NEWSLETTER

数据合规

2019 第九期 /总第九期

数据合规时事速递

北京市环球律师事务所

2019 年 10 月 8 日

目录

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。据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

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. 工信部《关于促进网络安全产业发展的指导意见（征求意见稿）》公开征求意见

2019 年 9 月 27 日，为贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，工业和信息化部会同有关部门起草了《关于促进网络安全产业发展的指导意见（征求意见稿）》（见附件），现面向社会公开征求意见。

总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平总书记关于网络安全的系列重要讲话精神，坚持新发展理念，树立正确的网络安全观，贯彻落实《网络安全法》，以服务国家网络空间安全战略需求为导向，主动应对互联网、大数据、人工智能和实体经济深度融合伴生的新风险，积极应对 5G、工业互联网、下一代互联网、物联网等新技术新应用带来的新挑战，坚持市场主导、政府引导，着力突破关键技术、构建产业生态、优化发展环境，推动我国网络安全产业高质量发展，为维护国家网络空间安全、保障网络强国建设提供有力的产业支撑。

（二）基本原则

创新驱动。大力推动技术、产品创新，突破技术瓶颈，着力提升网络安全核心技术能力。创新网络安全服务模式，提升网络安全专业化服务水平，实现产业发展逐步由产品主导向服务主导转变。

协同发展。充分调动各方力量，加强产学研合作，鼓励技术成果转化，推动强强联合、协同攻关，构建多方参与、优势互补、融合发展的产业生态体系。推动产融合作，引导社会资本参与网络安全产业发展。

需求引领。推动各行业各领域持续加大网络安全投入，坚持问题导向，加强供

需对接，促使产业更好满足金融、能源、通信、交通、电子政务等重点领域网络安全需求。

开放合作。推动网络安全产业国际交流合作，学习借鉴国外产业发展模式，促进技术、人才交流和信息共享，积极参与“一带一路”建设，提升产业国际竞争力。

（三）发展目标

网络安全技术创新能力显著增强，网络安全产品和服务体系更加健全，网络安全职业人才队伍日益壮大，政产学研用资协同发展的网络安全产业格局不断巩固，产业发展环境更加优化，网络安全产业维护国家网络空间安全、保障网络强国建设的支撑能力大幅提升。到 2025 年，培育形成一批年营收超过 20 亿的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿。

主要任务

（一）着力突破网络安全关键技术

以构建先进完备的网络安全产品体系为目标，聚焦网络安全事前防护、事中监测、事后处置、调查取证等环节需要，大力推动资产识别、漏洞挖掘、病毒查杀、边界防护、入侵防御、源码检测、数据保护、追踪溯源等网络安全产品演进升级，着力提升隐患排查、态势感知、应急处置和追踪溯源能力。加强 5G、下一代互联网、工业互联网、物联网、车联网等新兴领域网络安全威胁和风险分析，大力推动相关场景下的网络安全技术产品研发。支持云计算、大数据、人工智能、量子计算等技术在网络安全领域的应用，着力提升威胁情报分析、智能监测预警、加密通信等网络安全防御能力。积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。

（二）积极创新网络安全服务模式

针对网络安全专业性强、技术演进快、应用难度大的特点，倡导“安全即服务”的理念，鼓励网络安全企业由提供安全产品向提供安全服务和解决方案转变。支持专业机构和企业开展网络安全规划咨询、威胁情报、风险评估、检测认证、安全集成、应急响应等安全服务，规范漏洞扫描、披露等活动。支持合法设立的认证机构

依法开展网络安全认证。大力发展基于云模式的网络安全公共服务平台，提供远程实时在线的漏洞发现、网站防护、抗拒绝服务攻击、域名安全等服务。鼓励基础电信企业和云服务提供商发挥网络资源优势，面向客户提供网络安全监测预警、攻击防护、应急保障等增值服务。鼓励发展面向智慧城市建设、电子政务等领域的网络安全一体化运营外包服务。探索开展网络安全保险服务。

（三）合力打造网络安全产业生态

支持龙头骨干企业整合网络安全创新链、产业链、价值链，建立开放性网络安全技术研发、标准验证、成果转化平台，畅通创新能力对接转化渠道，实现大中小企业之间多维度、多触点的创新能力共享、创新成果转化和品牌协同。着力培育主营业务突出、竞争能力强、成长性好的网络安全中小企业，鼓励以专业化分工、服务外包、共享研发等方式与大企业相互合作，形成协同共赢格局。充分调动各类园区、企业、科研院所、金融机构等主体的积极性和主动性，鼓励集聚、集约、关联、成链、合作发展。培育建设一批网络安全技术、产品协同创新平台和实验室，开展共性重要问题和市场亟需方向的联合研究，充分发挥科技支撑引领作用，推动产业共性技术研发和推广应用，引导创新资源集聚。鼓励企业、研究机构、高校、行业组织等积极参与制定网络安全相关国家标准、行业标准。

（四）大力推广网络安全技术应用

充分发挥党政机关和相关行业主管部门作用，推动先进适用网络安全技术产品和服务在金融、能源、通信、交通、电子政务等重要领域的部署应用。加强工业互联网、车联网、物联网安全管理，督促指导相关企业采取必要的网络安全技术措施。大力促进商用密码技术在网络安全防护中的应用。财政投资的信息化项目应当同步配套建设网络安全技术设施，并单独开展安全验收。加大对网络安全技术应用试点示范项目的支持推广力度，鼓励示范企业将解决方案转化为标准指南并开展专题宣讲。鼓励开展网络安全技术论坛和产品服务展示活动。

（五）加快构建网络安全基础设施

推动相关行业主管部门、地方政府建设本行业、本地区网络安全态势感知平台，着力提升支撑网络安全管理、应对有组织高强度攻击的能力。鼓励重点行业、骨干企业建设漏洞库、病毒库等网络安全基础资源库，促进相关主体之间的信息共享。统筹建设国家网络安全信息共享平台和应急指挥平台，实现跨企业、跨行业、跨地区信息共享和协调联动。重点围绕工业互联网、车联网、物联网新型应用场景，建

设网络安全测试验证、培训演练、设备安全检测等共性基础平台。支持构建基于商用密码、指纹识别、人脸识别等技术的网络身份认证体系。

保障措施

（一）加强组织领导

各地相关部门要从网络强国战略高度充分认识发展网络安全产业的重要意义，加强组织领导和统筹谋划，强化部门合作，共同营造有利于网络安全产业发展的良好环境。深入贯彻落实《网络安全法》，加快制定配套法规政策，加大网络安全监管力度，督促网络运营者落实网络安全技术措施，带动网络安全市场需求。

（二）加大政策支持力度

中央网信办指导支持国家网络安全人才与创新基地建设，会同相关部委推动网络关键设备和网络安全专用产品认证和安全检测结果互认，避免重复认证、检测。工信部推动国家网络安全产业园区建设，建立网络安全产业运行监测体系，组织开展网络安全技术应用试点示范，指导举办中国网络安全产业高峰论坛。国家发展改革委加强网络安全领域规划、政策研究制定。中央财政统筹利用中国互联网投资基金等现有渠道，引导支持网络安全产业发展。各地可结合本地实际情况，在财政、人才引进、要素保障等方面研究制定有针对性的产业扶持政策。

（三）健全人才培养体系

推动高校设立网络空间安全学院或网络安全相关专业，加强一流网络安全学院和网络安全师资队伍建设。加强网络安全职业教育和技能培训，培养更多实用技能型人才。推动校企对接，支持设立网络安全联合实验室。鼓励举办高水平网络安全技能竞赛，健全人才发现选拔机制。支持职业技能鉴定机构、行业协会等开展网络安全人员技能鉴定和能力评定工作。

（四）推进国际交流合作

利用各种多边、双边对话机制或活动平台，加强网络安全技术、产业务实合作与交流。鼓励有实力的网络安全企业设立海外研发中心和联合实验室，引进海外高

端人才和先进技术。鼓励参加和举办有影响力的网络安全国际论坛和展会，积极参与网络安全国际标准制定和协调。推动相关地方发挥区位优势，打造国际、区域性网络安全技术、产业、人才交流平台。[1]

2. 加州消费者隐私保护法案 CCPA 最终版出炉，于 2020 年 1 月 1 日正式生效

2019 年 9 月 13 日，《加州消费者保护法案》进行了最后一次修改，修改后的法案交地方行政长官签署后，将于 2020 年 1 月 1 日起正式生效。

《加州消费者保护法案》从它开始起草到修订就引发了各界人士的关注，其原因主要是因为第一、相对于布鲁塞尔对欧盟隐私法立法的影响一样，加州一直对美国的隐私法有着示范效益，数十年来一直引领着美国隐私法的走向。可以想见，一旦《加州消费者保护法案》颁布，必然会成为美国各州模仿的对象。第二，《加州消费者保护法案》是在 GDPR 颁布实施一年多以后才即将颁布的，是在 GDPR 的基础上取长补短、吸收其中之精华而发展而来的，所以，它的实施也会给还没有完整的隐私立法的国家带来巨大的借鉴作用，从而形成与 GDPR 在全球隐私法立法领域抢地盘的局面。

《加州消费者保护法案》相较于 2018 年版本的主要修改点如下：

1. AB25 条把员工信息暂时排除在《加州消费者保护法案》适用范围之外，直到 2021 年 1 月 21 日才开始适用。也就是说原来提议里的想把企业在招聘、雇佣员工时候获得的信息排除在整个《加州消费者保护法案》之外的想法并没有得到此次修改的支持。相反的，《加州消费者保护法案》仍然适用于企业对于员工人力资源信息的收集和适用，只不过给了企业关于这类信息一年的宽限期。

2. AB1564 条增加了企业暂时不需设立免费呼叫中心的豁免，允许仅仅从事线上业务且与客户有直接联系的企业为客户提供电子邮件的方式来行驶《加州消

[1] 工业和信息化部。

费者保护法案》下赋予客户的各种权利。

3. AB874 条对于个人信息的定义增加了“合理”，且从个人信息的定义中删除了公共可用信息，即，如果某种信息是从联邦政府、州政府或者当地政府合法取得的信息，则该等信息不再被定义为个人信息。

4. AB1355 条在个人信息的定义中排除了脱敏、以及汇总的数据；

5. 同时，对于企业对企业（B2B）的网络运营者，增加了一年的免除《加州消费者保护法案》适用的缓冲期，但仅限于： a)在企业尽职调查中获取的其他公司、非盈利性机构、政府单位的信息；或 b)向其他公司、非盈利性机构、政府单位提供产品或服务、或接受产品或服务而获取的信息；

6. 明确了消费者信用调查机构、信用信息报告机构或使用消费者报告的使用者（如雇主）对信息的使用和披露不受《加州消费者保护法案》规制，而受《美国公平信用报告法》规范。但此豁免在数据泄露的时候则不再适用，消费者可以根据《加州消费者保护法案》项下的隐私权利提起诉讼。

7. AB1202 创设了数据中介的登记注册要求，企业需要衡量其是否构成了《加州消费者保护法案》项下收集及出售与其没有直接客户关系的客户信息的“数据中介”。

《加州消费者保护法案》（以下简称 CCPA）与 GDPR 在很多方面有所不同。首先 CCPA 和 GDPR 在适用的范围、收集信息的限制的程度、以及责任条款都不相同。整个 GDPR 都要求有一个合法基础来处理数据，但 CCPA 并没有此基础性要求。此外，CCPA 排除了在其他法律有规制的领域的信息的适用，比如医疗行业。CCPA 更强调信息处理、转移的透明度，赋予消费者随时要求商家披露信息走向、信息种类、信息的具体内容的权利，允许消费者选择“禁止交易倒卖我的个人信息”。在信息收集处理企业收购和转让时，允许企业选择拿回自己的信息，不再交付给收购和转让的继任者。[2]

[2] V 字号。

3. 美国外资审查实施细则出炉，新定义“个人敏感信息”

美国财政部近日针对外国资本监管出台具体规则，赋予去年通过的 FIRRMA 实质性意义，该法案最晚将于 2020 年 2 月 13 日生效，届时 CFIUS 将对外来投资拥有更大审核实权。

2018 年 6 月 18 日，美国参议院正式通过旨在扩大美国外国投资委员会权限的《外国投资风险审查现代化法案》。FIRRMA 为改变 CFIUS 运作方式以及扩大 CFIUS 对外国投资审查范围奠定基础。

此次出台的规则是对 FIRRMA 进行具体细化，分为两个部分：第一部分是长达 184 页的 31 CFR part800，负责执行 FIRRMA 大多数条款；另一部分是长达 135 页的 31 CFR part 802，作为补充条款，主要针对如何审核涉及房地产方面的投资。

这份细则显示，美国政府已将目光放在审查更多的房地产交易，并对以数据为中心的企业采取更有针对性的做法，同时首次考虑针对具体国家的豁免。

这份规则中提出很多新定义，这些新定义给予 CFIUS 较大裁量权。其中一个重要定义就是“个人敏感信息”，FIRRMA 认为如果让某些外国公司维护或收集美国公民的敏感个人数据，这些数据可能会被利用并威胁美国国家安全。

针对这一担忧，拟议细则特别规定凡交易对象所提供服务和产品包含美国政府人员或承包商的数据或涉及 100 万人以上数据，都将被严密审核。例如，交易若涉及研究消费习惯、GPS、生物识别以及处理政府人员安全许可公司都可能会被审查。

细则也对涉及关键基础设施的投资给予特别关注，加强对房地产领域投资审核被认为是 CFIUS 最大扩权领域，因为报告认为某些交易中的房地产地理位置会给美国国家安全带来风险。今后即便是购买未开发土地，也有可能受到 CFIUS 审查。接受审核的房产交易将包括临近机场、海港、军事和政府设施的房产， CFIUS 可以审查外国人购买军事设施或敏感政府设施周边 1.6 至 160 公里以内房产投标。

相对于对房地产投资的明确定义，对涉及关键科技的投资则仍有些模糊，这种缺乏明确性和确定性的情况将继续影响跨境收购和投资。美国财政部仍在研究对

关键科技投资的强制申报范围。去年 10 月，财政部推出了允许 CFIUS 审查更大范围交易的试点项目，以国家安全为由审查外国人与持有关键技术的美国企业成立合资公司或对其进行小规模投资的交易。这些试点为如何制定强制备案规定提供了新视角和新问题，将被添加至新规中，最终规则将于 2020 年 2 月出台。

另外一个值得注意的问题是 FIRRMA 此前没有针对任何特定国家，但拟议细则表明 CFIUS 正在使这项法规变得针对某些特定国家。新规将给予一些国家豁免（excepted foreignstates），被豁免国家名单将由 CFIUS 决定，必须要绝对多数票数才能通过，会在美国财政部网站公布。

新规将在明年 2 月正式实施，从此美国对外资审核将进入新阶段，这个阶段的一个标志性特征就是程序多、时间长。据悉，对于非房地产交易，CFIUS 将审核期限延长至 45 天，并可能在特殊情况下将该期限延长 15 天。房地产交易审查期限则更长，最长可能是常规 45 天加额外 45 天后续调查，再加上 15 天延期调查特殊情况。这意味涉及房地产的投资交易可能需要 105 天审查期。

虽然新规并未提及特别针对中国，但分析人士普遍认为这会影响未来中国对美投资，因为 CFIUS 审核已经使中国对美投资呈收缩态势。过去十年间，中国对美国的投资一直在加速，大量资金涌入汽车、科技、能源和农业领域，为密歇根、南卡罗来纳、密苏里、得克萨斯等州创造大量就业机会。随着中国经济蓬勃发展，州和地方政府以及美国公司都在争相寻求中国资本振兴当地经济，但特朗普的经济冷战扼杀这一趋势。

著名智库美国企业研究所（AEI）的数据显示，中国对美直接投资从 2016 年 541 亿美元峰值降至 2018 年的 97 亿美元。截至今年 6 月数据，中国大陆企业对美投资的规模为 25 亿美元。该智库数据显示，自 2005 年以来，中国对美投资主要集中在房地产、金融、科技、旅游、交通、能源和娱乐等领域， 其中房地产是最热门投资项目，达到 286 亿美元，其次是金融（259 亿美元）、交通（222 亿美元）和科技（217 亿美元）。接受投资最多的州是纽约州，高达 567 亿美元，其次是加州（372 亿美元）、伊利诺伊州（122 亿美元）和弗吉尼亚州（117 亿美元）。

虽然新规将于明年 2 月实施，但已对中国投资带来寒蝉效应。纽约荣鼎咨询报告认为中资对美企投资情况存在巨大不确定性，因为在 FIRRMA 出台后，投资者组成型态、及目标产业和技术发生明显变化。例如，中国创投资本已试图避开 CFIUS 密切关注的那些行业，比如人工智能、数据分析和网络安全。

上述报告还称，去年大约 40%的中资创投交易案集中在生物科技和制药企业。然而，美国国际战略研究中心（CSIS）防务与技术专家詹姆斯·李维斯（JamesLewis）表示，随着 CFIUS 加强对生物科技领域外资的审查，中资在该领域投资可能会变得更加困难。不仅如此，中资在电信领域投资也可能变得愈加艰难，纽约州参议员、民主党领袖查克·舒默（ChuckSchumer）正在呼吁联邦通信委员会（FCC）考虑阻止中国两家主要电信公司在美国开展业务。

面对新规带来的巨大风险和不确定性，中国资本该如何应对？CFIUS 前官员史蒂芬·海菲茨（StephenHeifetz）对《财经》记者指出，美国政治体系依靠周期性调整 CFIUS 以回应对外资的关切，新立法是过去几十年来对外国投资的一系列反应之一，这些反应与公众对国家安全关切交织在一起，即很多美国人都认为美国长期以来应对国际事务的方法并未奏效，其中就包括开放的投资政策。然而，美国科技公司受益于吸引包括中国在内的全球投资资本，在某种程度上，FIRRMA 可能会抑制投资，阻碍美国技术领先地位且削弱其利益。

在海菲茨看来，CFIUS 审查结果在很大程度上取决于交易细节以及应对 CFIUS 规则的方法。中国公司应该与经验丰富的 CFIUS 律师一起应对收购和投资交易，以便了解哪些交易是可行的。许多收购和投资仍然可能进行，但需要充分了解 CFIUS 风险、审核时间表以及如何将风险成本和时间成本最小化。[3]

[3] 《财经》杂志。

二、监管动态

1. 工信部《关于进一步做好电话用户实名登记管理有关工作的通知》要求实体渠道电话入网要人像对比

2019 年 9 月 27 日，工信部官网发布公告，称为依法推进电话用户实名登记管理，切实维护公民在网络空间的合法权益，有效适应防范治理电信网络诈骗等工作面临的新形势、应对新挑战，工信部办公厅印发了《关于进一步做好电话用户实名登记管理有关工作的通知》，指导电信企业扎实开展电话用户实名登记工作，夯实网络诚信体系建设基础。

此次印发《通知》，从夯实基础管理、加大防范治理、强化技术监管三方面提出了 11 项具体举措加强管理，进一步巩固工作成效。一是为确保电话入网环节人证一致，创新运用人工智能等技术手段，要求电信企业**自 2019 年 12 月 1 日起在实体渠道全面实施人像比对技术措施，人像比对一致后方可办理入网手续。**二是深入防范治理二次倒卖电话卡，各电信企业应于 2019 年 11 月底前，完善电信服务协议条款，明确用户不得二次转售、倒卖电话卡，并充分运用海报、广告、短信等多种方式积极开展宣传提醒，引导用户至正规营业场所购买电话卡。三是积极防范用户名下不知情办卡，要求电信企业自 2019 年 12 月 1 日起通过自有营业厅向用户提供查询名下手机号码的服务，对用户提出存在异议的手机号码应立即组织核查和处理，切实维护群众合法权益。[4]

2. 上海市政府发布《上海市公共数据开放暂行办法》官方解读

办法背景

上海市政府新闻办 9 月 25 日举行市政府新闻发布会，市政府副秘书长陈鸣波介绍了近期出台的《上海市公共数据开放暂行办法》。市经济信息化委主任吴金城，市政府办公厅副主任、市大数据中心主任朱宗尧，市司法局副局长罗培新出席发布

[4] 工业和信息化部。

会，共同回答记者提问。

公共数据开放是促进数字经济发展、保障社会民生的重要推动力，也是推进政务公开，提升政府管理理念、实现政府治理能力现代化的内在要求。上海市委、市政府高度重视公共数据开放利用，自 2012 年起在全国率先探索公共数据开放工作。2017 年至 2019 年，上海连续三年在第三方测评的中国地方政府数据开放排名中位列第一。日前，《上海市公共数据开放暂行办法》（以下简称《办法》）已经市政府常务会议审议通过，将于今年 10 月 1 日正式施行。

《办法》制订的总体考虑

《办法》作为国内首部针对公共数据开放的地方政府规章，将指导本市公共数据开放利用工作进入全新阶段。重点考虑了四个关系：

一是开放服务和管理责任的关系，公共数据开放是公共服务的重要内容之一，要面向市场和社会提供有效数据资源，通过开放利用，服务人民群众对美好生活的需求。同时，公共管理部门要建立完整的数据开放标准和规范，明确相关管理权限和义务。

二是数据开放和数据安全的关系，既要推进公共数据开放和深度利用，又要高度重视和保障数据安全、合法合规。制定严格的全流程数据安全保护措施，是此次立法工作的重要考量。

三是国际通行原则和上海实际情况的关系，在参考“完整、时效、原始”等国际通行原则基础上，将分级分类、脱敏脱密、匿名处理等作为开放前的重点要求，充分保护个人隐私、商业秘密等第三方合法权益，面向不同利用主体提供多种开放方式。

四是统一平台开放和多元合作生态的关系，要求公共数据按照统一标准，通过统一门户开放。同时，鼓励引导市场主体开展数据治理、提供数据服务、规范数据利用，共同打造健康、包容的生态体系，使数据赋能各行各业，助力数字经济发展。

《办法》的主要内容

《办法》共 8 章 48 条，明确总体原则、开放机制、平台建设、数据利用、多元开放、监督保障、法律责任等内容。

一是以安全可控为基本原则，分工推进公共数据开放。本市公共数据开放工作以“需求导向、安全可控、分级分类、统一标准、便捷高效”为原则，明确职责分工，并在总则中设立专门条款强调数据安全保护责任，防止公共数据被非法获取或不当利用。对公共数据开放重大事项进行统筹协调，引入专家委员会机制，增强公共数据开放工作的科学性和专业性，不断提升全市对于数据开放的认识水平和服务能力。

二是有序推进、主动服务社会需求，建立数据开放利用长效机制。在前期工作基础上，一方面主动制定开放清单，另一方面对接社会需求，根据年度开放重点，优先开放与民生紧密相关、社会迫切需要、行业增值潜力显著和产业战略意义重大的高价值公共数据。在国内首次提出分级分类开放模式，对开放数据进行标准化、精细化管理，提升开放数据质量，不断满足社会公众对公共数据的需求。

三是以统一平台为开放渠道，全面提升服务能力和安全保护水平。依托市大数据资源平台，建设统一标准、统一管理的公共数据开放平台，全面提升公共数据开放的服务能力。明确平台管理制度，建立透明化、可审计、可追溯的全过程管理机制，采取行为记录、数据纠错、权益保护等措施，打造高效便捷、安全可靠的服务载体。

四是以合法正当为数据利用原则，鼓励数据开发与加强行为监管并重。要求数据利用应当以合法正当、不得损害国家利益、社会公共利益和第三方合法权益为前提，在此基础上，鼓励开展多种形式的公共数据利用活动，特别鼓励数据利用的成果应用于行政监管和公共服务，对社会价值、市场价值显著的案例进行示范展示。另一方面，建立数据来源披露、利用情况跟踪、违规行为举报等制度，防范违法违规行为。例如，对采用非法手段获取、超出规定应用场景等行为，采取严格的关闭使用权限和实施公示披露等措施。

五是打造融合创新的生态体系，助力数字经济发展。通过产业政策引导、社会资本引入、应用模式创新以及优秀服务推荐、联合创新实验室等方式，推动“产学研用”协同发展，营造良好的数据应用创新生态。同时，推动公共数据和非公共数据的多元融合和规范流通，推动建立数据开放标准体系、技术规范，开展国内外交流合作，提升本市公共数据治理和创新应用能力，助力数字经济高质量发展。

六是守牢法律责任底线，建立多重监督保障制度。明确数据开放、数据利用、平台管理、安全管理等各个主体的法律责任和安全管理义务。通过设立专人专岗、加强专业培训、开展考核评估、合理责任豁免等多方面制度，加快提升各主体的专业性和积极性，保障数据开放工作的有力推进。

公共数据开放利用工作是一项前瞻性、系统性的工作，需要在不断实践中优化和创新。目前，根据社会需求确定了普惠金融、交通出行、医疗健康、文化旅游四个领域作为今年的开放重点。特别在普惠金融方面，上海已经开展了 8 个部门和 4 家试点银行间、以企业主体相关公共数据的授权开放应用试点，助力解决小微企业融资难、融资贵的问题，力争今年年底见实效。接下来，上海将加快《办法》的落地实施，加强组织协调、督促落实机制，安全有序推进各项工作。在实践中不断完善《办法》，加快提升政府公共治理能力水平，为经济社会高质量发展注入新的动力。

办法原文

上海市公共数据开放暂行办法

（2019 年 8 月 29 日上海市人民政府令第 21 号公布）

第一章　总则

第一条（目的和依据）

为了促进和规范本市公共数据开放和利用，提升政府治理能力和公共服务水平，推动数字经济发展，根据相关法律法规，结合本市实际，制定本办法。

第二条（适用范围）

本市行政区域内公共数据开放及其相关管理活动，适用本办法。

涉及国家秘密的公共数据管理，按照相关保密法律、法规的规定执行。

第三条（定义）

本办法所称公共数据，是指本市各级行政机关以及履行公共管理和服务职能的事业单位（以下统称公共管理和服务机构）在依法履职过程中，采集和产生的各类数据资源。

本办法所称公共数据开放，是指公共管理和服务机构在公共数据范围内，面向社会提供具备原始性、可机器读取、可供社会化再利用的数据集的公共服务。

第四条（工作原则）

本市公共数据开放工作，遵循“需求导向、安全可控、分级分类、统一标准、便捷高效”的原则。

第五条（职责分工）

市政府办公厅负责推动、监督本市公共数据开放工作。

市经济信息化部门负责指导协调、统筹推进本市公共数据开放、利用和相关产业发展。

市大数据中心负责本市公共数据统一开放平台（以下简称开放平台）的建设、运行和维护，并制订相关技术标准。

区人民政府确定的部门负责指导、推进和协调本行政区域内公共数据开放工作。

其他公共管理和服务机构根据相关法律、法规和规章，做好公共数据开放的相关工作。

第六条（数据安全保护）

市、区人民政府及各相关部门在公共数据开放过程中，应当落实数据安全管理要求，采取措施保护商业秘密和个人隐私，防止公共数据被非法获取或者不当利用。

第七条（协调机制）

市人民政府建立健全公共数据开放工作的协调机制，协调解决公共数据开放的重大事项。

第八条（专家委员会）

市经济信息化部门应当建立由高校、科研机构、企业、相关部门的专家组成的公共数据开放专家委员会。

公共数据开放专家委员会负责研究论证公共数据开放中的疑难问题，评估公共数据利用风险，对公共数据开放工作提出专业建议。

第二章　开放机制

第九条（数据开放主体）

市人民政府各部门、区人民政府以及其他公共管理和服务机构（以下统称数据开放主体）分别负责本系统、本行政区域和本单位的公共数据开放。

对于纳入开放范围的公共数据,应当在本市公共数据资源目录中列明数据开放主体。

第十条（开放重点）

市经济信息化部门应当根据本市经济社会发展需要，确定年度公共数据开放重点。与民生紧密相关、社会迫切需要、行业增值潜力显著和产业战略意义重大的公共数据，应当优先纳入公共数据开放重点。

市经济信息化部门在确定公共数据开放重点时，应当听取相关行业主管部门和社会公众的意见。

自然人、法人和非法人组织可以通过开放平台对公共数据的开放范围提出需求和意见建议。

第十一条（分级分类）

市经济信息化部门应当会同市大数据中心结合公共数据安全要求、个人信息保护要求和应用要求等因素，制定本市公共数据分级分类规则。数据开放主体应当按照分级分类规则，结合行业、区域特点，制定相应的实施细则，并对公共数据进行分级分类，确定开放类型、开放条件和监管措施。

对涉及商业秘密、个人隐私，或者法律法规规定不得开放的公共数据，列入非开放类；对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据，列入有条件开放类；其他公共数据列入无条件开放类。

非开放类公共数据依法进行脱密、脱敏处理，或者相关权利人同意开放的，可以列入无条件开放类或者有条件开放类。

第十二条（开放清单）

数据开放主体应当按照年度开放重点和公共数据分级分类规则，在本市公共数据资源目录范围内，制定公共数据开放清单（以下简称开放清单），列明可以向社会开放的公共数据。通过共享等手段获取的公共数据，不纳入本单位的开放清单。

开放清单应当标注数据领域、数据摘要、数据项和数据格式等信息，明确数据的开放类型、开放条件和更新频率等。

市经济信息化部门应当会同数据开放主体建立开放清单审查机制。经审查后，开放清单应当通过开放平台予以公布。

第十三条（动态调整）

数据开放主体应当在市经济信息化部门的指导下建立开放清单动态调整机制，对尚未开放的公共数据进行定期评估，及时更新开放清单，不断扩大公共数据的开放范围。

第十四条（无条件开放类数据获取方式）

对列入无条件开放类的公共数据，自然人、法人和非法人组织可以通过开放平台以数据下载或者接口调用的方式直接获取。

第十五条（有条件开放类数据获取方式）

对列入有条件开放类的公共数据，数据开放主体应当通过开放平台公布利用数据的技术能力和安全保障措施等条件，向符合条件的自然人、法人和非法人组织开放。

数据开放主体应当与符合条件的自然人、法人和非法人组织签订数据利用协议，明确数据利用的条件和具体要求，并按照协议约定通过数据下载、接口访问、数据沙箱等方式开放公共数据。

数据利用协议示范文本由市经济信息化部门会同市大数据中心和数据开放主体制定。

第十六条（数据质量）

数据开放主体应当按照相关技术标准和要求，对列入开放清单的公共数据（以下简称开放数据）进行整理、清洗、脱敏、格式转换等处理，并根据开放清单明确的更新频率，及时更新数据。

第三章　平台建设

第十七条（开放平台）

市大数据中心应当依托市大数据资源平台建设开放平台。

数据开放主体应当通过开放平台开放公共数据，原则上不再新建独立的开放渠道。已经建成的开放渠道，应当按照有关规定进行整合、归并，将其纳入开放平台。

第十八条（平台功能）

开放平台为数据开放主体提供数据预处理、安全加密、日志记录等数据管理功能。

开放平台为获取、使用和传播公共数据的自然人、法人和非法人组织（以下统称数据利用主体）提供数据查询、预览和获取等功能。

市大数据中心应当根据数据开放主体和数据利用主体的需求，推进开放平台技术升级、功能迭代和资源扩展，确保开放平台具备必要的服务能力。

第十九条（平台规范）

市大数据中心应当制定并公布开放平台管理制度，明确数据开放主体和数据利用主体在开放平台上的行为规范和安全责任，对开放平台上开放数据的存储、传输、利用等环节建立透明化、可审计、可追溯的全过程管理机制。

第二十条（行为记录）

市大数据中心应当依托开放平台，形成数据开放和利用行为的全程记录，为数据开放和利用的日常监管提供支撑。

数据开放主体应当对数据处理和数据开放情况进行记录；数据利用主体应当对有条件开放类公共数据的访问、调用和利用等情况进行记录。记录应当通过开放平台提交市大数据中心。

第二十一条（数据纠错）

自然人、法人和非法人组织认为开放数据存在错误、遗漏等情形，可以通过开放平台向数据开放主体提出异议。数据开放主体经基本确认后，应当立即进行异议标注，并由数据开放主体和市大数据中心在各自职责范围内，及时处理并反馈。

第二十二条（权益保护）

自然人、法人和非法人组织认为开放数据侵犯其商业秘密、个人隐私等合法权益的，可以通过开放平台告知数据开放主体，并提交相关证据材料。

数据开放主体收到相关证据材料后，认为必要的，应当立即中止开放，同时进行核实。根据核实结果，分别采取撤回数据、恢复开放或者处理后再开放等措施，并及时反馈。

第四章　数据利用

第二十三条（鼓励数据利用）

本市鼓励数据利用主体利用公共数据开展科技研究、咨询服务、产品开发、数据加工等活动。

数据利用主体应当遵循合法、正当的原则利用公共数据，不得损害国家利益、社会公共利益和第三方合法权益。

第二十四条（成果展示与合作应用）

市经济信息化部门应当会同市大数据中心和数据开放主体通过开放平台，对社会价值或者市场价值显著的公共数据利用案例进行示范展示。

本市鼓励数据利用主体与市经济信息化部门、市大数据中心以及数据开放主体开展合作，将利用公共数据形成的各类成果用于行政监管和公共服务，提升公共管理的科学性和有效性。

第二十五条（数据利用反馈与来源披露）

对有条件开放类公共数据，数据利用主体应当按照数据利用协议的约定，向数据开放主体反馈数据利用情况。

数据利用主体利用公共数据形成数据产品、研究报告、学术论文等成果的，应当在成果中注明数据来源。

第二十六条（数据利用安全保障）

数据利用主体应当按照开放平台管理制度的要求和数据利用协议的约定，在利用公共数据的过程中，采取必要的安全保障措施，并接受有关部门的监督检查。

第二十七条（利用监管）

数据开放主体应当建立有效的监管制度，对有条件开放类公共数据的利用情况进行跟踪，判断数据利用行为是否合法正当。

任何单位和个人可以对违法违规利用公共数据的行为向数据开放主体及有关部门举报。

第二十八条（违法违规行为处理）

数据利用主体在利用公共数据的过程中有下列行为之一，市经济信息化部门应当会同市大数据中心和数据开放主体对其予以记录：

（一）违反开放平台管理制度；

（二）采用非法手段获取公共数据；

（三）侵犯商业秘密、个人隐私等他人合法权益；

（四）超出数据利用协议限制的应用场景使用公共数据；

（五）违反法律、法规、规章和数据利用协议的其他行为。

对存在前款行为的数据利用主体，市大数据中心和数据开放主体应当按照各自职责，采取限制或者关闭其数据获取权限等措施，并可以在开放平台对违法违规行为和处理措施予以公示。

第五章　多元开放

第二十九条（优化开放环境）

市经济信息化部门结合本市大数据应用和产业发展现状，通过产业政策引导、社会资本引入、应用模式创新以及优秀服务推荐、联合创新实验室等方式，推动“产学研用”协同发展，营造良好的数据开放氛围。

第三十条（多元主体参与）

市经济信息化部门应当会同市大数据中心、相关行业主管部门建立多元化的数据合作交流机制，引导企业、行业协会等单位依法开放自有数据，促进公共数据和非公共数据的多维度开放和融合应用。

本市鼓励具备相应能力的企业、行业协会等专业服务机构通过开放平台提供各类数据服务。

第三十一条（非公共数据交易）

市经济信息化部门应当会同相关行业主管部门制定非公共数据交易流通标准，依托数据交易机构开展非公共数据交易流通的试点示范，推动建立合法合规、安全有序的数据交易体系。

第三十二条（标准体系和技术规范）

本市鼓励企业、科研机构和社会团体参与制订数据开放利用、数据安全保护等相关国家标准、行业标准、地方标准以及相关技术规范，推动形成相关行业公约，建立行业自律体系。

第三十三条（国际合作交流）

本市鼓励企业、科研机构和社会团体依法与境外企业、科研机构等开展公共数据开放领域的国际合作交流，提升本市公共数据开放的创新应用能力和认知水平。

第三十四条（表彰机制）

市经济信息化部门应当会同市大数据中心和相关行业主管部门对在数据技术研发、数据服务提供、数据利用实践、数据合作交流等方面有突出表现的单位和个人，按照规定给予表彰。

第六章　监督保障

第三十五条（安全管理职责）

市网信、公安等部门应当会同其他具有网络安全管理职能的部门建立本市公共数据开放的安全管理体系，协调处理公共数据开放重大安全事件，指导数据开放主体制定本机构的安全管理制度。

市大数据中心应当根据法律法规和相关要求，加强开放平台的安全管理，健全安全防护体系，完善安全防护措施，保障开放平台安全可靠运行。

数据开放主体应当制定并落实与公共数据分级分类开放相适应的安全管理制度，并按照相关法律法规，在数据开放前评估安全风险。

第三十六条（安全保障措施监管）

数据利用主体未按照开放平台管理制度和数据利用协议落实数据安全保障措施的，市大数据中心应当提出整改要求,并暂时关闭其数据获取权限；对未按照要求进行整改的，市大数据中心应当终止对其提供数据服务。

第三十七条（预警机制）

市网信、公安和保密部门应当会同数据开放主体建立公共数据开放安全预警机制，对涉密数据和敏感数据泄漏等异常情况进行监测和预警。

第三十八条（应急管理）

市网信、公安部门应当建立公共数据开放应急管理制度，指导数据开放主体制定安全处置应急预案、定期组织应急演练，确保公共数据开放工作安全有序。

第三十九条（组织保障）

数据开放主体应当加强公共数据开放工作的组织保障，明确牵头负责数据开放工作的机构，建立数据开放专人专岗管理制度。

市经济信息化部门应当会同市大数据中心制定公共数据开放工作培训计划，定期对数据开放工作相关机构工作人员开展培训，并纳入本市公务员培训工作体系。

第四十条（资金保障）

行政事业单位开展公共数据开放所涉及的信息系统建设、改造、运维以及考核评估等相关经费，按照有关规定纳入市、区两级财政资金预算。

第四十一条（考核评估）

市经济信息化部门可以委托第三方专业机构，对本市公共数据开放工作和数据利用成效等进行评估。评估结果纳入本市公共数据和一网通办管理考核。

市大数据中心应当对开放数据质量和开放平台运行情况进行监测统计，并将监测统计结果和开放平台运行报告提交市经济信息化部门，作为考核评估的依据。

第七章　法律责任

第四十二条（数据开放主体责任）

数据开放主体有下列行为之一，由本级人民政府或者上级主管部门责令改正；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分：

（一）未按照规定开放和更新本单位公共数据；

（二）未按照规定对开放数据进行脱敏、脱密等处理；

（三）不符合统一标准、新建独立开放渠道或者未按照规定将已有开放渠道纳入开放平台；

（四）未按照规定处理自然人、法人和非法人组织的异议或者告知；

（五）未按照规定履行数据开放职责的其他行为。

第四十三条（数据利用主体责任）

数据利用主体在数据利用过程中有下列行为之一，依法追究相应法律责任：

（一）未履行数据利用协议规定的义务；

（二）侵犯商业秘密、个人隐私等他人合法权益；

（三）利用公共数据获取非法收益；

（四）未按照规定采取安全保障措施，造成危害信息安全事件；

（五）违反本办法规定，依法应当追究法律责任的其他行为。

第四十四条（平台管理主体责任）

市大数据中心有下列行为之一，由主管部门责令改正；情节严重的，由主管部门对直接负责的主管人员和其他直接责任人员依法给予处分：

（一）未按照规定记录开放平台中公共数据开放和利用的全程行为；

（二）未按照规定处理自然人、法人和非法人组织的异议或者告知；

（三）未按照规定履行平台管理职责的其他行为。

第四十五条（安全管理主体责任）

市网信和公安部门、市大数据中心、数据开放主体等具有网络安全管理职能的部门及其工作人员未按照规定履行安全管理职责的，由本级人民政府或者上级主管部门责令改正；情节严重的，依法对直接主管人员和其他直接责任人员给予处分。

第四十六条（责任豁免）

数据开放主体按照法律、法规和规章的规定开放公共数据，并履行了监督管理职责和合理注意义务的，对因开放数据质量等问题导致数据利用主体或者其他第三方的损失，依法不承担或者免予承担相应责任。

第八章　附则

第四十七条（遵照执行）

水务、电力、燃气、通信、公共交通、民航、铁路等公用事业运营单位涉及公共属性的数据开放，适用本办法。法律法规另有规定的，从其规定。

第四十八条（实施日期）

本办法自 2019 年 10 月 1 日起施行

3. 央行官员关于“刷脸支付”的权威释疑

事件背景

前段时间一款名为 ZAO 的 App 爆火，用户上传一张照片，用 AI 换脸功能，将短视频中的演员换成自己的脸，就可以“过足戏瘾”，还能“和自己的偶像同框”。该 App 的火爆，亦引发担忧：在刷脸支付盛行的背景下，“换脸”后的小视频若落入他人之手，是否会危及刷脸支付的安全性？支付宝也就相关问题作出了回应。

每张照片搭配有一份数据文件，除了人脸位置的信息外，还有人脸的 106 处关键点，如眼睛、耳朵、鼻子、嘴、眉毛等的轮廓信息等。此外，数据中还能提供人物性别、表情情绪、颜值、是否戴眼镜等信息。

近期这些新闻的出现，让公众开始担心“刷脸支付”的安全性，日前，在 9 月 20 日举办的金融网络安全论坛上，央行科技司司长李伟表示就人脸支付安全问题表达了看法。

央行科技司司长李伟表示，人脸属于弱隐私生物特征，信息误用风险比较大。现实生活中通常综合人脸、声音、体态等多个弱隐私特征来认识他人，不光看你的脸，还要听你的声音、看你的动作，综合判断你是谁，来认识一个人，这些特征普遍显露在外，往往容易通过远程非接触的方式，在本人豪无察觉的情况下无声无息的采集，当前这是难以避免的现象。但问题在于，部分机构高估了弱隐私特征的识别作用，在网络空间仅依靠单一特征进行金融交易验证，存在严重隐患。

人脸识别支付应当遵循的原则

李伟表示，针对人脸识别支付应用，由于线上开放的网络环境中存在诸多风险，应用条件不成熟，而线下应用风险相对可控，基本具备试点应用的条件，应遵循以下几个原则：

一是信息采集要坚持“用户授权、最小够用”原则。

人脸特征是重要隐私，数据采集应提前告知信息使用方式，明确获得客户授权，避免与需求无关的特征采集，确保人脸特征采集的合理性和必要性。

二是支付交易要坚持“表达意愿、多重认证”原则。

考虑到人脸识别过程悄无声息，金融机构要严格落实消费者权益保护法，充分尊重用户的主观意愿，保护用户的知情权、财产安全权等合法权益，不得在用户不知情、未授权的情况下擅自发起交易，不要简单地将人脸特征作为唯一的交易验证因素，必须根据风险等级结合用户口令等其他因素进行多因素认证，平衡好金融服务的安全与便捷。

三是安全管理要坚持“风险补偿、全程防护”原则。

鉴于人脸识别高度依赖人工智能算法模型，攻防技术不断迭代升级，因此要主动建立健全风险赔付资金、保险计划、应急处置等风险补偿机制，综合运用多种信息技术，加强人脸特征信息端到端的全链条安全防护，切实保障消费者资金与信息的安全。后续，人民银行将对此强化监督检查和安全评估工作。另外在今年的 7 月 13 日，在由中国金融四十人论坛和金融城主办的“第四届全球金融科技（北京）峰会”上，人民银行科技司司长李伟表示，要纠正部分机构“有技术就滥用、有技术就任性”的乱象。

他以人脸支付举例称，人脸是非常敏感的个人信息，一旦泄露或被盗取，会带来非常大的影响。李伟以“3·15”提出的“隔空盗刷”问题作类比，认为问题在于支付场景没有表达出个人主观的支付意愿。

“如果进行人脸支付的时候，一刷脸钱就没了，更可怕。银行卡可能还揣在兜里，脸可是平常都露在外面，识别出来非常容易，现在有的技术在 3 公里之外就能识别人脸。当一个场景不能表达客户的主观意愿，这是多么可怕的一件事情。”因此，有技术也不能滥用，有技术也不能任性。”

李伟认为，尤其是一些企业在设计模式场景时没有考虑到这些问题。一方面刷脸，另一方面让人在大屏幕上输入手机号码，这是非常危险的。

对于这种创新，要及时指出来纠正。此外近日，中国人民银行印发银发【2019】209 号文件，《金融科技（FinTech）发展规划（2019-2021 年）》，明确提出未来三年金融科技工作的指导思想、基本原则、发展目标、重点任务和保障措施。在行业方面，刷脸支付也给出相应的指导意见。

《规划》表示探索人脸识别线下支付安全应用，借助密码识别、隐私计算、数据标签、模式识别等技术，利用专用口令、“无感”活体检测等实现交易验证，突破 1:N 人脸辨识支付应用性能瓶颈，由持牌金融机构构建以人脸特征为路由标识的转接清算模式，实现支付工具安全与便捷的统一。[5]

4. 国家计算机病毒应急处理中心：将进一步加强 App、SDK 检测

9 月 18 日，在 2019 年国家网络安全宣传周期间举办的国际反病毒大会上，国家计算机病毒应急处理中心常务副主任陈建民分析了当前移动互联网发展形势，将病毒中心受公安部委托开展的 App 和 SDK(软件开发工具包)的检验检测、通报处置工作进行了通报。

当前移动 App 强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题突出。”陈建民表示，在公安部指导下，国家计算机病毒应急处理中心将进一步加强对移动 APP 与 SDK 的检验检测，健全完善群众举报与企业自律工作机制，对发现的问题及时予以曝光，有效净化行业环境。

据了解，国家计算机病毒应急处理中心承担了全国移动 App 安全监测处置工作任务，建立移动互联网应用安全监测处置中心和移动 App 安全监测处置平台，对全国移动 App 分发平台开展技术监测，并受公安部委托以计算机防治产品实验室的名义，开展移动应用检验检测和通报处置工作，为适应移动互联网发展形势，加强行业监管提出新的举措。

[5] 支付观察。

为构建 App 和 SDK 安全治理的长效机制，国家计算机病毒应急处理中心将建立扁平化快速处置联动机制。比如，对国内主流 App 分发渠道实时监测，从而掌握国内现存 App 分发渠道数量、下载量、新增量、活跃度等情况，为监管部门掌握行业动态和发展规律提供基础信息；对检测发现的违法违规 App 和 SDK 及时通报应用商店和属地公安机关，实现从公安部、省级公安机关、市级公安机关到应用商店的扁平化快速处置联动机制等。

对于终端安全而言，过去只需要考虑 PC 端和各类虚拟主机的安全。在移动互联网时代，还需要考虑手机、平板电脑等各类移动终端的安全。而在未来的万物互联时代，就更多的要考虑物联网终端、车联网终端甚至是工业设备终端的安全问题。

实现企业级终端内生安全，应从自运营体系建设开始。网络安全的内涵和外延不断扩大，网络环境正经历着从互联网到网络空间的演化；终端安全正从过去的被动威胁防御向持续的安全运营转变，实现内生安全要从建设终端安全自运营体系开始，依靠信息化系统和安全系统的聚合产生自适应的安全能力。[6]

5. 2019 国家网络安全宣传周 公安部 CTID 平台牢筑个人身份信息安全防护墙

2019 年 9 月 16 日至 9 月 22 日，由中共中央宣传部、中央网信办、天津市人民政府指导、天津市委网信办主办的 2019 年国家网络安全宣传周网络安全博览会在天津梅江会展中心举办。在博览会上，由中央网信办、工业和信息化部、公安部、市场监管总局联合组成的 APP 专项治理工作组举办“APP 个人信息保护”主题展，CTID 作为 APP 个人信息保护的创新解决方案亮相主题展，带来网证保障个人身份信息安全的创新成果。

作为“APP 个人信息保护”题展区的重要组成部分，公安部第一研究所的 CTID 展台吸引了众多聚焦目光。“互联网+”可信身份认证平台（简称 CTID 平台）从系统架构、数据存储、数据传输、终端应用四大层面构建了全要素、全流程的安全体系，保障在不泄露身份信息的前提下实现全程端到端的可信安全认证，切实保护个

[6] 光明网。

人身份隐私数据流转。

系统架构安全方面：采用了安全隔离设计、冗余设计、系统加固等技术，层层设防，分区保护；采用“双活备份”，两条链路自动切换，防止硬件及网络故障导致系统瘫痪。

数据存储安全方面：业务服务区内仅存储经过国密算法变换的脱敏信息，原始身份信息均存储在公安网内，确保个人信息不被泄露。

数据传输安全方面：对传输信道上的全部数据进行加密。通过数字信封等技术保护业务数据；通过数字签名技术保证数据的完整性和有效性；通过时间戳等方法保证传输数据的时效性。

应用安全方面：采用自主研发的核心安全控件，身份认证时，终端不读取身份证信息，而是通过签发与法定身份证件一一对应的、去标识化的网证进行身份核验，用户无需再录入明文身份信息，实现端到端的隐私保护。

“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。”习近平总书记高屋建瓴的话语，为推动我国网络安全体系的建立，树立正确的网络安全观指明了方向。个人信息保护是网络安全课题中的重要挑战。CTID 平台将从隐私保护、跨域互联、可信认证、合法合规四个方面发挥自身价值，牢筑个人身份信息安全的防护墙。[7]

6.匈牙利国家银行发出重要公告 10 月 31 日前客户需核实个人信息

匈牙利国家银行日前发布公告，提请金融机构的客户注意，必须在 10 月 31 日前与银行、保险公司、养老基金机构核实个人信息，否则 11 月 1 日起账号的使用将受限，例如银行客户将无法进行新的交易。

除了拥有银行账号的人以外，该规定还适用于总部或分支机构在匈牙利的自费医疗和养老基金、投资服务提供商和人寿保险公司的客户。目前大型银行已扩充

[7] 站长之家。

办事员的人数，以避免客户的长时等待。有些机构在确认客户个人数据时，无需本人办理，而是可以通过邮局、电子邮件，甚至网上银行或实时视频完成该步骤。

国家银行表示，只有那些在 2017 年 6 月 26 日之前签订金融服务合同，且截至目前金融机构并未获得缺失数据的人，才需要核对数据。过去几个月，只有这些人获得了通知，其他客户则无需做任何事。国家银行建议客户不要到最后一刻才去进行数据核对，个人信息核准的方式都在各金融机构网站上刊登，也可以通过电话客服进行咨询。

进行数据核实时将复印客户的地址卡和带照片的身份证件，除此之外还需书面声明其不被视为重要的公众人物，或亲属及亲密关系人士。经济实体的情况下，必须复印有权代表公司或代表人的身份证件、地址文件及公司税号，并填写比以往要求更详细的实际所有权人的声明。[8]

[8] 匈牙利新导报。

三、相关案例

1. 某航班行程管理 App 被曝泄露隐私 回应称该功能为默认关闭

9 月 21 日晚，某航班行程管理 App 被网友质疑泄露乘客隐私，该网友称在上面选座后，陌生人可查看其姓名和头像，并表示自己受到骚扰(收到陌生人发来的“我可以约你吗”的私信)。同时，她表示也可以通过航旅纵横查看航班上其他乘客的名字和头像。

针对网友质疑，9 月 22 日凌晨，该 App 发微博回复称，该功能为默认关闭，在本人没有开通虚拟身份前，他人无法看到用户的信息。22 日上午，该 App 再次强调称，虚拟身份由用户自主选择是否开启。

据了解，用户首次注册登录该 App，进入个人主页后，用户必须要手动关闭“允许他人与我进行私聊”功能，即该功能为默认开启状态。不少网友还表示，关闭“允许他人与我进行私聊”的位置十分隐蔽，难以找到。

值得注意的是，这并非该 App 首次被爆泄露隐私。人民日报称，去年就有网友反映，在其 App 上，可以查看同航班其他乘客诸多信息，包括姓名、星座、常住地点和经常飞往的地方、喜欢的位置和航空公司。此外，还可以与该乘客私信联系。

虽然该 App 在微博上表示“非常抱歉”，并称已将引起争议的“虚拟个人主页”设置为默认关闭状态，但是道歉之后再无下文。[9]

2. 贵州 9 名被告人侵犯公民个人信息获刑

贵州省遵义市的刘义波、周银洁、赵云峰、田茂兵等 10 人，非法获取、出售或者提供公民个人信息，构成侵犯公民个人信息罪，其中 9 名被告人近日被遵义

[9] 人民日报、智通财经。

市中级人民法院分别判处有期徒刑 3 年 6 个月至有期徒刑 3 年、缓刑 3 年，另一名被告人则免予刑事处罚。9 名被告人还分别被处罚金 1000 元至 5000 元不等。

2017 年 7 月至 2018 年 3 月期间，遵义市无业人员刘义波通过非法渠道，获取包含公民姓名、联系电话、住宅小区名称、楼栋单元层号及面积的信息 28466 条，以及包含公民姓名、联系电话、住宅小区名称的信息 310 条，共计 28776 条公民个人信息存储于 U 盘中，用于非法出售或提供给他人以牟取利益。

2017 年下半年，刘义波的朋友、贵州巨江实建筑装饰工程有限公司负责人周银洁，从刘义波处非法获取上述 28776 条信息，并拷贝在公司的电脑上。

同年 11 月 8 日下午，刘义波到遵义市惠民房地产经纪有限公司桃溪寺分店，兜售上述信息。该店部门经理田茂兵叫员工胡佐顺，协助刘义波将信息存储于公司电脑上，后田茂兵经以 500 元价格购买上述信息。

同年 11 月中旬，刘义波到播州恒丰房屋信息服务公司兜售上述信息。该公司店长郭勇以 400 元的价格购买上述信息。

2018 年 3 月期间，刘义波分别到遵义黔北房产有限公司、遵义市祥瑞居房产经纪公司、遵义市厦千房地产经纪有限公司兜售上述信息。上述公司负责人李庆勋、董健、刘照利分别以 200 元至 300 元不等的价格购买上述信息。

同年 3 月至 4 月期间，刘义波的朋友、贵州七星阁装饰有限公司负责人赵云峰向刘义波索要上述信息。刘义波将上述信息无偿提供给赵云峰使用。

刘义波在推销上述信息过程中，手机不慎丢失，便给“客户”预留了好友周银洁的联系电话，以便继续出卖信息。2018 年 1 月的一天，周银洁接到贵州鑫富达房屋中介有限公司店长黄某(已判刑)购买公民个人信息的电话后，以 1000 元的价格将刘义波提供给他的 28776 条信息中的 5629 条，出卖给黄某。

2018 年 4 月，赵云峰与其公司合伙人杨晓飞为拓展公司业务，各出资 1000 元从温远欢(另案处理)处购买包含公民姓名、联系电话、住宅小区名称、楼栋单元层号及面积的信息 14039 条，以及包含公民姓名、联系电话及住宅小区名称的信息 102 条，共计 14141 条公民个人信息。

2018 年 5 月至 7 月，上述刘义波、周银洁、赵云峰、田茂兵等 10 人因涉嫌侵犯公民个人信息罪，被遵义公安机关逮捕。随后，遵义市汇川区人民检察院向汇川区人民法院提起公诉。

同年 12 月 19 日，汇川区人民法院认定上述 10 名被告人构成侵犯公民个人信息罪，其中刘义波、周银洁、赵云峰等 9 名被告人一审分别被判处有期徒刑 3 年 6 个月至 8 个月不等，另一名被告人胡佐顺免予刑事处罚。这 9 名被告人分别被处罚金 5000 元至 1000 元不等。

一审宣判后，汇川区人民检察院向遵义市中级人民法院提起抗诉，被告人刘义波及赵云峰则不服一审判决，向遵义市中级人民法院提出上诉。

遵义市中级人民法院审理认为，上诉人刘义波非法提供或贩卖的 28776 条公民个人信息中的 28466 条信息、上诉人赵云峰和原审被告人杨晓飞非法获取的 14141 条公民个人信息中的 14039 条信息，既包含公民姓名、电话等体现自然人身份的要素，同时还包含房产区位、楼栋及单元号、房屋面积等可以识别房产价值的要素，应认定为财产信息。原判认定涉案信息数量及性质不当，应予以纠正。抗诉机关所提“原判涉案信息未认定为财产信息，属适用法律错误”的抗诉理由成立，予以采纳。刘义波、赵云峰、田茂兵等 10 人所提“涉案信息应认定为一般公民个人信息”的辩解、辩护意见不能成立，不予采纳。

综上，遵义市中级人民法院认定原判决所认定的部分事实不清，且适用法律错误，予以改判。[10]

3. 警方摧毁百亿套路贷 两大套路模式指向大数据泄露

多家在当地颇为“知名”的贷款中介，由于业务模式激进，却最终变形，成为套取他人房产、汽车等的牟利工具。

9 月 17 日，广东省公安厅发布消息，粤港澳三地警方 10-11 日开展的一次清查行动期间，广州、深圳、佛山、惠州、东莞等地警方打掉“套路贷”犯罪团伙 16

[10] 中国消费者报。

个，抓获犯罪嫌疑人 140 余人，破获刑事案件 20 余起，查封扣押冻结涉案资产逾 9300 万元。

根据公安部 9 月 3 日发布的数据，全国公安机关共侦办“套路贷”团伙案件 1890 起，抓获犯罪嫌疑人 18651 人，破获各类刑事案件 18790 起，查扣涉案资产 161.76 亿元。

去年 8 月，最高人民法院下发《关于依法妥善审理民间借贷案件的通知》，对于披着民间借贷外衣，通过“虚增债务”“伪造证据”“恶意制造违约”“收取高额费用”等方式非法侵占财物的“套路贷”诈骗等新型犯罪，加强惩戒。

“套路贷”模式大致有两种：一是，贷款中介有意诱导借款人去其他中介借贷，利息越借越高；二是，有的套路贷平台故意制造贷款逾期，目的就是为了骗取借款人的房产等。

摧毁百亿“套路贷”

“证大系”百亿 P2P 捞财宝风险暴露后，证大集团戴志康向警方投案自首，但他的名字也与近期曝出的一家深圳贷款中介间接相关。

据广东省公安厅消息，今年 6 月 5 日，深圳市公安机关在深圳市及北京、上海、湖南、河南等地同步开展收网行动，打掉一个刘某峰为首的“套路贷”犯罪团伙，抓获犯罪嫌疑人 19 人，破获刑事案件 12 起，查封、冻结、扣押涉案资产约 2531 万元。深圳警方指出，在上述案件中，以盛天源、小小金融等金融公司为依托，非法高利放贷。

根据工商信息显示，“小小金融”的注册实体的唯一股东为深圳市小小信息技术有限公司（简称“小小信息”），其法定代表人、董事长兼总经理为刘小峰，刘小峰和一家名为德辉投资的公司分别持有小小信息 52.9%、30%股份。刘小峰即广东警方所指“刘某峰”，德辉投资的一名股东同时握有 P2P 捷越联合，而戴志康为捷越联合的股东之一。

与上述案件一起曝光的是，今年 4 月 19 日，广州市公安机关在广州市及广西南宁市、河南漯河市等地开展统一收网行动，打掉一个以梁某敏为首的“套路贷”犯罪团伙，抓获犯罪嫌疑人 37 人，破获敲诈勒索、寻衅滋事、非法入侵住宅、诈

骗等刑事案件 17 起，查封、冻结、扣押涉案资产数亿元。4 月 28 日，湛江市公安机关在湛江市霞山、赤坎、坡头、开发区和肇庆市等地实施收网行动，打掉一个以黄某伟为首的“套路贷”犯罪团伙，抓获犯罪嫌疑人 18 人，破获刑事案件 14 起，查封、冻结、扣押涉案资产 1975 万元。

“借几千元，最后债务滚成几十万。”这样夸张的案例显示的就是“套路贷”的风险所在。

9 月 17 日，重庆市公安局南岸区分局发布消息称，近日捣毁的一个特大“套路贷”团伙，涉及受害人 300 余人，警方共抓获团伙成员 30 余人，扣押、冻结涉案资产共计 600 余万元。

“套路贷”的两大套路

公安部 9 月 3 日指出，打掉“套路贷”团伙开发使用的非法放贷 APP、非法网络借贷平台，查扣银行账户及第三方支付平台的涉案资金、依法追缴，打掉专门从事非法催收业务的职业催讨团伙、依法处理。

9 月 17 日，广东省小额贷款公司协会常务副秘书长徐北对 21 世纪经济报道记者表示，“套路贷”模式大致有两种：一是无抵押的、被动性的套路贷，借款人无法偿还，贷款中介有意诱导借款人去其他中介借贷，利息越来越高，最初的几千元甚至被滚成几十万元；二是有抵押的、主动性的套路贷，有的套路贷平台故意制造贷款逾期，目的就是为了骗取借款人的房产等。

从已经曝光的“套路贷”模式看，警方指出，小小金融刘某峰涉嫌非法侵占房产。诱骗受害人签订空白合同、阴阳合同、全权委托授权书等，设置“砍头息”、高额逾期费，恶意垒高债务，继而单方制造违约，逼迫被害人转移、变卖抵押房产。

另一起以黄某伟为首的“套路贷”案件中，警方指出，该组织分工明确，并制定一整套组织纪律和行为规范进行管理，如实行 24 小时轮流值班制度，每周召开全员会议，研究放贷和索债情况等。在方式上，采取强收“斩头息”、虚增借款金额、制造虚假银行流水、转单平帐、罚息或强收违约金等所谓“行规”套路，非法占有被害人房产等。

“贷款中介这一‘助贷’模式，本意是为了提升资金方的获客能力和获客效率，

但一些中介却利用大数据泄露的机会违法操作。”一位资深业内人士指出，比如小小金融是当地比较早用线上方式做现金贷的贷款中介。

“套路贷”的猖獗，与大数据泄露密切相关

由于借款人的身份、手机通讯录、通话记录等被套路贷平台获取，“爆通讯录”、电话滋扰等暴力催收流行于各个平台。

例如，根据公安部披露，甘肃兰州王某焘“套路贷”犯罪团伙设立“甜兔网”等 24 个网贷平台，非法获取 482 万人的通话记录、电话号码本、银行卡号等公民个人信息。

警方正在从整个产业链铲除套路贷，包括大数据泄露。“大数据风控”行业最近也颇不平静。今年 9 月份以来，杭州某科技公司和某区块链公司先后被杭州警方调查。此外，上海某科技公司有高管被警方带走，协助调查，其 CEO 电话也一直无法接通。上述公司受此风波影响，或与运营商爬虫业务有关。多家和上海某科技公司有合作的机构人士表示，该科技公司停了运营商爬虫业务。另一家暂停运营商爬虫服务的机构表示，这是行业趋势。

警方指出，盛天源、小小金融等金融公司非法高利放贷，非法获取个人信息。通过非法手段获取大量公民个人信息，骨干成员曾因非法获取公民信息罪获刑，并通过拨打电话、网站广告等方式招揽客户。过度的借贷已经透支这些受害者的支付能力和消费观念，整个业态要逐渐恢复，至少需要 3-4 年的时间。[11]

4. “剪刀手”拍照泄露指纹信息?专家:难以威胁信息安全”

据多家媒体报道，在上海举行的国家网络安全宣传周全民体验日上，有网络安全专家称，摆“剪刀手”姿势拍照片，如果镜头距离太近，通过照片放大技术和人工智能增强技术，可以还原照片中人物的指纹信息。如果在 1.5 米内拍摄的剪刀手照片就能 100%还原出被摄者的指纹，1.5 米到 3 米的距离内拍摄的照片还原出 50%的指纹，而 3 米以外拍摄的照片就不用担心这个问题了。指纹被提取后通过专业

[11] 新浪财经。

材料制作成指纹膜，可能被不法分子利用，比如开指纹门锁、指纹支付等。消息一出，立刻引发了网络上的热烈讨论。

理论上可行操作层面难以威胁信息安全

中国科学院大学教授荆继武称，如果用剪刀手拍照，好一点的相机拍摄（单人像）可能能够还原指纹。现在的相机一部能达到 1200 万像素，也就是说拍一米长的物体，分辨率可达 0.25 毫米，利用多张照片有可能恢复指纹。一般情况下由于光线等原因，恢复有一定难度，但更高精度的相机恢复起来就简单些，任何方式泄漏指纹都会威胁用户的信息安全。有指纹就可模仿进行身份假冒，有可能能开一般的指纹电子锁，上班进门的指纹打卡等。

支付宝数字身份实验室负责人高谊称，媒体报道的拍照比“剪刀手”会泄露指纹信息，这事理论上可能，但实际上大家不用太担心：首先，目前手机指纹识别主要以电容式为主，即使拿到高清指纹，但要制作出导电材料的模拟指纹难度很高，加之部分手机还有活体检测能力，比如会检测皮肤的温度，所以几乎无法通过手机的指纹识别。其次，指纹信息是储存在手机本地，只有在本人的手机上才能使用，就算根据照片能制作出模拟指纹，拿不到对方的手机也是没有用的。[12]

5. 苹果承认“键盘数据泄露”，发布 iOS 和 iPadOS 13.1.1 补救

在上周二发布 iOS 和 iPadOS 13. 1 不久，苹果承认其最新操作系统存在 bug，在未经用户的允许下让一些第三方键盘获得其 iPhone 和 iPad 数据。虽然当时没有修复的具体时间安排，但是公司今日发布了其两款硬件产品的操作系统 13.1. 1 版本，解决了这一问题和其他 bug。

据苹果方面表示，此次键盘问题影响了诸如谷歌 Gboard 和微软 Swiftkey 等插件的使用，即使你没有批准该访问，也可以授予键盘扩展完全访问权限。苹果在 iOS 13. 0 中发布了自己的 Swiftkey 替代品，一款默认打开的可滑动键盘，使手势打字更容易，同时降低了传统键盘敲击的准确性。

[12] 央视财经。

发布说明证实，新的更新修复了第三方键盘应用程序的一个安全问题，并解决了一些未指明的问题，这些问题可能会导致电池更快耗尽，并可能阻止 iPhone 从备份中恢复。该补丁显然还修复了一些问题，这些问题导致最新款 iPhone 对 Siri 请求的识别能力下降，导致提醒同步速度变慢，甚至在关闭 Safari 搜索建议后，也重新启用了这些搜索建议。

13.1. 1 的更新现在可以通过苹果的无线软件更新机制在 iPhone 和 iPad 上使用。运行 13. 1 的设备将需要约 108MB 的空间进行在线更新，而 iOS12 的升级则需要 3.29GB 的下载空间。[13]

6. 美外卖公司 DoorDash 泄露近 500 万用户个人数据

9 月 26 日，美国外卖服务 DoorDash 公司宣布，该公司出现数据泄露，影响了近 500 万使用其平台的顾客、司机和商家。

这家总部位于旧金山的公司在一份声明中说，此次泄露的信息可能包括“姓名、电子邮件地址、交货地址、订单历史记录、电话号码”等。同时被访问的还有支付信息，包括支付卡的最后四位数字和近 10 万名“Dashers”的驾照号码。过，DoorDash 强调，公司并未记录完整的信用卡信息和银行账户信息。

该公司表示，在 9 月份，它发现一个未经授权的第三方在 2019 年 5 月 4 日访问了一些 DoorDash 用户数据。DoorDash 没有具体说明这次入侵的来源，但表示它涉及“第三方服务提供商“。它将采取措施来提高其平台的安全性，包括在数据周围增加额外的保护性安全层，加强对系统访问的安全协议控制，以及引入外部专家来增强识别和击退威胁的能力。[14]

7. 马印航空发生数据泄露，系其承包商公司两名前员工所为

据路透社 9 月 18 日报道，马来西亚马印航空公司表示，正调查一起涉及乘客

[13] 猎云网。

[14] 中管院数字经济中心。

个人信息的数据泄露事件。

在马印航空公司发表声明之前，莫斯科网络安全公司卡巴斯基实验室(Kaspersky Lab)发布的一份报告称，马印航空公司及其子公司泰国狮航(Thai Lion Air)约 3000 万名乘客的个人信息被发布在了一个在线论坛上。报道称，遭泄露的信息包括乘客的护照信息、地址和电话号码。

马印航空公司表示，正在向国际有关部门通报这一事件，并建议拥有飞行常客网络账户的客户更改密码。目前该公司拒绝提供更多调查细节，包括有多少客户受到影响，并表示没有在其服务器上存储任何客户的付款细节。

这些泄露文件数据被上传并存储在一个开放的亚马逊网络服务公司?(AWS)云存储器中，而这是一个公共云存储器。AWS 是马印航空公司的外部数据服务提供商，目前 AWS 还没有对此事发表评论。卡巴斯基表示，部分泄露的数据已经在暗网上公开叫卖。

马印航空 23 日发布一份声明，表示两名曾在该公司印度发展中心就职，供职于为马印航空提供电商服务的 GoQuo 公司前职员“不恰当地获取并盗窃了乘客的个人数据”。马印航空还表示数据泄露已经得到控制，并且已将案件报告给马来西亚及印度警方。[15]

8. 厄瓜多尔遭遇史上最严重数据泄露事件：涉 2 千万人

据美国有线电视新闻网(CNN)17 日报道，网络安全公司 vpnMentor 近日发现一起厄瓜多尔大部分民众个人数据遭到泄露事件。报道称，这是厄瓜多尔史上最严重的数据泄露事件之一，涉及到超过 2 千万人的数据，而其中 700 万人还是未成年人。

据悉，厄瓜多尔总人口约为 1600 万人，厄瓜多尔检察官办公室认为，泄露记录超过厄瓜多尔总人口的原因或系遭泄露的数据中包含了已故人士的相关信息。

[15] 环球时报。

而到目前为止，尚不清楚有多少在世的厄瓜多尔人个人信息受到牵连。

vpnMentor 周一提交的一份报告显示，这次数据泄露起因系厄瓜多尔数据分析公司 Novaestrat 位于迈阿密的服务器出现了漏洞。而泄露的数据包含了公民的全名，出生年月、地点，家庭住址、电子邮箱地址，身份证件号码，个人税号和雇佣信息等。此外，个人财务信息也被泄露，包括银行账户信息、个人收支情况和信用类型等。

报告还显示，维基解密创始人阿桑奇的个人信息也在泄露的数据之列。阿桑奇曾在厄瓜多尔申请政治庇护，在今年被捕前曾在该国的伦敦大使馆居住多年。

厄瓜多尔电信部表示，在 9 月 11 日收到 vpnMentor 公司提交的报告后，涉事数据库便立即被关闭，但为时已晚。vpnMentor 警告称，这次数据泄露将公司和个人置于身份盗窃、金融诈骗、商业间谍和其他安全风险之中。

针对此事数据泄露的原因，厄瓜多尔电信部在其官网发表声明称，该事件并非是政府数据库遭到黑客网络攻击引起的。声明还表示，政府机构的安保体系足以抵御潜在网络攻击，Novaestrat 公司可能联合了拥有获取信息权限的前政府职员。

周一(16 日)晚，厄瓜多尔电信部部长安德烈斯·米切莱纳表示，筹备数月的“个人数据保护法案”将在 72 小时内提交给国民议会。

此外，厄瓜多尔政府正全力追查此次数据泄露事件。16 日，检察官和联邦警察突击检查了 Novaestrat 公司法人代表威廉·罗尔特的寓所，缴获了一批电信设备和电脑。当晚，警方在厄瓜多尔西北部的埃斯梅拉达斯省发现并拘留了罗伯特。

厄瓜多尔内政部部长宝拉·罗莫在推特上表示，“我们会立即将他(罗伯特)转移，以便检察官能够投入调查，获取相关信息。”

电信部部长安德烈斯·米切莱纳亦发推称，“若他们(Novaestrat 公司)被证实侵

犯了厄瓜多尔人的隐私，这便构成了犯罪，必须受到相应的惩罚”。[16]

9. 女性生理期 App 涉嫌非法向 Facebook 共享隐私数据

9 月 12 日上午消息，据外媒援引最新研究发现报道，女性生理期跟踪应用涉嫌将女性的健康与性生活等私密个人信息发送给 Facebook。

对此，一名 Facebook 发言人表示，平台要求应用开发者明确地告知用户，哪些数据将与 Facebook 共享，以及对数据的披露和使用需建立在“合法基础”之上。

“我们有系统专门用于检测和删除某些特定类型的数据，比如社会保障号、密码和其他诸如电子邮件或电话号码等个人信息，”该发言人说，“我们也在探索改进系统和产品的途径，以检测和过滤出更多潜在的敏感数据类型。”

MIA Fem 建议用户输入的行为习惯信息极为广泛，从抽烟到咖啡因摄入和卫生棉的使用等，无所不包。隐私国际的分析发现，这些数据不是即时共享给 Facebook 的，但却可以让 MIA Fem 向用户推荐相关文章。而这些根据用户兴趣爱好所精挑细选的文章，会与 Facebook 共享。MIA Fem 还与 Facebook 分享应用内的避孕药服用“提醒”。

这些应用的行为进一步引发了人们对隐私问题的关注，即用户对此类私密信息与 Facebook 等外部公司共享的知情同意究竟有多大用处，尤其是当应用的服务条款冗长枯燥几乎没有用于愿意认真阅读的时候。

知识产权相关的专职律师林赛·巴瑞特（Lindsey Barrett）说：“这事件说明，用户同意根本不足以防范隐私侵犯。没有人愿意阅读隐私政策，因为有太多各种各样的隐私政策，一一细读几乎不现实，即便有人真的仔细阅读了，这些政策要么敷衍了事，要么有用信息寥寥无几。”

“成为痤疮药物广告的目标受众，有时候十分尴尬也有损自尊，但 Facebook 究竟是基于这些应用四处收集来的哪些避孕措施信息，来帮助广告主定位受众的

[16] 环球网。

呢？”巴瑞特继续说道，“Facebook 还与谁共享了这些信息？这里存在尊严问题，同时也存在歧视问题，当我们讨论个人隐私权的重要性的时候，这些问题都值得关注。”

22 岁的海兰（Chandana Hiran）是住在孟买的一位前 Maya 用户。她说，她很喜欢 Maya 应用是因为在该应用上记录生理期症状简单容易，应用的交互界面也简洁明了。但是她从未考虑过隐私问题。

“如果他们与其他人共享数据的话，那么泄露的都是一些非常私密的信息，”她说，“我当然不希望任何人拥有这些信息。某个应用与 Facebook 共享我的购物车或愿望清单，这是另一回事。但既然是非常隐蔽的私密信息，那就必须严格保密。”[17]

10. 谷歌赢得具有里程碑意义的诉讼 不必再全球范围内执行“被遗忘权”

据英国广播公司（BBC)报道，欧洲最高法院已裁定谷歌不必在全球范围内执行“被遗忘权”。这意味着该公司仅在收到适当的请求后才需要从其在欧洲的搜索结果中删除链接，而无需在其他地方删除该链接。

该裁决源于谷歌与法国数据保护监管机构“法国国家信息与自由委员会(CNIL)”之间的纠纷。

2015 年，CNIL 命令该公司在全球范围内删除该搜索引擎平台上的链接，如果这些链接指向包含破坏性或虚假信息。2016 年，谷歌推出了“地理封锁”功能，该功能可阻止欧洲用户看到遭限制的链接。

但是谷歌拒绝在全球范围内执行“被遗忘权”,该公司对 CNIL 试图施加的 10 万欧元罚款提出质疑。

[17] 新浪科技。

“目前，根据欧盟法律，对于允许数据主体取消引用的搜索引擎运营商没有义务……对其所有版本的搜索引擎进行这种取消引用，”欧洲法院在裁决中说道。

谷歌曾辩称，如果这项裁决要在欧洲以外实施，则专制政府可能会掩盖这项侵犯人权的行为。该公司在欧洲法院裁决后发表声明说：“自 2014 年以来，我们一直努力在欧洲执行被遗忘权，并在人们的信息获取权与隐私权之间取得合理的平衡。很高兴看到法院同意我们的论点。”

该技术公司得到了微软、维基媒体基金会，非营利的新闻自由记者委员会以及英国言论自由运动组织 Article 19 等组织的支持。

欧洲法院顾问 Maciej Szpunar 还得出结论，在今年早些时候向法院提出的不具约束力的建议中，被遗忘权仅限于欧洲。

自 2014 年 5 月欧洲法院首次确定欧洲公民在某些情况下可以迫使搜索公司从使用其姓名的查询中删除包含有关他们的敏感信息的网页时，谷歌便开始执行被遗忘权。

谷歌表示，自那时以来，该已经收到了超过 84.5 万个请求，总共删除了 330 万个网址，其中大约 45％的链接最终被删除。这包括从其欧洲网站（例如 Google.fr，Google.co.uk 和 Google.de）中删除结果，以及在其检测到正在搜索的情况下，从其其他网站（例如 Google.com）中限制结果。但是，这意味着，如果用户使用虚拟专用网络（VPN）或其他工具掩盖其位置，则仍然可以绕开该操作。[18]

11. 英国上诉法院重启针对谷歌的集体诉讼

10 月 2 日，据彭博社报道，英国上诉法院判定，针对谷歌收集超过 400 万 iPhone 用户信息行为的诉讼可以继续进行。

做出起诉的 iPhone 用户组织为“Google You Owe Us（谷歌你欠我们的）”，领头人为 Richard Lloyd。根据去年的法庭文件，原告方寻求超过 32 亿英镑的赔偿。

[18] cnBeta。

该组织称代表 400 万受影响的 iPhone 用户。

英国上诉法院称，根据英国 1998 数据保护行动法令，Richard Lloyd 可以推进对谷歌的起诉。

Lloyd 指控，在 2011 年 8 月至 2012 年 2 月间，谷歌秘密地跟踪了英国 iPhone 用户的上网行为，谷歌绕开了手机的隐私设定，从 Safari 浏览器中收集用户的浏览习惯数据，借此获得的信息包括用户的健康情况、性别、政治观点和财务状态。

英国金融时报报道称，谷歌据称通过这些信息为用户进行标记，比如“足球爱好者”，用于帮助广告客户定位受众。在美国，谷歌已经为越过 Safari 安全设定而向州政府及美国联邦贸易委员会支付了数百万美元罚金。

Lloyd 预计，如果在英国打赢官司，那么每位受到影响的 iPhone 用户可获赔 750 英镑，谷歌的整体损失达到 33 亿英镑。不过，这一数字还取决于最终的判决。

谷歌将会提起上诉，该公司称：“保护用户的隐私和安全永远是我们排名第一的事情，这一事件发生的时间几乎在十年前，而且我们当时就已经做出了处理。我们认为这没有任何价值，应该予以驳回。”

BBC 报道称，这是英国首次由个人代表拥有相同诉求的群体向科技巨头公司发起的数据滥用方面的诉讼。值得提出的是，这起诉讼曾在 2018 年 10 月被英国的法院否决。当时法院方面称，很难计算到底有多少用户受到了影响。而此次的最新判决显示，诉讼将被推进。[19]

[19] 澎湃新闻，《英国上诉法院重启针对谷歌的集体诉讼》。

12. 欧盟法院裁定 Cookie 的存储和利用需要征得互联网用户的积极同意和实质同意，预先勾选的复选框无效

10 月 1 日，欧盟法院就 cookies 技术做出裁决（preliminary ruling）。[20]根据该裁决，在使用 cookies 技术时，使用预选框的方式使用户只能通过取消勾选来表示拒绝，则不构成数据主体的同意。

德国消费者（Verbraucherzentrale Bundesverband eV）在德国法院起诉了一家名为“Planet49”的公司。这家公司试图通过预选的复选框来存储用户的浏览记录，并通过 cookies 收集信息并推广在线游戏。

欧盟法院审理后认为，通过预先选中的复选款的方式并不能表明网站用户的积极作为，不能构成有效的同意。

[20] Judgment of the Court (Grand Chamber) of 1 October 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH, Case C-673/17, available at http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0673&lang1=en&type=TXT&ancre=.

四、环球解读

1. 《开曼群岛数据保护法》的精要解读—兼议对采用 VIE 模式中国企业的意义

一、概述

对于通常会涉及数据资产或相关业务运营的 TMT 行业，通常会考虑搭建 VIE 红筹架构进行海外融资或上市。在这些 VIE 架构中，通常会在开曼群岛设立公司作为海外融资或上市主体。另外，在一些中国企业“走出去”进行境外投资时，有时也会在开曼群岛设立一层 SPV 持股主体。然而由于海外市场的国情、法律惯例、文化背景等方面存在差异，进入不熟悉的境外经营环境与投资环境必然伴随着一定的法律风险。大数据时代的来临给企业的海外投资带来了新的挑战，企业不仅要关注境外公司法、税法等方面的规则，还有必要了解当地数据保护方面的法律，增强数据合规和数据安全意识。

鉴于《开曼群岛数据保护法（2017）》（以下简称“DPL”）将于 2019 年 9 月 30 日生效，对于在开曼群岛注册海外融资或上市主体或在开曼设立 SPV 持股公司的中国企业而言，也有必要认真审视 DPL 这一开曼新规所可能带来的影响。因为 GDPR 已经实施一年多了，很多规则已经被大众较为熟悉。因此，在各国新出台数据保护法时，基本都会先拿它来作为衡量尺子，以评判新法的保护力度与处罚重轻。本文也不出例外，通过欧盟《通用数据保护条例》（以下简称“GDPR”）与 DPL 进行对比，介绍 DPL 数据保护法的内容和特性，尤其是为中国公司通过 VIE 的方式去开曼群岛注册公司时应当遵守的数据保护法律规则提供合规指引。

二、《开曼群岛数据保护法》与欧盟《通用数据保护条例》对比分析

（一）域外效力

DPL 与 GDPR 两者均具有域外效力。

具体而言，DPL 适用于：

- 在开曼群岛内设立的“数据控制者”处理个人数据；或

- 在开曼群岛以外设立的，且在开曼群岛内处理个人数据的“数据控制者”，但以通过开曼群岛传输个人数据为目的的除外。

如果设立于开曼群岛以外的数据控制者，在开曼群岛内处理数据，则需要指定一名位于群岛的当地代表作为数据控制者，以遵守 DPL。

相似的，GDPR 第 3、27 条规定 GDPR 适用于：

- 设立在欧盟内的组织；或

- 设立在欧盟外，但为欧盟内的数据主体提供商品或服务或对数据主体的活动进行监控的组织，在此种情况下数据控制者或处理者应当在欧盟内委任一名代表。

（二）重要定义与概念

DPL 与 GDPR 均对“同意”、“数据控制者”、“数据处理者”、“个人数据”、“处理”、“个人敏感数据/特殊类型的数据”进行了定义。具体对比如下：

（1） “同意”

对比项目	DPL	GDPR
同意	1. 数据主体的“同意”，是指数据主体通过声明或明确的肯定行动，表明同意处理与该数据主体相关的个人数据的任何自由、具体、知情且明确的，表示该数据主体意愿的指示； 2. 数据控制者负有证明同意的举证责任。同意可在任何时间被	1. 数据主体的“同意”指的是数据主体通过声明，或者通过某项清晰的确信行动而自由作出的、充分知悉的、不含混的、表明同意对其相关个人数据进行处理的意愿。 2. 当处理是建立在同意基础上的，控制者需要能证明，数据主

对比项目	DPL	GDPR
	撤回； 3. 同意的撤回不会影响在撤回之前，基于同意所做处理的合法性。	体已经同意对其个人数据进行处理。 3. 如果数据主体的同意是在涉及到其他事项的书面声明的情形下作出的，请求获得同意应当完全区别于其他事项，并且应当以一种容易理解的形式，使用清晰且平实的语言。任何违反本条例的声明都不具有约束力。 4. 数据主体应当有权随时撤回其同意。在撤回之前，对于基于同意的处理，其合法性不受影响。在数据主体表达同意之前，数据主体应当被告知这点。撤回同意应当和表达同意一样简单。 5. 分析同意是否是自由做出的，应当最大限度地考虑一点是：对契约的履行——包括履行条款所规定的服务——是否要求同意履行契约所不必要的个人数据处理。

通过对比 DPL 和 GDPR 的“同意”定义和相关规则可以发现，DPL 的同意规则在 GDPR 中均可以找到，且 GDPR 针对撤回同意的难易程度、如何判定同意是自由作出之两部分进行了额外规定。

（2） “数据控制者”

对比项目	DPL	GDPR
数据控制者	控制者是指单独或与他人共同决定任何个人数据的处理目的、	控制者是指那些决定—不论是单独决定还是共同决定—个人

对比项目	DPL	GDPR
	条件和方式的主体。包括当数据控制者建立在开曼群岛以外，但数据处理在开曼群岛以内，需要指定一位当地代表作为数据控制者的情形。	数据处理目的与方式的自然人或法人、公共机构、规制机构或其他实体；如果此类处理的方式是由欧盟或成员国的法律决定的，那么对控制者的定义或确定控制者的标准应当由欧盟或成员国的法律来规定。 设立在欧盟境外的数据控制者或处理者应当在欧盟内委任一名代表。

DPL 和 GDPR 关于“数据控制者”的定义和相关规则具有一致性，均为单独或与他人共同决定数据处理目的的主体；且设立在境外的受规制实体均需在法域内委任一名代表。

（3） “数据处理者”

对比项目	DPL	GDPR
数据处理者	“处理者”任何代表数据控制者处理个人数据的人（或实体），但不包括数据控制者的员工。	“处理者”指的是为数据控制者而处理个人数据的自然人或法人、公共机构、规制机构或其他实体。

DPL 和 GDPR 关于 “数据处理者”的定义和范围基本一致，但 DPL 明确说明数据控制者的员工不构成“数据处理者”。

（4） “数据主体”

对比项目	DPL	GDPR
数据主体	任何已被识别的自然人，或任何可能被数据控制者或任何其他人通过合理方式直接或间接识别的自然人，且该自然人并未死亡。	数据主体是指：任何已识别或可识别的自然人。

针对“数据主体”的定义，DPL 和 GDPR 均强调了自然人身份的可识别性，包括“已被识别”和“可被识别”两个方面。有趣的是，DPL 还明确规定数据主体必须处于未死亡状态，相对而言，保护范围有所限缩。

（5） “个人数据”

对比项目	DPL	GDPR
个人数据	与可识别的存活个体有关的数据，例如： 1. 存活个体的位置数据、在线标识符或者与特定个体的身体、生理、遗传、精神、经济、文化或社会身份相关的一个或多个因素; 2. 对存活个体的任何意见；或者 3. 表明数据控制者或与该存活个体相关的任何其他人的意图。	“个人数据”指的是任何已识别或可识别的自然人（“数据主体”）相关的信息；一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别个体。

相较于 GDPR，DPL 中“个人数据”的范围要更广，DPL 明确规定“对存活个体的意见”以及“表明数据控制者或与该存活个体相关的任何其他人的意图”亦属于“个人数据”，这在 GDPR 中是较难以被认定为“个人数据”的。

（6） “个人敏感数据”

对比项目	DPL	GDPR
个人敏感数据	1. 数据主体的种族或族裔出身; 2. 数据主体的政治意见; 3. 数据主体的宗教信仰或其他类似性质的信仰; 4. 该数据主体是否为工会成员; 5. 数据主体的遗传资料; 6. 数据主体的身体或精神健康或状况; 7. 医疗数据; 8. 数据主体的性生活; 9. 该数据主体的罪行，或被指控的罪行;或 就该数据主体所犯的任何罪行或被指控已犯的任何罪行提起的任何法律程序，处理该等法律程序或该群岛或其他地方法院的任何判决。	1. 特殊类型个人数据是指 对于那些显示种族或民族背景、政治观念、宗教或哲学信仰或工会成员的个人数据、基因数据、为了特定识别自然人的生物性识别数据、以及和自然人健康、个人性生活或性取向相关的数据，应当禁止处理。 2. 与刑事定罪和犯罪相关的个人数据的处理 对与刑事定罪和犯罪或保安处分相关的个人数据的处理，应当在官方机构的管理之下或者是在规定了保障数据主体权利与自由的措施的欧盟或成员国法律的授权之下进行。任何对刑事定罪信息的全面登记都只能在官方机构的管理下进行。

DPL 和 GDPR 关于“个人敏感数据”的措辞不一致，前者采用了“sensitive personal data”，后者采用了“special categories of personal data”，但二者在保护对象上基本是一致的，只是 GDPR 将“与刑事定罪和犯罪或保安处分相关的个人数据”另外做出了专条规定。

（7） “处理”

对比项目	DPL	GDPR
处理	“处理”是指获取、记录或保存数据，或对个人数据进行的任何操作或一系列操作，包括： 1. 组织、调适或更改个人数据; 2. 检索、查阅或使用个人数据; 3. 通过传输、传播或其他方式披露个人数据;或 4. 调整、合并、阻止、删除或销毁个人数据。	“处理”是指任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取收集、记录、组织、构造、存储、调整、更改、检索、咨询、使用、通过传输而公开、散布或其他方式对他人公开、排列或组合、限制、删除或销毁而公开等自动化方式。

DPL 与 GDPR 对于“处理”的定义是一致的，均为对个人数据进行的任何操作行为，包括收集、记录、存储、访问等等。

（三）数据保护原则

DPL 对数据控制者规定了实施八项数据保护原则（以下简称“DPP”）的义务，类似地，GDPR 第 5 条规定了处理数据的基本原则，即合法性、合理性、透明性；目的限制原则；数据最小化原则；准确性原则；限期存储原则；数据完整性与保密性原则和可问责原则。DPL 与 GDPR 对于此部分的规制既有相似部分也有特殊部分，以下将进行比较分析。

对比项目	DPL	GDPR
合法性原则	数据保护第一原则——公平合法处理 在此原则下要求公平处理个人数据。 1. 为了保证公平处理，必须有处理个人数据的法律依据（至少满足 DPL 附表 2 第 1-6 段中的	对涉及到数据主体的个人数据，应当以合法的…方式来进行处理。 1. 对于一般个人数据的处理，只有满足至少如下一项条件时，处理才是合法的，且处理的合法性只限于满足条件内的处理：

对比项目	DPL	GDPR
	条件之一）： (a) 同意； (b) 履行合同所必需； (c) 法律义务； (d) 保护重要利益； (e) 执行公务所必需； (f) 合法利益。 2. 对于个人敏感信息，至少满足 DPL 附表 3 中的条件之一： (a) 同意； (b) 雇佣； (c) 重要利益； (d) 非盈利性社团； (e) 数据主体公开的信息； (f) 法律程序； (g) 公共职能； (h) 医疗目的； (i) 法规规定的情形。 3. 在确定个人数据是否得到公平处理时，应考虑个人数据的取得方式，以及数据主体在数据处理的目的方面是否被欺骗或误导。此外，除非已向数据主体提供数据控制者的身份及数据处理的目的，否则将视为个人数据未获得公平处理。	(a) 数据主体已经同意基于一项或多项目的而对其个人数据进行处理； (b) 处理对于完成某项数据主体所参与的契约是必要的，或者在签订契约前基于数据主体的请求而进行的处理； (c) 处理是控制商履行其法定义务所必需的； (d) 处理对于保护数据主体或另一个自然人的核心利益所必要的； (e) 处理是数据控制者为了公共利益或基于官方权威而履行某项任务而进行的； (f) 处理对于控制者或第三方所追求的正当利益是必要的，这不包括需要通过个人数据保护以实现数据主体的优先性利益或基本权利与自由，特别是儿童的优先性利益或基本权利与自由。 第 1 段（f）点不适用公共机构在履行其任务时的处理。 2. 对于特殊类型数据的处理，则必须满足至少如下一项条件： (a) 数据主体明确同意基于一个或多个特定目的而授权处理其个人数据， (b) 处理对于控制者履行责任以及行使其特定权利是必要的，或者对于在雇佣、社会安全与社会保障法领域采取符合欧盟或成

对比项目	DPL	GDPR
		员国法律或集体协议的措施以保护数据主体的根本权利和利益是必要的； (c) 数据主体因为身体原因或法律原因而无法表达同意，但处理对于保护数据主体或另一自然人的核心利益却是必要的； (d) 基金、协会或其它具有政治、哲学、宗教或工会目的的非盈利机构的正当性活动中所进行的处理，并且已经采取了恰当的保护措施；或者处理目的仅仅和机构成员、之前成员或具有经常联系的人相关，并且个人数据在未经数据主体同意前不对实体外的人公开； (e) 对数据主体已经明显公开的相关个人数据的处理； (f) 当处理对于提起、行使或辩护法律性主张必要时，或者法院在其所有的司法活动中所进行的处理； (g) 处理对实现实质性的公共利益必要的，对实现目标是相称的，尊重数据保护权的核心要素，并且为数据主体的基本权利和利益提供合适和特定的保护措施； (h) 处理对于预防性医学或临床医学目的是必要的，或者对于评估雇员的工作能力、医疗诊断、提供——基于欧盟或成员国法律，或遵循和健康职业机构签订的契约并遵循第 3 段所规定的情

对比项目	DPL	GDPR
		形与保障措施——健康或社会保健或治疗或管理健康或社会保健体系是必要的； (i) 在公共健康领域，处理是为了实现公共利益所必要的，例如，在欧盟或成员国内已经为保障数据主体的权利与自由而采取合适与特定措施的法律基础上，处理对于预防严重的跨境健康威胁是必要的，或者为了保障医疗质量和安全、医疗产品或医疗设备的高质量和安全是必要的；或者 (j) 处理对于实现符合第 89(1)条公共利益、科学或历史研究目的或统计目的是必要的，处理采取了与其期望目的所相称的处理，尊重数据保护权的核心要素，并且对数据主体的基本权利与利益采取了合适与特定的措施。

DPL 和 GDPR 个人数据处理的合法依据总体上是一致的，而且均对个人敏感数据或特殊类别的个人数据处理合法依据做出了特殊规定，只是 GDPR 在条款的规定上更为细致。

对比项目	DPL	GDPR
目的限制原则	数据保护第二原则——为一个或多个具体的合法目的而被获取，且个人数据的后续处理不得违反以上目的。	个人数据应为特定、明确和合法的目的而被收集，并且个人数据的后续处理不得违反以上目的。依据本条例第 89 条第 1 款为公共利益进行档案管理、出于实现科学研究或历史研究目的、统计

对比项目	DPL	GDPR
		目的而进一步处理个人数据的，不应被视为不符合初始目的。

DPL 的数据保护第二原则基本上和 GDPR 的“目的限制”原则内容趋同，都强调了必须基于合法和特定目的收集数据，以及不得初始目的以外的其他目的处理数据，但 GDPR 另外规定了例外情形。

对比项目	DPL	GDPR
数据最小化原则	数据保护第三原则——就个人数据收集或处理的目的而言，个人数据必须充分、相关且不过量。	个人数据的处理应充分、相关并且应限制于为实现个人数据处理目的所需的最小限度内。

DPL 的数据保护第三原则和 GDPR 的“数据最小化”原则具有一致性，均强调了数据收集和处理的充分性、相关性和最小必要性。如果数据控制者持有的数据超过实现其目的所需的数据量，数据主体也有权要求停止数据处理。在用于所声明目的的数据不充分的情况下，数据主体可以基于更正权要求数据控制者补充不完整的数据。

对比项目	DPL	GDPR
准确性原则	数据保护第四原则——个人数据应当是准确的，如有必要，必须及时更新。	个人数据应当是准确的，如有必要，必须及时更新；必须采取合理措施确保不准确的个人数据，即违反初始目的的个人数据，及时得到删除或更正。

DPL 的数据保护第三原则对应于 GDPR 的“准确性”原则，内容基本一致。但是 DPL 对“不准确”的个人数据做出了明确定义，即指具有误导性、不完整或过时的数据。鉴于根据 DPL，数据主体的意见也属于个人数据，而意见具有主观

性，因此，意见的记录并不一定因为数据主体的不同意见或者意见被证明是错误的而成为不准确的个人数据。

对比项目	DPL	GDPR
限期存储原则	数据保护第五原则——个人数据的保存时间不得超过实现特定目的所需时间。	对于能够识别数据主体的个人数据，其储存时间不得超过实现其处理目的所必需的时间；超过此期限的数据处理只有在如下情况下才能被允许：为了实现公共利益、科学或历史研究目的或统计目的，为了保障数据主体的权利和自由，并采取了本条例第89（1）条所规定的合理技术与组织措施。

DPL 和 GDPR 均对个人数据的保存时间做出了规定。同时，DPL 第 23 条第 7 款明确规定“为了实现历史、统计或科学目的而处理的个人数据”也属于数据存储限制的例外情形。总体而言，数据控制者均应制定数据保存时间的策略，定期检查数据，并在不再需要时对该数据进行删除或匿名化处理。DPL 和 GDPR 都没有为各类数据规定特定的时间限制，因为它取决于为了实现特定目的而需要保存数据的时间。

对比项目	DPL	GDPR
数据主体的权利	数据保护原则第六原则——个人数据应根据本法规定的数据主体的权利进行处理。	/

相较于 GDPR，DPL 将“数据主体的权利”专门作为一项数据保护原则，这在某种程度上突出了对数据主体的保护。从数据主体享有的权利内容来看，GDPR 和 DPL 的规定基本上具有一致性，数据主体均享有访问权、更正权、停止/限制处理权、有关自动化决策的权利等。

对比项目	DPL	GDPR
数据完整性与保密性	数据保护第七项原则——对个人数据采取适当的技术和组织措施。	处理过程中应确保个人数据的安全，采取合理的技术手段、组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失。

DPL 第七项原则和 GDPR 的“完整性和保密性”原则的内容是一致的。在具体内容方面，DPL 做出了更为细致的规定。DPL 区分了物理安全和网络安全， 就物理安全而言，相关因素包括对商业设施的保护（如通过门锁、警报、安全警示灯、闭路电视监控等方式）、对商业设施设置访问权限和对访客的监控、信息技术设备（特别是移动设备）的安全性，就网络安全而言，需考虑的因素包括系统、数据、在线服务和设备的安全性。此外，数据控制者的全体工作人员都要理解保护个人数据的重要性，也要熟悉安全政策和程序。

对比项目	DPL	GDPR
数据跨境传输的充分保护	数据保护第八项原则——进行国际传输时，对数据主体权利和自由的保护应达到充分标准。	/

DPL 将数据跨境的“充分性保护”作为数据保护的原则之一，突出了数据出境场景下个人数据保护的重要性。另外，值得注意的是，监察专员（Ombudsman）认为，下列国家和地区的保护措施是充分的：适用欧盟 GDPR 的欧洲经济区成员国，以及欧盟委员会根据 GDPR 第 45（3）条作出认可决定的国家，或认可决定根据 GDPR 第 45（9）条仍处于有效状态的国家

（四）罚则

DPL 规定，违反 DPL（如未能根据数据主体的请求向其提供特定详细信息、在数据泄露时未能通知数据主体和行政监管部门、非法获取、披露、出售或获得个人数据、扣留、更改、隐瞒或销毁行政监管部门要求的信息、故意或过失披露信息、妨碍令状或做出虚假陈述、未能遵守执法或金钱性的强制执行令等行为）可能导致

每次违规单处或并处高达 CI$100,000 / US$122,000 的罚款以及最长 5 年的监禁。在严重违反 DPL 并可能对数据主体造成重大损害或严重影响的情况下，也可能产生高达 CI$250,000 / US$305,000 的其他罚款。

GDPR 则根据违反的条款不同，设置了不同情形下的最高额罚金：

- 如存在以下行为，则应当施加最高一千万欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额 2%的金额的罚款，两者取其高的一项进行罚款：

(a) 未准守儿童的同意的规定、未履行隐私保护设计以及默认隐私保护（PBD）、对于数据处理者的使用不合规；

(b) 违反数据泄露报告、处理安全、处理活动的记录义务；

(c) 违反数据保护影响评估和事前咨询义务/任命 DPO；

(d) 违反行为准则或认证要求。

- 如存在以下行为，则应当施加最高二千万欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额 4%的金额的罚款，两者取其高的一项进行罚款：

(a) 未符合个人数据保护原则规定、没有法定事由处理数据、未取得有效数据主体的同意、违反使用个人敏感信息的禁止性规定、不遵守数据主体权利请求或者剥夺数据主体权利、违反跨境传输的规定；

(b) 未遵照监管机构调查权/违反成员国法律；

(c) 违反数据流动暂停或终止监管要求/矫正指令。

比较 DPL 和 GDPR 的规定，就罚则类型而言，DPL 相较于 GDPR，额外规定了最长 5 年的监禁刑；就罚金额度而言，GDPR 的最高额远高于 DPL。

根据 DPL，除了罚款以外，对于有行政执法权的监管部门来说，相关部门还有权采取如下行动：

(a) 对申诉进行听证、调查和裁决；

(b) 对数据控制者的合规性进行监督、调查和报告；

(c) 对处理相关的业务进行干预、提供意见并发布指令；

(d) 命令更正、限制、删除或销毁数据；

(e) 对处理行为施加临时或永久禁令；

(f) 对一般性和针对特定数据控制者的改革提出建议；

(g) 参与违反 DPL 条款的诉讼程序，或将违反行为提交给相关监管部门；

(h) 与国际数据保护监管机构合作；

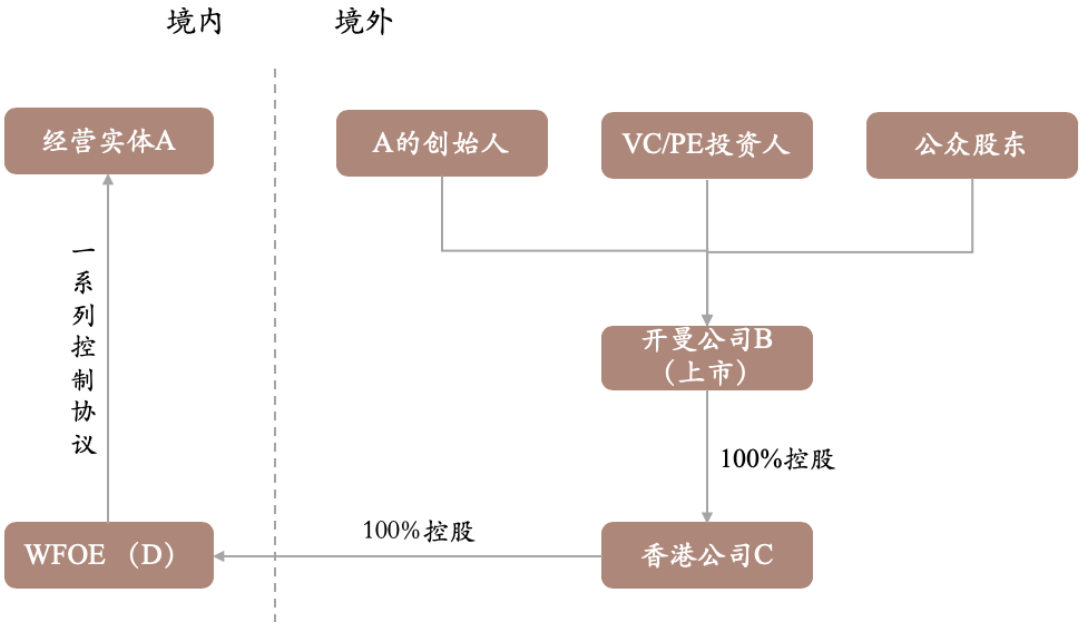
(i) 公布和宣传 DPL 的要求以及该法项下数据主体的权利；

(j) 其他看似偶然或有助于履行 DPL 所规定职能的事项。

三、DPL 生效对拟在开曼设立公司搭建 VIE 架构的企业的影响与意义简析

根据中国法律，部分行业具有严格的准入门槛，仅允许内资企业或中国籍居民从事，或者出于公司海外上市的需要，部分公司会选择通过采用 VIE 的模式，在开曼设立公司，从而实现其商业目的。

通常而言，在实践中，红筹架构的基本操作模式如下图所示：



鉴于采用 VIE 模式的公司通常会在开曼设立实体，并且在公司设立和年审过程中，在特定情形下会涉及到个人信息的收集和处理，因此，很有可能需要适用 DPL 的规定。比如说，在公司注册阶段，需要提交董事、股东的相关资料，如董事、股东为自然人的，则涉及到该主体的身份证/护照信息、个人住址、联系电话等信息。公司注册以后，为办理年审，也需要提交或更新自然人董事或股东的个人信息。因此，基于上述场景，通过 VIE 形式到开曼群岛设立公司搭建红筹架构进行海外融资或返程投资的企业有可能会被认定为是“数据控制者”，并且受到这样一部法律的约束。

此外，为了满足商业运营的需求，还有可能会涉及将开曼公司的相关数据（包括个人数据）传输至公司在第三方国家的运营实体的情形，在该场景下，公司还应当特别关注 DPL 关于数据出境的相关规定。根据 DPL 第八项数据保护原则，基于充分性保护传输个人数据应当考虑的因素包括：

(a) 个人数据的性质

(b) 数据的来源国

(c) 传输的目的国

(d) 拟处理个人数据的目的与时间

(e) 传输目的国现有的法律

(f) 传输目的国现有的国际义务

(g) 传输目的国现行的行为规范或标准

(h) 传输目的国针对数据的其他安全措施。

因此，建议该类企业在 DPL 生效之前了解这部数据保护法的基本要求、对数据的保护类型、保护原则、个人数据的权利的实现机制、以及可能受到处罚规则（高额罚款+高达 5 年的监禁）。根据不同企业在开曼处理数据的实际情况，制定并实施个人数据保护合规计划，建立有效的内部培训和治理机制，以应对 DPL 政策实现相关机构的批准、监督、实施和审查，也将成为必不可少的一环，从而避免相应的法律责任。[21]

2. 针对隐私信息管理的国际标准 ISO/IEC 27701 的简要解读（四）

如《针对隐私信息管理的国际标准 ISO/IEC 27701 的简要解读（三）》所述， ISO/IEC 27701:2019（以下简称“ISO/IEC 27701”）作为用于隐私信息管理的 ISO/IEC 27001 和 ISO/IEC 27002 的扩展，旨在增强各组织保护隐私信息的力度，但该标准对于企业在中国的合规实践并不像欧盟《通用数据保护条例》能直接给出与国内标准的相关条文对应关系那么明显。

2019 年 6 月 21 日，信安标委发布了最新版本《信息安全技术个人信息安全规范》的征求意见稿（以下简称“《个人信息安全规范（征求意见稿）》”），尽管《个人信息安全规范（征求意见稿）》仅是国家推荐标准，但在我国尚未出台《个人信息保护法》，且其他法律（包括《中华人民共和国网络安全法》）缺乏具体可操作的个人信息保护规则的情况下，《个人信息安全规范（征求意见稿）》已成为企业个人

[21] 作者：孟洁、刘成伟、谭德芳、张淑怡。

信息保护合规工作落地可参考的重要标尺。

故本文以我国国家标准《个人信息安全规范（征求意见稿）》为 ISO/IEC 27701 的对比项，解读 ISO/IEC 27701 对于企业在中国数据安全合规方面的意义。

一、《个人信息安全规范（征求意见稿）》与 ISO/IEC 27701 的对比

1. 个人信息与个人敏感信息

（1）个人信息

就个人信息的定义而言，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对个人信息下了定义，但采用了不同的表述，前者使用“personal information”，后者则使用“personal identifiableinformation”，但两者的定义在本质上是不偏离的，核心概念均为“识别”加“关联”到特定自然人，即由信息本身的特殊性识别出特定自然人和已知的特定自然人在其活动中产生的信息进行关联。但《个人信息安全规范（征求意见稿）》对个人信息的范围，在一定程度上，还会稍大一些，即它不仅涵盖了“识别”与“关联”的关系（从信息到人），而且将反映特定自然人的活动情况（从人到信息）也纳入到了个人信息的范围。

（2）个人敏感信息

《个人信息安全规范（征求意见稿）》对个人敏感信息做出了特别定义，即一旦被泄露、非法提供或滥用，可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等后果的个人信息，并在附表 B 中通过举例的方式为企业在数据合规过程中提出更具实践性的指导。

ISO/IEC 27701 采用的术语是“特殊类型的信息”，但考虑到各个国别不同的文化环境对于何为特殊类型信息的理解是不同的，ISO/IEC 27701 并未对其下明确的定义，但提示某些类别的 PII 如儿童信息、健康信息属于特殊类别的 PII，并对于该类信息应当基于更高的保护，明确要求组织在构建 PIMS 时应当结合标准所适用的所属国家数据保护法，结合当地法域中的相关规定做落地性的理解与操作。

2. 适用对象

《个人信息安全规范（征求意见稿）》的规制对象主要为个人信息控制者，虽然对委托处理行为也有相关段落的规定，但并没有明确提出个人信息处理者的概念；而 ISO/IEC 27701 则明确且详细规定了 PII 控制者和 PII 处理者的义务，并强调 PII 控制者与共同控制者、PII 控制者与 PII 处理者、PII 处理者与 PII 处理的分包商之间应当订立合同，保障对于涉及的数据采取了足够的安全和隐私保护措施，从而对个人信息在不同角色的控制或处理活动提供了全方位的保护。

就个人信息控制者的定义而言，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 对此定义规定得颇为相似，即个人信息控制者是指能够决定处理个人信息的目的和方法的控制者。但不同之处在于，ISO/IEC 27701 将出于个人目的使用数据的自然人排除在外，而《个人信息安全规范（征求意见稿）》则没有此限制。

3. 规范体系

从对个人信息处理的整个生命周期情况而言，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对个人信息的收集、保存、使用、委托处理、共享转让、公开披露进行了规定。除此之外，还通过对信息主体的权利、个人信息安全事件的处置和组织内部管理进行了规制，加强从组织与管理上对个人信息的安全与保护。但两份标准规定的颗粒度并不完全相同，具体分析如下：

（1）个人信息收集

《信息安全技术个人信息安全规范》	ISO/IEC 27701
合法性	有相似水平规定
最小必要性	有相似水平规定
不强迫接受多项业务功能	要求较低，仅提示注意某些法域的类似规定
收集个人信息时的授权同意与例外	有相似水平规定
隐私政策	要求较低，没有提供模板

从个人信息的「收集」来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对个人信息收集的合法性、最小必要性、不强迫接受多项业务功能、收集个人信息时的授权同意与例外做出规定，但《个人信息安全规范（征求意见稿）》对于组织不得强迫用户接受多项业务功能规定更为细致，包括不得捆绑产品或服务、不得频繁征求同意等，并对隐私政策应当写入的细节做出规定并提供相应的模板。作为对此条的细化，国内目前还通过 App 治理专项工作小组制定《App 违法违规收集使用个人信息自评估指南》（正面清单）与《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》（负面清单），对 App 收集用户个人信息的违法违规行为做了梳理与告诫，对企业如何正确制定隐私政策做出了细致的指引。

（2）个人信息的保存

《信息安全技术个人信息安全规范》	ISO/IEC 27701
个人信息保存时间最小化	要求更高
收集后去标识化处理	有相似水平规定
个人敏感信息的传输和存储	要求较低，仅提示注意某些法域的对特殊类型信息的特别规定
个人信息控制者停止运营	没有规定

从个人信息的「保存」来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对个人信息保存时间进行了规定，但《个人信息安全规范（征求意见稿）》对收集个人信息后推荐做去标识化处理、个人敏感信息的传输和存储和个人信息控制者停止运营后如何停止收集个人信息并删除个人信息或者做个人信息的匿名化处理都做出较为详细的规定。

（3）个人信息的使用

《信息安全技术个人信息安全规范》	ISO/IEC 27701
个人信息访问控制措施	有相似规定

个人信息的展示限制	要求较低
个人信息使用的目的限制	要求较低
用户画像的使用限制	要求较低
个性化展示及退出	没有规定
基于不同业务目的所收集的个人信息的汇聚融合	没有规定
信息系统自动决策机制的使用	要求更高

从个人信息的「使用」来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 规定的差异较大，两者虽均对个人信息的访问控制、个人信息的展示、使用目的限制、用户画像的使用限制、自动化决策进行了规定，但《个人信息安全规范（征求意见稿）》对个人信息展示限制、用户画像的使用限制、个性化展示和基于不同业务目的所收集的个人信息的汇聚融合做出较为详细的规定，相较 ISO/IEC 27701 更为全面，对于企业的实际操作性和实践性更强。

（4）信息主体的权利

《信息安全技术个人信息安全规范》	ISO/IEC 27701
查询权	要求更高
更正权	要求更高
删除权	要求较低
账户注销权	有相似水平规定
获取个人信息副本权	要求更高
响应个人信息主体的请求	要求更高

从信息主体的权利来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对查询权、更正权、删除权、注销权、获取信息副本权和响应个人信息主体请求做出规定，但 ISO/IEC 27701 对于查询权、更正权、获取信息副本权和响应个人信息主体请求权利的规定更为细致、要求更高，例如，针对查询权，《个人信息安全规范（征求意见稿）》规定组织应当向信息主体提供访问特定信息的方法，这些信息包括：

1）其所持有的关于该主体的个人信息或类型；

2）上述个人信息的来源、所用于的目的；

3）已经获得上述个人信息的第三方身份或类型。在个人信息主体提出查询非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。

而 ISO/IEC 27701 要求组织向 PII 主体提供的信息更多除上述信息外，组织还应额外提供：

1）PII 控制者或其代表人的联系方式；

2）PII 处理的法律基础；

3）PII 的传输；

4）PII 接收方的信息或 PII 接受方类别的信息

5）PII 存储期间的信息；等

此外，ISO/IEC27701 还对组织回应信息主体请求的形式做了要求，包括组织应当向 PII 主体提供清晰、易获取的与 PII 控制者和 PII 处理过程相关的信息，组织应当向 PII 主体提供及时、准确、完整、透明、易获得的信息，使用清晰、平实的表达，使目标读者易于理解，例如使用图标、图像能够帮助 PII 主体通过可视化的方式了解信息处理过程。通过对内容和形式上的要求，ISO/IEC 27701 尽可能的

保证 PII 主体的权利不仅能够实施，且可以有意义地实施。

（5）个人信息的共享、转让和公开披露

《信息安全技术个人信息安全规范》	ISO/IEC 27701
委托处理	要求更高
共享、转让	要求较低
公开披露	要求较低
跨境传输	要求更高

从个人信息的委托处理、共享、转让和公开披露来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对委托处理、共享转让、公开披露和跨境传输做出了规定，但两者对各个部分规制的颗粒度并不相同。《个人信息安全规范（征求意见稿）》对于共享转让和公开披露的要求更高，特别是《个人信息安全规范（征求意见稿）》额外考虑了组织收购、兼并、重组、破产时对个人信息转让的情况，这一点是 ISO/IEC 27701 没有涉及到的。但是 ISO/IEC 27701 在个人信息的委托处理与跨境传输机制上规定得更加丰满，比如《个人信息安全规范（征求意见稿）》并没有要求个人信息控制者对委托行为请求书面授权，仅要求信息控制者在做出委托行为时，不得超出已征得个人信息授权同意的范围。

而根据 ISO/IEC 27701 的规定，在两种情况下，组织的委托处理需要获得客户的书面授权：

1）如果组织将 PII 的部分或全部处理分包给另一个组织，则在分包商处理 PII 之前，向客户进行披露并获得客户的书面授权，既可以在 PII 处理者和客户签订的合同中约定适当授权条款，或者可以采用特定的“一次性”协议。

2）在委托处理部分 PII 或全部 PII 的组织发生变更时，需要在新的分包商处理 PII 之前，获得客户对于变更的书面授权。可以在 PII 处理者和客户签订的协议中约定适当条款，也可以采用特定的“一次性”协议的形式。

通过对于“授权”的要求，进一步提升了 PII 主体的知情权：其个人信息的全生命周期的收集和处理均可掌握。

（6）信息安全事件的报告和通知

《信息安全技术个人信息安全规范》	ISO/IEC 27701
个人信息安全事件应急处置和报告	要求更高
安全事件通知	要求更高

从个人信息安全事件的处置来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 均对个人信息安全事件应急处置和报告、告知信息主体进行了规定，但整体来看 ISO/IEC 27701 的要求更高，对于组织报告监管机构和信息主体的时间、记录义务和告知的内容更为细致，适用 ISO/IEC 27701 的相关指南有助于中国企业进一步提高合规基线，更好的处理安全事件的管理与预警。ISO/IEC 27701 对此块规定的详细内容，我们会在后期的解读中进行介绍与阐述。

（7）组织的管理要求

《信息安全技术个人信息安全规范》	ISO/IEC 27701
明确责任部门与人员	有规定，但差异较大
个人信息安全工程	要求更高
个人信息处理活动记录	有相似规定
开展个人信息安全影响评估	要求更高
数据安全能力	要求更高
人员管理与培训	有相似规定

安全审计	要求更高

从组织的管理要求来看，《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 的规制范围是相似的，但两份规定就单个要求的颗粒度差异较大。《个人信息安全规范（征求意见稿）》仅对从业人员达到 200 人或处理超过 100 万人的个人信息的组织推荐要求设立个人信息保护负责人，且对于个人信息保护负责人的职责要求较为全面；而 ISO/IEC 27701 没有限制应当设置信息保护负责人的组织类型，虽然仅对设置的信息保护负责人的职责做出了较低水平的规定，但 ISO/IEC 27701 特别要求负责人独立并直接向组织的适当管理层报告，以确保有效管理隐私风险；并要求负责人成为数据保护法律、法规和实践方面的专家。

此外，针对个人信息处理活动的记录义务，《个人信息安全规范（征求意见稿）》规定，组织“宜”建立、维护和更新所收集、使用的个人信息处理活动记录，即推荐组织进行记录但没有强制要求。

而 ISO/IEC 27701 则对此作了明确规定，为履行处理 PII 的义务，组织“应当”明确并安全保留必要的记录，并进一步要求组织应当记录的内容包括

1）处理的类型；

2）处理的目的；

3）对 PII 和 PII 主体类别的描述（如儿童）；

4）已经或者将要披露的 PII 的接收方类别，包括第三国的接收方或国际组织；

5）技术和组织安全措施的一般说明；以及

6）隐私影响评估报告。

ISO/IEC 27701 要求的个人信息处理活动的记录义务实际上对组织和信息主体均有助益。一方面，不仅有利于信息主体的访问权等权利的实现，另一方面有助于帮助企业证明合规。ISO/IEC 27701 在此方面的强制性规定。

二、结论

总体而言,《个人信息安全规范（征求意见稿）》和 ISO/IEC 27701 在适用范围、信息类别、规制对象、信息主体权利、个人信息整个生命周期（收集、保存、使用、委托处理、共享转让、公开披露）等方面所做规定的差异性并不太大，但《个人信息安全规范（征求意见稿）》作为中国的国内标准，在个人信息的定义和类别、个人信息的使用及其限制方面的规定更为全面细致，例如对于个人信息和个人敏感信息均有定义，并在附表中给出两类信息的样例，对隐私政策的内容进行要求，并给出相应的模板，特别是对于个人信息的使用部分的考虑了个性化推送、用户画像、不同业务收集数据融合 ISO/IEC 27701 未能考虑的部分。然而，ISO/IEC 27701 在信息主体的权利、组织的内控措施方面所做出的示范性要求全面且细致的，就信息主体的权利而言，不仅对于信息主体权利的内容作了更加全面的规定，例如 ISO/IEC 27701 对数据主体行使访问权时能够访问的数据相较《个人信息安全规范（征求意见稿）》更为全面，且对于组织满足数据权利的形式作了规定，例如传达的信息应当通俗易懂、准确等；就组织的内控措施而言，27701 不仅对信息安全的保护措施作了规定，还对隐私安全的保护措施作了规定，从而为构建起更为全面的信息安全和隐私保护体系，因此我们觉得值得推荐给国内的企业。

在隐私问题愈来愈严重和收到民众重视，且我国的国家标准的制定同样参考 ISO 国际标准的情况下，ISO/IEC 27701 的能够为企业构建符合多法域数据保护规定、证明企业合规性以及预测未来合规趋势提供助力。如果企业在国际化路线的布局上，可以将 ISO/IEC 27701 标准与我们国家《信息安全规范（征求意见稿）》的相关标准结合参考，将会更加有利于企业将隐私保护法律要求真正付诸企业实践。

3. 电商平台未采取足够保护措施，波兰数据保护机构开出高额罚单

2019 年 9 月 10 日，波兰数据保护机构 UODO 对遭受网络攻击的电商平台 Morele.net 处以 280 万波兰兹罗提（约 500 万人民币）的罚款。这是自 GDPR 生效以来，UODO 作出的第三笔也是罚金最高的一笔处罚。

事件背景

此次事件中，针对 Morele.net 的网络攻击发生于 2018 年 11 月和 12 月，攻击导致约 220 万人的数据落入他人手中，泄露的数据包括姓名、电话号码、电子邮件、邮寄地址。值得注意的是，本案中约 35000 人的分期付款申请书遭到泄露，然

而申请书上涵盖申请人的极为隐秘和重要的数据，包括申请人的身份证号码、其他身份证明文件、教育背景、注册地址、联络地址、收入来源、净收入额、生活开支、婚姻状况和信用承诺等。UODO 认为，Morele.net 未能采取充足的组织性和技术性保护措施，导致黑客成功入侵其系统获取了近 220 万人的数据，违反了 GDPR 第 5 条第（1）（f）项所规定的保密原则。

UODO 认为 Morele.net 采取安全措施存在以下两项漏洞：

1.**Morele.net 未能采取有效的数据访问身份验证措施。**在验证身份 Morele.net 采用的是易诱发数据泄露的单因子身份验证，没有遵循欧盟网络安全职能部门 ENISA 等机构推荐采纳的双因子安全验证措施。

2.**Morele.net 针对数据处理过程中发生的非正常网络活动未能有效监控并预警潜在的威胁。**该网站可以采取的方法包括引入入侵检测系统来警示可疑活动。在衡量罚金的金额时，一方面考虑到受影响数据主体人数高达 220 万，另一方面认识到公司为停止侵权所采取的措施、良好的配合态度且该公司之前未有触犯个人数据保护法的先例，UODO 最终给出较为缓和的 280 万波兰兹罗提的罚金。

不充足的安全保护措施将会招致更多的罚款

UODO 认为，考虑到泄露的信息的类型之特殊和受影响的群体之大，本事件属于严重的数据泄露事件，对于数据主体的个人数据落入他人之手的情况而言，对数据主体产生了高危的负面影响，他人很可能利用非法获取的数据从事身份盗窃或开具假发票等活动。Morele.net 发布声明称不接受 UODO 的处罚并已决定上诉，公司代表律师认为 UODO 对 Morele.net 处罚过于高昂，UODO 的第一笔处罚案例仅对涉事公司处以 94 万波兰兹罗提的罚款，仅为本案件罚款的三分之一左右。

纵向来看，**此次事件的罚金反映了欧洲监管机构普遍存在的增大罚金力度的趋势，特别是针对数据安全事件的处罚**；但横向来看，UODO 对 Morele.net 处以的罚金**相较于其他欧盟国家数据监管机构的罚金并不高**（例如 UK 的 ICO 今年 7 月对英国航空因数据泄露处以 1.84 亿英镑的罚金）。不管罚金如何，这起案件对于采取类似业务模式的互联网公司敲响了警钟，警示各网站须采取足够的安全保护措施（比如定期扫描漏洞、进行渗透性测试、攻防演练等）预防网络被攻击，保护好用户的个人数据的安全。

中国首家律师事务所

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