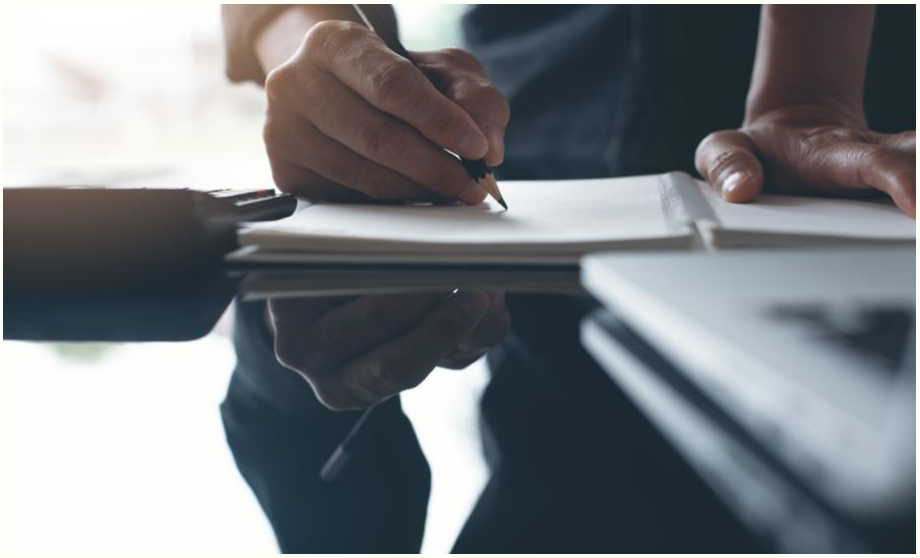
数据合规时事速递
NEWSLETTERS

2022 年 第九期 /总第四十三期



环球律师事务所
GLOBAL LAW OFFICE

2022 年 11 月 09 日

精彩导读

新规速递/ 《信息安全技术 关键信息基础设施安全保护要求》国标发布

监管动态/ 国家网信办依法集中查处 135 款违法违规 App

相关新闻/ 国新办发布《携手构建网络空间命运共同体》白皮书

环球解读/ 个人信息保护重点条款回顾——《个人信息保护法》实施一周年观察

环球律师事务所
GLOBAL LAW OFFICE

前　言

随着《网络安全法》、《数据安全法》、《个人信息保护法》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出台的重要法律法规、市场监管动向以及相关处罚案例，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。

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

环球律师事务所
GLOBAL LAW OFFICE

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

孟洁律师为环球律师事务所常驻北京的合伙人，主要执业领域为网络安全、个人信息保护、互联网、电商合规、反腐败反商业贿赂合规。孟律师曾在诺基亚等世界五百强跨国公司和知名律师事务所工作超过十余年，担任知名人工智能独角兽公司总法律顾问、DPO。孟洁律师曾经及目前服务于大型跨国公司及知名互联网企业、车企、IoT、电信、云服务、AI、金融、医疗领域企业进行境内/境外的数据合规体系建设与数据合规专项，总结出不少可落地的实操方法论，颇受客户好评。

她被 China Business Law Journal 评为“2022 年度律师新星”；荣登钱伯斯大中华区 2022 年法律指南“数据隐私保护”榜单、“科技、媒体、电信”榜单；被 Legal 500 评为 2020 年“TMT 领域特别推荐律师”；2021 年“TMT 领域领军人物”、“数据保护领域领军人物”、“Fintech 领域头部律师”，被 LEGALBAND 评为“2022 年度顶级律师排行榜：网络安全与数据合规”、“2021 年中国律师特别推荐榜：消费与零售”、“2021 年中国律师特别推荐榜：汽车与新能源”、“网络安全与数据合规特别推荐 15 强”、“2020 年度 LEGALBAND 中国律师特别推荐榜 15 强：网络安全与数据合规”，被北京市律协评为全国千名涉外专家律师。在各大期刊、公号发表过数百篇专业文章、著作，例如有《SDK 安全与合规白皮书》，《个性化展示安全与合规报告》、《Cookie 合规指引报告（2021）》、《国内外标准兼容下的个人信息合规体系构建》等。

许国盛 | 资深顾问
直线：86-010-6584-9306
手机：86-185-1085-6288
邮箱：xuguosheng@glo.com.cn

许国盛律师在金融服务与电信领域与合规官以及企业高管有丰富的合作经验。作为迪堡与诺基亚中国的前区域合规总监，许律师在数据保护规制以及中国监管事项方面有着多年经验。除此之外，他也经常协助跨国企业进行敏感的内部调查、监管检查、数据完整性问题检查以及应对政府执法。许律师曾负责管理整合来自不同国家的合规项目，并熟悉美国、欧盟以及亚洲国家的复杂法律法规。

许律师对如何运行合规项目有着极其深入的了解。在环球，许律师曾为客户的海外扩张提供数据合规方面的建议，包括国际数据隐私政策的本地化，员工或客户数据出境和共享，以及数据泄露的管理与向监管机构的自我报告等。许律师亦是《全球化与隐私保护指南（2020）》以及《GB/T 35273 与 ISO/IEC 27701 比较报告（2020）》的合著者。

本团队专门致力于为客户提供全面且专业的法律服务，包括以下业务领域：

- 网络安全与数据合规
- 互联网与电商合规
- 个人信息保护
- 反腐败/反商业贿赂合规

目录

新规速递

1. 《信息安全技术 关键信息基础设施安全保护要求》国标发布

11 月 7 日，市场监管总局标准技术司、中央网信办网络安全协调局、公安部网络安全保卫局在京联合召开《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）国家标准（以下简称《标准》）发布宣贯会。《标准》于 10 月 12 日经由国家市场监督管理总局（国家标准化管理委员会）批准，由全国信息安全标准化技术委员会归口，将于 2023 年 5 月 1 日正式实施。

《标准》是我国关键信息基础设施安全保护的总纲性标准，也是我国首个发布的关键信息基础设施安全保护标准，对指导我国关键信息基础设施安全保护工作，具有重大价值和深远意义。

《标准》提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护、以信息共享为基础的协同联防的关键信息基础设施安全保护 3 项基本原则；从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等 6 个方面提出了 111 条安全要求，为运营者开展关键信息基础设施保护工作需求提供了强有力的标准保障。[1]

《信息安全技术 关键信息基础设施安全保护要求》全文请参见：
https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=1D986D9DCCC518D19DAD9431DD76053E

2. 中央网信办印发《关于切实加强网络暴力治理的通知》

11 月 2 日，中央网信办秘书局印发《关于切实加强网络暴力治理的通知》（以下简称《通知》），目标是为切实加大网暴治理力度，进一步压实网站平台主体责任，健全完善长效工作机制，有效保障广大网民合法权益，维护文明健康的网络环境。

[1] 中国政府网。

《通知》首先提出要建立健全网暴预警预防机制，具体要加强内容识别预警、构建网暴技术识别模型和建立涉网暴舆情应急响应机制。

《通知》进一步规定了通过设置“一键防护”功能、优化私信规则、建立快速举报通道的方式加强对网暴当事人保护。

《通知》要求严防网暴信息传播扩散，为此应当加强评论环节管理，加强重点话题群组和板块管理，加强直播、短视频管理，加强权威信息披露。

《通知》明确了将依法分类处置网暴相关账号，严处借网暴恶意营销炒作等行为，问责处罚失职失责的网站平台。[2]

《关于切实加强网络暴力治理的通知》全文请参见：

http://www.cac.gov.cn/2022-11/04/c_1669204414682178.htm

3. 工信部就《关于促进网络安全保险规范健康发展的意见》公开征求意见

11 月 7 日，工信部网站发布《关于促进网络安全保险规范健康发展的意见（征求意见稿）》（以下简称《意见》），《意见》是为加快推动网络安全和金融服务创新融合发展、培育网络安全保险新业态。意见反馈截止时间为 11 月 18 日。

《意见》提出，要建立健全网络安全保险政策标准体系，加强网络安全保险产品服务创新，强化网络安全技术赋能保险发展，促进网络安全产业需求释放，培育网络安全保险发展生态。

《意见》明确，鼓励保险公司面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品，创新发展网络安全保险服务；强调围绕电信和互联网行业典型事件，以及工业互联网、车联网、物联网等新兴场景开展网络安全风险研究；要求开展网络安

[2] 国家网信办官网。

全保险全生命周期风险监测，覆盖事前、事中、事后等重要环节；提出面向电信和互联网、能源、金融、医疗卫生、工业互联网、车联网等行业和领域开展网络安全保险服务试点。[3]

《关于促进网络安全保险规范健康发展的意见（征求意见稿）》全文请参见：

https://www.miit.gov.cn/jgsj/waj/gzdt/art/2022/art_b88c071678ae408897478d1ab1f25aea.html

4. 五部门联合发布《虚拟现实与行业应用融合发展行动计划》

11 月 1 日，工业和信息化部、教育部、文化和旅游部、国家广播电视总局、国家体育总局联合发布《虚拟现实与行业应用融合发展行动计划（2022-2026 年）》（以下简称《行动计划》）。《行动计划》是为落实“十四五”规划的要求，促进“虚拟现实和增强现实”作为数字经济重点产业的发展。

《行动计划》提出的目标是，到 2026 年三维化、虚实融合沉浸影音关键技术重点突破，新一代适人化虚拟现实终端产品不断丰富，虚拟现实在经济社会重要行业领域实现规模化应用，形成具有国际竞争力的骨干企业和产业集群，打造技术、产品、服务和应用共同繁荣的产业发展格局。

《行动计划》部署五项重点任务，明确要推进虚拟现实与 5G、人工智能、大数据等关键技术融合创新，全面提升虚拟现实关键器件、终端外设、业务运营平台、内容生产工具、专用信息基础设施等的全产业链条供给能力，加速工业生产、文化旅游、融合媒体、教育培训等多行业多场景应用落地，加强产业公共服务平台建设，构建覆盖全产业链的融合应用标准体系。

《行动计划》提出三项三大专项工程，包括关键技术融合创新工程，全产业链条供给提升工程，多场景应用融合推广工程。

[3] 工业与信息化部官网。

为推进各项目标和重点任务的实施，《行动计划》还提出七项保障措施，强调加强统筹联动、优化发展环境、深化技术研发、开展应用试点、打造产业集群、强化人才支撑、推动交流合作。[4]

《虚拟现实与行业应用融合发展行动计划（2022-2026 年）》全文请参见：

https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_775aaa3f77264817a5b41421a8b2ce22.html

5. 工信部印发《网络产品安全漏洞收集平台备案管理办法》

10 月 28 日，工信部发布《关于印发<网络产品安全漏洞收集平台备案管理办法>的通知》（以下简称《办法》）。

《办法》共十条，适用于境内的网络产品安全漏洞收集平台的备案管理工作。“网络产品安全漏洞收集平台”系指相关组织或者个人设立的收集非自身网络产品安全漏洞的公共互联网平台，仅用于修补自身网络产品、网络和系统安全漏洞用途的除外。

《办法》明确，漏洞收集平台备案通过工信部网络安全威胁和漏洞信息共享平台开展，采用网上备案方式进行；拟设立漏洞收集平台的组织或个人，应当通过工信部网络安全威胁和漏洞信息共享平台如实填报网络产品安全漏洞收集平台备案登记规定的六类信息。《办法》还明确了备案信息变更、业务变更、备案时限等内容。[5]

《网络产品安全漏洞收集平台备案管理办法》全文请参见：

https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_8c3a9f746c324ac8a6c033f896356a0d.html

[4] 工业与信息化部官网。
[5] 工业与信息化部官网。

6. 国务院办公厅印发《全国一体化政务大数据体系建设指南》

10 月 28 日，中国政府网正式发布《国务院办公厅关于印发<全国一体化政务大数据体系建设指南>的通知》（以下简称《指南》）。

《指南》明确，全国一体化政务大数据体系包括三类平台和三大支撑。三类平台为“1+32+N”框架结构，即“1”个国家、“32”个省（自治区、直辖市）以及“N”个国务院有关部门。三大支撑包括管理机制、标准规范、安全保障三个方面。此外，还提出八项“一体化”任务，要求实现统筹管理、数据目录、数据资源、共享交换、数据服务、算力设施、标准规范、安全保障一体化。

《指南》强调，要建立完善政务大数据管理体系，全量、规范编制政务数据目录，推进政务数据归集，建设完善数据资源库，深入推进政务数据协同共享，加强政务大数据基础能力建设，完善算力管理体系，加快编制国家标准，健全数据安全制度规范等。[6]

《全国一体化政务大数据体系建设指南》全文请参见：

http://www.gov.cn/zhengce/content/2022-10/28/content_5722322.htm

7. 浙江省市监局就《数据资产确认工作指南》公开征求意见

10 月 11 日，浙江省市监局网站发布浙江省地方标准《数据资产确认工作指南(征求意见稿)》（以下简称《指南》），意见反馈截止时间为 11 月 10 日。

《指南》给出了数据资产确认的术语和定义，数据资产初始确认、后续确认和终止确认，适用于指引数据资产确认工作。其中，“数据资产”是指会计主体过去的交易或事项形成的，由会计主体拥有或者

[6] 中国政府网。

合法控制的，能进行可靠计量的，预期会给会计主体带来经济利益或产生服务潜力的数据资源。

《指南》还随附录发布了访问控制技术方法、数据资产价值评估方法等。[7]

《数据资产确认工作指南(征求意见稿)》全文请参见：

https://bz.zjamr.zj.gov.cn/public/news/view/consultation/1a76ae37d0c74a53afef4706063486ed.html

8. 上海市规划和自然资源局就《智能网联汽车高精度地图管理试点规定（草案）》公开征求意见

10 月 21 日，上海市规划和自然资源局发布《关于<上海市智能网联汽车高精度地图管理试点规定（草案）>公开征询社会公众意见与公平竞争审查征求意见的公告》（以下简称《规定》），意见反馈截止时间为 11 月 2 日。

《规定》全文包括总则、数据采集与制作、地图审核、地图服务、数据安全、监督检查与法律责任共七章二十条，服务于智能网联汽车产业发展，确保地理信息数据安全，适用于在上海市智能网联汽车测试与应用活动中开展高精度地图数据采集、存储、传输、处理、制作和成果使用等活动，以及相关监督管理工作。

《规定》主要明确了数据采集和制作所需的测绘资质，探索采用告知承诺方式进行地图审核，并规定了未依法履行数据出境安全评估和对外提供审批程序的高精度地图数据，不得向境外传输。[8]

《关于<上海市智能网联汽车高精度地图管理试点规定（草案）>公开征询社会公众意见与公平竞争审查征求意见的公告》全文请参见：

[7] 浙江省市场监督管理局官网。
[8] 上海市规划和自然资源局官网

https://ghzyj.sh.gov.cn/dczj/20221021/0f1f31ecb0964299bd99e80cdb6f7809.html

9. 深圳市监局就《深圳市电子商务经营者第三方信用评价与应用管理办法》公开征求意见

10 月 20 日，深圳市监局发布关于公开征求《深圳市电子商务经营者第三方信用评价与应用管理办法（征求意见稿）》（以下简称《办法》）的通知，反馈截止时间为 11 月 20 日。

《办法》全文共二十七条，主要规定了电子商务经营者第三方信用评价工作原则、管理机构、信用信息安全管理、信用评价标准规范和程序、信用评价对象权益保护、信用评价结果应用等。《办法》是对已期满失效的《深圳市电子商务经营者第三方信用评价与应用暂行办法》进行的修订，对原有的第三方信用评价与应用监管流程进行了补充和完善，新增信用评价机构网络安全责任、信用评价对象权益保护等条款，完善了信用评价过程中信用信息管理。

其中，《办法》明确了对信用评价对象知情权、异议权的保护，信用评价对象将有权向信用评价机构提出异议，要求更正相关信用信息。《办法》还规定，市场监管部门参考信用评价结果，对于电子商务经营者相关失信行为，可以通过市场监管部门官方网站、网络搜索引擎、经营者从事经营活动的主页面显著位置等途径公示，推进建立基于信用的分级分类监管机制。[9]

《深圳市电子商务经营者第三方信用评价与应用管理办法（征求意见稿）》全文请参见：

http://amr.sz.gov.cn/hdjlpt/yjzj/answer/24141

[9] 深圳市市场监督局官网。

10. 重庆市政府发布《重庆市建设智能网联新能源汽车零部件供应链体系行动计划（2022—2025 年）》

10 月 20 日，重庆市政府发布《关于印发重庆市建设智能网联新能源汽车零部件供应链体系行动计划（2022—2025 年）的通知》（以下简称《行动计划》）。

《行动计划》围绕构建零部件供应链体系，引进培育优质企业，增强技术创新能力，促进协同融合发展，优化统筹服务能力五方面，提出 20 项重点任务。

《行动计划》强调，要完善新能源关键零部件供应链体系，培育智能驾驶零部件供应链，做大智能座舱零部件规模，提升车联网零部件供应能力，推进基础材料产业协同发展。[10]

《关于印发重庆市建设智能网联新能源汽车零部件供应链体系行动计划（2022—2025 年）的通知》全文请参见：

https://www.cq.gov.cn/zwgk/zfxxgkml/szfwj/qtgw/202210/t20221020_11206925.html

11. 欧盟公布《数字服务法案》正式文本

10 月 27 日，《数字服务法案》（Digital Service Act，以下简称“DSA”）正式在欧洲联盟官方公报上公布。此前，欧洲议会和欧洲理事会已经就 DSA 文本达成合意，欧洲议会于 7 月 5 日进行了最后表决，最终以 539 票赞成、54 票反对和 30 票弃权获得通过。

DSA 适用主体为互联网中介服务提供商。无论其是否在欧盟境内成立，包括互联网接入提供商、域名注册商、托管服务（如云服务和虚拟主机服务）提供商、社交媒体、在线市场、大型在线平台和大型在线搜索引擎等。DSA 将上述互联网中介服务提供商分为四大类

[10] 重庆市人民政府官网。

别，第一类是中介服务提供商；第二类是托管服务提供商；第三类是在线平台；第四类是大型在线平台和大型在线搜索引擎，即在欧盟范围内平均月度活跃用户超过 4500 万的在线平台。

DSA 为这四类提供商设置了不同的义务：（1）内容审核义务。中介服务提供商应当履行内容审核义务，针对服务中的非法内容采取行动，并相应更新相关条款；（2）建立“通知和行动”机制。托管服务提供商应当建立“通知和行动”机制，确保用户可以自行标记非法内容，且其可以及时对此采取行动；（3）建立投诉内部机制，保障算法透明度。在线平台提供商应当建立有效的投诉处理内部机制，保障算法的透明度，禁止基于儿童的个人信息或种族、政治观点和性取向等特殊类型数据投放定向广告等；（4）大型在线平台和大型在线搜索引擎还拥有额外的独立审计和定期风险评估义务，需要与监管机构及研究人员共享数据。

根据最终文本，DSA 将在公布后第二十天起生效，并分阶段适用。其中第二十四条第二款、第三款、第六款、第三十三条第三款至第六款、第三十七条第七款、第四十条第十三款、第四十三条以及第四章第四节、第五节、第六节于 2022 年 11 月 16 日适用。其余条款则将在 2024 年 2 月 17 日起施行。[11]

《数字服务法案》全文请参见：
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A277%3ATOC

12. 乌克兰公布《个人数据保护法草案》

近日，乌克兰议会公布了《个人数据保护法草案》（以下简称《草案》）。根据议会发布的《草案》解释，近年来，包括乌克兰在内的全球互联网数据处理活动显著增加，特别是在大数据和社交媒体领域。鉴于国际上个人数据保护领域规则的发展，乌克兰国内

[11] 欧盟官网。

外的立法状态并不能完全保障乌克兰个人数据的安全，需要对立法及其应用进行全面更新，遂制定此法。

其中，受数据保护法规影响最大的部分乌克兰企业，主要客户群体位于欧洲。乌克兰企业也正在更新其隐私流程和个人数据处理的部门和规则，以期与乌克兰《个人数据保护法》及欧盟政策标准相符合，使个人数据保护规则与新标准接轨。

《草案》由十一章六十条组成，包括一般规定、处理个人数据的特殊要求、个人数据主体权利、控制者和经营者职责、个人数据跨境传输和第三方个人数据访问程序等内容，为处理个人数据、敏感信息以及其他特定类型的数据提供了依据。[12]

[12] DataGuidance 官网。

环球律师事务所
GLOBAL LAW OFFICE

监管动态

1. 国家网信办依法集中查处 135 款违法违规 App

近日，针对人民群众反映强烈的 App 以强制、诱导、欺诈等恶意方式违法违规处理个人信息行为，国家网信办依据《个人信息保护法》《App 违法违规收集使用个人信息行为认定方法》等法律法规规定，依法查处“超凡清理管家”等 135 款违法违规 App。

经查，“超凡清理管家”等 55 款 App 存在强制索要非必要权限、未经单独同意向第三方共享精确位置信息、无隐私政策、超范围收集上传通讯录等问题，违反《个人信息保护法》等法律法规规定，性质恶劣，依法予以下架处置；“东方头条”等 80 款 App 存在频繁索要非必要权限、首次启动未提示隐私政策、未告知相关个人信息处理规则、默认勾选隐私政策、无法或难以注销账号等问题，违反《个人信息保护法》等法律法规规定，依法责令限期 1 个月完成整改，逾期未完成整改的，依法予以下架处置。

国家网信办相关负责人表示，将始终坚持依法管网、依法治网，持续强化个人信息保护领域日常监管，不断加大执法工作力度，坚决维护人民群众个人信息合法权益。[13]

2. 北京市通管局通报 20 款问题 App

10 月 29 日，北京市通信管理局（以下简称“通管局”）发布北京市通信管理局关于 20 款存在问题的 App 名单的通报。

通管局依据《网络安全法》《数据安全法》《个人信息保护法》《网络产品安全漏洞管理规定》等法律法规，对北京地区 App 开展技术检测工作。经检测发现其中 20 款游戏类 App 存在“违规收集个人信息”、“应用分发平台上的 App 信息明示不到位”、“App 频繁自启动和关联启动”、“未按法律规定提供账号注销、删除、更正个人信息功能或未公布相关投诉举报方式”、存在“应用数据任意备份风险”等数据安全隐患、“违规向他人提供个人信息”等相关问题。

[13] 国家网信办官方网站。

通管局要求问题 App 相关企业立即整改，并于 11 月 15 日前提交整改报告。逾期不整改或整改不到位的，将依法依规处置。[14]

3. 河北省网信办通报 43 款问题 App

10 月 24 日，河北省互联网信息办公室（以下简称“河北省网信办”）发布《关于“简动”等 43 款 App 违法违规收集使用个人信息情况的通报》。

针对群众反映强烈的 App 非法获取、超范围收集、过度索权等侵害个人信息的现象，河北省网信办依《网络安全法》《数据安全法》《个人信息保护法》《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法律法规，组织对运动健身类、房屋租售类等常见类型且公众大量使用的 300 余款 App 收集使用个人信息的情况进行了检测，发现“简动”等 43 款 App 存在违法违规收集使用个人信息的行为。河北省网信办要求相关 App 运营者于通报发布之日起 15 个工作日内完成整改，逾期未完成的，将依法依规予以处置。[15]

4. 上海市通管局通报未落实通信网络安全防护管理要求的单位

上海市通信管理局（以下简称“通管局”）定期对本市电信和互联网企业的通信网络安全防护管理情况进行督查审查，并于 10 月 28 日发布《关于通信网络安全防护管理情况的通报》。

前期，通管局公开通报了 42 家存在未落实通信网络安全防护管理要求等违规行为的单位，并责令其限期整改。经复测核查，尚有 16 家单位未按照要求落实整改。通管局依据《网络安全法》《公共互联网网络安全威胁监测与处置办法》等法律法规要求，对上述 16 家单位的相关通信网络系统采取了停止互联网服务等措施。同时，经检查发现 15 家单位提交的 15 个定级系统存在反复提交仍未落实整改要

[14] 北京市通信管理局官方微信公众号。
[15] 河北省网信办官网。

求等问题。依据《网络安全法》《通信网络安全防护管理办法》等法律法规要求，通管局将依法依规组织开展处置和执法工作。[16]

5. 12 省网信办开通数据出境安全评估申报通道

国家互联网信息办公室编制了《数据出境安全评估申报指南（第一版）》，于 9 月 1 日发布，对数据出境安全评估申报方式、申报流程、申报材料等具体要求作出了说明。随后，多省网信部门陆续开通了数据出境安全评估通道，以指导和帮助数据处理者规范、有序申报数据出境安全评估。目前，我国已有山东省、福建省、海南省、上海市、浙江省、江苏省、北京市、天津市、河北省、贵州省、重庆市、内蒙古自治区共 12 省份开通了数据出境安全评估通道。[17]

申报通道汇总请参见：https://www.secrss.com/articles/48507

6. 欧洲数据保护委员会更新监管机构识别指南

10 月 21 日，欧洲数据保护委员会对第 8/2022 号指南中关于确定数据控制者或数据处理者的主要监管机构的更新部分向公众征求意见。本次更新和公众咨询涉及该指南第 29 到 34 段和附件 2.d.下的第(ii)和(iii)点。反馈意见截止于 2022 年 12 月 2 日。

此次更新的主要内容针对数据共同控制者的情形，该指南在 29 段指出：“《通用数据保护条例》（GDPR）没有具体指明在欧洲经济区设立有两个或更多数据控制者来共同决定处理目的和手段时——即共同控制者的情况下——如何确定一个主要的监管机构。”

根据新指南，共同控制者不能拥有一个共同的主要监管机构（lead supervisory authority），每个控制者需要分别确定一个主要机构并参与到欧盟“一站式”的执法调查中。这意味着，如果共同控

[16] 上海市通信管理局官方微信公众号。
[17] 安全内参。

制者需按照 GDPR 规定履行数据泄露事件通知义务时，每个数据控制者都必须将数据泄露事件通知其各自的主管监管机构。

对此，该指南明确了当涉及共同控制者时如何确定主要监管机构：(ii)分别确定每个共同控制者在欧洲经济区的中央管理机构（central administration）所在地（若此情形适用）；(iii)中央管理机构所在国的监管机构是各共同控制者的主要监管机构。[18]

[18] 欧盟数据保护委员会官网。

环球律师事务所
GLOBAL LAW OFFICE

相关新闻

1. 广东省高院发布六件个人信息保护典型案例

正值《个人信息保护法》施行一周年之际，广东省高级人民法院发布一批个人信息保护经典案例，其中包括2个刑事案件、4个民事案件，涵盖严厉打击侵犯公民个人信息犯罪、防止个人信息“过度收集”、保障行使个人信息查阅复制权、规范网络平台依法使用个人信息等内容。案件如下：

一、蔡某某等人非法买卖个人信息案：网络科技公司贩卖公民个人信息，情节特别严重，构成侵犯公民个人信息罪。

二、蔡某侵犯公民个人信息案：物流人员非法获取并出售公民个人信息，并从中非法获利，构成侵犯公民个人信息犯罪。

三、周某某诉某电子商务公司个人信息保护纠纷案：依法保护个人信息查阅复制权，引导个人信息处理者合规经营。

四、张某等人诉某商家网络侵权责任纠纷案：商家服务遭差评而擅自公布消费者个人信息应被认定为侵权。

五、杨某诉某互联网公司名誉权纠纷案：网贷平台向第三方提供其掌握的欠款人个人信息构成对公民个人信息的侵犯。

六、李某某诉某网络科技公司网络侵权责任纠纷案：网络平台未经用户许可监测、读取手机剪贴板信息属于对个人隐私权的侵害。[19]

2. 住建部和民政部开展完整社区建设试点工作，推进智能化服务

10月31日，住房和城乡建部网站发布《住房和城乡建设部办公厅 民政部办公厅关于开展完整社区建设试点工作的通知》（以下简称《通知》）。

[19] 广东省高级人民法院官网。

《通知》明确，试点工作自2022年10月开始，为期2年，重点围绕以下四方面内容探索可复制、可推广经验：（一）完善社区服务设施，规划建设社区综合服务设施、幼儿园、托儿所、老年服务站、社区卫生服务站以及便民商业服务设施等；（二）打造宜居生活环境，加强供水、排水、供电、道路、供气、供热、安防、停车及充电、慢行系统、无障碍和环境卫生等基础设施改造建设，落实海绵城市建设理念；（三）推进智能化服务，引入物联网、云计算、大数据、区块链和人工智能等技术，建设智慧物业管理服务平台，促进线上线下服务融合发展；（四）健全社区治理机制。[20]

住房和城乡建设部、民政部将会同有关部门加强调研指导，结合城市体检评估对完整社区试点工作情况进行综合评价，遴选一批完整社区样板，在全国范围内宣传推广。

3. 国新办发布《携手构建网络空间命运共同体》白皮书

国务院新闻办公室于11月7日发布《携手构建网络空间命运共同体》白皮书。白皮书介绍了新时代中国互联网发展和治理理念与实践，分享中国推动构建网络空间命运共同体的积极成果，展望网络空间国际合作前景。

白皮书共约2.4万字，以中、英、法、俄等八个语种发布。白皮书介绍，截至2021年，中国数字经济规模达到45.5万亿元，占国内生产总值比重为39.8%。截至2022年6月，中国网民规模达10.51亿，互联网普及率提升到74.4%。5G移动电话用户数达4.55亿，建成全球规模最大5G网络，成为5G标准和技术的全球引领者之一。

白皮书指出，随着新一轮科技革命和产业变革加速推进，互联网让世界变成了“地球村”，国际社会越来越成为你中有我、我中有你的命运共同体。白皮书说，中国立足新发展阶段、贯彻新发展理念、构建新发展格局，建设网络强国、数字中国，在激发数字经济活力、推进数字生态建设、营造清朗网络空间、防范网络安全风险等方面不

[20] 住房和城乡建设部官网。

断取得新的成效，为高质量发展提供了有力服务、支撑和保障，为构建网络空间命运共同体提供了坚实基础。

白皮书指出，互联网是人类的共同家园，让这个家园更繁荣、更干净、更安全，是国际社会的共同责任。中国愿同世界各国一道，共同构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间，携手构建网络空间命运共同体，开创人类更加美好的未来。[21]

白皮书详细内容请见：http://www.gov.cn/zhengce/2022-11/07/content_5725117.htm

4. 全球隐私大会通过有关面部识别技术中数据保护的决议

10 月 24 日，120 多个数据保护机构在土耳其伊斯坦布尔召开了第 44 届全球隐私大会，本次大会以“平衡问题——技术飞速发展时代的隐私”为主题。与会者讨论了国际关注和关注的隐私问题，例如面部识别技术、人工智能、大数据、网络上的大规模监控、区块链和元宇宙以及跨境数据传输。

大会通过了《关于在面部识别技术中适当使用个人信息的决议》。该决议提出了在使用面部识别技术时需要遵守的六项原则，包括：（1）合法性原则，使用人脸识别应具有收集和使用生物特征信息的明确合法依据；（2）合理性、必要性和相称性原则，应建立并能够证明其使用面部识别技术的合理性、必要性和相称性；（3）人权保障原则，尤其应评估和防止对隐私和其他人权的非法或任意干涉；（4）透明度原则，面部识别的使用对受影响的个人和群体应该是公开透明的；（5）问责原则，面部识别的使用应建立明确有效的问责机制；（6）数据保护原则，面部识别的使用应遵守所有数据保护原则。

参与的数据保护机构承诺将共同努力，向外部相关团体及其他组织推广这些原则，评估开发人员和用户对这些原则的实际应用，并向大会汇报数据保护机构的进展。[22]

[21] 中国政府网。
[22] 加拿大数据保护机构官网。

5. 因违法收集人脸图像数据，美国面部识别公司被罚 2 千万欧元

10 月 20 日，由于美国的面部识别公司 Clearview AI 没有对法国数据保护机构法国国家信息与自由委员会（CNIL）此前发出的通知作出任何回应，CNIL 限制委员会决定依据欧盟《通用数据保护条例》（GDPR）第 83 条，对 Clearview AI 处以最高 2,000 万欧元的罚款，并责令 Clearview AI 停止在没有法律依据的情况下收集和使用法国用户的数据，并删除已经收集的数据。

Clearview AI 从包括社交媒体在内的多个网站处收集所有可直接访问的照片（即无需登录账户就可查看的照片），还从所有平台上的在线视频中提取照片。该公司已经通过该方式在全球范围内收集了超过 200 亿张图片。此外，该公司的人脸识别技术可以应用于搜索引擎的检索，并能根据照片找到对应的个人。为了达到这种目的，该公司建立了一个“生物识别模板”，即人脸的数字表示，能够以独特的方式完成识别。然而，绝大多数照片被收集的个人都对 Clearview AI 的处理行为并不知情。

截至 2020 年 5 月， CNIL 收到若干个人对 Clearview AI 人脸识别软件的投诉，称其违反了 GDPR。2021 年 5 月，国际隐私组织也就 Clearview AI 对于人脸数据的处理行为向 CNIL 发出警告提示。根据 CNIL 开展的调查显示，Clearview AI 构成：（1）非法处理个人数据（违反 GDPR 第 6 条），因为其收集和使用生物识别数据的行为缺乏法律依据；（2）未能以有效方式维护个人权利，特别是对其数据的访问请求（违反 GDPR 第 12、15 和 17 条）。

2021 年 11 月 26 日，CNIL 主席决定向 Clearview AI 发出正式通知，要求该公司停止收集和使用法国境内人员的数据，为个人权利的行使提供便利，并满足个人提出的删除请求。Clearview AI 有两个月的时间来遵守通知中的要求，并向 CNIL 说明理由。然而，该公司并没有对此作出任何回应。因此，CNIL 主席将该事项提交给负责发布制裁的限制性委员会。根据提请，限制委员会依据 GDPR 第 83 条对 Clearview AI 作出了处罚。[23]

[23] 法国国家信息与自由委员会官网。

6. 英国公司因数据泄露被英国数据保护机构罚款 440 万英镑

10 月 24 日，英国信息专员办公室（ICO）宣布对一家建筑公司集团的英国母公司 Interserve Group Limited（Interserve）2020 年发生的一起数据泄露事件处以 440 万英镑的罚款。

2020 年 5 月，Interserve 向 ICO 报告了一起数据泄露事件，其中大约 113,000 名现任和前任员工的个人数据遭到泄露。这些数据包括电话号码、电子邮件地址、国民保险号码、银行账户详细信息、出生日期、婚姻状况、出生国家、性别、教育和工资，以及 GDPR 第 9 条所指的“特殊类别个人数据”，例如种族、残疾、健康信息、宗教和性取向。

该数据泄露事件的原因是公司内部员工将一封网络钓鱼电子转发给另一名员工，该员工打开了链接，将恶意软件安装计算机上，致使恶意软件侵入到 Interserve 服务器并加密了存储在此处的个人数据，使得 Interserve 无法访问这些数据。

调查中，ICO 发现 Interserve 在不兼容的操作系统上处理个人数据，这违反了公司内部政策和行业最佳实践。同时 Interserve 没有遵循技术安全基础设施和网络管理标准，并且未能通过实施适当的检测、预防和恢复控制来实施适当的端点保护。Interserve 也未能按照行业惯例和内部标准进行充分的漏洞扫描和渗透测试，没有要求对所有员工进行信息安全培训。此外，Interserve 对事件响应不充分，太多的员工在系统内拥有管理权限。ICO 认为 Interserve 违反了 GDPR 第 5(1)(f) 条和第 32 条。其中，第 5 条要求数据控制者以确保适当安全的方式处理个人数据；第 32 条规定实施适当的技术和组织措施，并及时恢复对个人数据的访问。

而在评估罚款数额时，ICO 考虑了事件的严重性和持续时间，包括公司对数据安全的疏忽态度，以及 Interserve 对事件的反应。ICO 将早期的数据泄露事件视为加重因素，但将公司独立和积极投资于补救措施（例如更新其服务器、减少具有管理权限的个人数量、实施新

的企业级端点保护）并任命首席信息保护官视为减轻因素。最终，ICO 决定处以 4,400,000 英镑的罚款。[24]

7. 美国联邦贸易委员会对 Chegg 数据泄露事件采取行动

10 月 31 日，美国联邦贸易委员会（FTC）宣布对教育技术服务提供商 Chegg Inc.发布一项拟议命令，控诉该公司因安全失误导致的数据泄露事件，致使约 4000 万客户和员工的个人信息泄露，由此违反了《联邦贸易委员会法》第 5(a)条。

Chegg 主要提供针对高中生和大学生的教育产品和服务，包括在线辅导和大学奖学金搜索服务。在经营过程中，该公司收集用户和员工的各类个人信息，其中包括社会安全号码、电子邮件地址、出生日期、财务和医疗数据等敏感个人信息。

在调查中，FTC 发现 Chegg 曾经发生了四次数据泄露事件。第一次是黑客通过网络钓鱼攻击 Chegg 多名员工，并访问了员工的直接存款信息。不到一年后，一位 Chegg 前承包商使用公司与员工和外部承包商共享的登录信息访问了 Chegg 的第三方云数据库，其中包含大约 4000 万客户的个人信息。在接下来的两年中，Chegg 又经历了两次涉及网络钓鱼的数据泄露事件，致使员工的敏感个人数据泄露。

FTC 认为：（1）Chegg 未能使用“商业上合理的安全措施”来保护其收集和存储的个人信息；（2）Chegg 以纯文本形式将个人数据存储在其云存储数据库中，使用过时且弱加密来保护用户密码；（3）未能制定足够的安全政策和培训。

因此，FTC 要求 Chegg（1）详细说明并限制数据收集，规定可以收集的个人信息、收集的原因以及保留期限；（2）提供消费者对数据的访问渠道，并允许提出删除请求；（3）对客户和雇员实施多因素认证或其他认证方法；（4）实施全面的安全计划，包括对消费者数据进行加密并向员工提供安全培训。[25]

[24] 英国信息专员办公室官网。
[25] 美国联邦贸易委员会官网。

环球律师事务所
GLOBAL LAW OFFICE

环球解读

1. 个人信息保护重点条款回顾——《个人信息保护法》实施一周年观察（上篇）

前言

2021 年 11 月 1 日，《中华人民共和国个人信息保护法》（以下简称《个保法》）正式生效实施，为个人信息处理者合法合规的处理个人信息提供了明确的指引。《个保法》实施一年以来，作为个人信息处理者的各企业如何履行法律义务并将诸合规要求落地？又在哪些领域面临着挑战？本文将结合监管动态、行业实践以及企业合规落地措施与现存问题，回顾并分析《个保法》六大部分重点条款的实施情况，并对下一步企业个人信息保护合规工作予以展望。本文分上下两篇，以期为企业数据合规实践带来参考。上篇将重点关注“合法性基础条款”、“单独同意规则”以及“个人信息主体权利条款”。

一、合法性基础条款

（一）规范要求

合法性原则是个人信息处理的重要原则之一，而《个保法》第十三条明确了七项具体的合法性基础，分别是（1）取得个人的同意；（2）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；（3）为履行法定职责或者法定义务所必需；（4）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；（5）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；（6）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；（7）法律、行政法规规定的其他情形。下文将对其中的四个条款展开分析重点说明企业目前的落地情况及实施展望。

（二）落地情况

1、取得个人的同意

“取得个人的同意”是个人信息处理合法性基础的明星条款，在《个保法》颁布之前，“同意”作为获取个人信息的合法性事由曾经一统天下。即便在《个保法》实施后，“同意”与第十三条的其他六项合法性基础并列，并且还被规定当且仅当其他合法性基础无法满足适用时，“同意”才能出场作为合法依据。并且，在实践中，在用户作出“同意”的意思表达之前，“告知”与“同意”常常伴随出现，共同体现在相关产品的隐私合规设计中。《个保法》第十七条规定的“告知”义务则是个人信息处理者开展处理行为的基础。例如，个人信息处理者通常通过“隐私政策的弹窗”形式完成告知，并会在相关页面设置勾选框或者通过同意按钮来取得用户的同意。同时，为了确保用户是在充分知情的情况下给出的同意，部分 App 还会在用户点击隐私政策后锁定同意按钮，强制用户翻阅完隐私政策后才能勾选“同意”或“不同意”；或者要求用户在一定时间（例如十秒钟）后才能勾选“同意”或“不同意”（图 1）。同时，以用户“主动”明示勾选，而非采用默认勾选隐私政策等非明示方式，也已成为实施个人信息主体“同意”的“标准”方式。

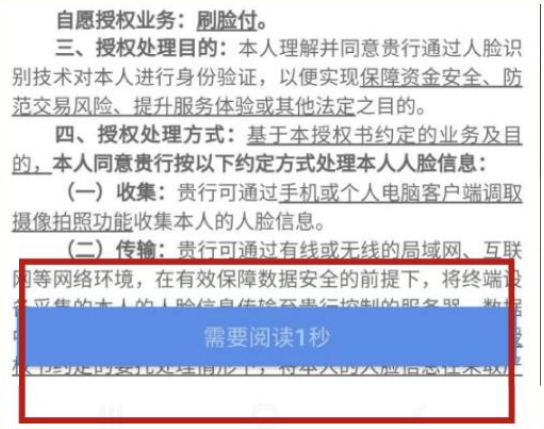


图 1

2、订立、履行合同所必需

当个人作为一方当事人与作为另一方当事人的处理者正在订立合同或者履行已经成立的合同时，处理者必须处理该个人的某些个人信息才能与之缔结合同或履行合同，该个人明知且自愿提供其个人信息以促成合同的缔结或者履行。这种情形仅适用于处理者与个人作为平等的民事主体之间订立或履行合同的场合。在实践中，较为常见的是在电子商务经营过程中，网店在接受顾客的订单后为了向顾客交货，不得不向用户收集收货人姓名、收货地址和联系方式。如果顾客通过银行转账或信用卡支付，那么网

店就需要处理顾客的银行卡信息账号或信用卡信息。以上这些场景下的个人信息处理行为均可以通过合同所必需这一项合法性基础进行支持。[26]但在实践中，即使这类案例还可以举出很多，但是由于对合同成立要件以及是否构成合同成立或履行所必须的要素判断，需要有较高的法律理论功底和实务经验，无论是企业还是执法机关均很有可能在实操中无法对某一特定事例快速达成一致理解。鉴于此，目前此事由在实践中被应用的机会反而不多。

3、法定职责与法定责任

所谓“法定职责”包括法定职权和法定责任，是指国家机关依据法律法规的规定而享有的职权以及必须履行的义务。为确保国家机关法定职责的履行，在此过程中获取所必需的个人信息不需取得个人同意。例如，我国《刑事诉讼法》第一百三十二条第一款规定：“为了确定被害人、犯罪嫌疑人的某些特征、伤害情况或者生理状态，可以对人身进行检查，可以提取指纹信息，采集血液、尿液等生物样本。”此时，公安机关或检察机关为侦查犯罪而强制收集个人生物识别信息等，就属于履行法定职责；又例如《出境入境管理法》第七条规定，经国务院批准，公安部、外交部根据出境入境管理的需要，可以留存出境入境人员的指纹等人体生物识别信息。如果国家机关将履行法定职责作为处理个人信息的合法性基础，根据《个保法》第三十四条，则应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

而“法定义务”是指个人信息处理者依据法律法规的规定而负有的义务。对于“法定义务”的“法”的范围和层级，立法者并没有给予明确的界定，而学者们对此也多有争论。[27]较为常见的法定义务诸如，在社会保险的征缴中，《社会保险法》要求企业收集参保员工的相关个人信息；在金融安全领域，《反洗钱法》第三条要求金融机构建立健全客户身份识别制度、客户身份资料和交易记录保存制度。在实践中，除了法律以外，也有部门规章给个人信息处理者施加了法定义务。例如，《互联网信息服

[26] 参见程啸,王苑：《论个人信息处理中无需取得个人同意的情形》，载《人民司法》2021 年第 22 期，第 79 页。

[27] 学者们大致分为“狭义”和“广义”两派。“狭义说”认为“法”应该仅限于“法律和行政法规”，而“广义说”认为“法”是广义的法，既包括全国人大及其常委会颁布的法律，也包括行政法规、地方性法规、部门规章和地方政府规章等规范性法律文件。

务管理办法》第十二条要求互联网信息服务提供者应当展示合理范围内的互联网用户账号的互联网协议（IP）地址归属地信息；《移动互联网应用程序信息服务管理规定》则要求应用程序提供者对申请注册的用户进行基于移动电话号码、身份证件号码或者统一社会信用代码等方式的真实身份信息认证。上述规定下的有关个人信息处理者，均可依据“法定义务”的合法性基础处理相关主体的个人信息。

除此之外，“法定义务”更多被运用在个人信息的保存期限制度上，即当个人信息处理者因履行这些“法定义务”而存储相关信息时，无需取得个人的同意。下表为部分法律法规规定的保存期限汇总。

法律规定	数据类型	最低保存期限
《互联网信息服务管理办法》第14条	信息内容及其发布时间、互联网地址或者域名	60日
《互联网电子邮件服务管理办法》第10条	邮件的发送接收、发送者和接收者的邮件地址与IP地址	
《互联网文化管理暂行规定》第20条	文化产品内容及其时间、互联网地址或者域名	
《互联网直播服务管理规定》第16条	使用者发布内容和日志信息	
《网络表演经营活动管理办法》第13条	网络表演视频资料	
《网络安全法》第21条	网络日志	6个月
《网络预约出租汽车经营服务管理暂行办法》第27条	采集的个人信息和生成的业务数据	2年
《规范促销行为暂行规定》第19条	设奖规则、公示信息、兑奖结果、获奖人员信息	
《电子商务法》第31条、《网络交易监督管理办法》第20条	商品和服务信息、交易信息	3年
《网络招聘服务管理规定》第26条	招聘信息、服务信息	
《道路旅客运输及客运站管理规定》第67条	采集的个人信息和生成的业务数据	
《反洗钱法》第19条	客户身份资料和交易记录	5年
《征信业管理条例》第16条第1款	个人不良信息	
《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》第29条	客户身份资料和交易记录	
《非银行支付机构网络支付业务管理办法》第16条	操作记录	
《网络借贷信息中介机构业务活动管理暂行办法》第23条	网络借贷业务活动数据和资料	

《缺陷汽车产品召回管理条例》第 11 条	汽车产品相关信息记录	
《电子签名法》第 24 条	与电子认证相关的信息	
《会计档案管理办法》第 14 条	会计档案	10 年和 30 年
《医疗机构病历管理规定》第 29 条	病历	15 年和 30 年
《证券法》第 137 条	客户开户资料、委托记录、交易记录和与内部管理、业务经营有关的各项信息	20 年
《精神卫生法》第 47 条	病历资料	30 年
《不动产登记暂行条例》第 13 条第 1 款	不动产登记簿	永久保存

4、突发公共事件

根据《突发公共卫生事件应急条例》第 2 条，“突发公共卫生事件”是指突然发生，造成或可能造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒以及其他严重影响公众健康的事件。在我国新冠肺炎疫情的防控过程中，借助大数据分析手段，位置信息、行动轨迹等个人信息在疫情预测预警、人员流动监控、物资调配分发等方面发挥了重要作用。而这些个人信息的处理行为很多都依赖于本项合法性基础，例如，各地健康宝对个人信息的处理。

（三）合规展望

合法性基础是个人信息处理行为的基石。《个保法》规定的七种合法性基础，各自有不同的实现要件和门槛。在实践中，企业仍需要对于这些合法性基础进行深入研究，方能准确地把握不同事由所对应的适用场景，避免企业应选取合法性基础错误或者不够准确而被认定为违法违规处理个人信息。

二、“单独同意”规则

（一）规范要求

《个保法》第十四条设立了“单独同意”制度，要求在法定情形下，个人信息处理者必须就其处理目的、行为等单独向个人

告知并取得同意，它是对《个保法》第十三条第二款第一项“同意”作为合法性基础的补充。

在《个保法》中，需要取得单独同意的场景包括：向其他个人信息处理者提供其处理的个人信息（第二十三条）、公开个人信息（第二十五条）、公共场所安装监控或身份识别信息（第二十六条）、处理敏感个人信息（第二十九条）以及向境外提供个人信息（第四十条）。

（二）落地情况

1、向其他个人信息处理者提供个人信息

在实践中，部分个人信息处理者的 App 产品在登录注册时允许用户使用其他平台的账号进行登录，此时便会存在用户的账号信息在两个处理者之间共享。此时，合规实践较好的 App 会跳出弹窗（单独授权）页面，将账号信息授权事项（明示）告知给用户，并征得用户对该共享的单独同意（如下图 2）。

图 2

此外，在一些聚合类打车平台上，当用户使用第三方打车平台服务时，平台也会弹出单独的告知页面，有些第三方出行企业还会展示自己（而非默认同意打车平台）的隐私政策并取得用户的单独同意（如下图 3）。

图 3

2、公开个人信息

绝大多数企业在业务过程中并不需要也不会公开其所收集的用户/客户的个人信息。实践中，更多时候个人信息公开是个人信息主体的主动选择行为。例如，某 App 公开抽奖活动的中奖人名单（有些还涉及公开微信昵称、头像或者手机号），此时企业需要在用户参与中奖活动前提供活动规则以及中奖后处理用户个人信息的情况，以供用户选择同意，同时也需要对公开的信息进行去标识化等处理措施。如企业会在隐私政策中告知用户“如必须公开时，我们会向您告知此次公开的目的、所公开信息的类型以及可能涉及的敏感个人信息，并征得您的明示同意”。除了单独同意外，企业也会在隐私政策中告知其他非基于同意的公开场景，例如基于法律法规或司法程序要求、保护其他方的人身财产安全等（如图 4）。

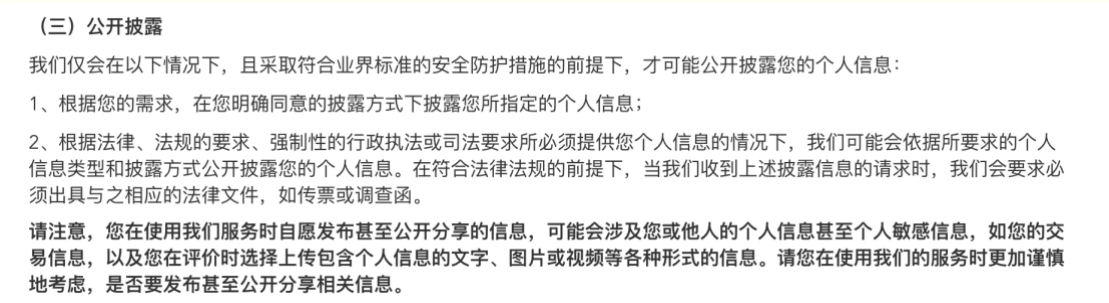


图 4

3、在公共场所安装监控或身份识别信息设备

例如315所爆光，某企业在线下门店安装带有人脸识别功能的摄像头，未告知客户并获取其同意，也无其他《个保法》下合法性基础的情况下违法违规处理个人信息，此类事件一直以来为社会各界所关注。《个保法》规定，除取得个人“单独同意”外，个人信息处理者在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的。

对于在线下门店安装摄像头采集个人信息的行为，监管部门对于构成有效的“单独同意”标准已较为严格。例如，在杭州房产置业公司案件中，虽然房产公司在售楼部主出入口、人脸识别摄像头安装点粘贴写有“温馨提示：本售楼处安装有人脸识别系统，您已进入视频监控区域，我们承诺保护您的人脸等信息安全，详情可扫描二维码或询问接待人员了解”字样的监控警示牌，并在警示牌旁放置二维码，内嵌《关于收集个人信息的知情同意书》。但经检察机关随机抽取10名客户进行询问，客户均表示自己对售楼部现场收集人脸生物识别信息、身份信息的情况并不知情，更未自愿作出同意的表示。《信息安全技术 个人信息安全规范》第3.6条规定，明示同意需要个人信息主体通过书面、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。而检察机关认为房产公司未能取得到访客户的书面同意，不能认为有效地取得了到访客户的“单独同意”，故不能将购房者的人脸信息用于监控安全以外的其他目的，特别对购房者进行精准营销或者通过结合其他数据对顾客进行大数据杀熟。

4、处理敏感个人信息

敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，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。国家标准《信息安全技术 个人信息安全规范》在附录中列出了敏感个人信息的类型示例。

对于敏感个人信息的单独同意，较为常见的是当涉及 App 向终端设备索取系统权限后收集敏感个人信息时，App 会通过跳出弹窗（修改系统弹窗的授权措词或者增加告知浮窗）的形式让用户充分知悉授权的目的与方式、获取敏感个人信息的类型，并获取用户的“单独同意”（如图 5）。

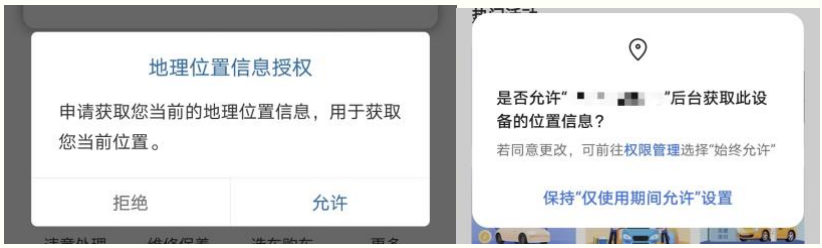


图 5

对于一些特殊行业的企业而言，在业务过程中有更多，更频繁的敏感个人信息的处理需求，此时能否有效地取得用户的单独同意成为避免合规风险的关键。例如，部分企业在用户登录或开展业务时会要求用户进行人脸识别验证。而人脸信息是典型的敏感个人信息，因此在识别之前需要通过例如弹窗或单独页面方式取得用户的单独同意（如图 6）。

图 6

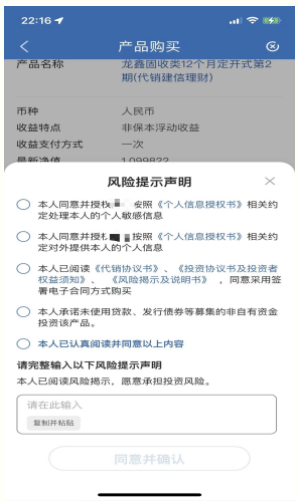


图 7

而在客户投资、购买理财产品时，金融机构往往需要取得客户对多个事项的同意，不仅包括敏感个人信息的处理，还可能包括风险提示以及其他金融资管的合规要求。为了将多个同意事项均能有效告知客户并落地单独同意要求，部分 App 产品采取了分段告知并逐项取得用户同意的方式（如图 7）。

5、向境外提供个人信息

《个保法》第三十九条要求个人信息处理者在向境外提供个人信息时向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

在实践中，相关 App 产品会在触发可能向境外传输个人信息的场景时，通过单独勾选的方式取得用户的单独同意。例如，在某 App 产品中，当用户订购国际机票时，订单下方的“下一步”按钮旁会显示《个人信息授权声明》。点击进入后，用户能看到《个保法》第三十九条要求的告知事项（如图 8）。

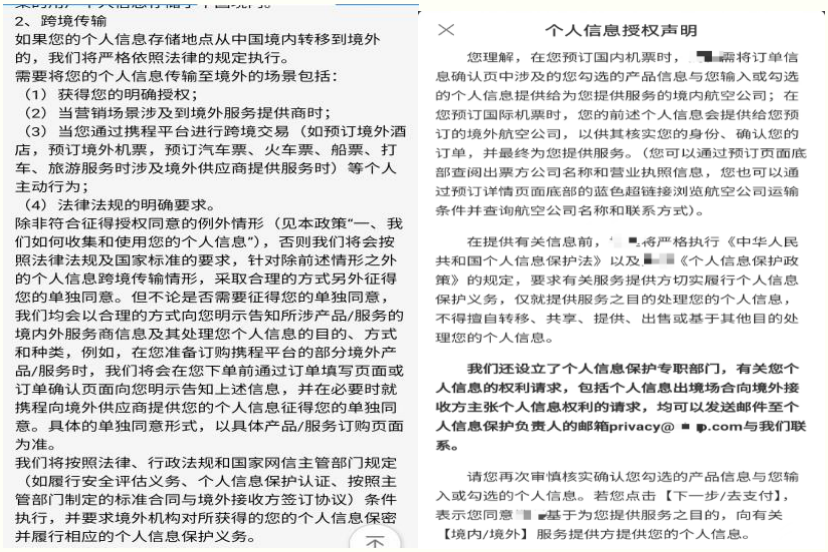


图 8

又如，某奢侈品网购小程序中在用户下单页面直接展示了与跨境传输个人信息相关的告知事项，并通过勾选框的形式征得用户的单独同意（如图 9）。

图 9

（三）合规展望

单独同意是个人信息保护的一项重点，也是企业经营过程合规与业务增长碰撞最为激烈的方面。究其原因，一方面，目前《个保法》对于“单独同意”的规定较为笼统，对于企业精准把握落地思路存在较多的不确定性；《网络数据安全管理条例（征求意见稿）》对“单独同意”进一步明确内涵与定义，即单独同意是指数据处理者在开展具体数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意，应当引起个人信息处理者的高度重视。[28]另一方面，从目前来看，个人信息主体在个人信息跨境传输、公共场所安装监控或身份识别信息设备、敏感个人信息处理（如在线问诊等产品）等领域，履行与落单独同意义务实仍有较大的改善空间。所幸，我们也不乏能看到一些企业有创新之举，实属可圈可点，例如充分利用 App、小程序等产品清晰地告知用户关键事项，保护用户的重要权益。而这些实践案例可以为各行业未来履行法律规定和合规要求提供一个参考范例。

三、个人信息主体权利条款

（一）规范要求

《个保法》第四章规定了个人信息主体在信息处理活动中享有的权利，分别是第四十四条的知情决定权、第四十五条的查阅复制权和可携带权、第四十六条的更正权、第四十七条的删除权、第四十八条的要求解释说明权以及第四十九条与逝者个人信息保护相关的权利。同时，第十五条给予了用户撤回同意的权利。此外，《个保法》第五十条还要求个人信息处理者应当建立便捷的个人行权申请受理和处理机制。

（二）落地情况

1、知情决定权

[28] 《网络数据安全管理条例（征求意见稿）》第七十三条（八）。

个人信息主体的知情权在实践中具体体现为对“告知”内容的了解，以及在此基础上作出是否允许个人信息处理者收集自己的个人信息。近年来监管部门在不断尝试优化处理者告知的方式。例如，工信部开展了“信息通信服务感知提升行动”，要求个人信息处理者建立“已收集个人信息清单”和“与第三方共享个人信息清单”（即“双清单”），清晰地列出 App（包括内嵌第三方软件工具开发包 SDK）收集和共享用户个人信息的基本情况。实践中，企业大多会将“双清单”放置在 App 的“设置”或“隐私管理”菜单栏中，或者嵌入隐私政策（如图 10）。在第三方共享清单中，企业还会区分共享/委托处理场景、关联场景以及第三方 SDK 场景，并分别制作清单展示。此外，“感知提升行动”还要求企业优化隐私政策和权限调用的展示方式，向用户提供 App 产品隐私政策摘要和清晰简易的权限调取信息，以使得用户更为便捷清晰地了解相应内容（如图 11）。

图 10

图 11

2、查阅与更正权

实践中，目前大多数企业基本上都为用户提供了专门的“个人信息查阅”的菜单，集中向用户披露企业所运营的终端设备收集用户的个人信息情况。但同时，“双清单”中的“个人信息收集清单”也在实践中部分承担了满足用户查阅权的功能。App 端的“个人信息收集清单”往往会设置成多级菜单，用户点击某一信息类型后便可以看到自己相应的个人信息，同时可在相应的个人信息栏中更改或补充部分个人信息（如下图 12）。同时，App 在用户申请查询时，也存在要求用户先进行身份验证，确保个人信息在查询时处于安全的设置（如下图 13）。

图 11

图 12

3、复制移转权

《个保法》第四十五条第二款、第三款规定了“复制转移权”。虽然法律目前没有明确行使可携带权的途径和条件，但现实中部分企业已经开始了探索。实践中，企业允许用户下载其收集的部分个人信息，但尚不能实现“转移”的功能。对于 App 提供的个人信息副本，内容大多较为简单，例如用户的基本个人资料等或账户信息个人信息（用户名、头像、注册信息等）。在下载路径方面，最普遍的提供途径为邮箱接收，根据不同类型企业的实践，一般当用户提交下载申请后的几分钟至数小时内便能收到企业传输的该请求用户的个人信息（如图 13）。如果需要企业进一步提供用户的其他个人信息，通常则需要向企业公开的联系方式提出请求。而企业提供下载的个人信息格式却有很大不同，有的企业提供的是 txt 文本，而有的则是 js 和 css，实践中尚未实行统一化处理，实际上企业向用户提供的个人信息格式往往已经从其内部数据库存储的格式进行过一次转码了，目的是保护内部数据库数据的安全和保密。

此外，根据相关司法案例可知，[29]法院认为个人信息主体实现复制权的客体范围既包括个人信息，也包括个人信息处理的相关情况，例如账户信息、设备信息、日志信息、与第三方共享的个人信息等；而行业惯例虽可以从一定程度上体现个人信息保护水平与相关行权成本，但并非个人信息处理者拒绝提供相应个人信

[29] 参见（2021）粤 0192 民初 17422 号、（2022）粤 01 民终 3937 号。

息的法定理由。从这个角度看，司法实践要求个人信息处理者需要切实落实个人信息主体对于复制权的行权要求。

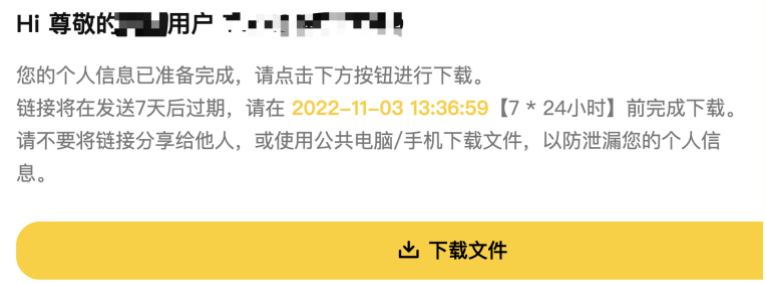


图 13

4、撤回同意权

《个保法》第十五条规定，基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。实践中，“权限”和“第三方共享”领域已经逐渐探索出了较为成熟的用户权利行使方式。很多 App 会在“权限管理”选项中允许用户对于特定权限进行自主地设置（即设置授权或者撤回授权的按钮），而部分 App 则需要用户跳转至终端设备系统的“设备管理”中才能操作对权限设置的修改（如图 14）。同时也有一些 App 专门为用户设置了管理第三方共享信息的开关，允许用户便捷地撤回授权和同意（如图 15）。

图 14

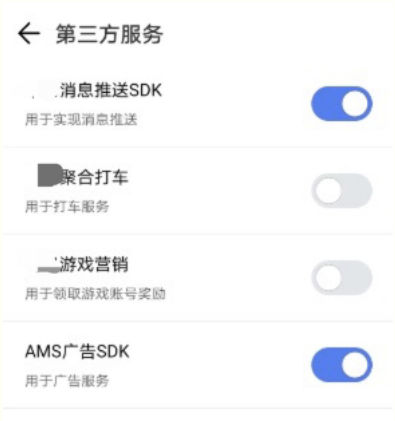


图 15

5、与自动化决策相关的权利

根据《个保法》第四十八条，个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。该项权利更多地被运用在自动化决策领域。除了解释说明，个人信息处理者在进行自动化决策时还需要确保决策的透明性和结果的公平公正，允许信息主体便捷地拒绝。目前，“个性化推荐关闭”功能已经在大多数具备此功能的 App 中落地，除了简单的开启或关闭外，部分 App 还允许用户对于个性化的标签进行管理（如图 16）。在实践中，部分企业会在隐私政策中公示自己所使用的算法，并通过独立说明的方式对基本原理、目的与主要运行机制进行说明，以满足相关法规要求（如图 17）。

图 16


二、算法原理说明

1、个性化推送类算法

算法名称	推荐算法
算法基本原理	为向 平台电商用户展示商品或服务信息，包括用户的访问足迹、历史搜索情况，我们会收集和使用用户在访问或使用 时的浏览、搜索记录。我们会结合依法收集的设备信息、服务日志信息，以及其他取得用户授权的信息，通过算法模型预测人群偏好特征。我们会基于人群偏好特征在 及其他第三方应用程序向相关人群推送可能感兴趣的商业广告及其他信息，或者商业性短信息。
算法运行机制	个性化推荐类算法会基于模型预测人群偏好特征，匹配人群可能感兴趣的商品、服务或其他信息，对展示的商品、服务或其他信息进行排序。我们会根据用户使用产品过程中的浏览行为，对推荐模型进行实时反馈，不断调整优化推荐结果。为满足多元需求，我们会在排序过程中引入多样性打散机制，拓展推荐的内容，避免同类型内容过度集中。 如用户不想看到我们在首页或支付完成页面等推荐的商品或服务，用户可以通过长按被推荐的商品或服务图片，在随后出现的弹窗中根据提示选择屏蔽类似商品或者商品或服务所属的类目；如用户想管理我们为其推送的个性化内容，可以在 “ -设置-隐私设置-推荐管理”中进行设置。
算法应用场景	平台首页、逛逛、支付完成页面等的商品或服务信息展示
算法目的意图	向用户展示商品或服务信息

图 17

6、删除权

实践中，删除权已经融入了日常的使用过程中，大部分 App 会给用户提供删除使用记录、历史记录、删除缓存的选项。而在

社交平台上，用户可以选择行使删除权的空间更大，可以删除的对象还包括聊天记录或在公开的朋友圈、社交小组中发表的内容记录。同时较为常见的还包括，在购物类 App 中，用户可以行权删除购物记录；在搜索类 App 中，用户可行权删除搜索记录。此外，还有 App 处理者允许用户删除“登录过的设备”记录（如图 18）。除此以外，大多数企业还会为用户提供注销账号的行权路径，并在用户注销前通过《注销须知》显著提示用户注销账号的后果，以及在哪些情况下不适用账号注销（如图 19）。

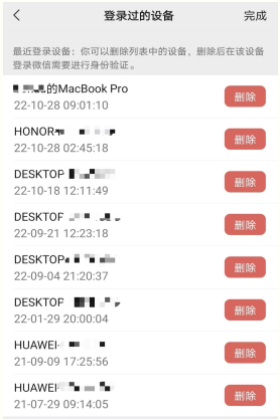
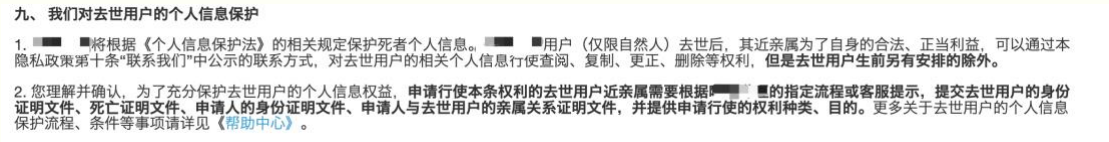


图 18

图 19

7、逝者个人信息

第四十九条规定，自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。在实践中，很多企业都在隐私政策中设置了“逝者个人信息保护”或者“逝者近亲属权利”的条款（如图 20）。


九、 我们对去世用户的个人信息保护

1. [redacted]将根据《个人信息保护法》的相关规定保护死者个人信息。[redacted]用户（仅限自然人）去世后，其近亲属为了自身的合法、正当利益，可以通过本隐私政策第十条“联系我们”中公示的联系方式，对去世用户的相关个人信息行使查阅、复制、更正、删除等权利，**但是去世用户生前另有安排的除外。**

2. 您理解并确认，为了充分保护去世用户的个人信息权益，**申请行使本条权利的去世用户近亲属需要根据[redacted]的指定流程或客服提示，提交去世用户的身份证明文件、死亡证明文件、申请人的身份证明文件、申请人与去世用户的亲属关系证明文件，并提供申请行使的权利种类、目的。**更多关于去世用户的个人信息保护流程、条件等事项请详见《帮助中心》。

图 20

目前，部分企业推出了“纪念账号”功能（如图 21）来尝试落实对于逝者个人信息的保护。当逝者的家属将逝者的账号申请为纪念账号后，账号会被冻结，之后任何人都将无法登录该账号。

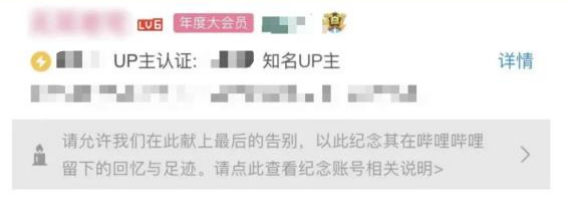
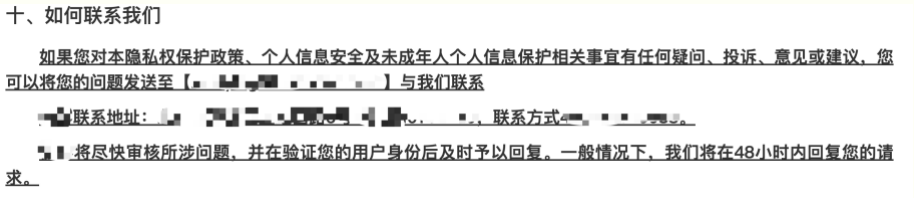


图 21

8、响应机制

实践中，很多企业会在隐私政策的末尾或者开头披露个人信息保护负责人（机构）的联系方式，多数为邮箱加上邮寄地址，有些还会同时提供客服电话。根据《App 违法违规收集使用个人信息行为认定方法》的要求，大部分企业都将承诺时间设定为 15 个工作日内，但也有企业对自己采取了更高的要求，承诺会在 48 小时内回复信息处理者的请求（如图 22）。根据实际调研可以发现，大部分主流 App 普遍在数小时内完成响应，同时较多国内 App 运营者均实现了十五个工作日内响应的法定要求。


十、如何联系我们

如果您对本隐私权保护政策、个人信息安全及未成年人个人信息保护相关事宜有任何疑问、投诉、意见或建议，您可以将您的问题发送至【 】与我们联系

联系地址： ，联系方式

将尽快审核所涉问题，并在验证您的用户身份后及时予以回复。一般情况下，我们将在48小时内回复您的请求。

图 22

（三）合规展望

信息主体的权利行使是指当个人主体的信息在受企业控制时主张其权益的有效手段，也是保护其权益免受侵害的重要途径。在《个保法》实施一周年的时间里，我们看到监管部门和各行业的个人信息处理者通过共同努力，已经为个人信息主体行使合法权利提供了良好的环境和平台。无论是从用户的知情权还是授权同意的管理，目前的实践已经较为成熟。同时，随着相关法律法规的进一步明确，诸如个人信息可携权中的另一层次—向指定第三方平台的转移权也应当被逐步探索，并寻求出行业普遍能够接受和遵循的落地施行方式，相信不会很远了。

2. 个人信息保护重点条款回顾——《个人信息保护法》实施一周年观察（下篇）

前言

承接本文上篇对《个人信息保护法》（下称“《个保法》”）中“合法性基础条款”“单独同意规则”以及“个人信息主体权利条款”的回顾，本文下篇将重点关注《个保法》中有关个人信息处理者的义务集群，即“个人信息处理者的一般合规义务”“针对特殊主体与特殊对象的个人信息保护义务”以及“特殊场景下的个人信息处理者义务”三部分内容，并尝试对个人信息保护的趋势与挑战进行简要论述，以求抛砖引玉。

据我们观察，在过往的一年中，《个保法》与2017年施行的《网络安全法》和2021年9月1日正式实施的《数据安全法》共同构建了我国网络安全、数据安全与个人信息保护的整体框架，且“三部大法”在实质内容层面也是互相耦合的。因此，我们不能抛弃《网络安全法》和《数据安全法》的背景与实施开展来单独论赏《个保法》下的义务的全面落地。这也同时意味着我们必须避免将个人信息保护同数据要素的流通利用、企业的数字化转型发展以及网络安全与国家安全保护等重要价值割裂评价，而应当坚持以整体的视野看待《个保法》及其重点规则。

以下，我们将从此视角出发，建议个人信息处理者一方面须持续关注“三部大法”及其配套法律法规与规范性文件的细化要求；另一方面也应避免生硬刻板地理解法律条文或生搬硬套他人实践。企业应当结合自身业务发展水平、行业特性、执行风格与行业普遍实施标准，尽本企业在人财物方面的最大能力，开展有效的合规管理与数据治理。并且，在落实个人信息保护责任的基础上有效发挥数据要素的利用价值，在个人信息的保护与利用之间达成效益的最大化。

一、个人信息处理者的一般合规义务

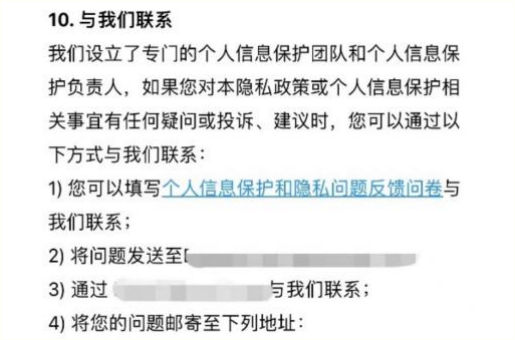
（一）内部制度的流程设计

制定与完善内部个人信息管理制度与流程，是企业数据合规体系建设的基础性工作。具体而言，个人信息处理者应当在内部管理制度或政策中明确内部管理组织与相应职责、管理方式、考核问责、合规审计等合规运作和保障机制，对内部数据安全管理、数据分类分级管理、个人信息保护影响评估、个人信息主体权利请求与响应、第三方合作伙伴管理、员工个人信息保护、个人信息安全事件应急处置、个人信息操作权限、个人信息安全培训等方面提出明确的落地要求和操作指引。

《个保法》实施一年过程中，许多企业已从面向用户的产品侧合规转向企业内部制度的搭建、落实与执行。例如，部分企业结合公司主营业务，自行或邀请外部律师按照多层级文件体系结构，梳理并设计整体数据合规与安全管理制度规范，并由公司内部相关负责机构组织公司各部门落实相关制度规范，组织宣贯、考核与内部审计执行状况。又如，针对数据分类分级这一难点问题，企业一方面制定分类分级策略、分类分级标准等内部制度指引，另一方面结合技术手段和支撑工具推行个人信息的分类分级管理，如利用数据资产梳理盘点及自动化分类分级工具开展敏感数据发现、排查、打标和数据分类分级工作，切实落地个人信息处理者的分类分级管理义务。

（二）个人信息保护负责人

《个保法》第五十二条规定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应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。实施一年以来，企业普遍采取的措施为在《隐私政策》中告知用户已设立专门的个人信息保护团队与负责人，并告知了相应的联系方式（如图 1）。个人信息保护负责人的设立旨在实现对个人信息处理者履行个人信息保护义务的指导、鞭策与协助，驱动企业选任具有专业背景与管理经验的人选负责个人信息保护工作，同时《个保法》从责任压实的角度对个人信息保护负责人的监督活动进行规制，从而真正提高企业的个人信息保护水平。从这个角度看，部分个人信息处理者还应在实践中进一步提升对个人信息保护负责人披露的透明度，例如在《隐私政策》中告知个人信息保护负责人的身份及职务等。


10. 与我们联系

我们设立了专门的个人信息保护团队和个人信息保护负责人，如果您对本隐私政策或个人信息保护相关事宜有任何疑问或投诉、建议时，您可以通过以下方式与我们联系：

1) 您可以填写个人信息保护和隐私问题反馈问卷与我们联系；

2) 将问题发送至[redacted]

3) 通过[redacted]与我们联系；

4) 将您的问题邮寄至下列地址：

图 1

除《个保法》第五十二条规定个人信息保护负责人外，《网络安全法》《数据安全法》及《信息安全技术 个人信息安全规范》（下称“《个人信息安全规范》”）均要求企业设置相关负责人。我们对其适用对象与职责简单总结为下表，建议尚未履行该义务的企业结合自身情况尽快选聘胜任的人选，并且合理设计不同法下相关责任人的配置以及与原岗位工作的兼顾比例。

设立依据	岗位名称	适用对象	职责	任职资格
网络安全法	第 21 条 网络安全责任人	第 21 条 网络运营者	第 21 条 落实网络安全保护责任	未规定
	第 34 条 专门安全管理机构和安全管理负责人	第 34 条 关键信息基础设施的运营者	未规定	第 34 条 关键信息基础设施的运营者，对该负责人和关键岗位的人员进行安全背景审查。
数据安全法	第 27 条 数据安全负责人和管理机构	第 27 条 重要数据处理者	第 27 条 落实数据安全保护责任。	未规定
个人信息保护法	第 52 条 个人信息保护负责人	第 52 条 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	第 52 条 负责对个人信息处理活动以及采取的保护措施等进行监督。	未规定
个人安全信息规范	个人信息保护负责人和个人信息保护工作机构	11.1 c） **满足以下条件之一的组织**，应设立专职的个人信息保护负责人和	个人信息保护负责人和个人信息保护工作机构的**职责**应包括但不限于：	b） 应任命个人信息保护负责人和个人信息保护工作机构，个人信息

		个人信息保护工作机构，负责个人信息安全工作： 1)主要业务涉及个人信息处理，且从业人员规模大于200 人； 2)处理超过100 万人的个人信息，或预计在12 个月内处理超过100 万人的个人信息； 3) 处理超过10 万人的个人敏感信息的。	1) 全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任； 2) 组织制定个人信息保护工作计划并督促落实； 3) 制定、签发、实施、定期更新个人信息保护政策和相关规程； 4)建立、维护和更新组织所持有的个人信息清单(包括个人信息的类型、数量、来源、接收方 等)和授权访问策略； 5) 开展个人信息安全影响评估，提出个人信息保护的对策建议，督促整改安全隐患； 6) 组织开展个人信息安全培训； 7)在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为； 8) 公布投诉、举报方式等信息并及时受理投诉举报； 9) 进行安全审计； 10) 与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。	保护负责人**应由具有相关管理工作经历和个人信息保护专业知识**的人员担任，参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作。

（三）个人信息影响评估

个人信息保护影响评估是基于风险防范理念的一项制度，关键在于检查个人信息处理行为的合法合规性，事前评估对个人信息合法权益的影响及保护措施的有效性。《个保法》将个人信息保护影响评估作为一项法定的强制性义务，明确了企业应当事前进行个人信息保护影响评估的下述场景以及评估报告和记录至少保存三年的要求：（一）处理敏感个人信息；（二）利用个人信息进行自动化决策；（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；（四）向境外提供个人信息；（五）其他对个人权益有重大影响的个人信息处理活动。评

估的内容应当包括：（一）个人信息的处理目的、处理方式等是否合法、正当、必要；（二）对个人权益的影响及安全风险；（三）所采取的保护措施是否合法、有效并与风险程度相适应。

自《个保法》实施以来，已经有越来越多的个人信息处理者将个人信息保护影响评估纳入了日常合规环节，体现隐私与产品设计相融合的理念，并将用户体验作为个人信息保护的重要衡量尺标之一。此外，目前实践中，也已有不少企业借助线上工具方式开展个人信息保护影响评估，通过创建评估问卷清单、部署风险识别库、设计风险评估表，以及跟踪风险降级流程等实现系统自动化的线上评估工作，在满足业务场景全覆盖的同时，大力提升企业各部门间沟通及管理效率。

（四）审计、记录与应急处置

个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计，以满足《个保法》对各项义务实施的检视要求。区别于事前开展的个人信息保护影响评估，企业合规审计主要体现为对个人信息处理事中及事后的风险得以监测与把控，并敦促防范企业发生个人信息安全事件。一周年的实践中，面对处理庞大数量、繁多场景下的个人信息，部分个人信息处理者已经将个人信息合规审计嵌入到各业务场景和企业年度规划中，如建立并开展专项的个人信息合规审计、年度个人信息审计、上市后个人信息保护合规审计等，但仍有大部分企业对此项工作的落实仍处于真空状态，亟待进一步改善。

同时，个人信息处理者应当建立、维护和更新其所处理的个人信息处理活动记录，记录内容可参照《个人信息安全规范》的相关规定。根据《个保法》的规定，履行个人信息保护职责的部门有权查阅、复制与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；而在发生个人信息侵权事件时，个人信息处理者应当承担无过错证明责任，而这种证明责任的实现在很大程度上依赖于对日常个人信息处理活动的记录与保存。因此，我们建议个人信息处理者完善日常记录与维护，当外部监管检查或个人信息侵权事件发生需要举证时，能够有的放矢。

此外，若企业发生了个人信息泄露、篡改、丢失等个人信息安全事件，应当根据《个保法》规定立即采取补救措施，并通知履行个人信息保护职责的部门和个人。一周年的实践中，大部分企业已经在内部建立了个人信息安全事件的管理制度，并从技术上采取加密、访问控制、防泄漏监控、渗透测试等措施防止安全事件的发生。同时，部分企业会开展个人信息的应急演练或攻防演练，并在公司层面上开展个人信息安全培训，以提升公司整体的事前预防与事后处置能力。

二、特殊主体与特殊对象的个人信息保护义务

（一）特殊主体——作为“守门人”的特殊个人信息处理者

1、条款回顾

《个保法》第五十八条规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行比较一般个人信息处理者更为严格的法律义务。域外的相关法规、指引或标准等将此类型主体称为“守门人”（gatekeeper），要求其履行建立健全个人信息保护合规制度体系、制定平台规则、管理规范平台内经营者和接受社会监督的义务。

2、落地情况

针对守门人处理者的合规义务可以分为三大层次，即对平台建设的义务、对平台内经营者的管理义务以及接受外部第三方监督的义务。在目前实践中，各守门人处理者均较为重视平台建设的落实，例如搭建完善且系统化的内部制度与外部政策、从顶层架构上设立专职组织及负责人、落实与第三方的信息传输及审查评估义务、发布算法规则及备案制度等。同时，在对平台内经营者进行管理的维度，截至目前，各守门人处理者也基本上做到了制定并公开平台规则，明确了平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务。

除上述较为完善的落地情况外，从个人信息保护的角度出发，守门人处理者作为具有较大社会影响力与控制力的个人信息处理

者，应当进一步完善并落实其法律义务。例如，根据《个保法》第五十八条的规定，守门人处理者应成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，但目前实践中较少有企业对此进行公开披露。又如，对于定期发布个人信息保护社会责任报告的履行，各守门人处理者较多采取了在社会责任报告中专题披露的形式，但披露内容的质量则参差不齐。对此，南方财经全媒体集团与中国社会科学院法学研究所共同研发的“守门人”社会责任指标体系值得关注，该项目根据公开的可查询渠道，严格依据指标，对 18 家大型平台企业的代表性 App 做出测评，并判断平台的社会责任履行情况。[30]

3、合规展望

守门人处理者作为特殊类型的个人信息处理者，相较于一般的个人信息处理者，因其复杂的业务类型和多变的应用场景而涉及更多维度的数据处理关系，包括个人信息在守门人处理者控制的各平台实体间互联互通、汇聚融合等多方面的个人信息保护义务。此外，守门人处理者还面临着诸如数据垄断、消费者权益保护及国家安全保护等多元的治理要求。例如，2022 年度国家有关部门对平台经济规范健康持续发展的系列意见，8 月 1 日《反垄断法》的正式实施等，均应当引起守门人处理者的高度重视。又如，“滴滴事件”中触发《个保法》第 66 条的高额处罚结果也为守门人处理者的合规运营敲响了警钟。因此，对于守门人处理者而言，如何在其业务与技术高速发展的同时平衡好包括个人信息保护、国家安全稳定、竞争秩序健康在内的多元价值，是其在未来所面临的挑战。

（二）特殊对象——对儿童个人信息的保护

1、规范要求

随着未成年人网络产品和服务的逐渐普及，未成年人个人信息泄露、未成年人个人权益缺乏保障等诸多问题也逐渐浮现。我国已相继出台了《儿童个人信息网络保护规定》《中华人民共和国未成年人保护法（2020 修订）》（以下简称《未成年人保护法》）

[30] 详情可参见 https://m.21jingji.com/article/20221101/herald/6be1656c89b1ad830ab0073ff1fd9000.html

《未成年人网络保护条例（征求意见稿）》等法律法规，逐步健全未成年人个人信息保护法律法规体系，加强未成年人网络环境治理。

在与《个保法》同年修订的《未成年人保护法》增设“网络保护”专章，首次在法律中明确规定未成年人的网络保护义务，要求信息处理者通过网络处理未成年人个人信息的，应当遵循合法、正当和必要的原则[31]，具有里程碑意义。《个保法》出台后，首次明确不满十四周岁未成年人（下称“儿童”）的个人信息为敏感个人信息，除了获取父母或者其他监护人的同意外，还要求个人信息处理者对此制定专门的个人信息处理规则以加强保护。此外，《儿童个人信息网络保护规定》第 9 条[32]、《未成年人网络保护条例（征求意见稿）》第 35 条[33]以及《个人信息安全规范》第 5.4 条 d 项[34]均明文规定了处理儿童个人信息须监护人同意的规则。根据《个保法》对敏感个人信息的定义及获得同意的方式可知，此处儿童监护人的“同意”，应为明示的、单独的同意。

然而，如何在网络虚拟空间中有效检验儿童用户的真实身份以及其监护人的有效同意，在技术实现与合规落地方面均面临着考验。目前，国内尚未有生效的法律法规、政策、标准等对监护人同意机制的验证方式及单独同意的交互问题进行明确规定。2021 年发布的《信息安全技术 个人信息告知同意指南（征求意见稿）》（以下简称《告知同意指南（征求意见稿）》），尝试对收集 14 周岁以下未成年人个人信息的告知同意机制进行设计，在儿童监护人同意机制上，《告知同意指南（征求意见稿）》主要从儿童及监护人的身份验证方式、告知及同意方式进行规定。

2、落地情况

[31] 《未成年人保护法》第七十二条明确规定“信息处理者通过网络处理未成年人个人信息的，应当遵循合法、正当和必要的原则。处理不满十四周岁未成年人个人信息的，应当征得未成年人的父母或者其他监护人同意，但法律、行政法规另有规定的除外。未成年人、父母或者其他监护人要求信息处理者更正、删除未成年人个人信息的，信息处理者应当及时采取措施予以更正、删除，但法律、行政法规另有规定的除外。”

[32] 《儿童个人信息网络保护规定》第 9 条规定：“网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式知儿童监护人，并应当征得儿童监护人的同意。”

[33] 2022 年 3 月 14 日《未成年人网络保护条例（征求意见稿）》第 35 条第 1 款规定：“个人信息处理者基于个人同意处理不满十四周岁未成年人个人信息的，应当取得未成年人的监护人同意。”

[34] 《信息安全技术 个人信息安全规范》第 5.4 条“收集个人信时的授权同意”规则：“收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监人的明示同意。”

App 产品侧合规是儿童个人信息保护执法的重点目标之一。我们关注到，自《个保法》及相关法律法规实施以来，大多面向儿童的 App 均主动落实合规义务，专门制定或更新了其《儿童个人信息保护指引》，以及完善其用户协议、隐私政策中儿童个人信息保护的章节（如图 2）。

图 2

对于不以儿童用户为受众群体的网站/App 产品来说，采用强制的年龄验证机制来防止儿童用户进行注册使用的方式尚未普及，且基于用户流量及开发成本的考虑，目前企业采用的最普遍的做法是在用户协议及隐私政策中推定使用其产品的用户为成年人，若为儿童用户则不允许注册使用或者要求在其监护人的指导和同意的前提下进行使用。而实际上，是否为成年人使用，企业一般不实行监测机制，在用户注册界面基本为手机号码或电子邮箱注册、以及使用第三方账号注册登录使用，无额外的用户年龄的验证措施。

对于受众群体包括儿童的网站/App，个人信息处理者在实践中较多则通过设置青少年模式落实身份验证机制。但此种模式主要为未成年人防沉迷而设，辅以落实未成年人个人信息的保护，主要合规策略是通过调整优化展示内容来实现的，对用户的准入暂无验真机制。

针对以儿童为全部受众群体的网站/App，企业在实践中使用的仍然是基于知识问答等较低层级的身份验证方法作为验证监护

人的首选方案[35]，例如在 App 中设置了基于成语排序、数学题等方式的验证家长身份的方式（如图 3）

图 3

3、合规展望

从一周年的行业实践来看，不论相关网站/App 产品的目标对象是否面向儿童用户，国内企业大多会在隐私政策中设置未成年人个人信息保护专章，阐明是否会收集儿童个人信息以及要求儿童获得其家长或监护人的同意。如果相关网站/App 产品的目标用户包含儿童，根据《个保法》《未成年人保护法》及《儿童个人信息网络保护规定》等规定，个人信息处理者也会制定单独的儿童个人信息保护规则。我们建议 App 运营者在考虑验证用户主体年龄的机制时，应遵循最小必要原则收集个人信息以完成验证；针对未成年人提供的产品或服务，企业在可能的情况下履行年龄识别的合理注意义务，在业务流程中增设未成年人识别机制。

三、特殊场景下的个人信息处理者义务

（一）与第三方的个人信息交互

本节所称的与第三方个人信息交互场景，既包括同一企业内部不同关联公司或不同产品线、业务部门之间所存储的个人信息交互，也包括企业与外部第三方之间的个人信息交互。

[35] 该验证方法由 Imperium 公司提出，于 2013 年 12 月被 FTC 正式审查通过并纳入。参见方巧娟：《儿童监护人同意机制国内外立法、实践及合规路径》，https://mp.weixin.qq.com/s/xyTzj0auCUQBXiC5XxhBFw

1、企业内部的个人信息交互

区别于向外部第三方个人信息处理者进行数据共享或委托外部第三方处理，作为个人信息处理者的各集团内部关联公司或公司内部产品线、业务部门，对落实统一的个人信息安全保护管理措施有较大优势。在《个保法》实施一周年的实践中，相较于外部的个人信息交互，企业对其内部不同实体和不同业务部门之间的数据融合、转让或共享规则的关注度相对较低。从履行《个保法》的视角出发，我们建议企业内部的个人信息交互仍应关注以下合规要点：

（1）区分个人信息融合与共享

个人信息的融合主要关注不同数据源的个人信息汇聚，其中包括了以共享方式的汇聚，以及不同数据源的个人信息使用目的的变化。而个人信息共享则是指决定个人信息处理的目的与方式发生变化。实践中，掌握一定数量个人信息的企业通过建立数据中台或管理平台对各业务部门或二三级子公司收集产生的个人信息进行统一管理。在此过程中，各业务部门或子公司向数据中台传输个人信息的行为，通常为个人信息的共享；而数据中台为进一步的加工使用而对不同来源个人信息的汇聚，则可理解为个人信息的融合。在此，个人信息汇聚融合后的权属确认，以及对该等数据进一步开发利用的保护问题，是企业合规面临的难点。

（2）用户授权

若企业内部的个人信息交互是基于个人信息处理者的委托处理，也即受托方不决定个人信息的处理与目的，则无需取得个人信息主体的授权同意。若集团内部发生用户个人信息共享，也即作为独立的个人信息处理者的法律实体向另一集团内实体提供个人信息的，则根据《个保法》的规定，提供个人信息的处理者应当取得个人的单独同意。目前，掌握较大体量个人信息（包括用户、客户、供应商、员工个人信息）的集团企业通常拥有处理不同业务板块的子公司，这些子公司之间的个人信息共享仍应当向个人履行告知义务并取得个人的单独同意。而在实践中，部分头部互联网公司在集团内不同实体发生数据共享时，如果是 App 产

品，则会在发生个人信息共享时采用弹窗的形式告知用户并取得用户的单独同意（详见本系列上篇“单独同意”章节），但在其他场景以及传统企业在这方面的实施表现上则稍逊一筹。

（3）符合用户的合理期待

无论是个人信息的集团内部共享和/或融合，该处理行为的目的以及方式，不应超出用户的合理预期。对于企业内部个人信息的交互而言，若汇聚或共享后的个人信息使用目的超出与收集个人信息时所声称目的具有直接或合理关联的范围，则应再次征得个人信息主体的明示同意。根据《个人信息安全规范》的规定，将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。在《个保法》实施一周年以来，较难看到个人信息处理者内部数据交互后向个人信息主体重新取得同意。是重来没有发生过融合/共享后的处理目的变化，还是企业都在观望或等待由第一个敢“吃螃蟹”的处理者就“重新获取授权”进行引领，还有待观察。

（4）开展个人信息保护影响评估

根据《个保法》的规定，企业内部若出现委托处理个人信息或向其他个人信息处理者提供个人信息情形的，均应按法定要求事先开展个人信息保护影响评估并记录。此外，根据《个人信息安全规范》的规定，个人信息处理者也应当根据汇聚融合后的个人信息的使用目的，开展个人信息保护影响评估，采取有效的个人信息保护措施。关于个人信息保护影响评估方面的具体要求，请参考上文。

（5）加强个人信息审计与保护措施

对于企业内部的个人信息交互而言，应当加强个人信息审计、评估以及保护措施，一方面落实《个保法》所要求的法定合规审计义务，另一方面也可控制个人信息共享和融合后带来的安全风险。例如，可采取将个人信息进行匿名化后再进行共享与融合的

措施以降低个人信息处理者的安全风险。关于个人信息审计与保护措施的具体要求，亦请参考上文。

2、企业与外部第三方的个人信息交互

根据《个保法》，目前个人信息处理者与外部第三方的个人信息交互场景同样分为两类：其一，个人信息处理者委托处理个人信息；其二，个人信息处理者向其他个人信息处理者提供个人信息以及个人信息处理者转移个人信息。本部分将重点就委托第三方处理个人信息与向第三方提供个人信息展开。

（1）委托处理

对于个人信息处理者而言，委托第三方处理个人信息的，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。受托人不应超出约定的处理目的、处理方式等处理个人信息，因而作为委托人的个人信息处理者仍对其处理的个人信息拥有控制权，且无需因委托行为额外取得用户的同意。在目前的实践中，企业普遍仅在《隐私政策》中对委托处理的情形向用户进行告知，但并未像个人信息共享场景披露共享的第三方那样详细。

在此，我们建议企业一方面在《隐私政策》中对委托处理的情形进行告知，另一方面也应当与受托方签订数据处理协议约定处理的目的、期限、处理方式、个人信息的种类、保护措施、双方的权利和义务以及转委托情形等，并真正落实对受托人个人信息处理活动的持续监督。

在委托第三方处理个人信息的场景中，一个当前普遍存在的实践是企业将内部员工个人信息委托外部第三方处理的情形。例如委托外部人力资源管理公司处理用人单位的员工个人信息等场景。根据《个保法》的规定，该等处理所依据的合法性基础为“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”。实践中，已有越来越多的企业重视规范《员工隐私保护政策》或《员工手册》，并在劳动合同及相关劳动规章中

明示委托处理员工个人信息的范围、数量、受托方等事宜，同时采取显著方式告知员工其所处理的敏感个人信息，以及处理的必要性与对个人权益的影响。这体现出企业普遍提高了对员工个人信息保护的重视程度，并将对员工个人信息与用户/客户个人信息采取同等力度的保护措施。此外，另一个普遍存在的实践为 IT 外包场景，在该场景下企业通常会委托外部第三方 IT 服务商处理企业的个人信息，包括员工个人信息以及用户个人信息。我们建议在此情形下，企业作为个人信息处理者，应当注意与作为受托方的 IT 服务商签订数据处理协议并切实落实对个人信息保护的管理义务，以及对外部第三方的评估与监督义务。

（2）向第三方提供个人信息

个人信息处理者向第三方提供个人信息的情形，主要表现为个人信息的共享。根据《个保法》的规定，向第三方提供个人信息的，个人信息处理者一方面应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，另一方面也应当取得个人信息主体的单独同意。我们已在本系列上篇文章中对该内容有所讨论，此处不再赘述。

对于在与外部第三方的个人信息共享场景中，较为常见的一类是第三方 SDK 的个人信息共享。在一周年的实践中，App 运营者普遍已在隐私政策和界面设计中落实了“第三方信息共享清单”的告知披露义务，其中包括了对第三方 SDK 的披露，以满足服务感知提升的监管要求。但同时，对于第三方 SDK 的个人信息共享仍存在如下几点难题有待解决：第一，目前 App 运营者大多在用户首次使用时，通过弹窗告知第三方合作清单，但较少有企业会满足用户对某一具体第三方 SDK 的同意或拒绝，同时也缺少对第三方 SDK 撤回同意的机制，这意味着用户无法完全实现对第三方 SDK 处理个人信息的自主决定权。第二，若第三方 SDK 提供者为独立的个人信息处理者，则此时采用三重授权原则（即“【用户-App 运营者】+【App 运营者-第三方 SDK 提供者】+【用户-第三方 SDK 提供者】”）可以解决 SDK 获取 App 用户个人信息的正当性问题。但在实践中，App 运营者通常较难与行业内有较大影响力的头部第三方 SDK 开方者达成线下的数据处理协议，也无法与之约定双方的数据处理关系及保护责任，因而在第三方 SDK 处理用户个人信息的合法性基础上亦存在问题。第三，对于第三方 SDK，App 运营者应当开展集成前的来源安全性评估、代

码安全性评估与行为安全性评估[36]，同时对集成的 SDK 开展持续的审核以确保其未超出用户同意范围处理个人信息。在实践中，App 运营者如何在事前评估与事中审核方面均存在合规挑战。

此外，自《个保法》实施以来，实践中另外一个较为复杂的发生个人信息共享的业务场景为数字广告营销。目前，广告发布者通常直接收集用户个人信息并取得个人信息主体的授权同意。而广告发布者的众多第三方合作伙伴则通过发布者实现对个人信息的间接收集。在此情况下，广告发布者向第三方合作伙伴提供其收集的个人信息时，应当满足告知用户第三方合作伙伴的基本情况、共享的个人信息种类、使用目的与共享方式等，并取得用户的单独同意。但在实践中，广告发布者通常不区分不同第三方合作伙伴的处理目的，仅通过一揽子的隐私政策获取用户同意，并且也不具体写明向哪些具体的第三方共享，基本笼统处理为广告主或者代理方平台，无法实质性地约束第三方合作伙伴可能存在的超出授权范围的违法处理行为。而从第三方合作伙伴角度出发，其也无法保证广告发布者获取了用户合法有效的单独同意，从而亦面临着处理用户个人信息时合法性基础存在缺陷的风险。

（二）个人信息的跨境提供

在全球化背景下，数据跨境流动已成为趋势。个人信息处理者在国际合作和海外市场拓展等业务活动中对数据跨境传输的需求激增，业务场景更是纷繁复杂。譬如，国内企业与其境外子公司进行数据共享和传输、与境外合作方开展业务合作与谈判、赴境外 IPO、派遣员工到海外出差、应对涉外司法执法事件等场景，均可能涉及个人信息的跨境提供。此外，较多在华的外资企业均存在个人信息向其境外母公司或者关联公司传输出境，并进而需要开展数据出境安全评估的情形，其涉及较多的场景为员工个人信息的出境、办公系统处理个人信息，以及在提供产品/服务场景下终端用户或消费者个人信息的出境。对于向境外提供个人信息的个人信息处理者，需至少履行以下义务：

第一，告知并取得个人信息主体的单独同意，包括向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信

[36] 详见《网络安全实践指南——App 使用软件开发工具包（SDK）安全指引》5.2 b）。

息的种类以及个人向境外接收方行使本法规定权利的方式等；第二，事先进行个人信息保护影响评估并对处理情况进行记录与保存，通过全面排查摸底确定出境的个人信息量级、敏感程度等；第三，根据自身实际情况选择数据出境安全评估（下称“安全评估”）、专业机构的个人信息保护认证、签订标准合同等不同出境路径（详见图 4）；第四，针对拟传输的数据采取加密或者其他形式的安全处理措施（例如采用去标识化等脱敏处理），并落实相关管理制度以及技术保障手段和能力。同时保障境外接收方处理个人信息的活动达到《个保法》规定的保护标准；第五，记录出境情况并进行保存，包括向境外提供个人信息的日期时间，境外接收方的身份（包括但不限于接收者的名称、地址、联系方式等），向境外提供的个人信息的类型及数量、敏感程度等。

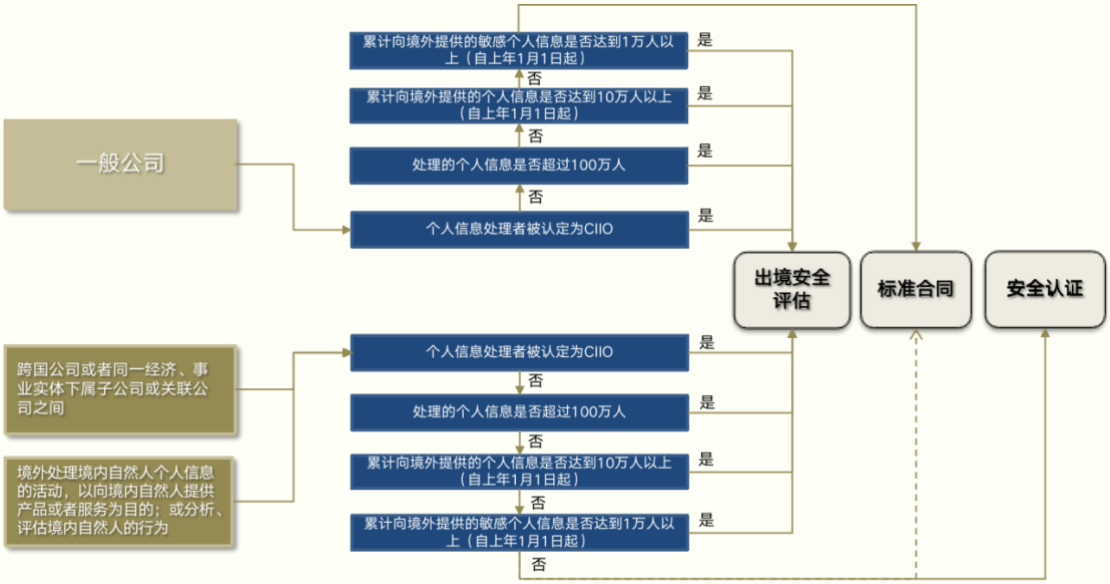


图 4

根据简要梳理，我们发现个人信息的跨境提供在实践落地过程中往往存在以下重点问题：

1、关于境外个人信息处理者是否需申报安全评估的问题

对于个人信息处理者于境外直接处理境内自然人个人信息的活动，因其行为满足《个保法》第三条第二款的规定而在是否属于并应当适用数据出境规则上存在较大争议。经向有关网信部门咨询，我们理解目前该场景构成数据出境，达到申报条件的，应进行数据出境安全评估申报。同时，鉴于境外个人信息处理者应

根据《个保法》第五十三条[37]在境内设立专门机构或者指定代表，具体申报部门的选择应根据该专门机构或者指定代表所在地确定。我们认为，对数据出境安全评估的违规，其性质与中概股企业未经网络安全审查赴国外上市相类似，其共同点均指向因数据出境而未申报所产生的国家安全风险。这一点上，我国与 GDPR 项下境外实体直接采集的规制思路有所不同，企业应尤其关注。

2、关于去标识化与匿名化的个人信息跨境传输的问题

首先，个人信息处理者应当注意去标识化与匿名化的实质区别。从法律性质上看，个人信息匿名化处理后不再属于个人信息，而去标识化处理后仍属于个人信息。从效果上看，匿名化的技术手段更彻底，经过匿名化后的个人信息因无法再识别到个人，因此不再是个人信息；而去标识化是个人信息处理者内部针对个人信息安全的一种保护手段，去标识化后的个人信息在借助额外信息的情况下仍可再次识别到个人，因此个人信息虽去标识化但仍属于个人信息。

在个人信息跨境传输的语境下，去标识化后究竟是否可能再次识别个人则取决于境外接收方是否可以通过技术手段并结合其他信息来识别具体个人。例如企业曾向境外接收方传输用户的手机号码、地址、姓名等完整字段，境外接收方也在其数据库中进行了保留，那么即使本次传输出境方企业使用了去标识化措施，境外接收方仍可以通过撞库或者用户 ID 映射的方式识别到具体个人，因此，离岸后的数据在此场景下依然保留个人信息的属性，应被认为属于个人信息出境。

3、关于哪些情形属于“法律、行政法规或者国家网信部门规定的条件”

除《网络安全法》《数据安全法》和《个保法》确立的数据和网络安全整体体系外，企业还应当考虑其他相关法律法规的要求。例如，根据《中华人民共和国保守国家秘密法》第三十条，机关、单位对外交往与合作中需要提供国家秘密事项，或者任用、

[37] 《个人信息保护法》第五十三条：“本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。”

聘用的境外人员因工作需要知悉国家秘密的，应当报国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门批准，并与对方签订保密协议。如涉及健康医疗大数据，则根据《国家健康医疗大数据标准、安全和服务管理办法（试行）》第三十条，应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。如涉及测绘成果，则根据《中华人民共和国测绘法》第三十四条，属于国家秘密的，适用保密法律、行政法规的规定；需要对外提供的，按照国务院和中央军事委员会规定的审批程序执行。如涉及人类遗传资源信息，则根据《中华人民共和国生物安全法》第五十七条，向境外组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院科学技术主管部门事先报告并提交信息备份。

4、关于境外接收方向境外第三方再次提供所接收的个人信息是否应再次签署“个人信息出境标准合同”（下称“标准合同”）的问题

如果在部分业务场景中境外接收方确需将所接收的个人信息提供给境外第三方，在满足向个人告知并取得单独同意等《个保法》中所列明的条件以外，还建议境内个人信息处理者在与境外数据接收方所签订的标准合同中，以排他性列举的方式明确境内个人信息处理者所认可的境外第三方（即分处理者或次处理者）情况；以及如果未经境内个人信息处理者同意，境外数据接收方不得再向境外第三方提供个人信息。同时境内个人信息处理者也应当要求境外数据接收方对第三方的过错承担连带责任。

若存在境外接收方向境外第三方再次提供所接收的个人信息的情况，境内个人信息处理者可以直接在与境外接收方所签的标准合同中约定关于境外第三方的相关条款，比如在《个人信息出境标准合同规定（征求意见稿）》（下称“《标准合同规定（征求意见稿）》”）附录一的第（六）项中阐明境外接收方可能再向哪些第三方主体提供个人信息，避免重复签订标准合同或补充协议以及进行多次备案。

而若境内个人信息处理者需通过安全评估方可跨境传输个人信息的，则根据《数据出境安全评估办法》（下称“《评估办法》”）

的规定，其应当事先在与境外接收方订立的法律文件中对接收方将出境数据再转移给其他组织、个人的约束性要求作出明确约定。此外，企业在起草与境外接收方拟订立的相关法律文件（如“数据跨境传输协议”）时，一方面可参考《标准合同规定（征求意见稿）》中“个人信息出境标准合同”模板，另一方面也应当参考《评估办法》补充相关重点内容。

六、个人信息保护的挑战与趋势

通过本文上下篇中的观察与阐释，在《个保法》正式实施一周年之际，我国个人信息保护工作取得了积极的成效，有关个人信息保护的配套法律法规日趋完善，保护工作机制进一步健全，个人信息保护的执法持续深入开展，个人信息处理者的保护意识显著提高、保护能力也显著增强。但从客观上看，综合本文上下两篇的分析，个人信息保护合规工作依然面临着不少难点与挑战。从各项合规义务细化落实层面看，至少包括如下难点问题：如何进一步明确规范个人信息转移权的实践落地措施？如何在儿童个人信息保护中实现监护人认证与验真机制？在 B 端长链条的个人信息流通中，如何解决个人信息主体授权的不真实不客观？在复杂的多方个人信息交互共享场景中，如何有效落实个人信息主体的单独同意？而从更为宏观的层面看，面临的难点与挑战主要为：如何进一步打通不同立法之间的概念衔接？（如《网络数据安全管理条例（征求意见稿）》中对“重要数据”与“100 万个人信息”的关系）如何实现“守门人处理者”在汇聚融合大量个人信息后的垄断标准判断及相关市场的界定？以及对于各领域各行业（包括正在经历数字化转型的传统行业）的个人信息处理者而言，如何更好地平衡个人信息的利用与保护的边界以最大化发挥数据要素价值？等等。

同时，结合过往实践经验与观察，我们尝试提出我国个人信息保护工作的可能趋势：首先，个人信息保护将进一步同数据价值利用、竞争秩序维护、国家安全保护等一系列重要领域相结合，呈现出更为一体自洽的完整合规体系；第二，我国的个人信息保护立法将进一步借鉴国外优秀的数据立法实践经验，同时《个保法》的国际化及影响力也将进一步提升；第三，个人信息保护监管的多元化与针对性将进一步提高，面对不同业务领域（如金融、生物医疗、智能网联汽车、传统制造业、电商与消费品、社交生活平台等等），各领域监管部门将开展更贴合行业本

身的执法与规制；而面对不同体量与发展阶段的个人信息处理者，则将结合其社会影响力及控制力施行更符合企业状况的监督与管理；最后，从个人信息处理者的合规管理角度看，个人信息保护工作将与技术手段进一步结合，传统信息安全技术与合规保护工作的分立状态将逐步向制度策略、安全架构和工具支撑的紧密结合过渡。

2022 年 第九期 /总第四十三期

数据合规时事速递
NEWSLETTERS

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。

若您有任何疑问和建议，欢迎随时与我们联系，联系邮箱：tianziyi@glo.com.cn。您也可以扫描上方二维码，关注我们的公众号“M 姐 数据合规评论”获取更多资讯。