Merits Tree
植德律师事务所

植德数字经济月报

2026 年 8 月

北京 | 上海 | 深圳 | 杭州 | 成都 | 青岛 | 广州 | 香港 | 硅谷

Beijing|Shanghai|Shenzhen|Hangzhou|Chengdu|Qingdao|Guangzhou|Hong Kong|Silicon Valley

www.meritsandtree.com

目录

政策速递

1. 《网络数据安全风险评估办法》8 月 20 日起施行并就实施有关事项答记者问

发布日期：2026 年 6 月 18 日、2026 年 8 月 20 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-06/18/c_1783525609815499.htm
- https://www.cac.gov.cn/2026-08/20/c_1788889498173657.htm

摘要：

2026 年 6 月 18 日，国家互联网信息办公室、工业和信息化部、公安部联合公布《网络数据安全风险评估办法》（下称《办法》），自 2026 年 8 月 20 日起施行。8 月 20 日，国家网信办公布《办法》实施有关事项答记者问。

《办法》规定，重要数据处理者应当每年度开展风险评估；重要数据安全状态发生重大变化可能对数据安全造成不利影响的，应当及时对发生变化及其影响的部分开展风险评估；鼓励处理一般数据的网络数据处理者至少每 3 年开展一次风险评估。风险评估可以自行开展，也可以委托第三方评估机构进行，自行开展的应当指定专人负责。

《办法》对评估机构提出系列要求：鼓励评估机构按照《认证认可条例》通过认证；评估机构不得转委托开展风险评估，同一评估机构及其关联机构不得连续 3 次以上对同一网络数据处理者开展年度风险评估；评估过程中发现重大数据安全风险的，应当及时通知数据处理者，并依法承担保密义务、妥善处置获知信息。

在报告报送与监管衔接方面，重要数据处理者应当在年度风险评估完成后的 20 个工作日内按照有关主管部门要求报送风险评估报告，主管部门不明确的，向省级网信部门或者国家网信部门报送；风险评估报告至少保存 3 年。对存在较大安全风险可能危害国家安全、公共利益，或者发生网络数据安全事件导致重要数据、大规模个人信息泄露被窃取等情形的，有关部门可以要求数据处理者委托通过认证的评估机构开展风险评估；对拒不整改或者未达整改要求的，可以采取要求其停止处理重要数据等措施。答记者问进一步明确了风险评估服务认证的申请路径，以及风险评估报告向国家和省级网信部门报送的联系方式。

植德短评

《办法》将《数据安全法》与《网络数据安全管理条例》中原则性的风险评估义务落实为年度化、机构化的可执行制度，“重要数据处理者每年一评、报告 20 个工作日内报送、至少保存 3 年”以及评估机构轮换（不得连续 3 次服务同一处理者）等规则，将直接改变企业的数据安全合规节奏。建议重要数据处理者尽快梳理重要数据目录并明确主管部门归属，规划年度评估排期与预算，审慎遴选评估机构并留存合作记录；一般数据处理者可将 3 年一评作为基线纳入内控。评估机构则需关注认证规则落地安排，避免转委托、关联机构重复执业带来的执业风险。

2. 《小型个人信息处理者个人信息保护简化措施规定》9 月 1 日起施行

发布日期：2026 年 7 月 24 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-07/24/c_1786638889704872.htm

摘要：

2026 年 7 月 24 日，国家互联网信息办公室、公安部联合公布《小型个人信息处理者个人信息保护简化措施规定》（下称《规定》），自 2026 年 9 月 1 日起施行。《规定》所称小型个人信息处理者，是指处理不满 10 万人个人信息的个人信息处理者。

《规定》以“与规模、能力相当”为原则为小型个人信息处理者提供简化合规路径：个人信息处理规则至少应当包括处理者名称、个人行使权利的受理部门或人员及联系方式、处理目的与方式、个人信息种类、保存期限等基本事项，线下收集的可以通过张贴公告等简便方式公开；处理不满 10 万人个人信息且不涉及敏感个人信息、不向其他处理者提供并不对外公开的，可以仅通过公开个人信息处理规则履行告知义务；仅依托网络平台开展处理活动且符合条件的小型个人信息处理者，可以适用平台统一制定的个人信息处理规则，并可不再重复开展合规审计和个人信息保护影响评估。

《规定》还在数据出境、审计评估等方面给予便利：明确为订立履行合同所必需、跨境人力资源管理所必需、紧急情况保护生命健康财产安全、履行法定职责或法定义务、累计向境外提供不满 10 万人个人信息（不含敏感个人信息）等情形，

免予申报数据出境安全评估、订立标准合同、通过认证；允许以附件自查表方式至少每 5 年开展一次合规审计、以附件评估表方式开展影响评估；并明确初次违法且危害后果轻微并及时改正的可以不予处罚等从轻、减轻处罚情形。

同时，《规定》强调底线义务不因规模而减免：处理敏感个人信息仍须取得个人单独同意，处理不满十四周岁未成年人个人信息仍须制定专门的个人信息处理规则并取得监护人同意；发生或者可能发生个人信息泄露、篡改、丢失的，仍应当立即采取补救措施，通知个人并按规定通知履行个人信息保护职责的部门。

植德短评

《规定》与《大型个人信息处理者个人信息保护规定（征求意见稿）》同月密集出台，标志着个人信息保护义务配置正式走向“大小分层、宽严相济”的差异化监管格局。对小微企业和个体工商户而言，5 年一次合规审计、简化告知、出境豁免等安排显著降低合规成本，但敏感个人信息单独同意、未成年人专门处理规则等底线义务并未松动。建议小型个人信息处理者先行测算自身处理量级并留存依据，用足园区统一规则、平台规则承继、简化审计评估等便利安排；网络平台则需同步完善面向平台上小型经营者的统一规则、合规审计与影响评估覆盖，避免因承继机制失效向平台内经营者传导合规风险。

3. 《大型个人信息处理者个人信息保护规定（征求意见稿）》公开征求意见

发布日期：2026 年 8 月 7 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-08/07/c_1787851071612596.htm

摘要：

2026 年 8 月 7 日，国家互联网信息办公室公布《大型个人信息处理者个人信息保护规定（征求意见稿）》（下称《规定》），公开征求意见截止时间为 2026 年 9 月 7 日。《规定》系对前期已分别公开征求意见的《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》《大型网络平台个人信息保护规定（征求意见稿）》的整合完善。

在认定标准上，《规定》明确对大型个人信息处理者的认定应当综合考虑：处理 1000 万人以上自然人个人信息；提供涉及个人信息处理的重要网络服务，或者经营范围涵盖多种业务且涉及个人信息处理；个人信息处理活动对国家安全、经济

运行、社会稳定、公共健康和安全等具有重要影响。符合条件的个人信息处理者应当通过所在地省级网信部门向国家网信部门申报认定，国家网信部门会同有关部门研究确定大型个人信息处理者清单并向社会公告。

在处理规则上，《规定》要求以结构化清单形式逐项列明个人信息处理规则，向其他处理者提供、对外提供、公开、处理敏感个人信息等情形取得单独同意；个人信息存储在境内，并选择符合条件的数据中心；设置个性化推荐关闭选项、提供用户标签删除功能；明确个人信息转移请求应在 30 个工作日内办理；规定处理目的实现、撤回同意、期限届满等情形下的主动删除义务。

在组织与监督义务上，《规定》要求指定管理层成员担任个人信息保护负责人，合规性意见不被采纳或被违反时可直接向省级网信部门报告；每两年至少开展一次个人信息保护合规审计、每年开展风险评估；每年编制并发布上一年度个人信息保护社会责任报告；自被认定之日起 6 个月内成立主要由外部成员组成的个人信息保护监督委员会，成员不少于 7 名、外部成员占比不低于三分之二，负责人由外部成员担任并应具备高级个人信息保护合规审计人员能力。

植德短评

从“大型网络平台”到“大型个人信息处理者”，监管对象口径的扩展叠加 1000 万人以上的量化门槛，意味着大量并非传统意义“平台”的企业（如智能制造、医疗健康、金融科技领域的头部机构）可能落入清单管理。个人信息保护负责人直报省级网信部门、外部成员占三分之二以上的监督委员会、重大产品上线前影响评估备案等安排，已将公司治理机制实质性引入个人信息保护领域。建议可能达标的企业提前开展认定条件的自评估与差距分析，预留个人信息保护负责人、数据中心信息报送及监督委员会组建的筹备周期，并在征求意见期内就认定标准、监督委员会运行成本等提交行业意见。

4. 《中华人民共和国反网络暴力法（征求意见稿）》公开征求意见

发布日期：2026 年 7 月 29 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-07/29/c_1787072711938509.htm

摘要：

2026 年 7 月 29 日，国家互联网信息办公室会同有关部门起草的《中华人民共和国反网络暴力法（征求意见稿）》（下称《征求意见稿》）向社会公开征求意见，意见反馈截止日期为 2026 年 8 月 28 日。《征求意见稿》共七章六十条，就网络暴力的概念定义与治理原则、平台治理、政府治理、社会共治、司法保护和法律责任作出系统规定。

《征求意见稿》界定，网络暴力是指通过网络对个人、组织集中或者持续实施的侵害名誉权、荣誉权、隐私权、肖像权、个人信息等合法权益的活动，包括集中发布含有侮辱谩骂、造谣诽谤、煽动仇恨、挑动对立、威逼胁迫、歧视偏见等内容的信息，违法集中发布他人个人信息，持续进行网络恐吓、网络骚扰等。

在平台治理方面，《征求意见稿》要求网络服务提供者建立健全用户注册、账号管理、信息发布审核、监测预警、识别处置、投诉举报等制度，对信息发布、即时通讯等服务落实真实身份信息要求；建立网络暴力特征库、典型案例样本库和预警模型；提供屏蔽陌生用户或特定用户、禁止转载或评论等防护功能，并在显著位置提供网络暴力快捷取证功能；明确用户数量巨大或具有显著影响的网络平台应当建立快速响应机制、定期开展网络暴力风险评估、发布年度治理报告。同时规定发现风险不得利用算法推荐推送相关信息，落实人工智能生成合成内容标识等制度，防范利用人工智能技术实施网络暴力。

在法律责任方面，《征求意见稿》区分义务类型设置了行政处罚梯度，情节特别严重的对网络服务提供者最高可处 1000 万元罚款；明确组织、策划、煽动、教唆实施相关行为依法从重处罚，网络暴力侵害自然人人身权益造成严重精神损害的，被侵权人有权请求精神损害赔偿；并就人格权侵害禁令、自诉与公诉衔接、检察公益诉讼等司法保护机制作出安排。

植德短评

反网络暴力立法从部门规章层面向专门法律跃升，将显著抬升平台注意义务的刚性：真实身份信息核验、预警模型、防护功能、快捷取证等义务均有明确罚则支撑，最高 1000 万元的罚款额度亦与既有网络立法保持梯度衔接。对平台企业而言，需重点评估三方面差距：内容识别与溯源的技术投入、涉网暴账号处置的申诉与救济流程、涉人工智能生成内容的标识与报告机制。同时，《征求意见稿》明确依法通过网络检举揭发违法犯罪或实施舆论监督不适用本法，平台在制定内部处置规则时应注意在治理网络暴力与保障正常监督表达之间作出精细化区分，避免“一刀切”式处置引发新的争议。

5. 国家网信办发布《个人信息保护政策法规问答（2026 年 8 月）》

发布日期：2026 年 8 月 12 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-08/12/c_1788195297373459.htm

摘要：

2026 年 8 月 12 日，国家互联网信息办公室公布《个人信息保护政策法规问答（2026 年 8 月）》（下称《问答》），围绕个人信息保护合规实务中的代表性问题作出解答。

关于处理已公开的个人信息，《问答》援引《个人信息保护法》第二十七条，重申个人信息处理者可以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，个人明确拒绝的除外；对个人权益有重大影响的，应当依照《个人信息保护法》规定取得个人同意。同时，《问答》结合《个人信息保护合规审计管理办法》附件《个人信息保护合规审计指引》第十二条，列举了违法违规处理已公开个人信息的具体情形，包括：向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；处理个人明确拒绝处理的已公开个人信息；对个人权益有重大影响未取得个人同意；收集、留存或处理已公开个人信息的规模、时间或使用目的超出合理范围。

关于导致个人信息泄露的常见原因，《问答》归纳为四类：个人信息明文存储和传输，未采取适当的加密、去标识化等安全技术措施；存储个人信息的信息系统、数据库等未采取有效安全措施，如使用弱口令、无登录验证措施；可通过互联网访问的数据接口未采取有效的身份验证措施；互联网网站页面上包含网站关联的信息系统、数据库的登录账号与口令等。

植德短评

《问答》延续监管“以案释法”式的合规指引风格，其价值在于将《个人信息保护合规审计指引》中的审计情形与《个人信息保护法》第二十七条的抽象规则直接对应，为企业自查“已公开信息处理”场景提供了具体刻度：来源合法、尊重拒绝、范围合理、重大影响取得同意，四道关口缺一不可。泄露原因的归纳则提示，监管对安全事件的关注点已从“是否泄露”前移至“基础安

全配置是否失守”，这意味着明文传输、弱口令、无验证接口、页面暴露凭据等基础性缺陷本身即可成为执法认定与民事诉讼中过错判断的依据。建议企业将上述情形纳入合规审计底稿与安全测试用例，形成常态化自查与整改闭环。

6. 国家网信办发布《数据出境安全管理政策法规问答（2026 年 9 月）》

发布日期：2026 年 9 月 11 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-09/11/c_1790876549989064.htm

摘要：

2026 年 9 月 11 日，国家互联网信息办公室公布《数据出境安全管理政策法规问答（2026 年 9 月）》（下称《问答》），围绕个人信息出境认证的适用情形、与数据出境安全评估的衔接及申请要求等代表性问题作出解答。

关于个人信息出境认证的适用情形，《问答》明确，非关键信息基础设施运营者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息，且不包括重要数据的，可以通过个人信息出境认证方式履行数据出境合规义务。此外，存在个人信息出境行为的处理者，不论出境个人信息规模大小，均可申请认证，以证明相关处理活动符合《信息安全技术 个人信息安全规范》《数据安全技术 个人信息跨境处理活动安全认证要求》等国家标准要求，但不得采取数量拆分等手段，以认证替代依法应当开展的数据出境安全评估。

关于认证与安全评估的衔接，《问答》指出，已通过认证的个人信息处理者，自当年 1 月 1 日起累计出境个人信息达到 100 万人以上（不含敏感个人信息）或者敏感个人信息达到 1 万人以上的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。申报时可附具已通过认证的有关情况，说明处理者及境外接收方的个人信息保护水平、个人信息权益保障等情况，供网信部门在安全评估过程中参考。

关于认证申请，《问答》强调，个人信息处理者在申请认证向境外提供个人信息前，应当依法履行告知、取得个人单独同意、开展个人信息保护影响评估等义务，并可向已通过备案的中国网络安全审查认证和市场监管大数据中心、中央网信办（国家网信办）数据与技术保障中心、北京赛西认证有限责任公司申请认证。

植德短评

《问答》进一步厘清了个人信息出境认证作为法定出境合规路径与作为合规能力证明的不同功能，特别值得关注的是认证结果可供安全评估参考，为既有合规成果的复用提供了明确依据，但不意味着豁免评估或当然通过安全评估。建议企业在建立每年出境人数和个人信息敏感程度的台账的前提下，提前评估认证与标准合同备案两条路径对企业的适配性，同时持续更新个人信息保护影响评估、境外接收方保护措施及权益保障材料，做好认证与标准合同备案两条路径的科学选择以及与安全评估之间的衔接。

行业新闻

1. 国家网信办发布近期网络安全、数据安全、个人信息保护等领域执法典型案例

发布日期：2026 年 9 月 15 日

来源：网信中国微信公众号

链接：

- https://mp.weixin.qq.com/s/S-f_K96o3axIYZtxT5sAdQ

摘要：

2026 年 9 月 15 日，国家互联网信息办公室发布了近期网络安全、数据安全、个人信息保护等领域的执法典型案例，共通报 10 起案件，涵盖网页篡改、设置恶意程序、数据窃取、数据泄露、个人信息泄露、强制收集使用非必要个人信息、违法收集人脸信息、违法出境个人信息、未落实人工智能生成合成内容标识要求、提供生成式人工智能服务未经安全评估等类型。执法依据包括《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》及人工智能、数据跨境流动相关规章等。

在网络安全与数据安全领域：上海某电子有限公司因门户网站后台长期存在管理员账号弱口令问题、遭攻击后被植入恶意代码且未及时启动应急预案并报告，被处罚款；北京某网络科技有限公司运营的应用程序（用户约 35 万）被离职员工植入恶意程序跳转推广链接，企业因疏于对应用程序及员工的管理被处罚款，涉事员工被移送公安机关；安徽某数据产业有限公司因使用存在未授权访问漏洞的 ES 开源组件且未及时删除测试数据，致 2400 余份审计报告、合同、会议纪要等内部文件被窃取；河南某医院体检系统存在弱口令漏洞，责令整改后复核发现防火墙、堡垒机等安全设备因授权过期失效，仍存 700 个安全漏洞（含 73 个高危漏洞），数据泄露风险未消除，上述企业（单位）均被警告、罚款，并对直接负责的主管人员予以罚款；广东某软件技术有限公司车载硬件产品存在未授权访问漏洞且个人信息传输未加密，被警告。

在个人信息保护领域：浙江某信息科技有限公司运营的运动管理 App 以“防止作弊”为由一次性强制索取定位、电话、存储等多项权限，拒绝授权即拒绝提供服务，超范围收集使用非必要个人信息；重庆某置业有限公司在办公场所安装 10 余处图像采集设备，未经单独同意收集、存储客户人脸信息 5000 余条并用于身份识别及匹配营销，均被责令改正并处罚款；上海某科技有限公司自 2022 年起持续超范围收集用户信息，且在未依法申报数据出境安全评估的情况下将个人信息传输至境外数据中心，被处罚款。

在人工智能领域：四川某科技有限公司运营的微信小程序提供 AI 文本对话、图片生成服务，未添加显式标识、未在元数据中嵌入隐式标识且未落实安全评估要求，被责令下线；江苏某科技股份有限公司以“API 中转站”方式调用多个大模型接口提供对话、问答服务，未按规定开展安全评估，被警告并从严处理责任人。国家网信办有关负责人表示，相关单位和企业要严格落实法律法规要求、切实履行主体责任，网信部门将持续加大相关执法工作力度。

植德短评

本批案例系国家网信办在网络安全、数据安全、个人信息保护与人工智能领域的执法成果，传递三方面信号：其一，执法贯穿“安全、数据、个保、AI”的全链条。弱口令、安全设备授权过期、整改复核后仍存高危漏洞等履行保护义务不到位的行为本身即可处罚；其二，人脸信息单独同意、最小必要原则、数据出境安全评估等高频义务成为处罚重点，并对直接负责的主管人员“双罚”，个人责任追究趋于常态化；其三，人工智能监管进入执法落地阶段，生成合成内容标识与安全评估成为新的执法抓手，“API 中转站”类套壳服务亦被纳入监管视野。

建议企业对照本批案例开展合规自查：重点复核账号口令与漏洞闭环管理、开发测试数据清理、离职员工权限回收与内部管控、权限索取与人脸信息单独同意、数据出境合规路径，以及 AI 应用的标识义务与安全评估要求，并注意处罚记录可能引发的招投标、上市合规问询等衍生影响。

2. 网络安全审查办公室对派拓公司在华销售产品启动网络安全审查

发布日期：2026 年 8 月 6 日

来源：中华人民共和国国家互联网信息办公室官网

链接：

- https://www.cac.gov.cn/2026-08/06/c_1787764332950791.htm

摘要：

2026 年 8 月 6 日，网络安全审查办公室发布《关于对派拓公司在华销售产品启动网络安全审查的公告》。为保障关键信息基础设施安全稳定运行，防范网络安全风险隐患，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和

国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对派拓公司（Palo Alto Networks）在华销售的产品实施网络安全审查。

植德短评

本次系网络安全审查办公室依据《网络安全审查办法》对单一外商网络安全厂商在华销售产品启动的专项审查，显示关键信息基础设施供应链安全监管持续收紧。对关键信息基础设施运营者及部署相关产品的企业而言，应持续关注审查进展及审查期间的相关义务要求，同步盘点存量产品的部署范围、日志与数据流向，评估替代方案的可行性，并对采购合同中的供应连续性、漏洞披露与服务保障条款作对应检视。跨国网络安全厂商则面临网络安全审查、数据出境合规与国际贸易环境等多重约束叠加，需要就其在华业务的合规架构作出更精细的安排。

3. 公安部网安局公布 10 起打击侵犯公民个人信息犯罪典型案例

发布日期：2026 年 8 月 11 日

来源：中华人民共和国公安部官网

链接：

- https://www.mps.gov.cn:8081/n2254098/n4904352/c10579188/content.html

摘要：

2026 年 8 月 11 日，公安部网安局公布 10 起打击侵犯公民个人信息犯罪典型案例。10 起案例覆盖多种作案手法：以“高薪兼职”“执照充场”为名招募人员手持身份证拍摄、非法注册电商账号及营业执照后倒卖；以“闲置账号高价变现”为名收购微信、QQ、抖音等实名网络账号层层转卖至境外诈骗团伙；搭建“社工库”提供收费查档服务；利用黑客技术挖掘系统漏洞、批量爬取并倒卖房产中介经纪人个人信息；以“订单解密”业务批量获取电商平台订单中的手机号码、收件地址等信息出售；教培、装修、医疗、物业等行业“内鬼”非法交换、出售客户信息；成立共享充电设备公司免费投放共享充电宝，换取宾旅馆住客个人信息并操控网络评价；以“私家侦探”“婚姻调查”“寻亲找人”名义非法获取行踪轨迹、开房记录等敏感信息。

据通报，涉案个人信息从数千条到数百万条不等。例如，某装修行业黑产链条非法获取公民个人信息 600 万余条；某共享充电宝评价操控案非法获取公民个人信

息 100 余万条、操控网络平台评价 10 万余条，涉案金额 1100 余万元。公安机关依据《中华人民共和国刑法》第二百五十三条之一及《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，对涉案人员依法追究刑事责任，并提示广大群众妥善保管、储存和使用个人信息，发现个人信息泄露线索及时向公安机关和有关部门投诉举报。

植德短评

本批案例集中呈现了侵犯公民个人信息犯罪“链条化、行业化、内外勾结”的特征：前端以兼职利诱、账号收购批量汇集信息，中端依托“社工库”“订单解密”等技术手段突破平台数据防线，末端流入诈骗、精准营销、评价操控等变现场景。对企业而言，启示有二：其一，“内鬼”风险贯穿房产、教培、医疗、物业等数据密集行业，访问权限最小化、操作留痕审计与离职权限回收应作为内控标配；其二，“订单解密”“爬虫补数”等所谓行业惯例可能直接触及刑法红线，涉及个人信息流转的第三方合作应开展合规审查。平台侧亦需防范订单接口、代理商账号等系统性泄露通道被黑产利用。

4. 国家计算机病毒应急处理中心通报 75 款违法违规收集使用个人信息的移动应用

发布日期：2026 年 8 月 14 日

来源：国家网络安全通报中心微信公众号

链接：

- https://mp.weixin.qq.com/s/zxQxAyWVlfwriHGT6XzS9g

摘要：

2026 年 8 月 14 日，根据中央网信办、工业和信息化部、公安部联合发布的《关于开展 2026 年个人信息保护系列专项行动的公告》，依据《网络安全法》《个人信息保护法》《网络数据安全管理条例》《App 违法违规收集使用个人信息行为认定方法》等法律法规和有关规定，经国家计算机病毒应急处理中心检测，75 款移动应用存在一项或者多项违法违规收集使用个人信息情况，由国家网络安全通报中心予以通报。本次检测时间为 2026 年 6 月 23 日至 7 月 28 日。

本批通报的违法违规情形主要包括：在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则、未以显著方式真实准确完整告知个人信

息处理者相关信息（涉及 26 款）；隐私政策未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围（涉及 39 款）；向其他个人信息处理者提供个人信息未告知并取得单独同意、向第三方提供未经同意且未做匿名化处理（涉及 8 款）；未在征得用户同意后开始收集个人信息或打开权限（涉及 4 款）；未提供有效的更正、删除个人信息及注销账号功能（涉及 4 款）；未建立便捷的个人行使权利申请受理和处理机制（涉及 1 款）；未提供撤回同意的途径方式（涉及 5 款）；未经同意定向推送且未提供拒绝方式（涉及 1 款）；处理不满十四周岁未成年人个人信息未制定专门规则、未取得监护人单独同意（涉及 5 款）；向境外提供个人信息未告知并取得单独同意（涉及 1 款）；未采取加密、去标识化等安全技术措施（涉及 22 款）；将人脸识别作为唯一验证方式（涉及 1 款）；无隐私政策（涉及 8 款）。被通报应用覆盖 App 及微信、支付宝、云闪付、百度小程序等多种形态，涉及出行、医疗、金融、教育、电商等领域。此外，上期通报的 72 款应用经复测仍有 24 款存在问题，相关应用已被下架。

植德短评

今年以来国家计算机病毒应急处理中心已连续多批次通报（4 月 30 日 67 款、6 月 3 日 71 款、7 月 9 日 72 款、8 月 14 日 75 款），专项检测通报已成常态化执法节奏，且通报对象向微信、支付宝、云闪付、百度小程序等轻应用形态全面延伸，复测下架机制亦已闭环。移动应用及小程序运营者应将通报列明的各类情形作为自查清单，重点排查小程序端隐私政策可达性、第三方代码与插件清单披露及权限触发时点，并在版本迭代时建立个人信息合规的复核机制；分发平台与宿主平台的审核、处置义务同步加压，轻应用生态的合规成本需要纳入商业模式测算。

5. 个人信息保护专项行动阶段性成效：400 余款 App/SDK 被下架处置

发布日期：2026 年 8 月 19 日

来源：网信中国微信公众号

链接：

- https://mp.weixin.qq.com/s/78kJBtp3-QdDYHglE-zFJA

摘要：

2026 年 8 月 19 日，“网信中国”微信公众号发布信息，介绍 2026 年个人信息保护系列专项行动取得的阶段性成效。专项行动由中央网信办、工业和信息化部、公安部会同相关部门开展。

阶段性成效主要包括：一是累计对 2 万余款 App、SDK 个人信息收集使用情况开展核查检测，督促 4000 余款完成合规整改，公开通报 1100 余款存在违法违规问题的 App、SDK，对 400 余款采取下架等处置处罚措施；二是针对个人信息处理规则未明确收集个人信息用于广告、用户画像，未提供个性化广告关闭选项等问题，对 1000 余家企业和机构的相关产品开展核查检测并督促整改；三是在教育、交通、卫生健康、金融等领域开展个人信息风险排查，累计摸排 9 万余家企业和机构，发现并督促整改各类隐患问题 1.2 万余个；四是加大个人信息违法犯罪打击力度，严打涉信息泄露、信息倒卖等违法犯罪行为，严惩行业“内鬼”。

下一步，中央网信办、工业和信息化部、公安部将深入推进个人信息保护系列专项行动，加强典型违法违规问题治理，加快推进国家网络身份认证公共服务推广应用，深化个人信息保护宣传教育，不断夯实个人信息保护工作基础。

植德短评

专项行动“2 万余款检测、4000 余款整改、1100 余款通报、400 余款下架”的数据组合，直观呈现了“检测—通报—整改—下架”的递进式执法闭环，也说明下架已非小概率事件，而是整改不力后的标准处置手段。个性化广告告知与关闭选项被单列为核查重点，与《个人信息保护法》自动化决策条款的执法化相呼应。建议企业对照专项行动四条主线开展年度合规体检：App 与 SDK 清单化管理、广告及画像场景的告知同意、重点行业数据风险排查、员工与供应商“内鬼”防控，并关注国家网络身份认证公共服务推广应用对现有身份核验流程的替代性影响。

6. 上海市网信办关于属地 App 个人信息收集使用问题的通报（2026 年第五批-未成年人保护专项）

发布日期：2026 年 9 月 4 日

来源：网信上海微信公众号

链接：

- https://mp.weixin.qq.com/s/wbtKHL1RFVI4iRMjdrSH1g

摘要：

2026 年 9 月 4 日，上海市互联网信息办公室通过“网信上海”微信公众号发布《关于属地 App 个人信息收集使用问题的通报（2026 年第五批-未成年人保护专项）》。根据中央网信办、工业和信息化部、公安部联合发布的《关于开展 2026 年个人信息保护系列专项行动的公告》，依据《网络安全法》《数据安全法》《个人信息保护法》《未成年人保护法》《网络数据安全管理条例》《App 违法违规收集使用个人信息行为认定方法》等法律法规和有关规定，上海市网信办组织对属地 App、小程序等服务产品收集使用个人信息行为进行检测，并对有关问题予以通报。

本批通报共涉及“沪学习”“壹点灵”“乐读”“口袋故事”“布布识字”“ahakid 启蒙”“布鲁可智趣版”“玩具反斗城官方商城”“英孚”“Stokke 官方会员”“宝可梦卡牌会员”等 11 款 App 及微信小程序，覆盖教育培训、儿童启蒙、玩具及线上商城等领域。存在的主要问题包括：处理敏感个人信息未取得个人单独同意、收集敏感个人信息未同步告知目的及必要性；告知的收集使用个人信息目的、方式、范围与实际收集使用情况不一致；频繁征求用户同意；在无关场景收集位置、通讯录、短信等个人信息；强制用户同意收集非必要个人信息；首次启动未提示用户阅读隐私政策、未公开个人信息收集使用规则；为注销用户账号设置不必要或不合理条件、注销后未及时删除个人信息；未及时响应个人信息权益诉求；超出最低必要频率调用个人信息权限；以及未针对不满十四周岁未成年人制定专门的个人信息处理规则等。

上海市网信办要求相关运营者于本通报发布之日起 15 个工作日内完成整改并将整改情况报该办，其将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。此外，上期通报的第四批（酒店住宿专项）所涉运营者经复测均已完成问题整改。

植德短评

本批通报传递出两个信号：其一，地方网信部门在专项行动中开始按“未成年人保护”“酒店住宿”等场景设置专项批次，检测对象延伸至小程序，未成年人个人信息正成为独立的执法维度，“专门处理规则、单独同意与监护人同意、最小必要调用权限”等要求将面临更密集的点验；其二，通报明确了“15 个工作日整改＋核查＋依法依规处置处罚”的处置链条，上期专项复测全部完成整改亦显示复测闭环压力真实存在。教育培训、母婴童、玩具等行业企业及运营未成年人相关产品的主体，应对照《个人信息保护法》《未成年人网络保护条例》及本通报列明情形逐项排

查未成年人信息处理规则、监护人同意机制、权限调用频率与注销删除流程，并建立版本迭代时的合规复核机制，避免在后续批次通报中被点名。

7. 国家数据局公布首批数据领域国际合作 10 地试点

发布日期：2026 年 8 月 18 日

来源：国家数据局官网

链接：

- https://www.nda.gov.cn/sjj/swdt/xwfb/0818/20260818214138823356282_pc.html

摘要：

2026 年 8 月 18 日，国家数据局举行 2026 上合组织数字经济论坛新闻发布会，介绍数据领域国际合作试点有关情况。国家数据局从数据基础设施、数据标准协议、国际合作载体、跨境服务生态、数字合作场景、沟通交流机制 6 个方面系统谋划了 20 项试点事项，首批选择 10 个地方开展试点，初步形成错位发展、优势互补的试点布局。

首批 10 个试点地方为：上海，海南，福建福州、厦门、泉州，湖南长沙，广东广州、深圳、横琴，广西南宁。各试点地方定位各有侧重：上海侧重构建设施领先、规则互认、载体赋能、场景融合的国际数据合作新体系；海南自由贸易港侧重数据跨境流动、国际数据服务等试点探索；福建福州侧重跨境电商、食品安全等领域数据跨境规则标准互认试点，厦门侧重智慧物流、智慧海港等场景的国际合作，泉州侧重数据赋能纺织鞋服等特色产业国际合作；湖南长沙侧重面向非洲的智慧医疗、智慧农业等合作；广东广州侧重医疗科研数据跨境流动便利化，深圳侧重培育国际数据服务新业态，横琴侧重面向葡语、西语国家的数据合作；广西南宁侧重面向东盟的数智技术应用合作。

试点工作按照统筹谋划、因地制宜，问题导向、务求实效，健全机制、压实责任三方面考虑组织，建立“央地协同、地方主抓、定期调度”的工作机制，鼓励地理位置相近、功能互补的试点地方共建共享国际合作平台，推动形成跨区域协同试点机制，在数据跨境流动、规则对接、标准互认、设施互联、数字人才培养等方面打造可复制、可推广的试点经验。

植德短评

数据领域国际合作试点的落地，延续了自贸区数据出境负面清单、公共数据示范场景等既有改革路径，首次将数据跨境流动便利化与国际数据服务新业态作为地方先行先试的系统性命题。10 地清单中的医疗科研（广州、长沙）、跨境电商（福州）、国际数据服务（深圳）等方向，与相关行业企业的高频数据出境场景高度重合，辖区内企业宜主动对接试点申报与调度机制，争取适用便利化安排；同时应注意试点安排与数据出境安全评估、标准合同、认证等现行制度的衔接边界，便利化不等于豁免，数据识别、风险自评估与全流程留痕仍是适用各类出境通道的合规基础。

8. 国家数据局发布第五批公共数据“跑起来”示范场景

发布日期：2026 年 8 月 25 日

来源：国家数据局官网

链接：

- https://www.nda.gov.cn/sjj/swdt/xwfb/0825/20260825221943908355266_pc.html

摘要：

2026 年 8 月 25 日，国家数据局在“数据价值化 我们在行动”系列新闻发布会（第五场）上发布第五批公共数据“跑起来”示范场景建设清单，50 个示范场景覆盖自然资源、社会管理、医疗健康、农业农村、人工智能等 23 个重点方向。

公共数据“跑起来”示范场景建设自 2024 年 10 月启动以来，已成为推动政策落地和价值释放的重要抓手。第五批示范场景申报数量创新高，共收到 703 份申报方案，申报内容更加丰富多元，涌现出部省协同、跨区域联合申报等创新形式；中宣部、民政部、住房城乡建设部等 12 个部委和新疆生产建设兵团等地方首次参与申报，公共数据资源开发利用示范场景影响力逐步扩大。

下一步，国家数据局将认真落实中央关于加快场景培育和开放的部署要求，持续推进公共数据“跑起来”示范场景建设与推广，以场景为牵引促进公共数据资源高水平应用，让数据要素更好赋能社会治理和产业发展，更好惠及民生福祉。

植德短评

第五批 703 份申报、12 个部委首次参与，显示公共数据开发利用正从地方试点走向条线协同，人工智能方向场景的集中入选亦提示高质量公共数据集将成为人工智能企业合规的数据供给渠道。对参与企业而言，示范场景既是数据产品与服务的市场化入口，也意味着承接场景时需同步解决公共数据授权运营的合规链条，授权主体、使用边界、收益分配与安全责任应在协议中予以固定；涉及个人信息的公共数据产品还应完成匿名化或去标识化处理，并留存相应的评估与审计记录，避免场景红利转化为合规风险。

9. 韩国农协银行北京分行完成全国银行业首例数据出境负面清单备案

发布日期：2026 年 8 月 17 日

来源：北京朝阳微信公众号

链接：

- https://mp.weixin.qq.com/s/d-ZmFZ7e8ZiZ2qbWISGLqQ

摘要：

2026 年 8 月上旬，韩国农协银行北京分行完成全国银行业首例数据出境负面清单备案，成为我国首家通过负面清单实现数据合规出境的银行业机构；其数据出境管理模式由标准合同备案转为负面清单框架下的安全有序自由流动。北京市互联网信息办公室于 8 月 6 日对外发布了这一信息。

本次备案依托北京市“两区”建设与数据跨境 3.0 版改革方案。2026 年 3 月，北京市发布《关于进一步深化数据跨境流动便利化综合配套改革实施方案》（数据跨境 3.0 版方案）；同年 5 月，北京市“两区”数据出境负面清单出台，采用“1+9”制度设计（1 套管理办法加 9 个领域清单），在原有 5 个领域基础上新增医疗器械、自动驾驶（智能网联汽车）、贸易物流、银行业 4 大领域，覆盖 67 个业务场景、612 个字段，适用范围从自贸试验区扩展至国家服务业扩大开放综合示范区（覆盖北京全市域）。

此前，北京朝阳区已推动全国首例人工智能领域数据出境负面清单案例，以及赛诺菲、默沙东、澳科利耳等医药医疗器械领域负面清单项目相继落地，本次银行业首例备案标志着北京数据跨境制度创新在金融领域实现突破。

植德短评

银行业首例负面清单备案的示范意义在于：负面清单模式从医药、人工智能等先行领域正式进入金融这一强监管行业，外资银行分行的客户与业务数据出境自此有了“一般数据自由流动＋负面清单管理”的新路径。对在京金融机构而言，应对照“1+9”清单逐场景评估自身业务能否适用，测算标准合同模式与负面清单模式之间的合规成本差异，并注意负面清单并非“免检通道”，清单外字段、新增业务场景仍须回归一般出境规则。其他地区金融机构亦可关注北京方案的复制推广节奏，提前整理出境业务场景清单与字段映射，为政策落地预留申报窗口。

境外要闻

1. 欧盟委员会依据 DSA 认定 ChatGPT 为超大型在线搜索引擎、Reddit 与 Roblox 为超大型在线平台

发布日期：2026 年 8 月 31 日

来源：European Commission 官网

链接：

- https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1772

摘要：

2026 年 8 月 31 日，欧盟委员会依据《数字服务法》（DSA）正式认定：ChatGPT 构成超大型在线搜索引擎（VLOSE），Reddit 与 Roblox 构成超大型在线平台（VLOP）。三项服务均申报其在欧盟境内平均月度活跃用户数达到 4500 万人以上，达到 DSA 规定的认定门槛。这是 DSA 项下首次将生成式人工智能助手认定为超大型在线搜索引擎，被认定的超大型在线平台和搜索引擎总数增至 28 家。

关于服务定性，欧盟委员会认为，ChatGPT 因其能够回应用户的提示与查询（包括通过检索网络信息作出回应）而符合 DSA 下在线搜索引擎的定义；Reddit 和 Roblox 则因允许用户向公众传播第三方内容而构成在线平台。据申报，截至 2026 年 3 月 31 日的六个月内，ChatGPT 在欧盟的月均活跃用户约为 1.59 亿，Reddit 约为 5720 万，Roblox 约为 4800 万。

被认定后，三项服务须在四个月内（至 2027 年 1 月）履行 DSA 为超大型在线平台和搜索引擎设定的附加义务，包括评估并缓解与其服务及算法系统相关的系统性风险（涉及非法内容传播、对未成年人的负面影响、用户身心健康、基本权利、选举进程与公共安全等）、接受独立审计、向监管机构及经审核的研究人员提供数据访问等。欧盟委员会将与爱尔兰数字服务协调员 Coimisiún na Meán（负责 ChatGPT 与 Reddit）及荷兰消费者与市场管理局（负责 Roblox）合作开展监督，违反相关义务最高可处全球年营业额 6%的罚款。

植德短评

对 ChatGPT 按“搜索引擎”而非“平台”定性，是监管机构首次将通用人工智能助手纳入 DSA 最高监管层级：认定锚点在于其检索网络并对外呈现第三方内容的功能，意味着 DSA 的算法透明度、系统性风险评估与独立审计义务将

首先作用于 AI 产品的“检索—呈现”环节，而非生成内容本身。对拟在欧盟提供服务的 AI 企业，启示在于：用户规模的统计口径（按功能还是按产品整体）将直接影响是否触发认定，需提前设计口径与留痕；未成年人保护、选举与公共安全等系统性风险自评应纳入产品上线前流程。DSA 与《人工智能法》对同一 AI 服务的叠加适用，也将成为后续欧盟 AI 合规架构设计的核心变量。

2. 美国加州 AB-1542 推进敏感个人信息出售或共享限制，完成送交编纂和登记程序

发布日期：2026 年 8 月 30 日

来源：California Legislative Information 官网

链接：

- https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202520260AB1542

摘要：

2026 年 8 月 30 日，加州立法信息官网显示，AB-1542（《敏感个人信息》）完成“参议院修正案获众议院同意，送交编纂和登记”程序，法案状态为 Active Bill - Passed。法案拟修改《民法典》第 1798.100 条和第 1798.121 条，限制受《加州消费者隐私法》（CCPA）约束的企业出售或共享消费者敏感个人信息。该法案尚未完成州长签署等后续程序。

植德短评

AB-1542 的立法逻辑，是将《加州消费者隐私法》（CCPA）项下消费者“限制敏感个人信息使用”的选择退出权利，升级为对出售、共享行为的全面禁止，且原则上不以消费者同意为例外，仅保留商业征信机构为确认消费者与企业的所有权关系而出售社保号等极窄豁免，敏感个人信息的流通自由将受到实质性收缩。若法案最终获州长签署，受 CCPA 管辖的企业需要重新梳理数据变现链条：广告技术与数据经纪业务中涉及精确地理位置、健康、性取向、社保号等敏感字段的出售与共享安排需逐项排查并改造合同结构；“共享”定义项下的第三方合作同样在禁止之列。建议相关企业持续跟踪法案签署进展与生效时间，同步评估现有数据流对业务收入的影响并制定替代方案。

3. 美国加州 SB 923 通过州众议院全院表决，拟扩大 CCPA 删除权并强制提供在线请求渠道

发布日期：2026 年 8 月 27 日

来源：California Legislative Information 官网

链接：

- https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202520260SB923

摘要：

2026 年 8 月下旬，美国加州 SB 923（《扩大隐私权法案》，Expanding Privacy Rights Act）完成州立法机构审议程序：8 月 27 日，州参议院以 36 票赞成、0 票反对同意州众议院修正案，法案送交编纂和登记（engrossing and enrolling），随后送交州长签署。该法案由州参议员 Josh Becker 提出、加州隐私保护局（CalPrivacy）发起支持，拟修改《加州民法典》第 1798.105 条和第 1798.130 条。

在删除权方面，现行 CCPA 仅要求企业删除其“从消费者处收集”的个人信息，企业自数据经纪商等第三方获取的信息不受删除请求约束。SB 923 将删除权扩展至企业持有的关于该消费者的全部非豁免个人信息，无论信息来源如何；企业未从消费者处直接获取信息的，可以通过留存删除请求记录及确保相关信息持续处于删除状态所需的最少数据的方式履行义务（即允许保留抑制清单），以防止已删除信息被再次使用或出售。

在权利行使渠道方面，法案要求仅在线经营且与消费者存在直接关系的企业，在现行提供电子邮箱之外，还须提供在线方式（如网页表单或在线门户）供消费者提交访问、更正、删除等隐私请求，以降低权利行使门槛。加州隐私保护局表示，该法案将使加州消费者的删除权与特拉华、印第安纳、马里兰、新泽西等州隐私立法保持同等水平。

植德短评

SB 923 针对的是删除权实践中最普遍的落空情形，企业以“信息并非直接从消费者收集”为由拒绝删除第三方补充数据。删除权扩展后，企业客户画像中来自数据经纪商、联盟营销等第三方来源的信息同样纳入删除义务，客观上要求企业建立以消费者为单位的跨源数据索引与抑制清单机制，并重新评估 CCPA 既有豁免（防欺诈、合规义务、同行评审研究等）在删除场景下的适用。

在线请求渠道的强制化，则意味着仅提供邮箱通道的企业需上线表单或门户并对接请求核验流程。叠加 2026 年 1 月起 DROP 平台对数据经纪商的强制覆盖，加州“删除权＋统一行使通道”的执法基础设施已趋完整，面向加州消费者的企业应将上述变化纳入 2026—2027 年度合规预算与产品改造计划。

4. 韩国 PIPC 对 GS Retail 数据泄露案处以 128.36 亿韩元罚款及 300 万韩元罚款

发布日期：2026 年 8 月 31 日

来源：PIPC 官网

链接：

- https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12425

摘要：

2026 年 8 月 31 日，韩国个人信息保护委员会（PIPC）宣布，因 GS Retail 发生个人信息泄露事故，对公司处以 128 亿 3600 万韩元行政罚款及 300 万韩元行政罚款。公开报道显示，凭证填充攻击导致 GS SHOP 及 GS25 相关客户约 166 万人个人信息受到影响。案件涉及个人信息安全保护、泄露防止及企业管理义务，PIPC 以韩国《个人信息保护法》为依据作出处罚。

植德短评

本案处罚的焦点并非泄露本身，而是“已知未防、已知未控”的响应失灵：凭证填充攻击的特征信号（同一 IP 短时间内大规模登录尝试及失败激增）未被检测、阻断；企业在 2025 年 1 月 4 日知悉 GS25 网站泄露后，直至同年 2 月 13 日才确认同一攻击正在 GS SHOP 延续，泄露因此多持续约 40 天；专属个人信息保护组织缺位、安全职能分散被认定为治理缺陷，对新增 1599 名受害者的 72 小时内通报义务迟延履行进一步加重责任。对企业的启示是系统性的：其一，登录风控应对凭证填充、撞库等攻击模式建立基线检测与阻断规则；其二，事件响应应从“单点处置”升级为“横向排查”，一次泄露线索应触发全业务线核查；其三，个人信息保护组织架构、首席隐私官职权与 72 小时通报流程需经演练验证。韩国个人信息保护委员会近年对头部企业持续高压执法，在韩经营的企业应对照《个人信息保护法》的安全保障措施与泄露通报要求开展自查。

5. 日本 PPC 公布修订《个人信息保护法》实施规则总体方案

发布日期：2026 年 8 月 26 日

来源：PPC 官网

链接：

- https://www.ppc.go.jp/aboutus/minutes/2026/20260826/

摘要：

日本个人信息保护委员会（PPC）在 8 月 26 日举行的第 366 次委员会会议上公布修订《个人信息保护法》配套政令、委员会规则、指引和问答的总体方案。方案提出，对仅用于统计制作等用途的个人数据第三方提供及已公开敏感个人信息获取，可在低风险条件下设置免同意路径，并明确可涵盖符合条件的 AI 开发；同时拟细化儿童数据、面部特征等生物识别数据、受托处理者义务、泄露报告、退出机制和重大违法行为行政罚款计算规则。PPC 计划自 9 月起分主题讨论、听取个人和企业代表意见，之后形成条文草案并启动公众意见征集。

植德短评

本次总体方案明确了 2026 年日本《个人信息保护法》大改正的实施规则路线图：政令将承载行政课征金的计算规则，委员会规则将承载统计作成等目的（含 AI 学习）免同意路径的适用条件及提供方、接收方的披露义务，配套指引与问答随后展开，整体向 2028 年 7 月前的施行时点推进。对在日经营及面向日本用户提供服务的企业而言，短期应关注 9 月起分主题征求意见的窗口，就 AI 训练数据利用条件、生物识别信息周知义务、16 岁以下未成年人同意规则等与自身业务直接相关的条款提交意见；中期则应预留制度切换成本，课征金制度落地后，以往行政指导框架下难以追缴的“违法收益”将被剥夺，受托处理、第三方提供、退出机制等环节的合同与留痕体系需对照新规则全面翻修。日本监管框架向“促进利用＋实效应责”并行的转向，也值得与 GDPR、我国《个人信息保护法》的义务清单作交叉映射，统筹全球合规基线。

特别声明

本刊物不代表本所正式法律意见，仅为研究、交流之用。非经北京植德律师事务所同意，本刊内容不应被用于研究、交流之外的其他目的。如有任何建议、意见或具体问题，欢迎垂询。

参与成员编委会：王希

本期执行编辑：刘含章

MeritsTree
植德律师事务所

前 行 之 路 植 德 守 护

www.meritsandtree.com