

NEWSLETTER

数据合规

2019 第十二期 / 总第十二期

数据合规时事速递

北京市环球律师事务所

2019 年 12 月 3 日

目录

前 言	4
一、新规速递	5
1. 教育部印发《教育移动互联网应用程序备案管理办法》，要求教育 App 进行备案	5
2. 网信办发布《网络安全威胁信息发布管理办法（征求意见稿）》	5
二、监管动态	9
1. 工信部：携号转网正式在全国提供服务，不得干涉用户自主选择	9
2. 国家网信办主任庄荣文：努力开创网络安全和信息化工作新局面 ..	10
3. 为禁止苹果等公司在中国存储用户数据，美参议院提出新法案	12
4. 美国国会提出隐私保护法案，侵犯隐私的科技巨头将被处罚	12
三、相关案例	14
1. 涉嫌泄露亿条公民信息，考拉征信被查	14
2. 麦子金服办公室突遭查封，创始人黄大容等高管接受警方调查	15
3. 全国大清剿：北京警方抓捕数十名区块链平台负责人	16
4. 4.68 亿个人信息泄露：2 块钱就可以查你的身份证	19
5. 骗取个人信息盗刷银行卡 “携号转网”这些骗局要小心	20
6. 租房中介成个人信息泄露“重灾区”	22
7. 1600 多名酒店房客被非法偷拍，黑色产业链被挖出	23

8. 个人信息被抢注？银行推广 ETC 催生灰色产业链.....	26
9. 库克重申不获取用户数据 苹果出台多项保护隐私举措.....	27
10. 谷歌将限制与广告商的数据共享 以保护用户隐私	28
11. 12 亿个人信息泄露，谷歌云服务器上发现庞大的未受保护数据库 .	30
12. Elasticsearch 服务器泄露 12 亿个人数据	31
13. FB、Twitter 数百用户因登录第三方应用个人信息泄露.....	33
14. 《Magic: The Gathering》开发商证实 安全漏洞使超 45 万玩家数据泄 露	34
15. 美国对“隐私保护”出现分歧 谷歌与微软公开发声	35
四、环球评论	38
1. 《GDPR 第 3 条域外效力指南》（2019 版）全文翻译.....	38
2. 公司 IPO/重组/投融资时，监管部门审查要点汇总及问题分析.....	64

前言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和网络安全监管。我国对个人信息保护和网络安全越来越重视，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。据时代的机遇与挑战。



团队介绍：

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

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

孟洁

合伙人律师

直线：86-10-6584-6768

总机：86-10-6584-6688

邮箱：

mengjie@glo.com.cn



一、新规速递

1. 教育部印发《教育移动互联网应用程序备案管理办法》，要求教育 App 进行备案

2019 年 11 月 11 日，教育部办公厅发布《教育移动互联网应用程序备案管理办法》的通知，要求教育类 App 在 2020 年 1 月 31 日前完成 ICP 备案和等级保护备案，并及时在公共服务体系上传、更新信息。2020 年 2 月 1 日起，未完成上述两个备案的教育移动应用备案将被撤销，并予以通报。

此外，该办法还要求建立以备案为基础建立监测预警通报机制，及时发现、处置问题隐患和安全事件。省级教育行政部门应建立本地区的监测预警通报机制，并与教育部进行数据共享。2020 年 2 月 1 日起，公共服务体系将向社会公众提供备案信息查询，接受社会监督。¹

《教育移动互联网应用程序备案管理办法》全文参见：

http://www.moe.gov.cn/srcsite/A16/s3342/201911/t20191122_409333.html

2. 网信办发布《网络安全威胁信息发布管理办法（征求意见稿）》

国家互联网信息办公室 11 月 20 日向社会公开征求对《网络安全威胁信息发布管理办法（征求意见稿）》（以下简称《办法》）意见，国家互联网信息办公室有关负责人接受采访，就《办法》相关问题回答了记者提问。

制定《办法》的背景

答：当前，网络安全产业迅猛发展，许多网络安全研究者和网络安全企业出于提高公民网络安全意识、交流网络安全技术、增强用户网络安全防范能力、促进网络安全产业发展等目的，积极向社会发布网络安全威胁信息，为维护国家网络空间安全做出很大贡献。但是也应看到，网络安全威胁信息的发布仍存在很多问题，有

¹ 教育部。

关单位、网络运营者反映强烈。例如，有组织或个人打着研究、交流、传授网络安全技术的旗号，随意发布计算机病毒、木马、勒索软件等恶意程序的源代码和制作方法，以及网络攻击、网络侵入过程和方法的细节，为恶意分子和网络黑产从业人员提供了技术资源，降低了网络攻击的门槛；有组织或个人未经网络运营者同意，公开网络规划设计、拓扑结构、资产信息、软件代码等属性信息和脆弱性信息，容易被恶意分子利用威胁网络运营者网络安全，特别是关键信息基础设施的相关信息一旦被公开，危害更大；部分网络安全企业和机构为推销产品、赚取眼球，不当评价有关地区、行业网络安全攻击、事件、风险、脆弱性状况，误导舆论，造成不良影响；部分媒体、网络安全企业随意发布网络安全预警信息，夸大危害和影响，容易造成社会恐慌。

制定《办法》的依据

答：《网络安全法》第二十六条规定，“开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。”目前，尚无规范网络安全威胁信息发布活动的法律法规。因此，为了进一步规范网络安全威胁信息发布行为，国家互联网信息办公室会同公安部等有关部门依据职责制定了《办法》。

为什么禁止发布恶意程序源代码、制作方法，能够完整复现网络攻击、网络侵入过程的细节信息等网络安全威胁信息？

答：上述网络安全威胁信息容易被恶意分子或网络黑产从业人员直接利用，降低了网络攻击的门槛，因此从维护网络安全的角度，要求发布网络安全威胁信息时不得包含上述内容。网络安全从业者、爱好者仍可通过多种方式加强原理和技术研究，提高网络安全能力水平。

禁止发布第四条规定的信息，是否会导致这些信息流入地下黑市？

答：为网络犯罪提供技术支持是法律明确禁止的违法犯罪行为，依法要承担相应的法律责任。我们相信，作为遵纪守法、有道德操守的网络安全工作者、爱好者，以前不会为网络黑产提供技术支持，今后同样也不会。

是否会对网络安全产业发展造成影响？

答：我们鼓励和支持网络安全企业向社会展示技术能力，促进网络安全意识提升，传播普及网络安全防护技术知识，提供网络安全服务。要求安全企业不向社会发布恶意程序的制作技术、网络攻击技术，并不意味着企业不能研究网络攻击技术，企业仍可通过研究网络攻防技术，不断提升网络安全防护能力，不但不影响安全产业发展，对提高网络安全产业发展水平还产生积极的促进作用。

媒体今后还能报道网络安全事件新闻吗？

答：媒体可以正常报道网络安全事件新闻，但需满足两个条件，一是如果属于办法第五条提到的网络和信息系统的网络安全事件，首次披露前要向所在地区地市级以上公安机关报告，以便有关部门及时掌握事件情况，采取处置措施，降低危害；二是不得包含网络安全事件泄露的数据内容本身，以免扩大事件的危害。

向网信部门、公安机关、行业主管部门等报告是否属于行政许可？

答：不属于行政许可，完成报告即为履行义务。

为什么发布具体网络和信息系统的风险、脆弱性的情况时，需要事先征得其运营者书面同意？

答：如果随意发布上述信息，恶意分子有可能利用这些信息入侵相关网络和信息系统的运营者利益受损。但如果根据发布的网络安全威胁信息，无法定位到具体网络和信息系统的名字、位置、域名、IP 地址等信息，就不需要征求其运营者同意。此外，如果相关风险、脆弱性已被消除或修复，或已提前 30 日向网信、电信、公安或相关行业主管部门举报，发布上述信息也可不经其运营者同意。

为什么发布网络安全威胁信息，标题中不得含有“预警”字样？

答：根据《国家网络安全事件应急预案》，网络安全预警是一种特定信息，具有权威性，应由政府部门按权限发布。但目前有的组织和个人随意发布预警，夸大事实，进行炒作，事实上破坏了预警的效力和权威性，所以我们要求发布网络安全

威胁信息，标题中不得含有“预警”字样。相关组织和个人可通过风险提示、威胁情报等方式提醒公众加强风险防范。²

《网络安全威胁信息发布管理办法（征求意见稿）》全文参见：

http://www.cac.gov.cn/2019-11/20/c_1575785387932969.htm

² 网信湖南。

二、监管动态

1. 工信部：携号转网正式在全国提供服务，不得干涉用户自主选择

11月27日，工信部召开携号转网启动仪式。11月27日起，携号转网正式在全国提供服务。在携号转网政策下，用户号码保持不变，符合条件可自由选择运营商；电信业务经营者不得干涉用户自主选择。这符合之前官方发布的携号转网铺开节奏。

按之前官方披露的信息，携号转网工作推进将分为三个阶段：9月20日前，天津市、海南省、江西省、湖北省、云南省5个试点省（市）完成试验，正式提供服务；11月10日至25日，其他26个省（自治区、直辖市）“携号转网”服务上线试运行；11月30日前，全国范围内正式提供服务。

所谓携号转网服务，是指在同一本地网范围内，蜂窝移动通信用户（不含物联网用户）变更签约的基础电信业务经营者而用户号码保持不变的一项服务。所谓“携号转网”，指的是用户在不改变移动电话号码的情况下，可以从现有运营商改用其他运营商的服务。以往消费者要想改用一家电信运营商的服务，必须更换这家运营商特有号段的电话号码。如今允许携号转网，将极大降低用户转换网络的门槛，运营商们将面临更为激烈的服务竞争环境。

11月9日，澎湃新闻记者获悉，中国移动、中国联通、中国电信三家电信运营商在上海已完成“携号转网”系统建设改造，11月10日，“携号转网”开启试运行，为11月底正式提供“携号转网”服务做好准备。

11月22日下午，工信部信息通信管理局在北京召开全国“携号转网”系统试运行分析电视电话会，全面总结试运行情况，分析存在的突出问题，研究制定解决方案。

会议认为，通过“携号转网”系统试运行，验证了系统性能，检验了服务能力，总体达到试运行效果，但部分省市电信企业违规设置携出条件等问题较为突出，“携号转网”服务与用户期待仍有差距，电信企业要落实企业主体责任，加快整改、

系统整改，为用户提供更加便捷高效的“携号转网”服务。³

2. 国家网信办主任庄荣文：努力开创网络安全和信息化工作新局面

数据资源成为“新生产要素”。农业时代，土地是最重要的战略资源，国家、民族之间的战争几乎都围绕着争夺土地展开。工业时代，以煤炭、石油为代表的能源矿产成为最重要的战略资源，能源控制权往往成为国家争夺的焦点。进入信息时代，随着信息技术和人类生产生活交汇融合，互联网快速普及，全球数据呈现爆发增长、海量集聚的特点，数据日益成为重要战略资源和新生产要素，对经济发展、国家治理、社会管理、人民生活都产生重大影响，数据掌控能力日益成为衡量国家竞争力的关键因素。

信息技术领域成为“新创新高地”。当前，以互联网为代表的新一代信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最强的科技创新领域，是全球技术创新的竞争高地。移动互联网、大数据、云计算、物联网、人工智能、区块链等新兴技术加速向各领域渗透融合，深刻改变人们生产生活方式，网络连接从人人互联迈向万物互联，技术应用从侧重消费环节转向更加侧重生产环节。

互联网、工业互联网、物联网等成为“新基础设施”。互联网是信息时代的新基础设施，是经济社会发展的“大动脉”。传统基础设施带来的是“乘数效应”，而互联网带来的是“幂数效应”。当前正处于全球网络信息技术加速创新变革、信息基础设施快速演进升级的关键“窗口期”，人工智能、工业互联网、物联网、大数据中心等新型基础设施将对经济社会发展产生更为重要的推动作用。

数字经济成为“新经济引擎”。当今世界，信息技术创新的扩散效应、信息和知识的溢出效应、数字技术释放的普惠效应日益凸显。各国加紧发展数字经济，推动新技术向实体经济各领域渗透融合，使新技术成为放大生产力的重要因素，为经济长期持续增长提供了强劲内生动力，数字技术正从助力经济发展的辅助工具向引领经济发展的核心引擎转变。

信息化成为“新治理手段”。新一代信息技术日新月异，为提升国家治理体系和治理能力现代化水平提供了有利条件。比如，移动互联网丰富了公共服务的渠道和范围，云服务为电子政务系统提供了更加灵活的建设和运维模式，大数据日益成为支撑政府科学决策、精准管理的重要工具。世界主要国家都把推进电子政务作为构

³ 澎湃新闻。

筑比较优势、提升国家竞争力的战略举措，数字政府建设步伐全面提速。

同时也要清醒地看到，互联网是“双刃剑”，既为我国经济社会发展注入强劲动力，也带来很多风险挑战和不确定因素。这就要求我们必须明辨方向、把握大势，抓住机遇、应对挑战，引领变局、争取主动，不断开创网络强国建设新局面。

习近平总书记指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”要统筹推进网络安全工作，坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重，切实保障国家网络安全和公民个人信息安全。

强化关键信息基础设施防护。关键信息基础设施是经济社会运行的神经中枢，涉及国家安全、国计民生以及公共利益，对于国家网络安全和信息化建设意义重大。要严格落实《中华人民共和国网络安全法》、网络安全工作责任制要求，夯实关键信息基础设施防护责任，强化不同地区、不同行业、不同领域关键信息基础设施之间的威胁信息共享和协同应对，建立完善关键信息基础设施安全保障体系。加强网络安全检查，明确保护范围和对象，及时发现隐患、修补漏洞，做到关口前移，防患于未然。

强化数据安全治理。在积极开发利用数据资源、充分释放数据效能的同时，切实保障数据安全，强化关键数据资源保护能力。健全管理和运用数据资源的法律制度和政策措施，推动出台数据安全管理办法，依法保护数据资源。加大个人信息保护力度，规范个人信息的收集、处理和利用，完善保护机制，依法坚决打击各种形式的网络诈骗、侵犯知识产权、侵犯公民隐私等网络违法犯罪活动。督促企业加强数据安全风险评估，加强对大数据企业的监督管理和责任追究，打造安全可靠的数据生态环境。

强化网络安全应急处置能力。加强网络安全信息统筹机制、手段、平台建设，实时监测预警网络安全重大事件，既掌握网络空间当前状态，又分析下一步动态，为科学决策指挥提供依据。加强网络安全事件应急指挥能力建设，健全完善网络安全监测预警响应机制，提升网络安全态势感知、事件分析、追踪溯源以及遭受攻击后的快速恢复能力。

强化网络安全工作基础。大力发展网络安全产业，加强网络安全产业统筹规划和整体布局，培育扶持一批具有国际竞争力的网络安全企业。加强网络安全教育，加快推进国家网络安全人才与创新基地建设，积极开展一流网络安全学院建设示

范项目。深入开展网络安全知识技能宣传普及，办好国家网络安全宣传周，不断提高广大人民群众网络安全意识和防护技能。⁴

3. 为禁止苹果等公司在中国存储用户数据，美参议院提出新法案

美共和党参议员乔希·霍利(Josh Hawley)提出了一项新法案，禁止苹果等科技公司在中国存储用户数据。这项新法规是在苹果去年被要求将部分 iCloud 数据转移到中国国有服务器之后出台的。

据 Axios 报道，这一限制的目的是防止中国公司收集美国用户的信息超过提供服务所需。参议员霍利表示像苹果这样在中国存储数据的公司是对美国国家安全的威胁。

除了苹果，霍利还通过立法瞄准了社交媒体应用 TikTok（海外版抖音）。他在一份声明中表示，美国用户在使用 TikTok 时，可能会被采集信息。

去年，为了遵守当地法律，苹果被要求将中国用户的 iCloud 数据转移到中国本土服务器上。尽管苹果承诺在过渡期间将保持强大的数据隐私和安全保护，但此举仍受到一些用户的批评。

只有中国 iCloud 账户的数据存储在云上贵州的服务器上，苹果坚称，美国和其他国家的用户不受到这项要求的影响。因此，尚不清楚 Hawley 的这项法案最终会如何影响苹果。

本月早些时候，Hawley 曾指责苹果和 TikTok 回避一场有关科技行业与中国关系的国会听证会。当时，他表示，苹果代表着美国科技企业在中国运营所面临的危险。⁵

4. 美国国会提出隐私保护法案，侵犯隐私的科技巨头将被处罚

据 CNBC 报道，美国国会参议院的部分民主党参议员提出隐私保护相关立法

⁴ 澎湃号。

⁵ 集微网。

草案《消费者线上隐私权法》(Consumer Online Privacy Rights Act), 如果 Facebook、Google 等科技企业错误处理用户数据, 这部新的法律将允许政府对它们进行处罚。

这部法律将使民众有权看到互联网企业收集到关于自己的信息, 也有权要求企业删除这些信息并阻止向第三方销售, 民众也可以对互联网企业侵犯隐私的行为提出诉讼。

大型科技企业曾一度被誉为美国经济最有活力的部分之一, 但收集用户信息、数据泄露、侵犯隐私等问题使人们感到担忧。报道称, 新法律的出台, 将使这些大型科技企业的光彩消退。

有业界人士担心, 如果美国不尽快制定相关法律, 其他州可能会效仿加州的法律, 使美国隐私监管制度碎片化。

由于隐私问题, Facebook 已经关闭了用于收集用户数据的 Onavo VPN 应用, 但该公司又推出另一款应用重启相似的数据收集工作。Viewpoints 是一款专门用于市场研究的应用程序, 可为参与调查的用户提供奖励。⁶

⁶ 动点科技。

三、相关案例

1. 涉嫌泄露亿条公民信息，考拉征信被查

个人信息泄露问题日益严峻，江苏淮安警方近日依法打击了 7 家涉嫌侵犯公民个人信息犯罪的公司，这 7 家公司涉嫌非法缓存公民个人信息 1 亿多条。其中，考拉征信因涉嫌非法提供身份证返照查询 9800 多万次，获利 3800 万元而“榜上有名”。警方目前已将考拉征信法定代表人、董事长、销售、技术等 20 余名涉案人员抓获。

据悉，广州诺涵信息科技有限公司将公民个人信息称为“流量”，该公司自己开发有“乐花管家”等多个小贷平台，在自身购买公民个人信息用于推销贷款、软暴力催收的同时，也和其他公司相互交换公民个人信息。警方侦查发现，诺涵科技的公民个人信息主要来自于湖南九象信息有限公司，湖南九象黑爬虫网站的“身份核验返照”业务端口则来自北京黑格科技有限公司，而黑格科技是从考拉征信等 4 家公司购买的查询接口。

经查，考拉征信从上游公司获取接口后，又违规将查询接口卖出，并非法缓存公民个人身份信息，供下游公司查询牟利，从而造成公民身份信息包括身份证照片的大量泄露。

考拉征信是央行批准的 8 家个人征信业务试点企业之一，是百行征信 9 家发起股东及董事单位之一，也是国内首家成立大数据征信模型专业实验室的征信机构，主要从事个人和小微企业信用状况评估业务。考拉征信被查也牵出了个人信息泄露这一黑色产业链。

11 月 21 日，记者来到考拉征信官网披露的注册地址，发现该地址与拉卡拉公司地址重合。大楼前台人员表示，考拉征信并不在此办公，整栋楼都属于拉卡拉。

从股权关系看，考拉征信由考拉昆仑全资控股，而后者的最大股东为拉卡拉，持股比例为 32.40%。不过，拉卡拉 11 月 21 日在深交所发布公告称，考拉征信涉及的相关案件正在侦办中，考拉征信正在配合司法机关的工作，目前确有人员处于取保候审阶段。拉卡拉同时澄清，该公司不能控制考拉昆仑董事会，亦不能控制、实际支配考拉昆仑全资子公司考拉征信。公司不存在利用个人信息违规开展业务活动的情况。

如此海量的个人信息被泄露暴露出怎样的制度漏洞？业内观察人士认为，转卖查询接口、非法缓存个人信息，这体现出部分从业机构的合规意识不强、部分从业人员法律意识淡漠，建议相关监管部门加大打击力度。

今年以来监管部门加快了对于用户个人信息保护机制的完善，加大了对大数据非法业务的打击力度。10月22日，央行紧急调研银行与大数据公司合作情况，排查的主要内容涉及数据采集、信用欺诈、信用评分、风控建模等，另外，央行还要求上报第三方公司的名称、股东背景、是否涉及爬虫等内容。⁷

2. 麦子金服办公室突遭查封，创始人黄大容等高管接受警方调查

作为上海较为知名的 P2P 平台，麦子金服办公室突然被警方查封，引起业内不小的震动。

原来，11月24日晚间，麦子金服一位高管在内部群发布一则通知：“目前麦子金服的高管包括黄总（注：黄大容），正在接受警方的调查，并且调查期间职场进行封闭。我会配合警方展开后续的一系列工作。明天起请同事暂时在家里办公，需要协调的同事，我会单独沟通。”

11月25日下午，21世纪经济报道记者来到上海市公安局浦东分局经侦支队，询问麦子金服情况，一位工作人员表示：“公安介入调查，平台处于涉案状态。投资者可以报案，递交相关材料，包括投资合同、身份证及银行卡复印件、银行流水、投资及已兑付情况等。”

麦子金服官网显示，麦子金服运营主体是上海诺诺镑客金融信息服务有限公司，自2009年开始提供网络借贷信息中介服务，目前已拥有1100万余个人及机构注册用户，目前麦子金服拥有约300余名员工。截至2019年8月31日，麦子金服借贷余额（指截至统计时点，经麦子金服撮合完成且尚未偿还的借款本金总金额，不包括利息部分）约24.38亿元。

此前，麦子金服负面舆情缠身。比如，2017年4月，麦子金服宣布获得招商银行系B轮融资，很快就被“打脸”，招商银行随即发布澄清声明称，招商银行及附属公司从未参与麦子金服融资，招商银行对以我行名义做不实宣传的行为保留追

⁷ 同花顺财经。

究法律责任的权利。

后来，麦子金服曾想反向收购纳斯达克上市公司鲈乡小贷，实现曲线上市，2017 年末，麦子金服和鲈乡小贷的矛盾突然公开化，2018 年初，收购计划宣告失败，详见 21 世纪经济报道《麦子金服反向收购鲈乡小贷失利：20 亿投资骗局隐现搅局》一文。

在网贷行业退出的大背景下，今年 10 月 16 日，麦子金服 CEO 黄大容在用户直播会上宣布，为了积极响应和配合监管“三降”要求，麦子金服暂停发布新标，出借人按照原借款协议正常回收对应债权。麦子金服将协助出借人将手中的债权转让给资管公司，通过合并债权后向法院起诉帮助出借人回款。⁸

3. 全国大清剿：北京警方抓捕数十名区块链平台负责人

虚拟货币死灰复燃的苗头已被监管部门高度关注。有权威数据显示，2019 年以来，全国共关闭境内新发现的虚拟货币交易平台 6 家，分 7 批技术处置了境外虚拟货币交易平台 203 家；通过两家大的非银行支付机构，关闭支付账户将近万个；微信平台方面，关闭宣传营销小程序和公众号接近 300 个。

目前，警方也开始介入相关案件。有业内人士透露，杭州、北京已经先后“端掉”虚拟货币交易所，目前进入起诉程序的已有 100 多人。有接近监管部门的人士透露，近日北京警方一举破获非法数字货币交易所 BISS 的诈骗案，抓捕犯罪嫌疑人数十人，有力震慑了不法机构，为广大投资人敲响警钟。

11 月 22 日，有接近国家互联网金融风险专项整治领导小组办公室（下称整治办）人士表示，区块链的内涵很丰富，并不等于虚拟货币。目前所有打着区块链旗号关于虚拟货币的推广宣传活动都是违法违规的。监管部门对于虚拟货币炒作和虚拟货币交易场所的打击态度没有丝毫改变。

据了解，目前监管部门已经通盘部署，要求全国各地全面排查属地借助区块链开展虚拟货币炒作活动的最新情况，出现问题及时打早打小。在下一阶段的工作中，监管部门将加大清理整顿虚拟货币及交易场所的力度，发现一起、处置一起。

⁸ 新浪财经。

（1）境内组织虚拟货币交易死灰复燃

早在 2017 年 9 月 4 日，七部门发布《关于防范代币发行融资风险的公告》，对 ICO 和虚拟货币交易场所进行清理整顿，明确向投资者筹集虚拟货币，涉嫌非法发售代币票券、非法发行证券，以及非法集资、金融诈骗、传销等违法犯罪活动。境内虚拟货币交易规模大幅下降，有效避免了虚拟货币价格暴涨暴跌对我国金融市场的冲击。

此后，针对在境外架设服务器向境内居民提供虚拟货币交易服务的行为，进一步加强监管，并从支付结算端入手持续加强清理整顿。

但是近期蹭着区块链的热度，虚拟货币有卷土重来之势，部分非法活动有死灰复燃迹象。一方面，包括比特币在内的虚拟货币价格出现飙升，市场出现类似“《关于防范代币发行融资风险的公告》已经过时”等不当言论；另一方面，有些机构虽然不涉币，但打着区块链的名义搞非法金融活动。

本月 13 日，央行官网也发布公告澄清，目前网传所谓法定数字货币发行，以及个别机构冒用人民银行名义推出“DC/EP”或“DCEP”在资产交易平台上进行交易的行为，可能涉及诈骗和传销，请广大公众提高风险意识，不偏信轻信，防范利益受损。

（2）全国性清理整顿已拉开大幕

最近两天，深圳、上海和北京等地的监管部门已经发出重拳出击非法虚拟货币的号令，全国性清理整顿的大幕已经开启。监管部门同时提醒投资者增强风险防范意识，对上述非法金融活动保持警惕，及时举报相关违法违规线索，谨防上当受骗。

11 月 21 日，深圳市互联网金融风险等专项整治工作领导小组办公室在深圳地方金融监督管理局官网发布一则“关于防范‘虚拟货币’非法活动的风险提示”。提示称，近期借区块链技术的推广宣传，虚拟货币炒作有所抬头，部分非法活动有死灰复燃迹象，根据国家互金整治办相关部署，深圳市互联网金融风险等专项整治工作领导小组办公室将对上述非法活动展开排查取证，一经发现，将按照《关于防范代币发行融资风险的公告》要求严肃处置。

11 月 22 日下午，上海市金融稳定联席会议办公室、人民银行上海总部也表示，要加大监管防控力度，打击虚拟货币交易。下一步，将对辖内虚拟货币业务活动进

行持续监测，一经发现立即处置，防患于未然。同时，两部门提醒广大投资者应注意不要将区块链技术和虚拟货币混同，虚拟货币发行融资与交易存在多重风险，包括虚假资产风险、经营失败风险、投资炒作风险等，投资者应增强风险防范意识，谨防上当受骗。投资者如发现各种形式的虚拟货币业务活动，以及通过部署境外服务器继续面向境内居民开展 ICO 及虚拟货币交易业务的组织或个人，可向监管部门举报，对其中涉嫌违法犯罪的，可向公安机关报案。

当日晚间，北京青年报记者了解到，为防范虚拟货币交易非法金融活动死灰复燃，切实保障广大投资人利益，根据全国互联网金融风险专项整治领导小组办公室工作部署，北京市地方金融监管局、人行营业管理部对以上非法金融活动坚持“露头就打”原则，持续保持监管高压态势，会同中国互联网金融协会、国家互联网应急中心对辖内虚拟货币交易场所等组织全面摸排，一经发现，将按照《关于防范代币发行融资风险的公告》等相关规定严肃处置。

据报道，中国互联网金融协会、应急中心也已开始全网搜排，对发现的新冒头的境内虚拟货币交易场所、ICO 活动，以及境外“出海”的虚拟货币交易平台，进行及时处置。同时，支付机构被要求从支付结算环节加强排查、清理。目前部分地区已经建立技术搜排系统，有些地区的金融办则与应急中心建立实时技术接口，定期由应急中心搜排本地存在问题的网站，及时发现及时处理。

(3) 区块链媒体陆续被封

《每日经济新闻》记者注意到，在去年 8 月份，火币资讯、深链财经、大炮评级、币世界快讯服务等区块链知名自媒体微信公众号曾遭过一次大规模封停。近期，针对区块链乱象，相关监管部门已经多次发文进行整治，整治的范围包括虚拟货币交易场所、冒用人民银行名义发行或推广法定数字货币等。

记者检索“币圈邦德、炒币学堂”微信公众号，已经搜索不到，搜索“币圈邦德”出现两个公众号“币圈邦德 1”和“币圈邦德服务号”。其中，“币圈邦德 1”显示“大号被封，此号为备用号”，今日早间已发布一条关于区块链的文章。

早在去年 8 月份，微信已经进行了一次大规模“封杀”，一批区块链知名自媒体被封停。彼时，腾讯方面对外表示，部分公众号涉嫌发布 ICO 和虚拟货币交易炒作信息，违反《即时通讯工具公众信息服务发展管理暂行规定》，已被责令屏蔽所

有内容，账号被永久封停。⁹

4. 4.68 亿个人信息泄露：2 块钱就可以查你的身份证

据央视网报道，近日江苏淮安警方依法打击了 7 家涉嫌侵犯公民个人信息犯罪的公司，涉嫌非法缓存公民个人信息 1 亿多条。

“截至目前，警方共立案侦查侵犯公民个人信息案件 29 起，抓获犯罪嫌疑人 288 人，缴获公民个人信息 4.68 亿多条，涉案金额 9400 多万元。”

数据到底是怎样被泄露的？

2018 年 4 月，江苏淮安警方在网上巡查时发现，有人非法购买公民个人信息，高某觉察到警方调查之后，主动到警方投案。

警方经过层层调查得知：高某贩卖数据给公司做营销，他的数据是从申某进行购买的；申某的数据是从谢某购买来的；泄密的数据又是从一个叫做“叮咚叮咚”的用户处购买；“叮咚叮咚”其实是广州诺涵科技公司的员工，他卖数据是为了给公司做业务；广州诺涵科技公司的数据来源有网上非法爬取、同行交换、上游公司购买；广州诺涵科技公司的购买数据来自湖南九象公司；湖南九象公司的数据又是从北京黑格科技公司购买的；北京黑格科技公司又是从北京考拉征信等四个公司购买的。

即本来公安部给北京考拉征信等有资质的公司因为业务需要而开的权限，结果这些公司毫无顾忌的将这些数据经过层层加价又毫无限制的对外出售而转辗到了个人的手上。价格也从最初的 0.1 元/条的查询到了最后的 2 元/条。整个链条经过 8 层倒卖层层加价贩卖个人信息。

非法获取数据都干了什么？

本来公民身份认证服务是直接服务于“互联网+政务”，用来提升政府公共服务

⁹ 腾讯网。

效能，防范欺诈和金融风险的。

现在层层加价后，这些数据被小贷公司利用，查询价格从源头的 0.1 元/条到查询底层时可能两三元/条，整整翻了二三十倍。身份证照片可以随意获取，这为小贷公实施“套路贷”犯罪、暴力催收敞开了罪恶之门。催收公司把这些非法获取的公民身份证照片 PS 成灵堂照片或者淫秽色情的照片发给贷款人本人，对其进行威胁。如果贷款人还不还款，PS 照片就会被小贷公司发给贷款人的亲友、同事、同学，毁坏贷款人声誉，逼迫其还款。还有就是被用于电信诈骗犯罪中的通缉令诈骗。

¹⁰

5. 骗取个人信息盗刷银行卡 “携号转网”这些骗局要小心

近日，联通、移动、电信三大运营商发布了携号转网的细则，大家期待已久的携号转网终于变成了现实。不过，骗子也用上了新招数。目前，全国已发生多起利用手机三大运营商携号转网服务实行诈骗的案件，受害者因点开诈骗分子发送的网站链接泄露个人信息银行卡被盗刷。为防止更多人上当受骗，公安部刑侦局发布紧急预警。

此外，针对电信企业，工业和信息化部日前发出通知，将组织技术力量开展对电信企业携号转网系统连续监测，并委托第三方开展用户暗访体验监测。

（1）骗局多为获取个人信息盗刷银行卡

为防止更多人上当受骗，近日，公安部刑事侦查局官方微博发布紧急预警，让大家提防诈骗分子利用携号转网服务进行诈骗。

此类诈骗作案手段为通过电话或短信方式联系受害人，利用受害人不清楚转网具体规则欺骗事主，声称转网可能带来诸多风险，进而引导其进入网站完善信息，事主进入网站后按引导填写身份证、银行卡、手机号等信息，因泄露个人信息导致银行卡被盗刷。

是否满足携号转网条件以官方短信为准。满足条件的，如有携号转网后受影响的其他业务，运营商将在反馈查询结果的同时告知用户受影响的业务，告知内容真

¹⁰ 新浪创世纪公众号。

实准确。用户向携出方申请获得授权码，带着身份证和有效期内的授权码到携入方申请办理携入。不满足条件的，将一次性明确告知用户不满足条件的原因、携号转网后受影响的业务以及咨询途径，并通过客服电话等方式为用户提供实现满足条件的咨询。

骗局 1

江西市民汪某接到自称某通讯商客服电话，称之前提交的电话号携转资格已经通过，但是想要获取携转授权码需要填写完整信息且绑定专属银行卡，事主通过对方发来的短信进入网站输入个人信息被骗 16000 元。

骗局 2

上海市民何某在上网时知悉携号转网后只能通过掌上营业厅和地面营业厅充值，不能使用支付宝和微信支付了，便在该条新闻下留言追问解决办法，后收到私信，对方称可以通过完善信息解决，事主点击对方的网站链接输入个人信息，损失了 6300 元。

骗局 3

常州市民许某收到陌生号码短信称，更换运营商后短信通道变更可能导致收不到银行卡、微信、支付宝等发送的短信，请及时登录附带链接的网址进行信息完善，许某进入网站输入身份证、银行卡号及密码、手机号码等个人信息，银行卡短时间内被刷走了 5000 元。

(2) 工信部将进行暗访监测

全国携号转网将正式提供服务。工业和信息化部日前发出通知，将组织技术力量开展对电信企业携号转网系统连续监测，并委托第三方开展用户暗访体验监测。正式提供服务后，工信部将组织对全国携号转网服务进行专项监督检查。

此前，工业和信息化部发布了《携号转网服务管理规定》，明确在携号转网服务中，电信业务经营者不得有妨碍服务、干扰用户选择、阻挠携转、降低通信服务质量、比较宣传、虚假宣传等 9 类违规行为。

根据中国信息通信研究院的预测，在当前携号转网的条件下，携号转网在全国实施后，预计年携转率将在 0.3%至 0.5%之间。随着用户认知的提升和各类携号转网问题的解决，预计携转率有可能进一步上升。从其他市场的经验看，高竞争强度的我国香港地区年携转率在 3.9%，我国台湾地区年携转率在 10%。

中国信息通信研究院产业与规划研究所战略研究部管理咨询师焦宗双认为，携号转网政策试点实行 8 年来，运营商内部的技术问题基本得到解决，已经形成相对成熟的方案。目前，最主要的问题是非电信运营企业（主要是互联网企业、金融企业）对携转号码的识别问题，具体包括第三方号码充值、验证码发送等问题。这些问题产生的原因是，很多非电信运营企业在识别手机号码时，采用的是固定号段识别方式，即在编程设计时将固定号段范围内号码设定为特定运营商号码，因而当某个号码转换运营商时该企业的系统不能及时调整和识别。这些非电信运营企业的系统在执行号码充值、验证码发送等服务时，仍然与原运营商的系统端口进行对接，造成相应业务的失败。

目前，中国信息通信研究院正牵头推动该问题的解决。一是牵头成立联盟，通过行业自律和政策引导的方式，要求非电信运营企业解除号段和电信运营企业之间的绑定关系，并能根据号码携带数据或者其他信息判断用户当前签约的运营企业；二是搭建了“号码标记服务平台”，帮助有此类困扰的企业解决号码识别和归属运营商更正的问题。¹¹

6. 租房中介成个人信息泄露“重灾区”

市场监管总局执法稽查局局长杨红灿透露，当前侵害消费者个人信息违法行为主要高发在房产租售、装饰装修、教育培训等三个领域。

值得注意的是，房产租售行业案件数量和涉案信息数量均列首位。例如，浙江某地产有限公司在收集到某小区业主姓名、房号、联系电话等个人信息后，未妥善保管，导致业主个人信息被其员工获取，以 1200 元的价格非法出售给他人获利，造成小区业主个人信息泄露。

2019 年 3 月，市场监管总局印发了《关于开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动的通知》，决定自 4 月 1 日至 9 月 30 日，针对房产租售、小贷金融、教育培训、保险经纪、美容健身、装饰装修、旅游住宿、快递、

¹¹ 环球网。

电话营销、网站或 APP 运营等侵害消费者个人信息违法问题突出的行业和领域开展专项执法行动。

“消费者权益保护法明确规定，消费者个人信息依法受到保护。”杨红灿说，专项行动重点打击未经消费者同意，收集、使用消费者个人信息；泄露、出售或者非法向他人提供所收集的消费者个人信息；未经消费者同意或者请求，或者消费者明确表示拒绝的，向其发送商业性信息等违法行为。

据统计，行动期间，全国市场监管部门共立案查办各类侵害消费者个人信息案件 1474 件，查获涉案信息 369.2 万条，罚没款 1946.4 万元，移送公安机关案件 154 件；组织执法联动 4225 次；开展行政约谈 3536 次；开展宣传活动 10653 次。¹²

7. 1600 多名酒店房客被非法偷拍，黑色产业链被挖出

近日，公安部网安局通报了一起非法生产、销售、使用联网型针孔摄像头大案。这种针孔摄像头利用配套的手机 App 等客户端，通过互联网远程控制摄像头，偷拍偷窥侵犯他人隐私。这次案件中涉及到的针孔摄像头非常难辨识。这究竟是什么样的设备呢？

浙江省公安机关在“净网 2019”专项行动中，针对非法生产、销售、使用联网型针孔摄像头的相关线索深挖经营，成功查明了一起从设计制作专用芯片、搭建远程控制平台，到加工组装伪装配件，并线上线下同步销售针孔摄像头的非法制售利益链条。

在侦查过程中，警方发现，制成的微型摄像头大多安装在像路由器、时钟、水杯这些商品内，原本几十元的普通商品立马升值成几百元的偷拍工具，再经各批发商代理，通过微信、网商平台等渠道对外销售。

浙江省杭州市公安局拱墅分局网警大队民警汤扬说：“这个是我们查获的一个偷拍装置，就是用路由器伪装的一个摄像头。这个路由器本身是嫌疑对象通过正常的渠道购买的，而且它具有路由器的功能。嫌疑人通过改装之后，把摄像头的一些配件放进去以后，就改装成了一个可以偷拍的路由器。这个是我们通过操作测试，才知道摄像头是在这个位置。从表面上来看，其实是完全看不出来摄像头放在哪个

¹² 经济日报。

位置。”

原来，嫌疑人在路由器上打孔安装了摄像头后，还特意在这个孔洞上方标注了字母 T 伪装成某种指示灯，非专业人士根本不会注意到这个多出来的小孔后却隐藏着偷窥的眼睛。

除了无线路由器和时钟，常被改造伪装的日常用品还有烟雾报警器、电源开关插座等屋内常备装置。此外，便携手持的常用设备，如充电宝、手表、打火机，甚至饮水杯，也常被改造成偷拍工具。

此次净网专项行动，浙江省公安部门历经 2 个月的侦查追捕，现已抓获并刑拘非法生产、销售窃照专用器材犯罪人员 26 名，查扣针孔摄像头成品及半成品 5000 多个。

从这些改造伪装的偷拍工具不难发现，利用这一类最常见、不起眼的日常物品进行改装就是不想被发现。那么这些伪装后的偷窥偷拍设备都被安装在哪里，又是被用来做什么呢？

浙江警方打掉这个制售针孔摄像头团伙后，立即在各地开展循线追踪。最终查明安装使用针孔摄像头的场所 245 个，查处非法安装使用针孔摄像头点位 196 个，查扣摄像头 179 个。

浙江省杭州市公安局网警分局三大队民警展福利谈到：“我们发现下游使用针孔摄像头的首先安装位置，包括家庭、宾馆以及隐私场所，甚至是办公场所都有存在。其安装意图也是不一样的，有的是为了偷窥他人隐私，还有的是为了传播淫秽物品的，甚至有组织卖淫的，还有组织考试作弊的，下游的犯罪是比较多的。”

据警方查实，杭州某男子在对外出租的房屋内安装针孔摄像头，长期窥探租客的生活隐私。福州某男子借住宿之机，先后在 28 家宾馆偷偷安装摄像头，偷拍录制了其他住宿客人多达 180G 的隐私视频。宁波一男子使用伪装在球鞋上的针孔摄像头，在车站、商场等公共场所用于偷拍女性裙底，共累计偷拍视频 90 多部，并准备将这些视频上传网络牟利。

浙江省杭州市公安局网警分局三大队民警展福利：“非法使用针孔摄像头，造成严重后果的，比如造成一个社会影响比较恶劣，引起一个社会舆情，那么是可以依法追究刑事责任的。”

浙江警方通过追踪针孔摄像头非法使用者，目前已治安拘留偷窥他人隐私人员 20 名，发现其他违法犯罪线索 13 条，治安拘留卖淫嫖娼等违法人员 25 名。

韩国：偷拍猖獗 视频供色情网站直播

近年来，韩国也是曝出多起隐形摄像头偷拍案件，而且令人防不胜防。因为这些隐形摄像头有可能放置在酒店、商店、餐厅，甚至洗手间，无处不在的暗洞令人防不胜防，更有犯罪团伙将偷拍视频上传到付费色情网站供人浏览，触目惊心。

“你的模样，正在外国色情网站上被直播！”这不是夸张，而是真实发生在韩国的偷拍案件。就在今年的三月份，韩国警方抓获了一个犯罪团伙，他们涉嫌在韩国 10 个城市的 30 家酒店里安装了 1 毫米超微型摄像头，对 1600 多名房客进行非法偷拍，并在海外色情网站上直播获取暴利。

韩国警察厅网络恐怖主义侦查队队长郑硕华：“我们发现多个地区的酒店客房内，装有大量针孔摄像头，偷拍的视频被用于商业网站。”

犯罪团伙利用摄像头对入住的房客进行偷拍，并在海外网站上在线直播，仅 6 个月内就非法拍摄了 800 多个视频，超过 800 对韩国伴侣在宾馆中生活的场景都被在线播放，而这些受害者大多完全不知情，这一度引发韩国民众的恐慌。

偷拍行为在韩国到底有多猖獗呢？韩国媒体记者走访了首尔市内的餐厅、咖啡厅、地铁、公共学习场所、公园、商店等地，用照片揭露了无处不在的暗洞。

受害人：“听到有冲水的声音，之后好像有快门的声音，但也一直没有人出来。我对其他人讲‘好像有什么不对’，结果门开了，一个男子就逃跑了。”

面对非法偷拍，女性究竟该如何保护自己呢？韩国 SBS 电视台还特别介绍了如何发现隐蔽摄像头的绝招。

韩国 SBS 电视台主持人：警方公开了发现隐蔽摄像头的方法，非常简便。只需要准备小时候玩的红色玻璃纸，用红色玻璃纸同时遮住手机镜头和闪光灯，在闪光灯开启的状态下给可疑的地方拍摄视频，如果发现发光发亮的物体，那就是针孔

摄像头，原理是它会在相机红光的照射下发生反射。¹³

8. 个人信息被抢注？银行推广 ETC 催生灰色产业链

如果评选今年的热词，ETC 入榜大概是毫无悬念的。

按照相关政策要求，到 2019 年底，各省（区、市）汽车 ETC 安装率要达到 80% 以上；而到 2020 年 12 月底前，要基本实现全国机场、火车站、客运站、港口码头等大型交通场站停车场景 ETC 服务全覆盖。

在政策要求与市场潜力的双重作用下，今年下半年以来，各家银行纷纷入局，层层下达任务指标，大力布局 ETC 业务。

然而，近期各地频频被爆出一些车主的车牌或个人信息被抢注 ETC 的事件。银行 ETC 营销大战背后的 ETC 代理产业链就此浮出水面。

按照政策要求，2020 年节假日无 ETC 的车辆过收费站将不再享受免费通行。不少没有安装 ETC 的车主开始主动去注册，然而当他们来到银行办理时才发现，自己竟然早已注册了 ETC。

据报道，河北省一些地方上的多名货车车主就遇到了上述情况。他们名下的车辆在未知情下，已被某大行抢先注册了，也从未收到过相关的 ETC 设备！如果他们想要继续办理，则还需要车主本人自己带着身份证到银行解绑。

车主们不禁疑惑：此前从未办理过 ETC，银行是如何获取个人身份信息的？背后产业链浮出。

今年 5 月份以来，无论是在“朋友圈”还是在停车场，只要有汽车在的地方，总能看到银行 ETC 的广告或银行员工忙碌推销的身影。

由于各家银行的基层员工都背负了巨量营销 ETC 的考核指标，为了完成任务，银行员工使出浑身解数去拉 ETC 客户。然而即使“攻陷”了亲朋好友、站岗了停车

¹³ 央视财经。

场和高速路口，离下达的考核指标仍有距离。

不过，各家银行跑马圈地争抢 ETC 客户，相应催生了 ETC 代理这一中介产业链，后者代理各大银行的 ETC 推广任务，帮助银行完成营销任务，并获取佣金。

“承接各大银行 ETC 任务”“日产 500 单、包数据”“只接银行一手单、专业地推团队”“欢迎有实力的银行老板来对接”……在咸鱼平台搜索“ETC 代理”等关键词，即可出现各种“花式”的代理中介。

一些 ETC 代理主要为“地推”模式。毕竟银行基层员工人数有限，这些代办中介自己招募推广员，依赖人力大战，在各个场所获取客户。

而在代理行业其中，潜藏着倒卖个人信息的灰色地带。目前，各平台 ETC 办理流程只需要填写身份证和行驶证相关信息，也可以拿着他人身份信息和复印件到网点“帮助”别人办理。这给一些倒卖个人信息的中介可乘之机。

据了解，一些代理商利用当前 ETC 注册程序漏洞，售卖车主个人信息，其中就包括利用车辆报废的时间差，贩卖原车主信息，将车牌号绑定注册 ETC。

目前，个人信息隐私数据被滥用，成为互联网时代必须面对的问题。面对个人信息被私下使用，车主发现后要及时向有关渠道反映，以保护自己的个人隐私。

值得注意的是，与个人隐私保护相关的法律正在不断完善，今年 8 月份，全国人大常委会法工委发言人对外表示，个人信息保护法已列入本届全国人大常委会立法规划。目前，法工委正在会同有关部门研究论证，加紧推进起草工作，将按照立法工作计划，适时提请常委会审议。¹⁴

9. 库克重申不获取用户数据 苹果出台多项保护隐私举措

11 月 24 日，据外媒报道称，苹果 CEO 库克最新接受采访时重申，苹果公司不会获取用户数据，更不会拿用户数据赚钱。

¹⁴ 中国证券网。

库克表示，大家对大公司都保持质疑的态度，但他认为隐私是最重要的事情。苹果公司不会获取用户的数据，用户的信息就该保存在用户的设备上，在用户和用户的手机之间，而不是用户和苹果公司之间。

库克重申：“我们不会太看重数据中心的物理位置在哪里，我们的服务器位于世界上许多不同的国家。每个国家的数据保密措施都是一样严格的，不存在从一个国家的数据中心窃取数据比从其他国家的数据中心更简单的这种情况。”

库克称：“将利润放在隐私之前的想法并不是什么新鲜事，我们不应美化这样的做法（拿用户隐私来改善服务当借口），这其实是一种监视，并且这些个人数据库只会让收集它们的公司数据更加丰富，对于苹果来说是不需要用户隐私数据来改善服务的。”

11月6日，苹果公司对其官网上的隐私说明页面进行了全球更新，针对有些APP不当收集用户信息、侵犯用户权益的做法，苹果升级了自己的解决方案：对App获取用户信息的权限控制进一步加强，同时也对自己的软件在隐私保护上做了升级。Safari浏览器新推出了智能防跟踪功能，阻止广告商跨网站对用户进行跟踪。但Siri不会与用户身份关联，用户可自主选择是否保留录音内容用于改进算法。

库克表示，苹果的看法与某些公司不同，他们把隐私视作一项基本人权，而不会利用用户数据赚钱。

最后，库克补充说：“从个人角度来看非常担心，这个世界没有任何隐私。如果你知道你的隐私被公司长时间监控，你就会开始少表现，比如开始控制自己的行为，减少浏览，减少探索等。那不是我想生活的世界，也不是想让孩子生活的世界。”

此前，库克也曾对媒体表示，苹果有责任去保护苹果用户的个人数据和隐私的，比如之前他们回绝了FBI（美国联邦调查局）要求其解锁iPhone的请求。¹⁵

10.谷歌将限制与广告商的数据共享 以保护用户隐私

11月15日消息，据国外媒体报道，美国时间周四，谷歌母公司Alphabet在一

¹⁵ 36氪。

篇博客文章中宣布,从 2020 年 2 月开始,在谷歌发送给广告买家的投标邀请书中,将不再包含广告出现的语境的内容类别的信息。

内容类别是对特定页面、网站或应用上的内容类型的描述。例如,这些类别可以说明内容是否与新闻或天气有关,目的是为广告商提供可能出现其广告的网站或应用的语境信息。它们可以帮助广告商避免在不适合其品牌的某些类型的内容上显示广告,或者帮助广告商识别他们确实想要投放广告的内容类型。

这种精确瞄准是谷歌能够吸收大量在线广告的主要原因,这些在线广告通过机器进行买和卖,即所谓的程序化广告。谷歌一直不向外界透露其来自网络展示广告业务的营收数据,但经常将程序化广告业务作为其收入增长的关键驱动力。

不过,谷歌一直因其处理个性化在线广告数据的方式而受到批评。

今年 5 月,针对谷歌如何在广告交易中处理用户数据,爱尔兰数据保护监管机构展开了调查。这家监管机构正试图确定谷歌的做法是否符合欧盟严格的用户隐私保护法,这些法律要求很高的透明度和尽量减少数据收集。

谷歌不再提供广告出现的语境的内容类别信息,是为了防止某些广告商将用户资料与敏感内容类别联系起来。目前还不清楚谷歌的某些广告客户过去是否能够建立这样的联系,或者他们现在是否能够这样做。

谷歌表示,它是在“与数据保护机构接触”后做出这一改变的,并将继续与“调查其广告业务中数据保护行为”的机构合作。谷歌负责用户信任和隐私的高级产品经理切特纳·宾德拉(Chetna Bindra)在文章中还表示,公司将更新针对出版商、广告商和授权买家的《欧盟地区用户意见征求政策》(EU User Consent Policy)的审核程序。

这位高管还解释称,谷歌的实时竞价(RTB)平台,即出版商出售广告的地方,已经有了“强有力的措施”来保护隐私。出版商需要获得用户的同意才能向他们展示个性化的内容。与此同时,谷歌使用的数据最小化实践应该会阻止标识用户的作法,“包括截断设备 IP 地址并只使用可重新设置的用户 ID”。

一些人认为,这只是谷歌在加强隐私保护上走出的一小步。

美国广告拦截浏览器公司 Brave Software Inc 首席政策官约翰尼·瑞恩(Johnny

Ryan)指出：“谷歌仍将‘招标邀请书’发送给无数公司，而其中包含你正在观看、阅读或收听的内容的细节。这些邀请书将包括关于你的位置信息，以及其它足够的数据，以便在一段时间内将事情联系起来。”

此前，Brave Software Inc 曾就谷歌的广告拍卖技术向欧洲数据保护当局提起法律诉讼。¹⁶

11. 12 亿个人信息泄露，谷歌云服务器上发现庞大的未受保护数据库

10 月，一个汇总了 12 亿用户个人信息的数据库被发现毫无保护的存在于某个服务器上，这些个人信息中包括社交媒体帐户、电子邮件地址和电话号码。到目前为止还不清楚该数据库出现在这个服务器上的原因。

总部在圣路易斯的 Night Lion Security 的首席执行官 Vinny Troia 表示，数据库中的大多数数据是由一家名为人员数据实验室(People Data Labs)的公司收集的。人员数据实验室自称可以提供多达 15 亿人的工作电子邮件和社交媒体帐户详细信息。该公司的网站称，数据通过多种来源获得，购买数据的用户可以据此来接触“美国、英国和加拿大超过 70%的决策者”。

Troia 说，未受保护的数据并非是存放在人员数据实验室的服务器上，而是出现在一个谷歌云服务器上。谷歌没有回应谁在租用该服务器的问题。

人员数据实验室的联合创始人兼首席执行官 Sean Thorne 表示，只有一部分数据来自他的公司，他怀疑这些数据是由另一家公司汇总收集的。

Troia 在 10 月份在例行扫描未受保护的数据时发现了这个数据库，并向联邦调查局报告了这个 4 TB 数据库及其位置。他说，此后服务器已关闭。联邦调查局没有立即回应置评请求。¹⁷

¹⁶ 网易科技。

¹⁷ 腾讯证券。

12. Elasticsearch 服务器泄露 12 亿个人数据

近日，研究人员鲍勃·迪亚琴科（ Bob Diachenko ）和文尼·特罗亚（ Vinny Troia ）发现了一个“宝箱”。原来，这是一个 Elasticsearch 服务器，其中包含 12 亿用户账户，该服务器被公开在暗网上，任何人都可以“到此一游”。

数据来自何方？

研究人员分析，当人们通过 BinaryEdge 和 Shodan 寻找公开信息时，偶然发现服务器的 IP 地址可以追溯到 Google Cloud Services 。总体而言，该数据库存储着超过 4 TB 的公开数据供公众访问。

作为全文检索搜索引擎的核心技术， Elasticsearch 作为基于 Lucene 库的搜索引擎而存在，其被应用于企业信息网站、媒体网站、政府站点、商业网站、数字图书馆和搜索引擎中。

查看研究人员分享的详细信息后发现，该数据是从社交媒体平台（包括 Twitter ， Facebook ， LinkedIn 和 GitHub ）中抓取，而该平台同样为 Git （一个开源的分布式版本控制系统）的存储库执行托管服务。

这些数据在服务器中被分类成四个不同的数据集，其中三个被标记为“ People Data Labs ”的数据代理，而另一个则被标记为“ OxyData ”的数据代理。

Troia 称，他在 People Data Labs （ PDL ）中发现了自己 10 年前在 AT&T 公司办理的一个固话号码。这个号码他从未使用过，但是当时录入的信息却被保留在了这里。

经研究发现，在该服务器中包含了近 30 亿 PDL 用户记录，近 12 亿唯一人员和 6.5 亿唯一电子邮件地址。这些数据数量不光与 PDL 公司的宣传相符，甚至研究人员还可以通过 PDL API 返回的信息来反向查询这些数据。

另外，研究人员通过将数据库和上述两家公司的公开数据进行比对，发现至少在一定程度上源自它们。研究人员在博客文章中专门针对 PDL 的措辞进行了详细说明：“在打开的 Elasticsearch 服务器上发现的数据几乎与 People Data Labs API 返回的数据完全匹配。唯一的区别是 PDL 返回的数据还包含教育历史记录。从服

务器下载的任何数据中都没有教育信息。其他所有内容都完全相同，包括具有多个电子邮件地址和多个电话号码的帐户。”

但是，PDL 联合创始人 Sean Thorne 否认公司拥有该服务器的说法，并称，该服务器的所有者可能使用了 PDL 提供的一种扩充产品，以及其他数据扩充或许可性服务。

另一方面，4TB 用户数据（包括 3.8 亿个配置文件）被证实来自 OxyData 公司，但是该公司同样回应称并没有服务器的所有权。

截止目前，研究人员并不能确定是谁将服务器公开在互联网上，但信息泄露意味着将会影响到两家公司的共同客户，并使其面临数据滥用的风险。

除了这次事件，Elasticsearch 服务器曾多次被向公众公开，这同样将毫无戒心的用户和企业的个人数据置于风险之中：“今年早些时候，Elasticsearch 服务器上公开了超过 2000 万俄罗斯公民的个人信息。今年 5 月，在 Freedom Mobile 拥有的 Elasticsearch 数据库在线泄漏后，具有数百万加拿大人 CVV 码的个人和支付卡数据再次暴露。去年 12 月，另一个包含 8200 万美国人个人信息的数据库在网上暴露了出来。”

Elasticsearch 服务器有关的数据泄漏事件屡屡出现，也吸引了大量攻击者的目光，因为这可能成为其攻击行动的切入点。

Cequence Security 公司的一名黑客 Jason Kent 评论称，“我们看到一种不同于以往的全新且具有潜在危险的数据关联。如果攻击者持有丰富的数据集，那么就能够制作针对性极高的攻击。这种攻击可导致密码恢复信息、财务数据、通信模式、社会结构等被暴露，这是高级别在位人员可遭针对性攻击的方式。

两名研究员将这一发现上报了联邦调查局，尽管通常情况下几个小时内 Elasticsearch 服务器即可完成数据脱机操作。但是，后者在收到消息后并未给出明确回复。

ARM Insight 首席执行官 Randy Koch 分析，此次大规模数据泄露事件对那些被看成持有数据所有权的企业来说造成巨大破坏，同时也会造成数十亿人的信息外泄到世界各地。

所包含的个人数据如此庞大，加上识别数据所有者很复杂，因此有可能会引发我们现行隐私和数据泄露通知法律有效性的问题。

如果具有数据掌控权的公司将其用户信息收集并进行集中合成，则可以有效预防此事件，因为数据合成的过程在模仿真实数据的同时消除了用户的可识别特征。

正确合成后，它就不能被黑客进行逆向工程，并同时保留了原始数据集的所有统计价值，因此它仍然可以用于分析、市场营销、客户细分和 AI 算法训练等等。

但是，集中数据会抵消作为数据掌控企业的名誉，且在隐私、合规性上也颇具风险。¹⁸

13. FB、Twitter 数百用户因登录第三方应用个人信息泄露

Facebook 和 Twitter 11 月 25 日表示，数百名用户的个人数据可能在他们使用自己的账号登录从谷歌 Play 商店下载的某些 Android 应用时泄露。

Facebook 和 Twitter 收到来自安全研究报告称，他们发现名为 One Audience 的软件开发工具包允许第三方开发者访问个人数据，包括使用 Twitter 帐户登录 Giant Square 和 Photofy 等应用的用户电子邮件地址、用户名和最近发布的 Twitter 消息。

Twitter 还表示，这个漏洞可能导致用户的 Twitter 帐户被他人控制。不过目前没有证据表明，已经发生了这样的情况。

Twitter 发言人林赛·麦卡勒姆（Lindsay McCallum）表示：“我们认为，对人们来说，重要的是需要知道问题的存在，以及评估用自己账号去登录的应用。”

Twitter 表示，将向受影响用户发出通知。此外，该公司还通知了谷歌和苹果，以便这些公司可以采取下一步的行动。

¹⁸ 雷锋网。

目前，关于外部开发者利用个人数据跟踪和瞄准平台用户的行为，Facebook、谷歌和 Twitter 都面临监管机构、立法者和用户更严格的审视。自 2018 年 3 月 Facebook 的“剑桥分析”丑闻曝光以来，这个问题一直备受关注。

Facebook 发言人就 11 月 25 日的事件发表了以下声明：“安全研究人员最近通知我们，有两个恶意行为者，分别是 One Audience 和 Mobiburn。他们向开发者付费，让他们在热门应用商店的某些应用中集成恶意的软件开发工具包。经过调查，我们将违反平台政策的应用从我们的平台删除，并向 One Audience 和 Mobiburn 发出禁止令。对于授权这些应用访问自己个人资料，从而导致信息可能泄露的用户，我们计划发出通知。我们同时呼吁人们在给予第三方授权时保持谨慎。”¹⁹

14. 《Magic: The Gathering》开发商证实 安全漏洞使超 45 万玩家数据泄露

据外媒 TechCrunch 报道，游戏《Magic: The Gathering》的开发商 Wizards of the Coast 已经确认，安全漏洞使数十万游戏玩家的数据遭泄露。该游戏开发商将数据库备份文件留在了公共的 Amazon Web Services 存储桶中。但是存储桶上没有密码，任何人都可以访问其中的文件。

据悉，自 9 月初以来，该存储桶就已经遭泄露。但是英国网络安全公司 Fidus Information Security 最近找到数据库并报告了此事。

对数据库文件的检查显示，其中包括有 452634 名玩家的信息，含与 Wizards of the Coast 员工相关的约 470 个电子邮件地址。该数据库包括玩家名称和用户名，电子邮件地址，以及创建帐户的日期和时间。该数据库还具有用户密码，这些密码经过哈希处理，因此很难但并非不可能被解密。没有数据被加密。根据外媒 TechCrunch 对数据的审查，这些帐户的日期至少可以追溯到 2012 年，但是一些最近的条目可以追溯到 2018 年年中。

Fidus 联系 Wizards of the Coast，但没有听到任何回应。直到 TechCrunch 与该公司取得之后，这家游戏制造商才将存储桶脱机。

该公司发言人 Bruce Dugan 在一份声明中对 TechCrunch 表示：“我们了解到，

¹⁹ 新浪科技。

已被停止使用的网站上的数据库文件被无意间从公司外部访问了。”他表示：“我们从服务器上删除了数据库文件，并开始了调查以确定事件的范围。我们认为这是一起孤立事件，我们没有理由相信对数据进行了任何恶意使用，”但是发言人没有提供任何证据证明这一说法。

他表示：“但是，出于谨慎考虑，我们会通知玩家其信息已包含在数据库中，并要求他们在我们当前的系统上重置密码。”

Fidus 研发总监 Harriet Lester 表示：“在当今时代，错误的配置和缺乏基本的安全卫生措施仍然令人感到惊讶，尤其是当涉及到拥有超过 45 万个帐户用户的大型公司时。”“我们的研究团队不断工作，寻找诸如此类的错误配置，以尽快提醒公司，避免数据落入不法分子之手。这是我们帮助互联网更安全的小方法，”她告诉 TechCrunch。

这家游戏机制造商表示，已根据欧洲 GDPR 法规的违规通知规则将有关泄露情况告知了英国数据保护部门。英国信息专员办公室没有立即回应此事。

对于违反 GDPR 的公司，可能会最高被处以相当于其全球年收入 4% 的罚款。

20

15. 美国对“隐私保护”出现分歧 谷歌与微软公开发声

《加州消费者隐私法案》(简称 CCPA)，即将于 2020 年 1 月 1 日生效。该法案旨在加强消费者隐私权和数据安全保护，并被认为是美国国内最严格的隐私立法。

而据外媒报道，CCPA 一直是加州立法机关和国会许多隐私斗争的主题。参议院和众议院都在为他们自己的数据隐私而战，每隔几周就会有新的法案被提出。许多民主党议员认为，任何国家立法都应该以加州为基准，在全国范围内扩大这些保护措施并在必要时增加更多的保护措施。共和党人和行业利益相关者则不同意这一观点，他们普遍认为，CCPA 管得太过，并且任何联邦法律都应该废除它、其他任何一个州的法律都应该避免出现隐私法规的拼凑现象。

最近，以微软和谷歌为代表的高科技公司做出了相应的表态。

微软宣布将尊重加州标志性数据隐私法为加州人提供的“核心权利”并将这一权利扩展到整个美国。微软首席隐私官 Julie Brill 于近日在博文中表示，就像去年推广欧盟《一般数据保护条例(GDPR)》一样，公司将把《加州消费者隐私法(CCPA)》的主要原则推广到美国各地。

在 CCPA 的规定下，公司必须向用户披露其收集的个人资料、资料是否会出售及出售对象，并容户选择不出售个人的资料。另外，用户还必须能够访问自己的数据并能要求公司删除它们。

Brill 写道：“根据 CCPA，公司必须对数据收集和使用透明，并为人们提供防止个人信息被出售的选择。CCPA 完成这些目标的具体要求仍在制定中。微软将密切关注政府要求公司在 CCPA 下执行新透明度和控制要求的任何变化。”

Brill 在博文中表示：“在美国，CCPA 标志着向人们提供对其数据更有力的控制迈出了重要的一步。”，“这也表明，即使国会不能或不愿采取行动，我们也可以在国家层面加强隐私保护上取得进展。”

以广告为核心收入的谷歌则在 2019 一整年都在隐私保护方面有着积极的表现。

尽管有人质疑谷歌的说法，认为这只是其营销策略，但谷歌似乎对这种说法并不在意。并一直宣称对改善其产品的用户数据保护更感兴趣，并宣布了将对其广告业务的运作方式做出重要改变。

在谷歌的广告经理博客上，Chetna Bindra 表示，从 2020 年 2 月开始，谷歌将不再在它发送给广告买家的投标请求中包含语境内容类别。

此举则是为了防止某些广告商将用户资料跟敏感类别联系起来。目前还不清楚部分广告客户过去是否能够建立这样的联系，或他们现在是否还能这样做。

谷歌表示，它是在跟数据保护机构接触之后做出了这一改变的，并将继续跟在授权买家的背景下调查数据保护实践的机构合作。谷歌负责用户信任和隐私的高级产品经理还表示，公司将更新针对出版商、广告商和授权买家的欧盟用户同意政策审计程序。

据悉，谷歌的实时竞价(RTB)平台即出版商出售广告的地方，已经采取了强有力的措施来保护隐私。出版商需要获得用户的同意才能向他们展示个性化内容。与此同时，谷歌使用的数据最小化实践应该会阻止对用户的标识。

值得一提的是，谷歌近日在美国不仅陷入反垄断的大规模调查。同时，谷歌的“南丁格尔计划(Project Nightingale)”被指在患者及医生并不知情的情况下秘密收集了数百万美国人的个人健康数据。报道称，收集的数据包括实验室结果、医生诊断和住院记录等，此外还有患者完整的健康史及姓名、出生日期等其他信息。谷歌计划利用上述数据设计一个软件，该软件能运用人工智能与机器学习技术针对不同的患者制定个性化的护理服务。

谷歌的发言人对此表示：“谷歌严格遵守法律规定”。根据谷歌的说法，Ascension 的医疗数据独立存储在谷歌的云服务器上，仅 Ascension 的员工有权访问这些数据。“所有数据逻辑上为 Ascension 独立存储，保存在使用专用密钥加密的虚拟私有空间内，”谷歌云业务首席执行官托马斯·库里兰表示：“谷歌不会出售、分享 Ascension 的数据，或将这些数据与其他任何数据做整合。”²¹

²¹ 太平洋电脑网。

四、环球评论

1. 《GDPR 第 3 条域外效力指南》（2019 版）全文翻译

欧洲数据保护委员会

考虑到欧洲议会和委员会于 2016 年 4 月 27 日颁布的第 2016/679/EU 号法规第 70 (1)(e) 条中关于处理个人信息时对数据主体权益的保护要求和个人信息自由流动的相关规定，同时为废除 95/46/EC 指令。

制定了下列准则：

引言

《通用数据保护条例》（以下简称“GDPR”或“《条例》”）第三条规定了该条例适用的地域范围，与 95/46/EC 指令所规定的范围相比有了重大变化。在一定程度上，GDPR 确认了欧盟立法者和法院在 95/46/EC 指令中的立场，但也引入了新的考量因素。其中最重要的是，95/46/EC 指令第 4 条的主要目的在于规定哪些成员国的国内法可以适用，而 GDPR 第 3 条直接规定了此条例适用的地域范围。此外，根据 95/46/EC 指令第 4 条的规定，将“非设立在欧盟境内的”经营者纳入欧盟数据保护法适用范围的前提是其使用了位于欧盟领土内的“设备”处理个人信息，但是 GDPR 第 3 条中并未采纳此种说法。

GDPR 第 3 条反映了立法者为欧盟的数据主体提供更全面的法律保护，并在全球数据流动的背景下，为活跃在欧盟市场上的公司在数据保护要求方面建立一个公平竞争环境。

GDPR 第 3 条主要依据两个标准对该法适用的地域范围进行界定：第 3 条第（1）款规定的“实体”标准；以及第 3 条第（2）款规定的“目标指向”标准。符合前述两标准其一的控制者或者处理者对个人数据的相关处理应遵循 GDPR 的有关规定。此外，第 3 条第（3）款规定，如根据国际公法的约定须适用欧盟成员国法律的，应当适用 GDPR。

本指南旨在通过对条例的统一解释，以确保欧盟不同数据保护机构在评估由控制者或处理者进行的特定处理是否属于 GDPR 适用范围时，能够形成一致意见。通过本指南，EDPB 规定并明确了 GDPR 适用地域范围的标准。这种一致性意见对

于欧盟内外的控制者和处理者也是十分重要，以便他们据此评估在某一特定处理活动中是否需要遵守 GDPR。

鉴于未设立在欧盟境内但从事第 3 条（2）款所述处理活动的控制者或处理者需要在欧盟境内指定一名代表人，本指南也将对第 27 条中指定该代表的程序及其责任和义务做出明确说明。

一般而言，EDPB 认为个人数据的处理若属于 GDPR 管辖范围，则应适用 GDPR 的全部规定。但是，本指南将根据数据处理活动的类型、开展数据处理活动的实体类型或该主体的所在地，具体列明 GDPR 在可能发生的各种情形下的适用。因此，数据控制者和处理者，特别是面向全球提供产品和服务的控制者和处理者必须对其处理活动进行仔细且具体的评估，以确定相关的个人数据处理活动是否受 GDPR 的约束。

EDPB 强调，第 3 条的适用旨在确定某一特定的处理行为是否属于 GDPR 规制的范围，而不是某一个人(法人或者自然人)是否属于 GDPR 的规制范围。因此，控制者或处理者对个人数据的某些处理行为可能属于 GDPR 的规制范围，但同一控制者或处理者对个人数据的其他处理行为可能不属于 GDPR 的规制范围。

EDPB 最初于 2018 年 11 月 16 日通过此指南，并于 2018 年 11 月 23 日至 2019 年 1 月 18 日向社会征求意见，并根据收到的意见和反馈进行了更新。

1.“实体”标准的应用-第 3 条第（1）款

GDPR 第 3 条第（1）款规定，“本条例适用于控制者或处理者设立在欧盟境内的实体进行的对个人数据的处理行为，无论其处理行为是否发生在欧盟境内”。

GDPR 第 3 条第（1）款不仅适用于控制者，同时也适用于处理者。因此，处理者对个人数据的处理活动也可能因为其在欧盟境内设有实体而受到欧盟法律的约束。

第 3 条第（1）款保证了 GDPR 对控制者或处理者在其欧盟境内的实体进行的个人数据的处理行为，不论实际发生的处理的所在地为何。因此，EDPB 建议在根据第 3 条第（1）款来确定个人数据的处理是否属于 GDPR 的规制范围时应从三个维度进行评估。

以下各节将阐明“实体标准”的应用：首先应考虑在欧盟数据保护法意义下“实体”的定义；其次应考虑“在欧盟境内的实体营业范围内进行的个人数据处理”的含义；最后确认无论此实体进行的数据处理行为是否发生在欧盟境内，GDPR 都将适用。

1.1“在欧盟境内的实体”

在考虑“在欧盟境内的实体”的含义之前，首先需要确定实施处理活动的数据控制者与数据处理者的身份。根据 GDPR 第 4 条第（7）款规定，数据控制者是“能单独或共同决定个人信息的目的和方式的自然人、法人、公共机构、行政机关或其他非法人组织。”根据 GDPR 第 4 条第（8）款的规定，数据处理者是“为数据控制者处理个人信息的自然人、法人、公共机构、行政机关或其他实体。”根据相关欧洲法院判例和此前第 29 条工作组发布的指南的规定，确定一个实体是否是欧盟数据保护法中界定的数据控制者或处理者是评估相关个人数据处理活动是否适用 GDPR 的关键。

虽然 GDPR 第 4 条第（16）款对“主要实体”进行了定义，但未对第 3 条中“实体”进行定义。但序言第 22 条对“实体”存在如下说明，即“实体”意味着通过稳定的安排有效且真实地开展活动，而该等安排的法律形式（无论是通过分支机构或具有法律人格的子公司）并非判断其是否可以成为实体的决定性因素”。

这一措辞与 95/46/EC 指令的序言第 19 条的措辞相同，并被欧洲法院在多个判决中引用。与企业的实体为其公司注册地的形式主义方法不同，欧洲法院扩大了对“实体”一词的解释。事实上，欧洲法院通过判决将实体的概念延伸到任何通过稳定的安排进行真正有效活动的场所，即便活动量极少。为了确定在设立在欧盟境外的实体在欧盟成员国内是否有实体，必须基于活动和提供服务的特定性质来判断安排的稳定程度和在该成员国从事活动的有效性，特别是在确认专门通过互联网提供服务的企业是否在欧盟境内有实体这一情况。

当数据控制者的活动涉及在线提供服务时，“稳定安排”的门槛实际上可能相当低。因此，在某些情况下，如果该雇员或代理人的行为具有足够的稳定性，则非欧盟实体在欧盟境内拥有一名雇员或代理人可能足以满足“稳定的安排”（符合 GDPR 第 3 条第（1）款规定的“实体”）这一要求。与之相反，如果一名员工在欧盟工作，但数据处理行为并不是此在欧盟境内的员工的活动范围（即该处理活动与欧盟境外控制者的活动范围相关），则该员工在欧盟境内的存在并不会导致该数据处理行为适用 GDPR。换言之，仅凭在欧盟境内存在雇员这一条件，不足以触发 GDPR 适用，所涉处理活动必须属于欧盟境内雇员的营业活动范围才能适用 GDPR。

负责数据处理的非欧盟实体在欧盟成员国没有分支机构或子公司这一事实并不妨碍其构成欧盟数据保护法项下的在欧盟境内拥有实体。虽然实体的概念较为广泛，但并非没有限制。不能仅仅因为企业的网站可在欧盟境内访问，就断定该非欧盟实体在欧盟境内拥有实体。

例 1： 总部设在美国的一家汽车制造公司在布鲁塞尔设立了全资分支机构，负责监督其在欧洲的包括营销和广告在内的所有业务。比利时分支机构可以被认为稳定的安排，根据此汽车制造公司的经济活动的性质开展了真实有效的活动。因此，比利时分支机构可以被视为是 GDPR 项下在欧盟境内的实体。

一旦得出控制者或处理者在欧盟拥有实体的结论，则随后应进行结合具体情况进行分析，以确定数据处理活动是否属于该实体的营业活动范围，并进一步确认第 3 条第（1）款是否适用。如果在欧盟境外的数据控制者或处理者通过“稳定安排”，在欧盟成员国内开展了“真实、有效的活动——哪怕这种活动量很小”，无论其法律形式为何（例如子公司，分支机构，办公室等），该控制者或处理者可被视为在该成员国拥有实体。因此，下一步则需要考量个人数据的处理是否属于序言第 22 条中强调在此类实体“进行的活动”。

1.2 在实体的“经营活动范围内”进行的个人数据处理活动。

第 3 条第（1）款的适用不以由设立在“欧盟境内的实体”进行处理为必要条件。如果该处理行为属于“欧盟境内实体的营业范围”，则控制者或处理者就该处理行为应承担 GDPR 规定的义务。EDPB 建议，某处理行为是否属于 GDPR 第 3 条第（1）款规定的欧盟境内实体的营业活动应进行个案分析，每种情况都必须结合案件的具体事实和相关背景进行确认。

EDPB 认为，应根据相关判例理解第 3 条第（1）款规定的在“控制者或处理者在欧盟境内的实体营业活动范围内进行的对个人数据处理”的含义。一方面，为了实现全面有效的保护目标，不应对其含义进行限缩性解释；另一方面，也不应进行过于宽泛的解释，以致欧盟境内实体的营业活动与非欧盟实体的数据处理活动的关联度非常弱时，也将这种处理纳入欧盟数据保护法的适用范围。例如，非欧盟实体在成员国内进行的某些商业活动可能与该实体的数据处理活动关联性极弱，故而该实体在欧盟内进行的商业活动中涉及的数据处理活动不应受欧盟数据保护法的规制。

以下两个因素可以帮助确定数据处理是否属于控制者或处理者在欧盟境内的实体的营业活动：

(1) 欧盟境外的数据控制者或处理者与其在欧盟境内的实体之间的关系

在欧盟境外设立的数据控制者或处理者的数据处理活动可能与在它在欧盟成员国境内设立的实体的活动之间发生不可分割的联系，从而导致欧盟法的适用，即使欧盟境内的实体没有实质上参与该数据处理活动。如果对事实的个案分析表明非欧盟数据控制者或处理者的数据处理活动与其在欧盟境内实体的活动之间存在密切关联，则无论其在欧盟的实体是否参与此数据处理。欧盟法均对该非欧盟实体产生约束力。

(2) 有来自欧盟境内的收入

若欧盟境内某实体在欧盟进行了营收活动，且该营收活动与在欧盟境外进行的个人数据处理活动和欧盟居民“紧密关联”，则可认定“该非欧盟的控制者或处理者的处理活动属于在欧盟境内实体进行的营业活动”，该等处理活动进而可能因此受到欧盟法规制。

EDPB 建议非欧盟组织对其处理活动进行评估，评估内容为：首先确定是否处理个人数据；其次确定处理数据活动与该组织在欧盟内的任何活动之间的潜在关联。如果确定存在这种关联，则这种关联的性质将是决定数据处理是否适用 GDPR 的关键，组织应根据上述列出的两个要素进行评估。

例 2：某电子商务网站由一家中国公司运营。该公司的个人数据处理活动仅在中国进行。这家中国公司已在柏林设立了欧洲办公室，以领导并实施针对欧盟市场的商业拓展和营销活动。

在此案中，鉴于在欧洲市场开展商业拓展和营销活动的营利性，柏林欧洲工作室进行的商业拓展和市场营销活动可以被认定为与该中国公司在中国进行的数据处理行为密切关联。

因此，中国公司处理与欧盟销售有关的个人数据可以被认定为是在欧盟的实体进行的营业活动。因此，中国公司进行的处理活动应遵守 GDPR 第 3 条第 (1) 款的规定。

例 3：南非的一家连锁度假酒店通过其网站提供成套交易，并提供英语，德语，法语和西班牙语服务。该公司在欧盟没有任何办公室，代表或稳定的安排。

在本案中，该连锁酒店在欧盟境内没有任何代表人或稳定部署，似乎没有任何实体与此南非的数据控制者有联系，使其有在 GDPR 项下的欧盟境内的实体。因此，相关数据处理不受 GDPR 第 3 条第（1）款规定的约束。

但是，欧盟境外的数据控制者所进行的数据处理是否受 GDPR 第 3 条第（2）款的约束必须另行具体分析。

1.3 GDPR 应用于欧盟境内的控制者或处理者的实体，而处理是否在欧盟内进行在所不论

根据 GDPR 第 3 条第（1）款的规定，属于控制者或处理者在欧盟境内实体的营业活动的数据处理活动会触发 GDPR 的适用，数据控制者或处理者因此而需履行 GDPR 项下的相关义务。

GDPR 明确规定，本条例适用于在欧盟境内实体营业活动内的处理行为，“无论处理行为是否在欧盟内进行”。数据控制者或处理者在欧盟内的实体的存在，和数据处理行为属于此实体的营业活动的事实，触发了 GDPR 对此数据处理活动的适用。因此，在确定数据处理是否是在欧盟实体的营业活动范围内进行，而适用 GDPR 时，数据处理的地理位置不是考虑因素。

例 4：某法国公司专门面向摩洛哥，阿尔及利亚和突尼斯的客户开发了一款汽车共享应用程序。该服务仅在这三个国家/地区可用，但所有个人数据处理活动均由在法国的数据控制者进行。

尽管个人数据的收集是在非欧盟国家/地区进行的，但是个人数据的后续处理是数据控制者在欧盟境内的实体进行的营业活动范围内。因此，即使处理的个人数据对应的数据主体不属于欧盟居民，但根据 GDPR 第 3 条第（1）款的规定，该法国公司进行的数据处理活动须受 GDPR 的约束。

例 5：总部位于斯德哥尔摩的某制药公司将与临床试验数据有关的所有个人数据处理活动都安排给了其位于新加坡的分支机构进行。

在这种情况下，虽然处理活动在新加坡进行，但处理属于斯德哥尔摩制药公司的营业活动，即属于在欧盟境内设立的数据控制者的营业活动。因此，根据 GDPR 第 3 条第（1）款规定，该数据处理活动应受 GDPR 的约束。

在确定 GDPR 适用的地域范围，以下两种情况中相关实体所在的地理位置在认定是否属于第 3 条第（1）款提及的实体非常重要：

- 控制者或处理者本身所在地理位置（设立在欧盟境内还是境外）；
- 非欧盟控制者或处理者在欧盟境内有无业务活动（即在欧盟境内有没有实体）

但是，根据第 3 条第（1）款的目的，数据处理活动发生的地理位置或被处理的个人数据对应的数据主体的所在地并不重要。

第 3 条第（1）款并未将 GDPR 的适用范围局限于在欧盟境内进行的个人数据处理活动。因此，EDPB 认为，控制者或处理者在其位于欧盟境内实体营业活动范围内进行的数据处理活动均受 GDPR 的约束，无论处理的个人数据对应的数据主体的所在地或国籍如何。这一观点在 GDPR 序言第 14 条也有所体现，该条规定：“本条例提供的保护适用于与个人数据处理有关的自然人，不论其国籍或居住地在何处”。

1.4 数据控制者和处理者实体标准的应用

就属于第 3 条第（1）款范围的处理活动而言，EDPB 认为此类规定适用于其数据处理活动是属于控制者和处理者在各自欧盟境内实体的营业活动范围的情形。虽然在控制者和处理者之间建立关系的条件与数据控制者或处理者实体的地理位置并无关系,但 EDPB 认为，当根据 GDPR 第 3 条第（1）款判断实体的不同义务时，须对每个实体所进行的数据处理单独分析。

GDPR 为数据控制者和处理者规定了不同和专门的规定或义务，因此，如果数据控制者或处理者根据第 3 条第（1）款须受 GDPR 的规制时，则将分别负担不同的义务。在这方面，EDPB 明确认为,欧盟境内的数据处理者不应仅凭借其代数据控制者的进行处理而被认为是第 3 条第（1）款意义上的数据控制者的实体。

如果数据控制者和数据处理者中有一个不是在欧盟境内设立的，那么两者之间关系的存在不必然导致 GDPR 对两者都适用。

一个组织若依另一个组织（客户公司）的指示代表其处理个人数据，则该组织将被认定为是客户公司（数据控制者）的处理者。如果处理者设立在欧盟境内，

则该处理者须遵守 GDPR 对处理者规定的义务（“GDPR 数据处理者义务”）。如果向数据处理者下达指令的数据控制者也位于欧盟，则该数据控制者必须遵守 GDPR 规定的控制者的义务（“GDPR 控制者义务”）。数据控制者进行的数据处理活动符合 GDPR 第 3 条第（1）款的规定时，该处理活动将不会仅因为数据控制者指示的代其处理个人数据的处理者位于欧盟境外而逃脱 GDPR 的规制。

（1）设立在欧盟境内的控制者指令设立在欧盟境外的处理者进行的数据处理活动。

适用 GDPR 的控制者委托不适用 GDPR 的处理者处理数据时，控制者应通过合同或其他法律文件确保处理者会根据 GDPR 的要求处理数据。GDPR 第 28 条第 3 条规定，处理者的数据处理行为应当受合同或其他法律文件约束。因此，控制者须确保与处理者签订的合同中列明 GDPR 第 28 条第（3）款规定的各项要求。此外，为了确保 GDPR 第 28 条第 1 款规定的义务的履行——即选择能提供充分保障按照 GDPR 的要求处理个人数据的处理者，控制者可考虑把 GDPR 对处理者的要求写入与处理者的合同中。也就是说，控制者应参照 GDPR 第 28 条第（3）款的要求，确保不受 GDPR 约束的处理者的处理行为受到合同或欧盟或各成员国法律规定的法律行为的约束。

因此，不受 GDPR 管辖的处理者将基于 GDPR 第 28 条规定通过合同规定间接地受到 GDPR 关于数据控制者的特定义务的约束，也可能适用 GDPR 第五章的规定。

例 6：芬兰研究机构对萨米人进行了研究。该研究所启动某一项目仅涉及俄罗斯萨米人。在这个项目中，研究所委托了位于加拿大的数据处理者处理个人数据。

芬兰的控制者须仅委托能够提供足够的保证，并实施满足 GDPR 要求的措施保护数据主体权利的处理者。芬兰的数据控制者需要与加拿大的数据处理者签订数据处理协议，该协议将规定数据处理者的责任。

（2）在位于欧盟境内的数据处理者的营业活动范围内的数据处理行为

虽然判例法使我们清楚地了解到控制者在欧盟境内的实体的营业活动范围内进行的数据处理的影响，而处理者在欧盟实体营业活动范围内的数据处理活动的影响并不清晰。

EDPB 强调，在考虑数据控制者和数据处理者的实体是否设立在欧盟时，应将两者分开考虑。

第一个问题是，控制者本身在欧盟境内是否有实体，且在该实体的营业活动范围内进行了数据处理。若控制者的数据处理行为不是发生在位于欧盟境内的实体的营业活动范围内，则该数据控制者不因第 3 条第（1）款规定而受 GDPR 管辖（尽管可能因第 3 条第（2）款规定受 GDPR 管辖）。除非存在其他因素，否则数据处理者在欧盟境内有实体将不被视为数据控制者在欧盟境内有实体。

另一个问题是处理者的处理行为是否属于欧盟境内实体的营业活动。如果是，则处理者将受到第 3 条第（1）款规定的 GDPR 处理者义务的约束。

然而，这并不会导致非欧盟控制者受到 GDPR 的约束。也就是说，“非欧盟”控制者（如上所述）不会仅因为委托欧盟境内的处理者而受 GDPR 的约束。

不受 GDPR 约束的控制者不会因指示欧盟境内处理者处理个人数据而被认定为属于“处理者在欧盟境内营业活动范围”。

数据处理行为属于控制者自身的营业活动；处理者只是提供处理服务，与控制者的活动没有“不可分割的联系”。

如上所述，对于在欧盟境内设立的数据处理者，并代表在欧盟境外设立且不符合第 3 条第（2）款规定而不受 GDPR 约束的控制者进行处理的情形，EDPB 认为，控制者的处理活动不会仅因为委托欧盟境内的处理者代其处理而受 GDPR 的规制，但是处理者将因 GDPR 第 3 条第（1）款的规定而受 GDPR 的约束。

例 7：一家墨西哥零售公司与一家在西班牙建立的处理者签订合同，以处理与墨西哥公司客户有关的个人数据。

这家墨西哥公司专门向墨西哥市场提供服务，且其处理的个人信息仅涉及欧盟境外的数据主体。

在这种情况下，墨西哥零售公司向欧盟境内居民提供产品或服务，也不监控欧盟境内居民的行为。

因此，设立在欧盟境外的控制者进行处理不因第 3 条第（2）款的规定而受 GDPR 的约束。同样，数据控制者的活动不属于在欧盟境内的实体的营业活动范围内，从而不因第 3 条第（1）款的规定而受到 GDPR 的约束。

本案中，数据处理者位于西班牙，因此根据 GDPR 第 3 条第 1 款的规定，其处理行为将受 GDPR 的规制。处理者在其营业活动范围内进行的数据处理须遵守 GDPR 关于处理者义务的规定。

当在欧盟境内的数据处理者代表在欧盟境外数据控制者处理数据，且不适用 GDPR 第 3 条第 2 款规定时，该处理者应遵守 GDPR 项下的处理者的义务。

- 根据 GDPR 第 28 条第（2）款、第（3）款、第（4）款、第（5）款和第（6）款的规定，处理者有义务订立数据处理协议，但为协助数据控制者履行其 GDPR 项下关于控制者的义务的除外。
- 处理者及任何受控制者或处理者委托的有权访问个人数据的人，非经控制者指示不得处理该等数据，除非适用 GDPR 第 29 条及第 32 条第（4）款的规定或欧盟或成员国法律的要求，
- 如适用，处理者应按照 GDPR 第 30 条第（2）款的要求保留代表控制者进行的所有处理活动的记录。
- 如适用，处理者应按照 GDPR 第 30 条第（2）款的要求配合监督机构执行其任务。
- 处理者应根据 GDPR 第 32 条的规定采取技术和组织措施，以确保安全水平与风险相当。
- 处理者应根据 GDPR 第 33 条的规定，在发现个人数据泄露后立即通知控制者，不得无故拖延。
- 如适用，处理者应按照 GDPR 第 37 条和第 38 条的要求指定一名数据保护官。
- 符合第五章关于向第三国或国际组织传输个人数据的规定。

此外，由于此类处理活动属于处理者在欧盟境内的实体的营业活动范围，EDPB 要求，处理者必须确保其处理行为遵从了欧盟法或成员国法律的义务。GDPR 第 28 条第 3 款还规定，“如果处理者认为控制者的指令违反本条例或其他联盟或成员国数据保护规定，应立即通知控制者。”

根据第 29 条工作组先前采取的立场，EDPB 认为，欧盟不能被用作“数据避风港”。例如，当处理活动涉及不可接受的道德问题时，或存在欧盟数据保护法适用范围以外的某些法律义务，特别是欧洲数据保护法以及国家有关公共秩序的规定时，数据处理者在任何情况下遵守相关规则，不论数据处理者所在国家为何。

此外，在执行欧盟法律过程中，GDPR 和相关国家法律规定须受《欧盟基本权利宪章》的约束。

但是，这并不意味着欧盟境外的控制者的不属于 GDPR 管辖范围的处理行为须承担额外义务。

2. 目标市场指向标准的应用——第 3 条第（2）款

在欧盟境内不存在实体并不一定意味着第三国的数据控制者或处理者进行的处理活动将不适用 GDPR 的规定。GDPR 第 3 条第（2）则针对设立于欧盟境外的控制者或处理者的适用条件作出规定。

在这种情况下，EDPB 认为在欧盟境内没有实体的控制者或处理者不能受益于 GDPR 第 56 条规定的一站式管辖。实际上，GDPR 的合作和一致性机制仅适用于在欧盟范围内拥有一个或多个实体的控制者和处理者。

尽管本指南旨在阐明 GDPR 的地域管辖范围，但 EDPB 仍希望强调，控制者和处理者还需要考虑其他适用的法律未见，例如欧盟或成员国的部门立法和国家法律。

GDPR 的某些条款确实允许成员国在某些领域或与特定处理情况相关的条件下引入附加条件，制定特定的数据保护框架。

控制者和处理者因此必须确保他们了解并遵守这些附加条件和特殊数据保护框架。上述附加条件不同成员国存在不同规定。

其中就以下 GDPR 条款各成员国规定的差异较为明显：GDPR 第 8 条关于信息社会服务中儿童可给予有效同意的年龄门槛（可能在 13 至 16 岁之间）；第 9 条关于特殊类别数据的处理；第 23 条关于权利义务范围的限制或与 GDPR 第九章言论和信息自由所载规定有关的规定（包括言论和信息自由；公众查阅官方文件；居民身份证号码；就业背景；出于公共利益、科学、历史研究或统计目的的处理；秘密；教会和宗教协会）。

GDPR 第 3 条第（2）款规定，“本条例适用于由未在欧盟设立的控制方或处理方处理在欧盟内的数据主体的个人数据，如果处理活动涉及：（a）向欧盟境内的数据主体提供产品或服务，不论数据主体是否需要支付费用。或（b）对数据主体在欧盟境内的行为进行监控。

GDPR 第 3 条第（2）款，规定了“目标指向标准”。欧盟境外的控制者或处理者的两种特定的与欧盟境内数据主题相关的处理行为可能处罚该条款的规定，从而受到 GDPR 的规制。

除了仅适用于设立欧盟境外的控制者或处理者的处理之外，目标指向标准主要侧重于与“处理活动”“有关”的内容，并应进行个案分析。

EDPB 强调，控制者或处理者的某些处理行为可能受到 GDPR 的约束，但其他处理行为不受 GDPR 约束。

GDPR 关于地域管辖的第 3 条第（2）款是否适用的关键取决于有关的处理活动性质。

因此，在评估是否适用目标指向标准时，EDPB 建议采用双重方法，首先确定处理是否与在欧盟境内的数据主体的个人数据有关；第二，处理是否与提供的产品或服务有关，或与监测数据主体在欧盟的行为有关。

2.1 欧盟境内的数据主体

第 3 条第（2）款的措词是“欧盟境内数据主体的个人数据”。

因此，目标指向标准的适用不受正在处理个人数据对应的数据主体的公民身份、居住地或其他类型法律地位的限制。

序言第 14 条确认了这一观点，并指出“本条例所提供的保护适用于与其个人数据处理有关的自然人，不论其国籍或居住地如何，涉及其个人数据的处理”。

GDPR 的这一规定反映了欧盟法律保护个人数据的广泛性，即不限于欧盟公民，《欧盟基本权利宪章》第 8 条规定，人人均享有个人数据得到保护的权利

尽管数据主体位于欧盟境界是决定是否适用第 3 条第（2）款的决定因素，但 EDPB 认为，欧盟境内的数据主体的国籍或法律地位 不能限制 GDPR 的地域管辖范围。

数据主体是否在欧盟境内必须在提供产品或服务，或在发生监测行为的语境下进行分析。提供产品或服务，或检测行为发生的时长在所不论。

但是，EDPB 认为，就与服务提供有关的处理活动而言，该规定针对的是有意而非无意或偶然地针对欧盟境内个人的活动。

因此，如果处理涉及仅向欧盟以外的个人提供的服务，但当这些个人进入欧盟境内时，服务并未撤回，则相关处理将不受 GDPR 的约束。

在这种情况下，这一行为并非故意指向欧盟境内的个人，而是指向欧盟境外的个人，无论这些个人是留在欧盟境外还是访问欧境内。

例 8：澳大利亚某公司根据用户的喜好和兴趣提供移动新闻和视频内容服务。用户每日或每周收到更新。此项服务仅提供给位于澳大利亚的用户，用户在订阅时必须提供澳大利亚电话号码。

该服务的一位澳大利亚订阅者在德国度假期间继续使用该服务。

尽管该澳大利亚用户在欧盟境内期间继续使用该服务，但该服务并非针对欧盟内的个人，而是仅针对澳大利亚境内的个人，因此澳大利亚公司对个人数据的处理不属于 GDPR 的规制范围。

例 9：某美国设立的初创企业，欧盟没有任何业务存在或经营场所。该公司为游客提供城市地图 App。该 App 处理用户在特定城市使用该应用程序时的地理位置，以便就游客参观的地点提供周边的餐馆、酒吧和酒店等有定向广告。该 App 适

用于游览纽约、旧金山、多伦多、伦敦、巴黎和罗马的游客。

该美国企业通过其城市地图 App，面向欧盟(特别是伦敦、巴黎和罗马)的数据主体提供了服务，所提供的其对欧盟境内数据主体的个人数据的处理活动与其面向欧盟数据主体提供的服务相关，根据第 3 条第 2 款受 GDPR 约束。

EDPB 还希望强调，非欧盟控制者或处理者仅在欧盟境内处理个人数据的事实不足以触发 GDPR 的适用，必须始终存在“针对”欧盟境内的个人的这一要素，无论是通过向他们提供产品或服务，还是通过监视他们的行为（以下会详细描述）。

例 10：一位美国公民在欧洲旅游度假期间下载并使用了某美国公司提供的新闻类 App。从 App 的使用协议和将美元作为唯一可供支付货币来看，该 App 显而易见专门针对美国市场。这家美国公司通过 App 收集美国游客的个人数据不受 GDPR 的约束。

此外，只要处理过程专门针对欧盟居民也不涉及对其在欧盟境内行为的监控，在第三国处理欧盟公民或居民的个人数据不会触发 GDPR 的应用。

例 11：台湾的一家银行有居住在台湾但持有德国国籍的客户。该银行只在台湾开展业务，其活动不针对欧盟市场。该银行处理德国客户的个人数据不受 GDPR 的约束。

例 12：加拿大移民局在入境时处理欧盟公民的个人信息，以审查他们的签证申请。此处理过程不受 GDPR 的约束。

2.2 向欧盟境内的数据主体提供产品或服务，无论是否需要数据主体对产品或服务进行付款。

触发 GDPR 第 3 条第（2）款适用的第一个行为是“提供产品或服务”，欧盟法律和判例对此作出了进一步阐释，在理解时应当参照上述说明的相关要求。提供服务也包括提供信息社会服务，在（欧盟）2015/1535 号指令第 1（1）条第（b）点将信息社会服务定义为“任何信息社会服务，也就是说，通常应服务接受者的个别要求，以电子方式远距离提供报酬的任何服务”。

GDPR 第 3 条第（2）款（a）项规定，不论是否需要数据主体付款，关于提供货物或服务的目标指向标准均适用。因此，非在本欧盟境内设立的控制者或处理者

的活动是否应被视为提供货物或服务并不取决于是否付款以换取所提供的产品或服务。

例 13：一家在欧盟境内没有实体的美国公司处理临时出差到法国、比利时和荷兰的员工的个人资料，具体目的是报销他们的住宿费用和支付每日津贴，不同国家的报销额不同。

在这种情况下，虽然处理活动与欧盟境内的人员（即临时在法国，比利时和荷兰出差的员工）有特殊关系，但是它并不涉及向这些个人提供服务，而是雇主履行其合同义务和与个人就业有关的人力资源职责所必需的处理行为。这处理行为不涉及服务的提供务，因此不因第 3 条第（2）款（a）项而受 GDPR 的约束。

在确定能否满足第 3 条第(2)款(a)项的目标指向标准时，另一个需要评估的关键因素是货物或服务的提供是否针对欧盟境内的人，即控制者的处理目的和方式是否表明其向欧盟的数据主体提供产品或服务的意图。GDPR 序言第 23 条明确阐释了“为了确定此类控制者或处理者是否向欧盟境内的数据主体提供商品或服务，应确定控制者或处理者是否明显想向欧盟内一个或多个成员国的数据主体提供服务。”

序言进一步规定：“鉴于仅仅访问或联系控制者、处理者或者中间人的在欧盟的网站、电子邮件地址或者其联系方式或者使用控制者 设有营业场所的第三国通常使用的语言，并不足以确定这样的动机，其他因素，诸如使用通常在一个或多个成员国内使用的语言或者货币并且可能以该其他语言订购商品或者服务，或者提及欧盟境内的客户或用户，可以明确反映控制者试图向欧盟境内的数据主体提供商品或服务”。

序言第 23 条所列的要素呼应并符合欧盟关于民商事管辖权和判决的承认与执行第 44/2001 号条例判例法的相关规定，特别是关于第 15 条第（1）款（c）项的规定。在 *Pammer v. Reederei Karl Schlüter GmbH & Co* 和 *Hotel Alpenhof v. Heller*（C-585 / 08 和 C-144 / 09）中，法院被要求解释欧盟第 44/2001 号条例第 15 条第（1）款（c）项所指的“指向性活动”的含义。欧盟法院认为，在第 15 条第(1)款(c)项的语境下，为了确定交易者是否“直接”将其活动“指向”消费者住所的成员国内，该交易者必须表明其与这些消费者建立商业关系的意图。在本案中，欧洲法院认为有证据表明该交易者想要与成员国内的消费者开展业务。

尽管“指向性活动”的概念不同于“提供商品或服务”，但 EDPB 认为 *Pammer v Reederei Karl Schlüter GmbH & Co* 和 *Hotel Alpenhof v Heller*（C-585/08 和 C-144/09）

的判例可能有助于认定是否向欧盟中的数据主体提供产品或服务。因此，在考虑到案件的具体事实时，可以考虑或结合考虑以下因素：

- 提供的商品或服务中至少指明了欧盟或一个成员国；
- 数据控制者或处理者向搜索引擎运营商支付互联网参考服务的费用，以方便欧盟消费者访问其网站；或者控制者或处理者已针对欧盟国家的受众发起营销和广告活动；
- 有关活动的国际性质，如某些旅游活动；
- 欧盟国家可访问的地址或电话号码；
- 使用不同于控制者或处理者的第三个国家/地区以外的顶级域名，例如“.de”，或使用中立的顶级域名，例如“.eu”；
- 从一个或多个其他欧盟成员国到提供服务地点的旅行说明；
- 由多个欧盟成员国的客户组成的国际客户，特别是通过展示此类客户书面的帐户；
- 使用交易者所在国家/地区以外的语言或货币，尤其是一个或多个欧盟成员国的语言或货币；
- 数据控制者可在欧盟成员国内交付货物。

如前所述，如果单独列出上述几个要素，可能不足以明确表明数据控制者打算向欧盟的数据主体提供货物或服务。然而，在进行任何具体分析时都应考虑到这些因素，以便确定与数据控制者的商业活动相关的因素组合是否可以认定构成向欧盟数据主体的提供产品或服务。

但是，序言第 23 条确认了仅在欧盟境内可以访问控制者，处理者或中间人的网站，在网站上提供电子邮件或地理地址，或共非国际代码的电话号码本身并不能充分证明控制者或处理者想要向位于欧盟中的数据主体提供商品或服务。在这种情况下，EDPB 认为无意或偶然地向欧盟内的人提供货物或服务而处理个人数据的

行为将不受 GDPR 的约束。

例 14：某个在土耳其建立和管理的网站提供个性化家庭相册的创建，编辑，打印和运输服务。该网站提供英语，法语，荷兰语和德语版本，并且可以用欧元付款。该网站表明只能在法国，比荷卢三国和德国提供邮寄服务。

在本案中，很明显制作、编辑和印刷个性化家庭相册是欧盟法律意义上的服务。该网站以欧盟的四种语言提供服务，并且可以在六个欧盟成员国内邮寄相册，这表明土耳其网站有意向欧盟的个人提供服务。

因此土耳其网站作为数据控制者所进行的处理涉及向欧盟中的数据主体提供服务，因此依据 GDPR 第 3 条第（2）款（a）项的规定须受 GDPR 的约束并履行 GDPR 项下的义务。

根据 GDPR 第 27 条的规定，数据控制者必须在欧盟指定一名代表人。

例 15：摩纳哥某私营公司为支付工资而处理其雇员的个人数据。该公司员工大部分是法国和意大利居民。

在这种情况下，虽然该公司进行的处理涉及法国和意大利的数据主体，但并非在提供产品或服务的情况下进行。事实上，人力资源管理，包括第三国公司的工资支付，不能被认定为第 3 条第（2）款（a）项所指的提供服务。该处理行为不是向欧盟境内数据主体提供货物或服务（也不涉及对行为的监控），按照第 3 条的规定因此不受 GDPR 第 3 条的约束。前述分析不影响第三国有关法律的适用。

例 16：苏黎世某瑞士大学提供在线平台以选拔硕士学位。候选人可以上传其简历、求职信以及联系方式。任何具有充足德语和英语水平并持有学士学位的学生均可参加选拔。这所大学并没有向欧盟境内大学的学生做特别宣传，也只接受瑞士货币的支付。

由于在本硕士学位的申请和遴选过程中没有对来自欧盟的学生进行区分或说明，因此无法确定瑞士大学有意针对特定欧盟成员国的学生。足够的德语和英语水平是适用于任何申请人的一项一般要求，无论该申请人是瑞士居民，欧盟人员还是来自第三国的学生。如果没有其他因素表明欧盟成员国学生的具体目标，那么就不能确定所涉及的处理与向欧盟数据主体提供教育服务有关，因此此类处理将不受 GDPR 规定的约束。

瑞士大学还提供国际关系暑期课程，并专门在德国和奥地利的大学中宣传此课程，以最大程度地提高课程的出勤率。在这种情况下，瑞士大学明确打算向欧盟中的数据主体提供此类服务，GDPR 将适用于相关的处理活动。

2.3 监控数据主体的行为

触发适用第 3 条第 (2) 款的第二类活动是对数据主体在欧盟内行为的监控。

序言第 24 条阐明：“非欧盟境内内设立的控制者或处理者处理欧盟内数据主体的个人数据时，如果涉及对此类数据主体在欧盟内行为的监控，则也应遵守本条例。”

根据第 3 条第 (2) 款 (b) 项的规定，所监控的行为必须首先与欧盟内的数据主体有关，且所监控的行为必须在欧盟境内发生，二者须同时满足。

监控主体行为的处理活动的性质在序言第 24 条中作了进一步的规定，其中要求“为了确定是否可以将处理活动视为监控数据主体的行为，应查明是否在互联网上对自然人进行跟踪，包括随后可能使用的个人数据处理技术，这些技术包括对自然人进行特征分析，特别是为了对自然人作出决定，或分析或预测自然人的个人偏好、行为和态度。”虽然序言第 24 条指向的是通过跟踪互联网上的人来监控行为，但 EDPB 认为，在确定处理活动是否属于对主题活动的监控时，还应考虑通过其他类型网络或技术进行跟踪的个人数据处理，例如，通过可穿戴设备和其他智能设备。

与 GDPR 第 3 条第 (2) 款 (a) 项的规定相反，GDPR 第 3 条第 (2) 款 (b) 项或序言第 24 条均未明确规定数据控制者或处理者具有“目标指向”的必要程度，以确定监控活动是否会引起 GDPR 的适用。但是，“监控”一词的使用意味着控制者有一个特定的目的，即收集和再利用在欧盟境内的个人行为的相关数据。EDPB 认为在线收集或分析欧盟境内的个人数据不会自动被视为“监控”。这将有必要考虑控制者处理数据的目的，特别是涉及该数据的任何后续行为分析或识别分析技术。EDPB 钻研了第 24 条的措辞，该措辞表明要确定数据处理是否涉及监控数据主体的行为，对互联网上自然人的跟踪（包括随后可能使用的识别分析技术）是关键考虑因素。

因此，根据第 3 条第 (2) 款 (b) 项的规定，数据控制者或处理者监控在欧盟境内数据主体的行为可包括广泛的监控活动，特别是包括：

- 用户行为广告
- 地理定位，特别是用于营销
- 通过使用 cookies 或其他跟踪技术（如指纹识别)进行在线跟踪
- 个性化饮食和健康在线分析服务
- 闭路电视
- 基于用户画像的市场调查和其他行为研究
- 监控或定期报告个人健康状况

例 17：在美国成立的零售咨询公司通过 Wi-Fi 追踪收集顾客在购物中心的移动情况，为法国某购物中心提供零售布局方面的建议。通过 Wi-Fi 追踪分析顾客在购物中心内的活动相当于监控主体的活动。在本例中，由于购物中心位于法国，故数据对象的行为发生在欧盟境内。因此，作为数据控制者的该资讯公司以此为目的处理该等数据时，须根据 GDPR 第 3 条第 (2)款 (b)项的规定受 GDPR 约束。

根据 GDPR 第 27 条的规定，该数据控制者美国咨询公司必须在欧盟境内指定一位代表人。

例 18：某设立于加拿大，在欧盟境内没有实体的 App 开发者监控欧盟境内数据主体的行为，因此根据 GDPR 第 3 条第 (2) 款 (b) 项的规定受 GDPR 的约束。该 App 开发者使用在美国设立的处理者进行应用优化和维护。

就委托处理的行为而言，根据，加拿大数据控制者有义务仅使用合适的处理者，确保其履行 GDPR 第 28 条项下的义务，并反映在管理其与美国处理者关系的合同或法律行为中。

2.4 设立在欧盟境外的数据处理者

如果处理活动与 GDPR 第 3 条第 (2)款要求的目标指向活动“相关”的处理，则

应受 GDPR 的规制。EDPB 认为处理活动和提供产品或服务之间需要有联系，但是需要考虑控制者和处理者的处理活动是否均是相关的。

对于设立在欧盟境外的数据处理者，为了确定其数据处理是否符合 GDPR 第 3 条第 (2) 款的规定，有必要审查处理者的数据处理活动是否与控制者的目标活动“相关”。

EDPB 认为，如果数据控制者的数据处理活动涉及商品或服务的提供或对个人在联盟中行为的监控(“目标指向”)，则根据第 3 条第(2)款的规定，任何指示其代表控制者执行该处理活动的处理者均属于 GDPR 的适用范围。

数据处理活动的“目标指向”性质与其目的和方法有关;只有作为数据控制者的实体才能决定是否将欧盟境内的个人作为目标。这样的解释并不排除处理者将积极参与与目标指向相关的数据处理活动(即处理者接受控制者的指令、代控制者提供产品或服务或实施监控主体行动)的可能性。

因此，EDPB 认为重点应是处理者执行的处理活动与数据控制者执行的目标指向活动之间的关联。

例 19: 某巴西公司在网上销售食品配料和当地食谱向欧盟境内让居民提供产品。该公司采取投放广告的措施，并在法国，西班牙和葡萄牙提供送货服务。在本案中，公司指示同样在巴西设立的数据处理者基于法国、西班牙和葡萄牙的客户之前的订单开发特别优惠，进行相关的数据处理。

处理者在控制者的指令下进行的处理活动与向联盟境内的数据主体提供货物有关。此外，通过开发这些定制的报价，数据处理者可以直接监视欧盟中的数据主体。因此，根据第 3 条第 (2) 款，处理者的数据处理活动应受 GDPR 的管辖。

例 20: 某美国公司开发了一款健康和生活方式 App，允许用户记录他们的个人指标(睡眠时间、体重、血压、心跳等)。然后，该 App 为用户提供每日的饮食和运动建议。处理由美国数据控制者执行。该 App 提供给欧盟境内的个人使用。在数据存储方面，美国公司使用在美国设立的处理者(云服务提供商)

在运行该 App 时，它将“瞄准”欧盟境内的个人，构成对欧盟境内个人的监控，从而根据 GDPR 第 3 条第(2)款须受 GDPR 的约束。

在根据美国公司的指示并代表该公司进行处理时，该云服务商/处理者正在执行的处理活动与其控制者针对欧盟的个人目标指向活动“相关”。根据 GDPR 第 3 条第(2)款的规定，处理者代表其数据控制者进行的数据处理活动属于 GDPR 的规制范围。

例 21：某土耳其公司提供中东文化旅游服务，导游会说英语、法语和西班牙语。该旅游服务通过三种语言在网站上宣传并提供该服务。该网站允许在线预订，支持欧元和英镑的支付。出于营销和商业前景的考虑，该公司指示一个设在突尼斯的数据处理者(一个呼叫中心)联系以前在爱尔兰、法国、比利时和西班牙的客户，以便获得他们对旅行的反馈，并告知他们新的优惠和对应的目的地。控制者的“目标”是通过向欧盟的个人提供服务，根据 GDPR 第 3 条第(2)款其处理将属于 GDPR 的规制范围。

突尼斯处理者的数据处理活动促进了数据控制者对欧盟境内个人的服务，也与控制者提供的服务相关联，因此根据 GDPR 第 3 条第(2)款其处理也属于 GDPR 的规制范围。此外，在本案中，突尼斯的处理者积极参与与控制者目标指向相关的处理活动，代表土耳其控制者并根据其指示提供服务。

2.5 与其他 GDPR 条款和其他法律的相互作用

EDPB 还将进一步评估根据第 3 条适用的 GDPR 领域范围与根据第五章关于国际数据传输的规定之间的相互作用。如有必要，可能会就此发布额外的指导意见。

在处理个人数据方面，设立在欧盟境外的第三国控制者或处理者须遵守其本国法律。但是，如果这种处理根据 GDPR 第 3 条第(2)款涉及针对联盟境内的个人，则除要遵守其国家/地区的法律外，控制者还必须遵守 GDPR 的规定。不管处理是按照第三国的法律义务进行的，还是仅仅是由控制者选择而进行的处理，情况都是如此。

3.在成员国法律因国际公法而适用的 GDPR 进行数据处理

第 3 条第(3)款规定：“本条例适用于非设立于欧盟境内但根据国际公法的规定适用成员国法律的数据控制者所进行的个人数据处理行为。”在第 25 条立法理由中对该条款进行了扩展，该条规定：“当成员国法律因国际公法而适用时，本条例也应适用于非设立于欧盟境内的数据控制者，如成员国的大使馆或者领事馆。”

因此，EDPB 认为 GDPR 适用于欧盟成员国驻欧盟以外的使领馆进行的个人数据处理，因为根据第 3 条第(3)款，此类处理属于 GDPR 的范围。成员国的外交或领事机构作为数据控制者或处理者，将须遵守 GDPR 的所有有关规定，包括涉及数据主体的权利、与控制者和处理者有关的一般义务以及向第三国或国际组织传输个人数据。

例 22: 荷兰驻牙买加金斯敦领事馆为征聘当地工作人员开设了在线申请流程，以支持其行政管理。虽然荷兰驻牙买加金斯敦的领事馆设立在欧盟境外，但它是欧盟成员国的领事馆，根据第 3 条第(3)款的规定，依据国际公法适用成员国法律，从而 GDPR 适用该领事馆对个人数据的处理。

例 23: 在国际水域旅行的某德国游轮处理船上客人的数据，以便定制邮轮内娱乐优惠。虽然该船舶位于欧盟以外国际水域，但该国是德国注册的游轮这一事实意味着，根据第 3 条第(3)款的规定，依据国际公法适用成员国法律，从而 GDPR 适用该游轮对个人数据的处理。

虽然与 GDPR 第 3 条第(3)款的适用无关，但根据 1961 年《维也纳外交关系公约》、1963 年《维也纳领事关系公约》或国际组织与所在国在欧盟缔结的总部协定国际法的规定，在欧盟境内设立的某些实体、机构或组织享有特权和豁免。在此方面，EDPB 认为 GDPR 的适用并不影响国际法的规定，例如关于非欧盟外交使团和领事馆以及国际组织的特权和豁免的规定。同时，必须强调任何属于 GDPR 关系范围以及与此类实体、机构和组织交换个人数据的控制者或处理者必须遵守 GDPR，包括其向第三国或国际组织传输数据（如适用）的规则。

4. 设立与欧盟境外的控制者或处理者的代表人

根据 GDPR 第 3 条第(2)款的规定，受 GDPR 约束的数据控制者或处理者有义务在欧盟境内指定一名代表人。因此，未在欧盟内设立但受 GDPR 约束的控制者或处理者如未能在欧盟内指定代表将违反该条例。

这并不是一项全新的规定，因为 95/46/EC 指令已经规定了类似的义务。根据该指令，本条所述的控制者并非在共同体领土内设立，而该等控制者为处理个人数据使用位于成员国领土内的自动化或其他设备。除符合第 27 条第(2)款规定的豁免标准外，根据第 3 条第(2)款而受 GDPR 约束的任何控制者或处理者需在欧盟境内指定代表人。为了便利这一具体规定的适用，EDPB 认为有必要根据第 27 条对欧盟代表的指定程序、设立义务和责任提供进一步的指导。

值得注意的是，设立在欧盟境外的数据控制者或处理者应在欧盟境内指定一名代表。这不属于第 3 条第（1）款的范围，换言之在欧盟境内的代表不会导致成立了 GDPR 第 3 条第（1）款所定义的“实体”。

4.1 指定代表人

序言第 80 条阐明：“数据控制者或处理者应当以书面授权方式明确指定其代表人以代表其履行本条例项下的义务。指定代表人并不影响数据控制者或处理者在本条例项下的义务与责任。该代表人应根据从数据控制者或处理者处获得的授权执行任务，包括与有权监管机构合作，实施任何确保遵守本条例的活动。”

因此，在不影响数据控制者或处理者在 GDPR 项下的义务与责任的条件下，欧盟境外数据控制者或数据处理者应当按照引言第 80 条的要求以书面授权的方式在欧盟境内明确指定其代表人。该控制者或处理者与代表人之间的关系以及各自的义务应当参照该书面授权的规定。在欧盟境内的代表人既可以是自然人也可以是法人。该代表人应当有能力担任欧盟境外的数据控制者或处理者履行 GDPR 项下的义务时的代表。

在实践中，欧盟境内代表的职能可以依据与欧盟境外数据控制者或处理者之间订立的服务协议行使，因此可以由各种不同类别的商业或非商业实体担任，例如律师事务所、咨询公司、私人企业等，只要该等实体设立在欧盟境内。同一实体可以担任多家欧盟境外数据控制者或数据处理者在欧盟境内的代表。

如果该代表是由公司或其他类型的组织担任的，我们推荐制定某一个人担任主要联络人，“负责”其代表的数据控制者或处理者。通常而言有必要在服务协议中明确这一点。

根据 GDPR 的规定，EDPB 认为，在控制者或处理者的处理行为适用 GDPR 第 3 条第（2）款的规定（且不适用 GDPR 第 27 条第（2）款规定的豁免）的情况下，该控制者或处理者无须之于不同的处理行为任命多名代表。EDPB 认为，欧盟境内代表人的职责不等于在欧盟中设立的外部 DPO 的职责。GDPR 第 38 条第 3 款为 DPO 履行其职责拥有足够的自治权规定了一些基本保障，特别是要求控制者或处理者应当确保“DPO 不会收到任何有关执行其工作任务的指示”。此外，引言第 97 条规定，DPO“无论是否是控制者的雇员，都应当独立履行其义务与职责”。这种对 DPO 足够的自治权和独立权的规定似乎与欧盟境内代表人的职能不一致。代表人受制于控制者或处理者的委托，代表其行事，并因此受其直接指导，与 DPO 独立处理工作的要求不一致。

此外，为补充说明这一解释，EDPB 回顾了第 29 条工作组的立场，并强调“如果在诸如涉及数据保护的案例中要求外部 DPO 在法庭上代表控制人或处理人，也可能会产生利益冲突”。

同样，鉴于在执法程序中可能存在的义务和利益冲突，EDPB 不认为数据控制者欧盟境内代表人的作用与该控制者的 DPO 的作用相一致，特别是在职责和合规性方面。

尽管 GDPR 并没有要求数据控制者或其代表人有义务将对代表人的任命通知监管机构，但 EDPB 认为，根据 GDPR 第 13 条第（1）款 a 项和第 14 条第（1）款 a 项的规定，数据控制者应当将对代表人的任命以及代表人的身份告知数据主体，以履行其告知义务，例如通过隐私政策等形式在收集数据之前告知数据主体。设立在欧盟境外且符合第 3 条第（2）款的适用条件的控制者未能告知用户该等代表人的存在以及身份的行为则违反了 GDPR 规定的透明性原则。

例 24: 在例 12 中提及了某设立并在土耳其进行管理的网站提供定制化家庭相册的创建、编辑、打印和寄送服务。该网站提供英语、法语、荷兰语和德语的版本，且支持欧元或英镑付款。该网站声明，仅支持将相册在英国、法国、比荷卢经济联盟国家和德国境内的邮递。根据 GDPR 第 3 条第（2）款（a）项的规定，该网站受 GDPR 的约束，并应当在欧盟境内指定一名代表人。

代表人必须设立在服务接受方的其中一个欧盟成员国内，根据本案例的细节，即网站应当选择在英国、法国、比利时、荷兰、卢森堡或德国境内指定一名代表。数据控制者及其欧盟境内代表的名称和联系方式必须在数据主体开始创建其相册前在线告知该数据主体，并写入网站的一般隐私声明中。

4.2 指定代表义务的免除

尽管 GDPR 第 3 条第（2）款要求于设立于欧盟境外的数据控制者或处理者应当在欧盟境内指定一名代表，但 GDPR 第 27 条第（2）款规定了两种豁免情形：

- 对数据的处理是“偶尔发生的，且不包括第 9 条第 1 款规定的对特殊个人数据的大规模处理或第 10 条规定的有关刑事违法和定罪的数据处理”，且该等处理“依据处理行为的性质、环境、范围和目的，对自然人的权利和自由产生风险的可能性较小”

参考第 29 条工作组的立场，EDPB 认为处理活动只有在如下情况下才能被认定为“偶尔发生的”，即数据处理不是定期进行的，且在控制者或处理者的日常经营范围之外。

此外，尽管 GDPR 并未明确定义什么是对个人数据的大规模处理，但第 29 条工作组先前在关于 DPO 的 WP243 指南中建议，在认定是否属于大规模处理时应考虑如下因素：所涉数据主体的数量——具体数额或所占人口的比例；数据体量和/或正在被处理的不同数据的范围；数据处理活动进行的时长或持续性；以及数据处理活动的地理范围。

最后，EDPB 强调 GDPR 第 27 条的豁免适用的情形是“对自然人的权利和自由产生风险的可能性较小”的处理行为，即不将豁免局限在不会对数据主体的权利和自由产生高风险的处理行为。根据引言第 75 条的建议，在评估对数据主体权利和自由的风险时，应当同时考虑风险发生的可能性和严重性。

或者：

- 该等处理是由“公共机关或团体”进行的。

欧盟境外组织是否构成“公共机关或团体”须由监管机构根据个案的具体情况具体分析。EDPB 认为，考虑到监管机构的任务和目标的性质，第三国组织以公共机关或团体的身份向欧盟境内数据主体提供商品或服务，或监督数据主体在欧盟境内活动的情况较为少见。

4.3 在被处理的个人信息对应的数据主体所在国设立

GDPR 第 27 条第（3）款规定，“代表人应当在拟向其提供或服务而处理的个人信息或监控其行为的数据主体所在的成员国之一设立”。如果被处理的数据对应的数据主体大部分位于某一个特定成员国，作为良好实践，EDPB 推荐该代表人设立在该特定成员国。但是，如果数据主体被提供商品或服务，或其行为被监控，但其所在国没有设立代表人的，则应当保证该等数据主体可以轻易联络到该代表人。

EDPB 认定，代表人设定国别的选择标准为正在被处理的个人数据对应的数据主体所在的国家。数据处理行为所在地（即便在另一个成员国进行）不是选择代表人设定国别的考虑因素。

例 25：印度一家制药公司在欧盟既不存在业务，也没有实体，但根据 GDPR 第 3 条第（2）款的规定，须受 GDPR 的约束。该公司赞助了在比利时、卢森堡和荷兰的研究人员（医院）开展临床试验。参与临床试验的大多数患者位于比利时。

该印度制药公司作为数据控制者，应当在作为数据主体的参与临床试验所在的三个成员国（比利时、卢森堡或荷兰）之一指定欧盟境内的代表人。由于带多数患者是比利时公民，因此建议该代表人设立在比利时。在这种情况下，应当保证荷兰和卢森堡的数据主体和监管机构可以方便地联络到该位于比利时的代表人。

在此案例中，根据欧盟临床试验条例（Regulation (EU) 536/2014）第 74 条的规定，欧盟境内的代表可以是欧盟境界内赞助商的法定代表人，但前提是必须在三个成员国之一设立，且代表人职能的行使须符合各个成员国的法律规定。

4.4 代表人的责任和义务

代表人负责在欧盟境内以控制者或处理者代表该组织履行在 GDPR 项下的义务，特别是与数据主体权利相关的义务。如上所述，组织应当根据第 13 条和第 14 条的要求，将该代表人的身份和联络信息告知数据主体。尽管代表人不负责响应数据主体的权利主张，该代表人应当促进与数据主体和其代表的控制者或控制者之间的沟通，以保障数据主体权利的有效行使。

根据 GDPR 第 30 条的规定，控制者或者处理者的代表应当注意保留其所代表的控制者或处理者处理数据的记录。EDPB 认为，尽管控制者或处理者及其欧盟境内代表人均负有保留对数据处理活动的记录的义务，设立在欧盟境外的控制者或处理者对主要内容以及对记录的更新负责，并应将所有准确和更新后的信息实时提供给欧盟境内代表人，以便该代表人履行其记录义务。同时当发生 GDPR 第 27 条第（4）款规定的特殊情形时，例如监管机关授权代表人处理与数据处理有关的争议，欧盟境内的代表人则全权负责根据 GDPR 第 27 条规定，履行上述义务。

引言第 80 条的规定，该代表应当根据控制者或处理者书面授权的内容履行其职责，包括配合有权的监管机关要求履行 GDPR 项下的义务。

在实践中，监管机构可能就欧盟境外控制者或处理者的数据合规的任何事项联络该代表人，该代表人应当促进监管机构和境外控制者或处理者之间任何信息上或程序上的交流。

如有必要，在团队的帮助下，欧盟境内代表人须有效与数据主体进行沟通，并配合监管机构的工作。此类沟通原则上应当使用监管机构和相关数据主体使用的一种或多种语言进行。如此类沟通将带来不合理的负担，代表人应当采取其他方式和技术以确保有效沟通。因此代表人沟通的便利性对于确保数据主体和监管机构与非欧盟控制者或处理者的方便沟通至关重要。根据 GDPR 引言第 80 条和第 27 条第（5）款的规定，在欧盟境内指定代表人并不影响控制者或处理者在 GDPR 项下的责任和义务，且不影响对该控制者或处理者本身提起法律诉讼。GDPR 并没有对欧盟境内代表人为控制者或处理者履行替代责任作出规定

应当指出的是，GDPR 中引入代表人制度的目的是促进与因 GDPR 第 3 条第（2）款而受到 GDPR 约束的控制者或处理者之间的沟通并保证 GDPR 的有效执行。因此，使得执法者能够通过欧盟境外控制者或处理者指定的欧盟境内代表发起执法行动，包括依据 GDPR 第 58 条第（2）款和第 83 条责令境外控制者或处理者改正或施以行政罚款和行政处罚。代表人的直接责任仅限于 GDPR 第 30 条和第 58 条第（1）款的规定。

EDPB 进一步强调，GDPR 第 50 条的立法主旨为减轻对第三国和国际组织执法的困难，此外，EDPB 正在考虑在此方面加强国际合作。²²

2. 公司 IPO/重组/投融资时，监管部门审查要点汇总及问题分析

一、事件背景

今年 10 月 11 日，证监会第十八届发行审核委员会 2019 年第 142 次发审委员会召开，此次申请上市的企业包括墨迹科技、天迈科技、斯迪克、电声营销 4 家公司。根据会议审核结果公告显示，北京墨迹风云科技股份有限公司的首发未获得通过，也是上述四家企业中唯一首发没有通过的公司。

根据证监会发布的公告显示，发审委员会针对墨迹科技提出的最主要的质询问题包括四个方面，第一，墨迹科技运营的网站、“墨迹天气 App”存在未经其许可违规发布互联网新闻信息，被责令限期整改的情形；第二，墨迹科技通过自主收集及第三方途径获取用户数据及标签，并利用数据进行商业化变现，其中涉及的数据安全问题有待公司说明；第三，报告期内发行人互联网广告信息服务收入占比超过 95%；第四，报告期内与发行人存在直接或间接股权关系的客户（阿里、苏宁、腾

²² 作者：孟洁律师团队，<https://mp.weixin.qq.com/s/vZFQ-XVnfUx588ovAtWSgQ>

讯，以下称“股权相关方”）直接或间接贡献收入金额及占比较大。

其中，较引人注目的地方是第二点，有关墨迹科技数据安全问题。在 2019 年 7 月，App 专项治理工作组对墨迹科技发出《关于 App 收集使用个人信息相关问题的通知》，提出了其相关的数据不合规的问题。对于被点名整改这一情况，墨迹天气相关负责人对媒体表示，墨迹天气最新版本已根据国家标准完善了用户隐私协议，并且已初步通过国家的 App 安全认证初步审核。但此次事件仍旧对其上市造成了影响。

二、该事件有关的数据合规问题分析

在此次发布的公告中，证监会在关于数据安全方面主要提出了五个问题：

（一）数据的收集

公告原文，“发行人获取用户数据及标签的过程及方法，是否对用户有明示提示，用户授权在法律上是否完备，是否明确告知收集信息的范围及使用用途，发行人获取用户数据的手段及方式是否合法合规。”

此问题主要是针对用户数据的收集过程，收集行为作为整个数据生命周期的前端，其合规性直接影响数据后续使用过程的合规性。根据《信息安全技术 个人信息安全规范》（10.22 版）（以下简称“个人信息安全规范”）条款 5.4 中的规定，该条文对个人信息控制者的要求包括：“a) 收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围，并获得个人信息主体的授权同意；”。同时，App 专项治理小组发布的《App 违法违规收集使用个人信息自评估指南》中的评估点 23 也提到了 App 是否向用户明示收集、使用个人信息的目的、方式、范围。

其实，墨迹科技并不是第一例因为数据收集问题导致其在资本市场的发展受到阻碍的案例。许多公司在进行重组或者投融资时，数据收集问题都成为了审批部门关注的问题。具体案例详见下表：

时间	项目名称	证监会反馈意见
----	------	---------

2018.8.2	北京梅泰诺通信技术股份有限公司发行股份及支付现金购买资产并募集配套资金暨关联交易	证监会要求公司补充说明其 对用户信息的收集、传输、保存及应用的现状 是否符合2018年5月1日实施的《信息安全技术 个人信息安全规范》的要求。若否，要求公司充分提示相关风险并说明后续整改措施。
2019.5.13	北京航天宏图信息技术股份有限公司首次公开发行股票并在科创板上市	证监会要求发行人补充披露其主营业务涉及的 数据来源、数据获取方式、数据获取成本、数据使用期限 。
2019.7.1	博拉网络股份有限公司科创板首次公开发行股票	证监会要求发行人说明是否对 数据来源进行分类，数据采集和应用过程中是否获得用户许可 ，是否存在侵犯用户权益(隐私权、肖像权等)的情形。
2019.7.23	广西慧金科吸收合并北京天下秀暨关联交易	证监会要求公司说明标的资产 收集用户数据 的行为是否符合相关法律规定。
2019.9.16	杭州壹网壹创科技股份有限公司首次公开发行股票并在创业板上市网上发行	关于发行人的推广方式，证监会要求发行人区分报告期内发行人合作的线上平台，分别说明发行人进行精准营销采用大数据分析的 数据来源、具体内容、定价及公允性 。
2019.9.24	北京慧辰资道资讯股份有限公司科创板首次公开发行股票	证监会要求发行人说明 获取、分析、使用 业务所涉及的数据是否合规。

数据收集作为整个数据全生命周期的起点，使得数据收集合规工作对整个数据合规工作具有巨大的意义。从上述案例我们可以看出，数据收集的核心焦点在于保证所收集数据来源的合法性。

对于公司直接收集的数据，公司则须履行告知义务并征得用户同意。企业履行告知义务的具体要求和方式方法又因业务场景的不同有所区分。不同场景如个人信息的收集、个人敏感信息的收集以及将个人信息与第三方的共享等情形下的告知义务法律均有不同的要求。

对于通过合作、委托处理等方式间接获取的数据，则需采取必要、适当的手段

进行核实或者签订承诺函等方式保证数据来源的合法性。如根据最新版的《个人信息安全规范（征求意见稿）》，个人信息控制者应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露、删除等；如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意，或通过个人信息提供方征得个人信息主体的明示同意。

综上，我们建议企业在收集用户个人信息之前，一方面应当充分利用隐私政策、用户协议、PBD（Privacy By Design）来履行告知义务，详细说明其所收集的个人信息，及其方式和目的，搭建企业数据合规工作的基石；另一方面，对于间接获取的数据则应当通过签订承诺函并采取合适的措施等方式审查数据来源的合法性。

此外，根据目前的执法趋势，执法机关对于通过“一揽子授权”获得用户个人信息用于市场营销等特殊目的情形则予以严厉打击。运营者还应就不同数据收集使用场景，制定不同的征得用户授权同意方案。

（二）数据的使用

公告原文，“发行人使用用户数据是否合法合规，尤其是商业化变现的合规性，结合相关媒体报道的墨迹天气上传用户隐私等情况，对照《网络安全法》、《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》等法规和司法解释，说明报告期发行人是否存在侵犯用户隐私或数据的情况，是否存在法律风险或潜在法律风险；”

在此问题的问询中，证监会重点关注了当数据进行商业化变现时的合规性问题。数据作为企业的重要资产，其合理的使用能够给公司创在巨大的价值，但其使用也有着诸多限制，突破这些限制就可能引发侵犯用户隐私的风险。

根据《网络安全法》第四十一条的规定，使用个人信息要遵守合法、正当和必要的原则。《个人信息安全规范》第 7.3 条也规定，“使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意；”由此可以看出，使用个人信息的范围应当遵循个人信息主体授权同意的范围。

事实上除了墨迹科技之外，许多公司在进行重组或者投融资时，数据使用问题都成为了审批部门关注的问题。具体案例详见下表：

时间	项目名称	证监会反馈意见
2018.8.2	北京梅泰诺通信技术股份有限公司发行股份及支付现金购买资产并募集配套资金暨关联交易	标的公司通过向第三方数据供应商购买用户数据，因此证监会要求公司补充说明第三方数据商是否具有相关数据的所有权，该 第三方数据商授权 标的公司使用相关数据的行为是否需要经过终端用户或者其他第三方的同意，以及该授权是否合法。
2019.4.8	拉卡拉支付股份有限公司首次公开发行股票并在创业板上市	1、证监会要求发行人进一步说明和披露：发行人是否向剥离公司提供发行人积累的商户信息。 2、证监会要求发行人说明在报告期内发行人对主营业务中形成的个人信息进行使用和维护的合规性，是否存在发行人利用相关商户或个人信息进行牟利等违法违规行为，是否存在侵犯个人隐私、商业秘密或其他侵权方面的情形，是否存在纠纷或潜在纠纷，并提示风险。
2019.5.13	北京航天宏图信息技术股份有限公司首次公开发行股票并在科创板上市	证监会要求发行人补充披露其主营业务涉及的数据来源、数据获取方式、数据获取成本、 数据使用期限 ，说明并披露 授权 第三方使用该等数据是否存在法律障碍。
2019.7.1	博拉网络股份有限公司科创板首次公开发行股票	证监会要求发行人说明是否对数据来源进行分类，数据采集和应用过程中是否获得用户许可，是否存在侵犯用户权益(隐私权、肖像权等)的情形。
2019.9.16	杭州壹网壹创科技股份有限公司首次公开发行股票并在创业板上市网上发行	证监会要求发行人说明在报告期内发行人对个人消费者及企业客户信息等数据资源的 使用和维护的合法合规性 ，是否存在发行人利用相关个人消费者或企业客户信息进行牟利等违法违规行为，是否存在侵犯个人隐私、商业秘密或其他侵权方面的情形， 是否存在纠纷或潜在纠纷，并进行风险提示。
2019.9.24	北京慧辰资道资讯股份有限公司科创板首次公开发行股票	证监会要求发行人说明获取、分析、使用业务所涉及的数据是否合规，是否涉及侵犯个人隐私

		或其他侵权风险，是否存在潜在纠纷，如存在相关风险，请进行风险提示。
--	--	-----------------------------------

在数据商业变现过程中，数据交易也是企业常见的做法之一，从上述案例可看出，授权第三方使用数据行为本身的合规性越来越受到证监会的关注。即向第三方机构提供用户的个人信息，同样需要获得用户的授权同意，如果对法益的侵害达到一定程度，还有可能存在侵犯公民个人信息的刑事风险。根据《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》，《刑法》第二百五十三条之一中规定过的“提供公民个人信息的情形”包括未经被收集者同意，将合法收集的公民个人信息向他人提供等情形。

综上，企业不仅在自己使用用户数据时需要履行法律上的合规义务，当企业向第三方提供公民个人信息以实现相应商业目的时，也同样需要注意获取用户授权同意，避免被认定为非法提供公民个人信息情形的发生。

（三）内部控制制度

公告原文，“数据获取、使用、处理等过程的内部控制制度及执行情况，对数据安全和个人隐私的保护措施与手段，是否出现过个人信息、隐私泄露事件，是否存在纠纷或潜在纠纷。”

对于个人信息保护的监管，不限于对隐私政策等外部制度文件的监管，还包括对公司个人信息保护的内部制度的监管。《个人信息安全规范》第 7.1 条规定了企业对个人信息访问进行的控制措施，要求对被授权访问个人信息的人员，应建立最小授权的访问控制策略，并对安全管理人员、数据操作人员、审计人员的角色进行分离设置等。

除此之外，《个人信息安全规范》第 5.6 条还规定，个人信息控制者制定的隐私政策应当包括“遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明”。

由标准规定的内容可以看出，公司关于数据保护的内部制度也是公司合规义务中重要的一部分。公司要注重加强在内部管理上的文化和制度建设，以避免潜在的信息安全事件。《个人信息安全规范》第 5.6 条没有阐述公开数据安全和个人信息保护相关的合规证明的“必要”的具体情景，根据司法实践，此情景可能发生在用

户提出要求，监管部门进行核查或者发生数据安全事件时作为免责事由的证明等。无论在何种情境中，企业内部的合规建设都有着重要的作用。

企业内部数据安全内控制度的建设情况同样是审批部门重点关注的问题，具体案例详见下表：

时间	项目名称	证监会反馈意见
2018.6.22	茂业通信网络股份有限公司行政许可申请	证监会认为公司标的资产在从事移动信息发送及金融服务外包业务时存在泄露用户个人信息的风险，因此要求公司补充披露其标的资产在提供服务过程中掌握的个人信息已采取的 防泄密措施 及其效果。
2018.12.9	中孚信息股份有限公司发行股份及支付现金购买资产并募集配套资金暨关联交易	证监会要求公司补充披露剑通信息在提供产品、服务过程中对掌握的个人信息、国家安全信息所采取的 防泄密措施 及其效果，以及是否有泄露国家秘密、个人隐私的风险。
2019.1.25	南威软件股份有限公司公开发行可转换公司债券募集	证监会要求发行人说明： 1、开展现有业务、本次募投项目是否需要依法进行 信息安全等级保护测评 ； 2、发行人是否已就维护网络安全、保护个人、政府以及第三方信息安全等事项建立了完善的 内部控制制度 ，以及该制度的执行是否有效。
2019.3.12	三六零安全科技股份有限公司非公开发行股票申请	证监会要求申请人补充披露在提供产品、服务过程中对掌握的个人信息及国家安全信息所采取的 防泄密措施 及效果，有无泄露国家秘密、个人隐私的风险。
2019.4.8	拉卡拉支付股份有限公司首次公开发行股票并在创业板上市	证监会要求发行人补充说明在开展业务过程中能否获取用户相关个人信息和商业秘密等用户数据，是否已 建立完善防泄密和保障网络安全的内部管理制度 。

2019.5.6	优刻得科技股份有限公司科创板首次公开发行股票	证监会要求发行人补充说明: 数据安全相关制度及措施 ,包括但不限于数据的备份机制、防范数据窃取及泄露的措施、对用户隐私数据加密措施以及对于到期数据的处理机制。
2019.5.31	深圳和而泰智能控制股份有限公司发行可转换公司债券	证监会要求申请人说明:开展现有业务、本次募投项目是否需要 进行信息安全等级保护测评 ;
2019.6.25	贵州白山云科技股份有限公司科创板首次公开发行股票	证监会要求发行人说明在其具体业务中 防止客户数据向外泄露的措施 及其有效性。
2019.7.1	北京值得买科技股份有限公司首次公开发行股票并在创业板上市	证监会要求发行人说明对用户 个人信息采取的保护措施 ,并就对用户个人信息保护不到位可能引致的风险作风险提示。
2019.7.23	广西慧金科吸收合并北京天下秀暨关联交易	证监会认为公司在业务经营过程中存在影响标的资产信息系统正常运行;导致标的资产信息数据资源泄露;以及导致用户隐私信息泄露或不当使用的风险,因此要求公司补充披露:标的资产对提供产品、服务过程中掌握的数据资源以及个人隐私所采取的 防泄密措施 及其效果,有无泄密风险。
2019.9.16	杭州壹网壹创科技股份有限公司首次公开发行股票并在创业板上市网上发行	证监会要求发行人说明实施的 数据备份和网络安全措施 以及发行人是否曾发生泄漏客户信息的风险事件,是否存在被处罚或被要求赔偿的风险;发行人相关 客户信息保密工作 是否符合《中华人民共和国网络安全法》的规定。
2019.9.24	北京慧辰资道资讯股份有限公司科创板首次公开发行股票	证监会要求发行人说明相关 内部控制措施 是否健全且得到有效执行。
2019.10.14	荣科科技股份有限公司重组项目	证监会要求申请人具体说明对外包人员 接触病案及个人隐私的保护措施 ,如何确保病案涉及的个人信息、隐私不被盗取、泄漏。

基于以上监管案例，我们建议拟上市企业还应构建和完善企业内部管理制度，主要包括领导决策、人员管理、安全技术方面的管理制度以及风险管理制度三个维度。

领导决策

根据最新版《个人信息安全规范（征求意见稿）》第 10.1 条的规定，法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等。在实践中，公司多采取在内部设立委员会的方式，对公司的数据合规策略与治理进行共同决策。

2、人员管理制度

对于新入职员工，企业应当组织个人信息保护方面的培训并与其签署保密协议。对于在职员工，要明确信息保护的权责，设立专职的个人信息保护负责人和个人信息保护工作机构，形成个人信息保护工作的责任制。对于离职员工，应当要求在一定时期继续履行保密义务。

3、安全技术方面的管理制度

安全技术方面的管理制度包括访问权限管理制度、数据加密管理制度、信息系统安全等级保护制度等。第一，在权限管理制度的构建上，企业应做对被授权访问个人信息的人员，建立最小授权的访问控制策略，使其只能访问职责所需的最少的个人信息。同时对于重要数据访问的请求方、授权方、管理方应当实现职责分离，不同级别的访问权限需要专人审批。对于外部人员访问相关数据，则应签订相关的保密协议，对其访问进行监督等。第二，企业在进行数据的存储、传输等过程中要严格进行加密措施，常见的加密措施包括 MD5 等。第三，企业需要构建信息系统安全等级保护制度，制定等保指引文件并按照文件要求落实系统定级、网络备案、网络安全建设整改、等级测评、企业自查等工作。

4、应急事件管理制度

企业应当构建和完善应急事件的管理制度。首先，企业应当成立专门的应急处置小组，面对数据安全突发事件应立即采取初步补救措施，并对相关部门人员进行追责。其次，评估事件可能造成的影响，并采取必要措施控制事态，消除隐患。再次，企业应按《国家网络安全事件应急预案》的有关规定和要求及时上报。最后，

企业应按照法律规定履行安全事件的告知义务并进行后期整改建设。

（四）监管趋势下的业务影响

公告原文，“日益加强的数据行业监管及个人隐私保护政策对发行人业务的影响及相关应对措施”。

自 2016 年《网络安全法》颁布以来，我国相继出台了许多的法律法规来保障数据收集和使用的安全。包括《数据安全管理办法（征求意见稿）》、《儿童个人信息网络保护规定》、《个人信息安全规范（征求意见稿）》等等。在层层监管下，对于企业来说，合规建设也需要包含内外部契约的制定：

- (1) 外部契约：无论是对于用户还是对于监管机构，像隐私政策和用户协议等外部契约，是其展示自身合规水准的第一层标签。做好外部制度的建设，也是规避法律风险的第一道屏障；
- (2) 第三方契约：不同于外部契约，第三方契约是企业与和其业务有关联的第三方合作方所签订的相关契约。因为数据流转是数据生命周期流程中非常重要的一个环节。当企业从第三方获取数据，需要第三方保障数据来源的合法性；如果是企业向第三方共享数据，需要获得用户的授权同意、对第三方的安全能力要进行安全评估、并且对共享后第三方处理数据的行为进行合理审计。
- (3) 内部制度：内部制度建设是防止信息安全事件最重要的一个环节。从数据内部使用的审批制度，到数据每一个收集使用环节的审计制度，到发生信息安全事件时的应急响应制度，每一个步骤都达到相应的合规标准才能增强企业对个人信息整体保护能力。

（五）整改情况及整改效果

公告原文，“发行人针对 APP 专项治理工作组通知指出问题的整改情况及整改效果，是否获得主管部门的认可，是否面临被处罚的风险。”

从 2018 年下半年开始，监管部门开始加强对 App 的监管。App 专项治理小组，消费者保护协会等部门开始对市场上热门的 App 进行测评并发布公告，对不

合规的企业进行点名批评，并对其约谈要求整改。最近工信部发布《关于开展 APP 侵害用户权益专项整治工作的通知》，针对 APP 服务提供者和 APP 分发服务提供者的四个方面、八个突出问题进行 APP 专项整治。

目前，法律法规中对于违法违规收集使用个人信息的处罚方式包括，公开曝光、约谈、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等；构成犯罪的，还会依法承担相应的刑事责任。在具体实践中，监管部门往往会采取先测评，根据测评结果进行整改，如果整改不力进行约谈的步骤，若企业仍旧不及时更改相应不合规的问题将面临相应的处罚。

根据墨迹科技的回应，墨迹天气已对隐私政策进行修改和完善，也通过了 App 安全认证初步审核。不过，这一问题仍对其 IPO 造成拖累。由此企业需要警惕，不要只等到监管机构曝光之后才对不合规的问题进行整改，否则被点名或约谈的记录仍然会对企业后续业务以及声誉造成影响。在监管找上门来之前，先构建好自身的合规体系对企业未来在资本市场的发展有着重要意义。

综上所述，我们认为企业首先应当充分认识数据合规工作的重要性以及对公司发展的影响，特别是在进行 IPO、重组、投融资时应当注重数据合规，梳理数据资产，分析公司现有业务存在的风险与问题，再针对这些问题有针对性地进行有效整改，从而保证公司为数据资产提供全生命周期的安全保护。在上市或完成重组或投融资后，应当持续关注我国关于数据以及个人信息的立法动态，及时完善公司的数据合规策略，并在企业进行数据共享、转让、公开披露，发生重大安全事件或者公司业务模式、信息系统、运行环境发生重大变更时进行个人信息安全评估。对整个制度以及机制的落实情况也要随着上市过程、投融资进展审查是否完整落实，针对一些不合适的地方，还要考虑进行调整与优化。需要组织人员进行培训，对梳理出来的问题整改情况与法律法规的跟踪变化进行比对并进一步复盘并更新完善，最后构成一个有效的合规闭环。

数据合规非一日之功，建议企业在监管趋严的趋势之下，及早考虑并完成数据合规，不要等到重大投资决策时方才为了应对监管或者为了完成交易而匆忙补课、临时抱佛脚地进行整改。如果拟上市企业需要体系化制定数据合规架构的，也可以考虑聘请相关专业律师团队协助企业开展企业数据全生命周期的合规治理。²³

²³ 作者：孟洁律师团队。

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

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

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