以下的儿童访问，即使该网站不是针对儿童，那么该网站也应当遵循AADC的要求。自AADC生效之日起，企业有12个月的时间实施必要的修改。

（<https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>）

✧ 欧盟

- 9月13日，欧盟网络安全署（“ENISA”）发布了一项网络安全评估方法（“SCSA”），用于行业ICT系统的网络安全认证。ENISA官网介绍，该文件为ENISA的利益相关者提供了一个全面的ICT安全评估工具和行业网络安全认证方案。应用SCSA将产生有关行业ICT系统和相关利益方之间关系的可靠信息，提供与ICT相关风险的透明度，以及优化行业ICT系统、ICT安全实施的潜力。

（<https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>）

✧ 澳大利亚

- 9月12日，根据澳大利亚联邦警察官网的报道，一项新通过的监视立法修正案（识别与干扰）将允许澳大利亚联邦警察（Australian Federal Police, “AFP”）和澳大利亚刑事事情报委员会（Australian Criminal Intelligence Commission, “ACIC”）添加、复制、更改和删除计算机中的数据，以阻止在线发生的严重刑事犯罪。AFP或ACIC必须有合理理由怀疑控制在线账户对于获取有关严重刑事犯罪的证据是必要的，且只能在获得联邦法官或指定行政上诉法庭成员的合格授权书授权的情况下才能执行此操作。

（<https://www.afp.gov.au/news-media/media-releases/fast-facts-afp-powers-under-slaid-legislation>）

✧ 沙特

- 9月15日，沙特内阁批准通过《个人数据保护法》，自颁布之日起180天后实施，旨在加强对个人隐私的尊重，并为创建基于数据的数字经济做出贡献。沙特数据与人工智能管理局主席在一份声明中表示，该法律将有助于加快数字化转型进程并创建信息化社会，数字化转型赋予私营部门权力，创造有利于业务增长的监管环境，吸引外国投资。

（<https://www.indiatvnews.com/news/world/saudi-arabia-approves-law-protect-personal-data-latest-international-news-updates-734006>）



执法聚焦

➤ 境内执法

- 8月27日，国家网信办启动清朗·移动应用程序 PUSH 弹窗突出问题专项整治，聚焦突出问题靶向施策，推动 PUSH 弹窗传播秩序短期内实现明显好转。国家网信办此次专项整治重点面向新闻客户端、手机浏览器、公众账号平台、工具类应用等 4 类移动应用程序，分类施策，明确六项整改要求：一是禁止 PUSH 弹窗推送商业网站平台和“自媒体”账号违规采编发布、转载的新闻信息，推送新闻信息必须采用规范稿源。二是 PUSH 弹窗推送新闻信息不得渲染炒作舆情热点，断章取义、篡改原意吸引眼球、误导网民。三是未取得互联网新闻信息服务许可的工具类应用不得 PUSH 弹窗推送新闻信息。四是禁止 PUSH 弹窗推送娱乐八卦、明星绯闻、血腥暴力、奇闻异事、低俗恶俗等有悖社会主义核心价值观内容。五是禁止通过 PUSH 弹窗渠道放大传播失德艺人、负面争议人物的有关言论。六是遇突发事件、灾难事故，不得渲染血腥现场、过度强调案件血腥细节等，不得扎堆 PUSH 弹窗推送相关信息。

（http://www.cac.gov.cn/2021-08/27/c_1631652531585631.htm）

简析：随着针对移动应用程序隐私政策等个人信息收集处理活动进行监督管理的专项整治行动取得一定效果，以及社会公众对于 PUSH 弹窗问题的广泛意见，加之对于网络信息内容的监管要求，对于 PUSH 弹窗专项整治活动将会成为下一个监管重点领域。

- 9月1日，交通运输部会同中央网络安全和信息化委员会办公室（“中央网信办”）、工信部、公安部、市场监管总局等交通运输新业态协同监管部际联席会议成员单位，对 T3 出行、美团出行、曹操出行、高德、滴滴出行、首汽约车、嘀嗒出行等 11 家网约车平台公司进行联合约谈。约谈指出，近期部分平台公司通过多种营销手段恶性竞争，并招募或诱导未取得许可的驾驶员和车辆“带车加盟”，开展非法营运，扰乱公平竞争市场秩序，影响行业安全稳定，损害司乘人员合法权益。约谈强调，各平台公司要排查自身问题，立即整改，要加快推进合规化，制定切实可行的网约车合规化工作方案，明确时间表、目标和工作举措，特别是要提出到今年年底前车辆、驾驶员合规化工作的具体目标。

（参考来源：微信公众号“网络法实务圈”）

（<https://mp.weixin.qq.com/s/dZ403x2jy70J0D2b9EP4XA>）

- 9月1日，江苏省市场监督管理局公布三起非法采集消费者人脸信息典型案例，分别为苏州万店掌网络科技有限公司销售万店掌会员识别分析仪及人脸识别服务、无锡洲樾房地产有限公司楼盘售楼处采购安装具有人脸识别功能的摄像设备、江阴和谦置业有限公司楼盘售楼处及洽谈区域安装人脸信息抓拍摄像机。相关部门提醒，企业确需收集、使用个人信息，应当同时遵循合法、正当、必要原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。消费者如发现自身权益受到侵犯，可及时拨打 12315 服务热线进行维权。

（参考来源：微信公众号“江苏市场监管”）

（<https://mp.weixin.qq.com/s/rgg46PRGnlZtmzSj6ZrvLg>）

- 9月8日，中央宣传部、国家新闻出版署有关负责人会同中央网信办、文化和旅游部等部门，对腾讯、网易等重点网络游戏企业和游戏账号租售平台、游戏直播平台进行约谈。此次约谈中强调的“不得以任何形式向未成年人提供网络游戏账号租售交易服务”等要求，证实了防沉迷政策一改此前粗犷的监管风格，更加落实到执行细节，不仅在政策层面上更为务实，监管的跟进速度也在不断加快。

（参考来源：微信公众号“合规科技研究”）

（https://mp.weixin.qq.com/s/SxaH_qA5x3N9E43rU-n01w）

- 9月13日，杭州互联网法院发布了一起平台算法规制的典型案例，认定平台有权对存在违规推广行为的原告采取处罚措施。该案中，原告在被告A公司运营的网站注册账户并开展推广活动，经大数据排查，被告认定原告账户“流量异常”，冻结其账户内佣金17万余元。法院指出，网络平台借助大数据分析的算法，对海量交易进行高密度的筛查，发现网络用户存在违规行为时，依据双方网络服务协议约定的自动化决策机制作出处罚，已经成为遏制网络用户不良行为的有效手段。同时，法院认为平台自治程序应具有正当性，平台行使算法权力应当公开透明，事先披露治理机制、管理规则以及相关技术原理。

（参考来源：微信公众号“杭州互联网法院”）

（https://mp.weixin.qq.com/s/I5_ZzMat8BlepW3nLo-nZg）

- 9月17日，国务院新闻办公室（“国新办”）举行新闻发布会。会议强调，十八大以来，全国公安机关集中打击整治人民群众深恶痛绝的突出网络犯罪、网络黑产及网络乱象，办理网络犯罪案件50余万起，全力营造清朗有序的网络空间。全国公安机关坚持以开展涉网犯罪专项打击为抓手，坚决维护网上公共秩序。2020年全国公安机关巡查发现并清理处置的各类违法有害信息共计237万余条，发现并下架处置违法违规APP 6万余个，封停违法直播平台账号4.6万个，关闭违法直播间3.6万个。

（http://www.cnr.cn/tech/techds/20210917/t20210917_525605108.shtml）

➤ 境外执法

✧ 爱尔兰

- 9月2日，爱尔兰数据保护委员会公布对于脸书的即时通信工具 WhatsApp 的裁决：WhatsApp 因违反 GDPR 的相关规定，被处以 2.25 亿欧元的罚款。爱尔兰数据保护委员会认定，WhatsApp 处理用户个人信息时未能充分告知相关事项，包括如何与母公司脸书共享这些信息，由此违反了欧盟 GDPR 的有关规定。爱尔兰数据保护委员会要求 WhatsApp 进行整改，根据监管要求采取一系列补救措施，以符合欧盟 GDPR 的规定。对此，WhatsApp 表示不认同爱尔兰数据保护委员会的裁决，已提起上诉。

（参考来源：中国新闻网）

（<http://www.chinanews.com/cj/2021/09-03/9557161.shtml>）

- 9月14日，爱尔兰数据保护委员会宣布对 TikTok 涉嫌违反欧盟 GDPR 规定展开 2 项调查。第一项调查将检查 TikTok 是否遵守 GDPR 的数据保护设计和默认要求，以及 TikTok 在处理 18 岁以下用户的个人数据时是否遵守了 GDPR 规定的透明度义务。第二项调查将重点关注 Tiktok 向中国传输个人数据的情况，以及 TikTok 是否遵守 GDPR 中向第三国传输个人数据的要求。

（<https://www.dataprotection.ie/en/news-media/latest-news/dpc-launches-two-inquiries-tiktok-concerning-compliance-gdpr-requirements-relating-processing>）

行业新闻

境内新闻

- 8月27日，中国互联网金融协会（“协会”）发布《关于2021年度移动金融客户端应用软件备案外部评估的通知》，要求金融机构需每年开展一次移动金融 APP 外部评估工作，评估结果同时也是客户端软件备案的必要材料。协会指出备案工作的目的是为了保证金融行业客户端软件的整体安全和合规水平，维护金融消费者权益。协会结合金融行业标准和国家对客户端软件行业的相关标准和要求，对评估工作的范围进行动态调整，并且公布了最新外部评估标准和范围。
(<https://www.nifa.org.cn/nifa/2986584/2986590/3000012/index.html>)
- 9月1日，工信部网络安全管理局组织建设的网络安全威胁和漏洞信息共享平台（“平台”）（网址：<https://www.nvdb.org.cn>）正式上线运行。根据《网络产品安全漏洞管理规定》，网络产品提供者应当及时向平台报送相关漏洞信息，鼓励漏洞收集平台和其他发现漏洞的组织或个人向平台报送漏洞信息。平台包括通用网络产品安全漏洞专业库（网址：<https://www.cnvdb.org.cn>）、工业控制产品安全漏洞专业库（网址：<https://www.cics-vd.org.cn>）、移动互联网 APP 产品安全漏洞专业库（网址：<https://cappvd.cstc.org.cn/>）、车联网产品安全漏洞专业库（网址：<https://cavd.org.cn>）等，支持开展网络产品安全漏洞技术评估，督促网络产品提供者及时修补和合理发布自身产品安全漏洞。
(参考来源：微信公众号“工信微报”)
(<https://mp.weixin.qq.com/s/4-4Jbp1k5lw-Bwumq85qug>)
- 9月3日，2021中国国际金融科技论坛在北京首钢园召开，该论坛由北京市地方金融监督管理局、北京市朝阳区人民政府主办，中国互联网金融协会、中国银行业协会等单位支持。央行科技司副司长李兴锋出席了会议并发表了主题演讲。他表示，当前，新一轮科技革命和产业革命正在重构全球的创新版图，重塑世界经济结构，以数据为关键生产要素、以数字技术为核心驱动力的生产方式正加速推动人类社会迈进数字经济时代。
(参考来源：微信公众号“数据法盟”)
(<https://mp.weixin.qq.com/s/QE42jUyMMU2pR0Pm2Vw6AA>)
- 9月6日，可持续发展大数据国际研究中心在京成立，这是全球首个以大数据服务联合国《2030年可持续发展议程》的国际科研机构。数据缺失、发展不均衡、目标间关联且相互制约等问题正在成为实现可持续发展目标（SDGs）的主要挑战，2020年全球新冠肺炎疫情的爆发，使 SDGs 如期实现面临更为严峻的局面，这对科技创新提出了更高的需求。为此，可持续发展大数据国际研究中心将建立全球可持续发展目标监测与评估体系，为联合国相关机构、成员国提供数据共享、科技支撑、决策支持。
(http://www.cnr.cn/tech/techyw/technews/20210906/t20210906_525592785.shtml)

- 9月13日，工信部装备工业发展中心发布《关于开展汽车数据安全、网络安全等自查工作的通知》（“《通知》”），组织开展汽车数据安全、网络安全、软件在线升级（又称 OTA 升级）和驾驶辅助功能情况自查工作，旨在落实此前发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》的有关要求。《通知》中明确了本次自查工作的自查范围、自查内容和方式以及相关时间安排。

（http://www.miit-eidc.org.cn/art/2021/9/13/art_54_14395.html）

- 9月16日，教育部办公厅等六部门发布《关于做好现有线上学科类培训机构由备案改为审批工作的通知》。其中，网络安全标准与教育移动互联网应用程序（教育 APP）管理的统一设置要求如下：严格落实《中华人民共和国网络安全法》和《中华人民共和国数据安全法》等法律法规要求，达到网络安全保护三级（含）以上防护标准；教育移动应用提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制，储存 100 万人以上个人信息的线上校外培训 APP，应通过个人信息保护影响评估、认证或合规审计。

（http://www.moe.gov.cn/srcsite/A29/202109/t20210918_564368.html）

简析：随着“双减”工作的要求和推进，对于教育培训类 APP 的管理将更加具体和强化。

➤ 境外新闻

- 9月16日，亚马逊宣布其亚马逊网络服务 GDPR 数据处理附录和在线服务条款已经修订，包括了欧盟委员会更新的标准合同条款（SCCs）。亚马逊表示，新的 SCCs 将更好地适应其客户如何在云中运行他们的应用程序或运行他们的工作负载，因为它们涵盖了不同的传输场景，并且还数据传输提供了增强保护。

（<https://aws.amazon.com/cn/blogs/security/new-standard-contractual-clauses-now-part-of-the-aws-gdpr-data-processing-addendum-for-customers/>）

简析：《个保法》中，将按照国家网信部门制定的标准合同与境外接收方订立合同作为个人信息跨境提供的规则条件之一。国家网信部门制定的标准合同的内容和出台时间成为广大企业的关注问题。在该标准合同公布之前，参照包括欧盟的 SCCs 以及《个人信息出境安全评估办法（征求意见稿）》中对于与个人信息接收者签订合同内容的有关要求，在数据出境时与接收方签订合同，约定双方的权利义务是现阶段可以考虑的对应方案。

- 9月7日，荷兰某消费者基金会（The Mass Damage & Consumer Foundation）宣布其已开始针对 TikTok 大规模侵犯荷兰消费者基本权利采取集体行动。该基金会强调 TikTok 违反了各种法律法规，其将特别关注 TikTok 收集的用于创建个人资料或与广告商共享的消费者个人信息。该基金会表示其将通过集体行动捍卫 TikTok 所有用户的权利，并在阿姆斯特丹法院向 TikTok 提出了超过 60 亿欧元的索赔要求。
（<https://www.dataguidance.com/news/netherlands-mass-damage-consumer-foundation-files-%E2%82%AC6>）

热点评述

2021年8月20日,《中华人民共和国个人信息保护法》(以下简称“《个保法》”)通过并发布,将于2021年11月1日起正式生效。《个保法》是我国第一部关于个人信息保护的专门性基本法律,本期热点评述我们将通过对《个保法》重点问题的解读,理清法律脉络,希望为企业研究合规对策提供借鉴。

星星之火—《个人信息保护法》重点问题的解读

叶鹏

2021年8月20日,《中华人民共和国个人信息保护法》(以下简称“《个保法》”)通过并发布。《个保法》是我国第一部关于个人信息保护的专门性基本法律,点燃了我国个人信息保护的星星之火,将与2017年出台的《网络安全法》和2021年9月起正式施行的《数据安全法》共同构建关于网络安全和数据保护的基本法律框架,我国网络安全和数据保护的合规工作将进入新的局面。

随着信息时代的来临,作为大数据核心资源的个人信息的有效流通和合理利用成为中国数字经济发展的课题。另一方面,由于个人信息被过度滥用引发了诸多社会问题,也客观加速了个人及社会对于个人信息和隐私保护意识的觉醒。此外,国内外相关立法活动的推动也使得中国个人信息保护的专门立法工作箭在弦上。本次《个保法》的立法工作自2019年12月被明确列入全国人大常委会的立法工作计划,到2020年10月首次公开《个人信息保护法(草案)》(以下简称“《草案》”)并向社会征求意见,再到2021年4月《个人信息保护法(草案二审稿)》(以下简称“《二审稿》”)提请审议,直至本次《个保法》的正式出台,其过程一直受到社会各界的普遍关注。

《个保法》的立法结合我国国情和实际需要,同时吸收并借鉴了国外相关立法经验,在处理个人信息权益的保护以及促进个人信息合理有效利用的平衡这一世界性立法难题上做出了努力尝试。最终出台的《个保法》回应了诸多社会关注的热点问题。将于11月1日起正式施行的《个保法》确立了个人信息保护的基本法律框架,对于企业合规提出了明确的要求,同时也与每一个体的权益息息相关。本文试图通过对《个保法》重点问题的解读,理清法律脉络,为企业研究合规对策提供借鉴。

一、《个保法》的适用范围

(一) 适用原则

《个保法》采取以属地管辖为基础,辅以适度的域外适用规则。即在明确《个保法》适用任何主体在中华人民共和国境内处理自然人个人信息的活动的同时,

规定在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，如果符合（1）以向境内自然人提供产品或者服务为目的；（2）分析、评估境内自然人的行为；（3）法律、行政法规规定的其他情形¹中的任一情形，也应适用《个保法》。

（二）重点概念

1. 中华人民共和国境内

参照有关法律法规的规定，应当指除香港特别行政区、澳门特别行政区和台湾地区之外的中国大陆地区。只要是在中国境内进行的个人信息处理活动，无论个人信息处理者来自境内或境外，也不管个人信息的主体是境内还是境外，都应当适用《个保法》。换言之，外国公司在中国境内处理外国自然人的个人信息同样应当适用《个保法》。同时，符合前述任一情形的，无论境内还是境外的个人信息处理者，即便在中国境外，处理中国境内自然人的个人信息时，也应适用《个保法》。

2. 个人信息

《个保法》规定个人信息是指以电子或者其他方式记录的、与已识别或者可识别的自然人有关的各种信息²。历经《网络安全法》《民法典》对个人信息定义的调整，作为个人信息保护的专门法律，《个保法》对个人信息的最终定义与欧盟的《通用数据保护条例（General Data Protection Regulations）》（以下简称“GDPR”）相类似，采取了“可识别”“已识别”的概念，与2020年10月施行的国家标准《信息安全技术 个人信息安全规范》（GB/T 35272-2020）（以下简称“《安全规范》”）中提出的“识别”+“关联”的判定方式一致。即个人信息既包括由信息本身的特殊性识别特定自然人的信息，也包括由特定自然人在其活动中产生的信息。

3. 处理活动

《个保法》规范的对象是个人信息的处理活动，包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等³。相较《草案》和《二审稿》，《个保法》对于个人信息的处理的定义，增加了“删除”一项，进一步补充和完善了处理活动，即包括个人信息全生命周期内的各种活动。

二、个人信息处理者及其义务

（一）个人信息处理者的定义

《个保法》对个人信息处理者的定义是，在个人信息处理活动中自主决定处理目的、处理方式的组织、个人⁴。与《草案》《二审稿》相比，《个保法》对于个人处理的定义最终聚焦在“处理目的、处理方式”，删除了“等个人信息处理事项”的表述，更加明确具体。个人信息处理者的定义中另一个关键词是“自主决定”，我们认为根据《个保法》的规定，只有根据自身需要可以独立决定个人信息的处理目的和处理方式的组织或个人，才能构成《个保法》中的个人信息处理者，承担《个保法》中规定应由个人信息处理者承担的义务和责任。

在个人信息处理活动的实务中，可能存在多种不同身份的主体，甚至同一主体在个人信息生命周期处理活动的不同阶段，可能会承担不同角色。不同身份主体之间的关系不同，承担的义务和责任也不同。个人信息处理活动中主体之间的关系主要可分为以下两种：

1. 共同处理

两个以上的主体共同决定个人信息的处理目的和处理方式的，两个以上的主体都同时构成个人信息处理者，彼此之间是共同处理者的关系。共同处理者应当约定各自的权利和义务，个人可以向任一个个人信息处理者主张权利，个人信息处理者应当对侵害个人信息权益造成的损害承担连带责任⁵。

2. 委托处理

接受个人信息处理者委托处理个人信息，构成委托处理关系。受委托人对处理目的和方式没有决定权，应当依照委托人的委托内容实施处理活动。个人信息处理者应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督⁶。个人信息处理者除了需要在委托前进行个人信息保护影响评估之外，对于《个保法》要求的监督活动，可以参照《安全规范》的内容，对受委托人进行审计、记录和存储委托处理个人信息的情况、发生时采取补救措施等⁷。受委托人虽然不是个人信息处理者，但是仍负有采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行法律法规规定的义务⁸。同时受委托人还负有按照与委托处理的个人信息处理者的合同约定进行处理活动的合同义务，违反合同约定应当承担违约责任。受委托人超出委托范围自行决定处理活动，可能构成个人信息处理者承担相应责任。

（二）个人信息处理者的义务

个人信息处理者应当依照《个保法》规定的个人信息处理规则进行处理活动，《个保法》中还专章规定了个人信息处理者的义务，具体包括⁹：

- （1）制定管理制度和操作规程
- （2）个人信息分类管理
- （3）必要安全技术措施（加密/去标识化）
- （4）确定合理权限，进行安全培训教育
- （5）制定应急预案，进行定期合规审计，实施个人信息保护影响评估
- （6）对个人信息安全事件的补救和通知义务
- （7）处理个人信息达到国家网信部门规定数量的，指定个人信息保护负责人，公开并报送
- （8）境外个人信息处理者在中国境内设立专门机构或指定代表并备案的义务

此外，个人信息处理者应当保证个人在个人信息处理活动中的权利，并为个人行使权利提供便捷方式。《个保法》中个人在个人信息处理活动中的权利包括：知情权、决定权、查询复制权、可携带权、更正补充权、删除权、撤回同意权、

要求解释权等。其中可携带权借鉴了 GDPR 的做法，是《个保法》中最新追加的一项个人主体权利。可携带权设立的目的在于强化保证个人拥有个人信息控制权的同时，对平台可能出现的数据垄断问题提供解决方案。但是，《个保法》规定的可携带权是有限权利，需要“符合国家网信部门规定条件”¹⁰，相关条件以及可携带权行使的方式、费用承担等仍有待相关细则加以明确。

《个保法》对于个人信息处理者义务的规定中另一个亮点，在于从《二审稿》开始，针对提供重要互联网平台服务¹¹、用户数量巨大、业务类型复杂的个人信息处理者设置了单独的义务条款，内容包括建立健全合规制度体系，成立主要由外部成员组成的独立机构进行监督；制定平台规则，明确平台内产品或服务提供者的义务并对严重违法的相关提供者停止服务；定期发布个人信息保护社会责任报告。专门条款强化了大型数据企业等的合规义务。

（三）个人信息处理者的过错推定原则

为了强化个人信息处理者的义务履行，从《二审稿》开始增加了对个人信息处理者侵权责任的过错推定原则。《个保法》中的表述稍有调整，最终规定为“处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。”¹²个人信息处理者如何证明自己没有过错，需要结合司法解释和审判实践在今后进一步确认，但是我们认为企业切实履行《个保法》规定的个人信息处理者义务，并保存相关记录，对于个人信息处理者的履行举证责任将起到至关重要的作用。

三、个人信息处理的合法性基础和原则

（一）《个保法》对个人信息处理合法性基础的重构

《个保法》在个人信息处理规则中，确立了以下个人信息处理的合法性规则：“（一）取得个人的同意；（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；（三）为履行法定职责或者法定义务所必需；（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；（七）法律、行政法规规定的其他情形。”¹³

在《个保法》之前，全国人民代表大会常务委员会在 2012 年发布的《关于加强网络信息保护的決定》（以下称“《決定》”）被长期作为个人信息保护领域的基础法律依据。《決定》确立了个人信息收集、使用的合法基础是“经被收集者同意”¹⁴，这一规则也被沿用至此后的相关法律法规之中，包括《消费者权益保护法》（2013 年修正）¹⁵、《网络安全法》¹⁶等。但是，随着数据资源重要性的不断提升，单一的“个人同意”规则，越来越不能满足社会和经济对于个人信息有效利用日益高涨的实际需求。2020 年的《安全规范》中规定了收集、使用中征得授权同意的例外和共享、转让、公开披露个人信息时事先征得授权同意

的例外¹⁷。在2021年正式施行的《民法典》中，虽然仍然延续了“同意”的合法性原则，但是同时规定“法律、行政法规另有规定的除外”¹⁸，为专门法律法规的规定留下接口和空间，同时将公开信息的合理使用和为了公共利益或自然人合法权益的合理使用以法定免责（民事责任）的形式，实际纳入到民事领域的合法性基础范围内。

《个保法》此次在取得个人同意之外，对于个人信息处理的合法性基础增加并明确规定上述（二）至（七）项情形的，不需取得个人同意¹⁹，体现了《个保法》兼顾个人信息权益保护和促进个人信息合理有效利用之间平衡的立法价值。《个保法》的合法性基础第（二）项，在《草案》和《二审稿》的基础上，新增了“实施人力资源管理所必需”，也是该立法价值的具体体现。我们理解同为合法性基础的个人信息同意，与其后的（二）到（七）项是平行关系，可以互为替代。

（二）个人信息处理的原则

《个保法》在承继自《决定》开始确立的个人信息处理应当遵循的合法、正当、必要原则的基础上，追加了诚信原则，规定不得通过误导、欺诈、胁迫等方式处理个人信息²⁰。对于必要原则，《个保法》进一步明确规定“与处理目的直接相关”“采取对个人权益影响最小的方式”“限于实现处理目的的最小范围，不得过度收集”²¹，从目的、方式、范围的维度对于必要原则加强了阐明。除此之外，《个保法》强调公开、透明原则，要求“公开个人信息处理规则，明示处理的目的、方式和范围。”²²需要企业特别注意的是，依照前述合法性基础处理个人信息时，同样需要遵循个人信息处理的原则要求。合法性基础（二）到（七）项免除的只是取得个人同意，并不意味着免除《个保法》及相关法律法规规定的个人信息处理过程中其他的义务和责任。例如，在个人信息跨境提供的场景，符合合法性基础中（二）到（七）项，只是无需取得个人信息主体单独同意的理由，而非无需遵守合法、正当、必要和诚信原则，公开处理规则，进行个人信息保护影响评估以及满足其他法律规定的具体条件的理由。但是，在依法无需取得个人同意的场景下，如何实现公开个人信息处理规则的要求，需要根据实施细则的具体规定以及结合实际场景具体研究。

（三）个人同意和有效性

诚然如前所述，《个保法》重构了个人信息处理的合法性基础。但是，无论从个人信息保护的人格权益属性，个人信息保护的底层要求，还是实际应用场景的数量上，个人同意仍然是个人信息处理合法性原则的核心。因此，个人同意有效性的考量仍然是企业合规工作中的重中之重。

个人同意有效性的前提是满足个人信息处理的原则要求。超越原则，不具有明确、合理的目的，超过最小必要的范围处理个人信息，或者没有通过个人信息处理规则明确告知处理的目的、方式和范围等，即使取得个人同意，仍然存在重大的合规瑕疵。为了保证上述前提，《个保法》对于个人同意的方式、个人撤回同意时的处理、对个人履行告知义务的方式、内容、形式等都进行了具体规定²³。

此外，2021年3月，国家互联网信息办公室（以下称“国家网信办”）、工业和信息化部（以下称“工信部”）、公安部和国家市场监督管理总局（以下称“市监总局”）联合发布了《常见类型移动互联网应用程序必要个人信息范围规定》，虽然该规定主要为了规范移动互联网应用程序（App）收集个人信息行为，对于一般场景处理个人信息活动的最小必要范围的判定仍有一定参考借鉴的意义。

取得个人同意的方式也是个人同意有效性的另一个重要因素。《个保法》中明确规定了单独同意的取得个人同意的方式。明确了针对特定的个人信息处理活动（提供²⁴、公开²⁵）、特殊个人信息类型（敏感个人信息²⁶）、特别处理场景（个人图像、身份识别信息用于公共安全之外目的²⁷以及个人信息的跨境提供²⁸）需要采取单独同意的要求。另一方面，单独同意区别于《安全规范》中的明示同意和授权同意，从文义上，与2021年5月生效的《网络交易监督管理办法》中规定收集、使用敏感信息应当“逐项取得消费者同意”²⁹也应当有所不同。我们理解单独同意的重点在于与其他同意事项相区分，目的在于对个人起到单独提示的作用，并不得与其他事项进行捆绑。虽然，有关单独同意的具体认定，还需要结合实施细则和规范性文件的规定以及通过执法实践进一步验证，但是我们理解实务中应当基于法律的立法本意，结合线上或线下处理的实际场景，在平衡合规要求和注重用户体验的前提下，综合考虑具体的落地方法。

四、个人信息处理活动的特殊规则

（一）敏感个人信息的处理规则

《个保法》在一般个人信息的基础上，明确定义了敏感个人信息，并规定了敏感个人信息处理的特殊规则。《个保法》对敏感个人信息的定义，仍然沿用了《安全规范》中以发生个人信息事故时的危害结果作为界定标准的方式。其中，个人信息事故包括信息的泄露或非法使用，危害结果是指容易导致自然人的的人格尊严受到侵害或者人身、财产安全受到危害³⁰。虽然《个保法》对敏感个人信息定义的表述较《安全规范》有所变化，我们理解主要是由于《民法典》明确了人格尊严受法律保护³¹，个人信息保护属于“自然人享有基于人身自由、人格尊严产生的其他人格权益³²”，实质上《个保法》对于敏感个人信息的定义没有本质变化。除了《个保法》中举例的敏感个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息之外，《安全规范》中的列示对于判断敏感个人信息同样有重要参考意义。

《个保法》对于敏感个人信息处理的特殊规则，包括更高的必要性要求；更严格的保护措施要求；单独同意或书面同意的要求；更充分告知义务的要求以及针对不满十四岁未成年人信息，制定专门的个人信息处理规则和取得未成年人父母或其他监护人的同意的强化要求。此外，对于个人信息处理者在处理敏感个人信息之前还要求进行个人信息保护影响评估，并对处理情况进行记录。

（二）自动化决策的处理规则

针对大数据分析和人工智能等技术运用的迅猛发展,《个保法》对于该技术的重要应用自动化决策进行了专门规定³³。包括(1)个人信息处理者应当保证决策的透明度和结果公平、公正,强调不得对个人在交易价格等交易条件上实行不合理的差别待遇。此规定意图规范和禁止普遍关注的“大数据杀熟”问题,也是《个保法》在《草案》《二审稿》基础上补充强调的内容。(2)通过自动化决策方式向个人进行信息推送、商业营销,应当同时提供不针对其个人特征的选项,或者向个人提供便捷的拒绝方式。强调保护个人对自动化决策推送信息的选择权,以防范“信息茧房”问题。(3)通过自动化决策方式作出对个人权益有重大影响的决定,个人有权要求个人信息处理者予以说明,并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。其中对个人权益有重大影响的决定,参照《安全规范》中的举例,包括自动决定个人征信及贷款额度,或用于面试人员的自动筛选等³⁴。此外,《个保法》还要求个人信息处理者在利用个人信息进行自动化决策之前,要进行个人信息保护影响评估,并对处理情况进行记录³⁵。

2021年8月27日,国家互联网信息办公室(以下称“国家网信办”)公布了《互联网信息服务算法推荐管理规定(征求意见稿)》(以下称“《算法推荐规定》”)并向社会公开征求意见。虽然并非所有自动化决策都利用个人信息,《算法推荐规定》中的应用算法推荐技术也并非仅用于自动化决策,或者全部使用个人信息,但不可否认二者仍有着紧密的关系。《算法推荐规定》中第14条对于算法推荐服务透明度的规定,第10条加强用户模型和用户标签管理的规定,第15条提供关闭算法推进服务选项等均与《个保法》关于自动化决策的前述规定一以贯之。特别值得注意的是,根据《算法推荐规定》,对于应用算法推荐技术提供互联网信息服务的服务提供者(以下称“算法推荐服务提供者”),国家将实施分类分级管理。对于其中具有舆论属性或者社会动员能力的算法推荐服务提供者,将要求实施备案和强制的安全评估。

(三) 个人信息的跨境提供规则

互联网技术的发展、经济全球化和数据资源的广泛利用,使得数据跨境成为必然要求,另一方面,数据的跨境关系到数据安全、个人信息和隐私权利的保护,甚至关联国家安全和国家数据主权,因此数据跨境问题,特别是个人信息的跨境规则一直备受瞩目。

在中国的相关立法中,自《网络安全法》开始明确规定关键信息基础设施的运营者(以下称“CIIO”)对在中国境内运营中收集和产生的个人信息和重要数据的本地化存储原则要求,同时规定确需向境外提供的,需要进行安全评估。作为对跨境提供规则的落实,中国先后推出了《个人信息和重要数据出境安全评估办法(征求意见稿)》(2017)、《信息安全技术 数据出境安全评估指南(送审稿)》(2017)、《个人信息出境安全评估办法(征求意见稿)》(2019)等相关法规和规范性文件,但是除了将适用对象由CIIO统一扩大到了一般的网络运营者,对于具体适用措施,则一直存在变动,始终未能确定。《个保法》终于

确定了个人信息的跨境规则，并以专章进行了规定。具体规则的概要可参见下表³⁶：

规则	规则内容	适用对象
一般规则	通过国家网信部门组织的安全评估	CIIO 和处理个人信息达到国家网信部门规定数量的个人信息处理者
	经专业机构进行个人信息保护认证	上述之外的个人信息处理者
	按照国家网信部门制定的标准合同与境外接收方订立合同	
	法律、行政法规或者国家网信部门规定的其他条件	
例外规则	中华人民共和国缔结或者参加的国际条约、协定对中国境外提供个人信息的条件等有规定的。	所有个人信息处理者
前提条件	向个人告知并取得个人的单独同意。	所有个人信息处理者
	应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。	
	事前进行个人信息保护影响评估，并对处理情况进行记录	
特殊规则	依外国司法或者执法机构关于提供存储于境内个人信息的请求提供个人信息须经中国主管机关批准。	所有个人信息处理者
	被国家网信部门列入限制或者禁止个人信息提供清单，予以公告，应当依照限制或者禁止向其提供个人信息等措施的规定。	
	针对对中国采取歧视性的禁止、限制或者其他类似措施的国家或地区，依照中国采取的对等措施。	

《个保法》借鉴了包括 GDPR 在内国外立法的经验，采用了标准合同的规则方式以及确认“充分保护标准”的要求等，基本明晰了个人信息跨境的规则框架。同时，与《出口管制法》等相关法律进行了衔接。但是，涉及个人信息跨境提供的实际问题，包括跨境提供的认定、安全评估的具体内容和流程、认证机构的确定、标准合同的公布、采取必要措施的认定以及过境数据的处理规则等，仍需要实施细则和规范性文件加以明确。我们估计相关细则和规范性文件正在紧锣密鼓的制定过程中，很有可能在 11 月 1 日《个保法》施行前后出台。

五、个人信息保护的监管及法律责任

（一）监管部门和职责权限

与《网络安全法》《数据安全法》基本一致,《个保法》规定国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依法在各自职责范围内负责个人信息保护和监督管理工作³⁷。国务院有关部门在实务中主要包括工信部、公安部 and 市监总局。从2019年1月开始的App违法违规收集使用个人信息专项治理即是由上述四个部门联合行动的。从《个保法》立法之初,各界一直有建立统一的执法机关专门管理个人信息保护工作的呼声。但出于国家机构编制改革,以及各个部门的各自主管领域短期内恐难整合等诸多因素的考虑,最终仍然维持了《网络安全法》建立的管理体制,不能不说是本次立法中一个“遗憾”,“九龙治水、多头共管”的监督管理格局仍将继续。

《个保法》在规定履行个人信息保护职责的部门的工作职责的同时,赋权相关部门可以采取包括询问当事人、查阅、复制有关资料、现场检查、查封或扣押、约谈个人信息处理者负责人、要求进行合规审计、处理投诉、举报等多项措施³⁸,并规定了当事人应当协助配合的义务。

（二）法律责任

相较于《网络安全法》,《个保法》对于违法处理个人信息,或者处理个人信息未履行《个保法》规定的个人信息保护义务的行为,规定了更加严格的法律责任。根据违法行为的情节,最高可以处五千万以下或者上一年度营业额百分之五以下罚款,并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。同时,对直接负责的主管人员和其他直接责任人员可以最高处十万元以上一百万元以下罚款,并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。³⁹其中,最高罚款金额据说是借鉴了GDPR(4%)和《反垄断法》(1%-10%)二者的经验⁴⁰。

在法律责任的规定中,除了前文中介绍的个人信息处理者侵权责任的过错推定原则之外,《个保法》规定的公益诉讼制度,同样备受关注。人民检察院、法律规定的消费者组织和由国家网信部门确定的组织将可以就个人信息处理者违法处理并侵害众多个人的权益的情形,向人民法院提起诉讼。除了行政责任之外,预计涉及侵害个人信息保护的权益的民事案件也会大幅增加。

结语

《个人信息保护法》是基础性法律,规定的是原则性问题,规定的执行和落地还需要与相关细则和实施规范相结合。《个人信息保护法》的出台和正式施行,必将带动相关配套法规和规范性文件的出台。中国网络安全和数据保护的法律体系已经初步建成,并将日趋完善和严格,这也对企业合规工作提出了新的要求。我们会持续关注有关法律动向,助力企业合规成长。

¹ 《个人信息保护法》第三条

² 《个人信息保护法》第四条



- 3 《个人信息保护法》第四条
- 4 《个人信息保护法》第七十三条
- 5 《个人信息保护法》第二十条
- 6 《个人信息保护法》第二十一条
- 7 《信息安全技术 个人信息安全规范》（GB/T 35272-2020）9.1
- 8 《个人信息保护法》第五十九条
- 9 《个人信息保护法》第五章
- 10 《个人信息保护法》第四十五条
- 11 《二审稿》中的表述为基础性互联网平台服务
- 12 《个人信息保护法》第六十九条
- 13 《个人信息保护法》第十三条
- 14 《全国人民代表大会常务委员会关于加强网络信息保护的決定》第二条
- 15 《消费者权益保护法》（2013 年修正）第二十九条
- 16 《网络安全法》第四十一条
- 17 《信息安全技术 个人信息安全规范》（GB/T 35272-2020）5.6、9.5
- 18 《民法典》第一千零三十五条
- 19 《个人信息保护法》第十三条
- 20 《个人信息保护法》第五条
- 21 《个人信息保护法》第六条
- 22 《个人信息保护法》第七条
- 23 《个人信息保护法》第十四条、第十五条、第十六条、第十七条
- 24 《个人信息保护法》第二十三条
- 25 《个人信息保护法》第二十五条
- 26 《个人信息保护法》第二十九条
- 27 《个人信息保护法》第二十六条
- 28 《个人信息保护法》第三十九条
- 29 《网络交易监督管理办法》第十三条
- 30 《个人信息保护法》第二十八条
- 31 《民法典》第一百零九条
- 32 《民法典》第九百九十条
- 33 《个人信息保护法》第二十四条
- 34 《信息安全技术 个人信息安全规范》（GB/T 35272-2020）7.7
- 35 《个人信息保护法》第五十五条
- 36 《个人信息保护法》第三章
- 37 《个人信息保护法》第六十条
- 38 《个人信息保护法》第六十三条、第六十四条、第六十五条
- 39 《个人信息保护法》第六十六条
- 40 南方都市报 APP·隐私护卫队课题组：详解个保法：区分大小企业保护义务，违法人员或被限制从业
https://m.mp.oeeee.com/a/BAAFRD000020210820587568.html?layer=2&share=chat&isndappinstalled=0&wxuid=ogVRcdAjENHcM_LSN5oI3X9Lzqk8&wxsalt=9f5284（最后访问时间：2021 年 8 月 30 日）