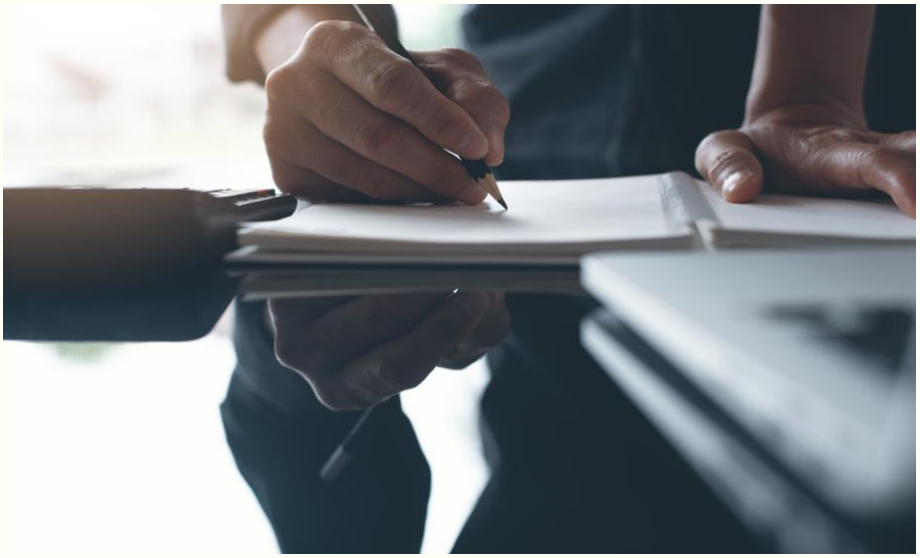
数据合规时事速递
NEWSLETTERS

2022 年 第十期 /总第四十四期



环球律师事务所
GLOBAL LAW OFFICE

2022 年 11 月 30 日

精彩导读

新规速递/ 市监总局就《反不正当竞争法（修订草案）》公开征求意见

监管动态/ 北京市监局、江苏市监局公布一批网络交易执法典型案例

相关新闻/ 2022 世界互联网大会在乌镇召开，发布中国与世界的《互联网报告》

环球解读/ 个人信息出境合规指引之三——《网络安全标准实践指南 个人信息跨境处理活动安全认证规范》

环球律师事务所
GLOBAL LAW OFFICE

前　言

随着《网络安全法》、《数据安全法》、《个人信息保护法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。

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

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

环球律师事务所
GLOBAL LAW OFFICE

孟洁 | 合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：mengjie@glo.com.cn

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

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

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

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

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

本团队专门致力于为客户提供全面且专业的法律服务，包括以下业务领域：

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

目录

新规速递

1. 市监总局就《反不正当竞争法（修订草案）》公开征求意见

11 月 22 日，国家市场监管总局发布公告，就《中华人民共和国反不正当竞争法（修订草案征求意见稿）》（下称《修订草案》）向社会公开征求意见，意见反馈截止时间为 2022 年 12 月 22 日。本次修法回应了党中央、国务院于 2022 年 3 月印发的《关于加快建设全国统一大市场的意见》中提出的要求，对现有不正当竞争行为的表现形式进行补充完善，并重点聚焦于规制数字经济下实施的新型不正当竞争行为。修改的主要内容包括：

（一）完善数字经济反不正当竞争规则，规范治理新经济、新业态、新模式发展中出现的扰乱竞争秩序的行为。《修订草案》针对数据获取和使用中的不正当竞争行为、利用算法实施的不正当竞争行为，以及阻碍开放共享等网络新型不正当竞争行为作出详细规定。同时，规定了判断是否构成不正当竞争行为的考量因素，增强制度的可预期性和执法的规范性。此外，还规定了平台经营者加强竞争合规管理的责任，推动反不正当竞争的社会共治。

（二）针对监管执法实践中存在的突出问题，对现有不正当竞争行为的表现形式进行补充完善。一是完善商业混淆条款，补充构成商业混淆的标识类型，增加自媒体名称、应用软件名称等；将销售混淆商品，以及为实施混淆行为提供便利条件的行为纳入规制范围，并区分主观故意，设定相应的法律责任。二是在商业贿赂条款中，对受贿行为作出禁止性规定。三是细化虚假宣传条款，对商业宣传的行为类型作出描述，明确禁止通过组织虚假交易、虚构评价等方式帮助其他经营者进行虚假宣传。四是加强商业秘密保护，建立健全自我保护、行政保护、司法保护一体的商业秘密保护体系。五是将指使他人实施商业诋毁的行为纳入规制范围。

（三）填补法律空白，新增不正当竞争行为的类型。一是新增损害公平交易行为，强化对中小市场主体合法权益的保护。《修订草案》对目前较为典型的损害公平交易行为进行类型化，列举了“二选一”、强制搭售等六类行为，并对如何判断“相对优势地位”作出指引。二是新增恶意交易行为，针对故意实施恶意交易，触发其他经营者受到相关规则惩戒，从而妨碍、破坏其他经营者正常经营的行为进行归纳列举，予以禁止。

（四）按照强化反不正当竞争的要求，完善法律责任。一是对损害公平交易、实施恶意交易，以及新型网络不正当竞争行为等新增违法行为设定了相应的处罚。二是增设了部分违法行为的法律责任。三是科学调整违法行为的处罚额度，降低了虚假宣传的处罚下限；同时，对于情节特别严重、性质特别恶劣、严重损害公平竞争秩序或者社会公共利益的不正当竞争行为，进一步加大打击力度。[1]

关于对《反不正当竞争法（修订草案征求意见稿）》的解读，请参见团队最新文章：《反不正当竞争法（修订草案征求意见稿）系列解读之一：完善数字经济领域的反不正当竞争规则》。敬请关注我们的后续解读。

《反不正当竞争法（修订草案征求意见稿）》全文请参见：

https://www.samr.gov.cn/hd/zjdc/202211/t20221121_351812.html

2. 国家网信办发布新修订的《互联网跟帖评论服务管理规定》

近日，国家互联网信息办公室发布新修订的《互联网跟帖评论服务管理规定》（下简新《规定》）。新《规定》自 2022 年 12 月 15 日起施行。新《规定》旨在加强对互联网跟帖评论服务的规范管理，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益，促进互联网跟帖评论服务健康发展。

《互联网跟帖评论服务管理规定》自 2017 年 10 月 1 日施行以来，对于规范跟帖评论环节信息秩序，维护良好网络环境发挥了积极作用。但随着互联网新技术新应用的快速发展，互联网跟帖评论服务也出现了许多新情况、新问题，需要适应形势发展变化进行修订完善。新《规定》共 16 条，重点明确了跟帖评论服务提供者跟帖评论管理责任、跟帖评论服务使用者和公众账号生产运营者应当遵守的有关要求等内容。

[1] 国家市场监督管理总局官网。

新《规定》明确，跟帖评论服务提供者应当按照用户服务协议对跟帖评论服务使用者和公众账号生产运营者进行规范管理。

新《规定》要求，公众账号生产运营者应当对账号跟帖评论信息内容加强审核管理，及时发现跟帖评论环节违法和不良信息内容并采取必要措施。

新《规定》强调，公众账号生产运营者可按照用户服务协议向跟帖评论服务提供者申请跟帖评论区管理权限。跟帖评论服务提供者应当对公众账号生产运营者的跟帖评论管理情况进行信用评估后，合理设置管理权限，提供相关技术支持。[2]

新修订《互联网跟帖评论服务管理规定》全文请参见：

http://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm

3. 国家市监局、国家网信办发布《个人信息保护认证实施规则》

11 月 18 日，国家市场监督管理总局与国家互联网信息办公室联合发布《关于实施个人信息保护认证的公告》，决定实施个人信息保护认证，鼓励个人信息处理者通过认证方式提升个人信息保护能力。个人信息保护认证机构应当经批准后开展有关认证活动，并按照《个人信息保护认证实施规则》（下称《规则》）实施认证。

《规则》依据《中华人民共和国认证认可条例》制定，规定了对个人信息处理者开展个人信息处理活动进行认证的基本原则和要求。

《规则》要求，个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求。对于开展跨境处理活动的个人信息处理者，还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。

[2] 国家网信办官网。

《规则》规定个人信息保护认证模式为：技术验证 + 现场审核 + 获证后监督。具体而言，首先由认证机构明确需提交的认证委托资料，并确定认证方案；技术验证机构根据认证方案实施技术认证并出具报告；认证机构实施现场审核并出具报告；再由认证机构根据上述资料作出认证决定。获得认证后，认证机构还会进行持续监督。[3]

《个人信息保护认证实施规则》全文请参见：

http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm

4. 信安标委就国标《网络安全标准实践指南 个人信息跨境处理活动安全认证规范 v2.0》公开征求意见

11 月 8 日，全国信息安全标准化技术委员会秘书处发布国家标准《信息安全技术 个人信息跨境处理活动安全认证规范 v2.0（征求意见稿）》（下称《规范 v2.0》），意见反馈截止时间为 11 月 15 日。此前，《网络安全标准标准实践指南 个人信息跨境处理活动安全认证规范》于今年 6 月 24 日正式发布。

《规范 v2.0》主要包括基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面内容，明确开展跨境处理活动的个人信息处理者申请个人信息保护认证应符合 GB/T 35273《信息安全技术 个人信息安全规范》和本文件的要求。

《规范 v2.0》要求个人信息处理者对其信息提供活动开展个人信息保护影响评估，形成报告并至少保存 3 年；明确个人信息主体有权拒绝个人信息处理者仅通过自动化决策方式作出的个人信息跨境处理决定。[4]

关于对《规范 v2.0》的解读，请参见团队最新文章：

[3] 国家网信办官网。
[4] 全国信息安全标准化技术委员会官网。

《个人信息出境合规指引之三——<网络安全标准实践指南 个人信息跨境处理活动安全认证规范>》

《信息安全技术 个人信息跨境处理活动安全认证规范 v2.0（征求意见稿）》全文请参见：

https://www.tc260.org.cn/upload/2022-11-08/1667901838651062562.pdf

5. 信安标委就国标《信息安全技术 关键信息基础设施网络安全应急体系框架》公开征求意见

11 月 17 日，全国信息安全标准化技术委员会秘书处发布国家标准《信息安全技术 关键信息基础设施网络安全应急体系框架（征求意见稿）》（下称《框架》），意见反馈截止时间为 2023 年 1 月 16 日。

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

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

《网络产品安全漏洞收集平台备案管理办法》全文请参见：

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

[5] 工业与信息化部官网。

6. 《北京市数字经济促进条例》表决通过

11 月 25 日，北京市第十五届人大常委会第四十五次会议审议了《北京市数字经济促进条例（草案三次审议稿）》，并通过了《北京市数字经济促进条例（表决稿）》（下称《条例》）。

《条例》共九章五十八条，立足北京数字经济资源禀赋、积极回应数字经济发展的客观需求，从优化数字基础设施建设、促进数据资源开发利用、做大做强数字经济产业、推进智慧城市建设，再到强化数字经济安全和保障措施，《条例》将北京行之有效的经验上升为地方立法，该条例自 2023 年 1 月 1 日起施行。

针对数字经济发展的“三要素”，即数字基础设施、数据资源和信息技术，《条例》规定了信息网络基础设施、算力基础设施、新技术基础设施等的建设要求，规定了数据汇聚、利用、开放、交易等规则。针对数字经济发展的“两条路”，即数字产业化和产业数字化，条例规定了数字产业化的技术、产业方向和企业发展目标，列举了数字化转型提升的产业领域及推动措施，还专章规定了具有北京特色的智慧城市建设，并对强化数字安全、弥合“信息鸿沟”等进行了制度设计。

《条例》规定，市、区人民政府及其有关部门应当支持数字产业基础研究和关键核心技术攻关，引导企业、高校、科研院所、新型研发机构、开源社区等，围绕前沿领域，提升基础软硬件、核心元器件、关键基础材料和生产装备的供给水平，重点培育高端芯片、新型显示、基础软件、工业软件、人工智能、区块链、大数据、云计算等数字经济核心产业。支持企业发展数字产业，培育多层次的企业梯队。

《条例》明确，支持网络安全、数据安全、算法安全技术和软硬件产品的研发应用，鼓励安全咨询设计、安全评估、数据资产保护、存储加密、隐私计算、检测认证、监测预警、应急处置等数据安全服务业发展；支持相关专业机构依法提供服务；鼓励公共机构等单位提高数据安全投入水平。支持平台企业规范健康发展，鼓励利用互联网优势，加大创新研发投入，加强平台企业间、平台企业与中小企业间

的合作共享，优化平台发展生态，促进数字技术与实体经济融合发展，赋能经济社会转型升级。[6]

《北京市数字经济促进条例》全文请参见：

http://www.bjrd.gov.cn/rdzl/dfxfgk/dfxfg/202211/t20221128_2867577.html

7. 北京市监局发布《网络交易经营者落实主体责任合规指引》

11 月 11 日，北京市市场监督管理局（下称“市监局”）网站发布《网络交易经营者落实主体责任合规指引（市场监管领域）》（下称《指引》），按照“线上线下一体化”的监管原则，立足市场监管职能，结合日常监管实践中企业合规问题突出以及企业对合规指导需求较多的领域，进一步明确市场监管领域对平台企业的合规要求，指导企业强化合规管理，帮助企业提前化解合规风险。

《指引》涉及 35 部法律、行政法规、部门规章，从整体上系统把握的同时着眼细节，聚焦关键领域、重点领域，分章节提出具体的合规要求，给网络交易经营者提供一般性的指导，帮助企业合规健康发展。

《指引》框架包括两个部分：第一部分主要为与市场监管职权事项相关的合规要求，涉及协同治理、公示提醒、反垄断、反不正当竞争、消费者权益保护、价格、互联网广告、产品质量以及食品安全九个章节，共 117 条。第二部分为其他行业领域的合规要求，市场监管部门主要是协同配合，包括个人信息保护、数据安全、算法合规、劳动者权益保护、特殊人群权益保护、其他方面合规六个章节，共 32 条。[7]

《网络交易经营者落实主体责任合规指引》全文请参见：

[6] 北京市人民代表常务委员会官网、中国工业新闻网。
[7] 北京市场监督管理局官网。

http://scjgj.beijing.gov.cn/zwxx/scjgdt/202211/t20221111_2857336.html

8. 北京市经信局印发《北京市数字化车间与智能工厂认定管理办法》

11 月 8 日，北京市经济与信息化局（下称“市经信局”）在北京市人民政府网站上发布《关于印发<北京市数字化车间与智能工厂认定管理办法>的通知》（下称《办法》）。

《办法》是为贯彻落实《北京市“十四五”时期高精尖产业发展规划》《北京市“新智造 100”工程实施方案（2021—2025 年）》等文件精神，加快数字化车间、智能工厂建设，打造北京市智能制造标杆示范，引导和鼓励北京市制造业数字化、网络化、智能化转型升级。

《办法》共六章十七条，适用于北京市数字化车间、智能工厂的认定，主要规定了申请条件、认定程序、支持措施、管理服务等内容，并随附件发布了北京市数字化车间、智能工厂建设关键要素。

《办法》明确北京市数字化车间和智能工厂每年认定一次，由市经信局负责组织实施，申报主体前一年的产值需达到一亿元以上。市经信局后续将通过北京市高精尖产业发展资金积极支持企业投资建设北京市数字化车间、智能工厂。[8]

《北京市数字化车间与智能工厂认定管理办法》全文请参见：

http://www.beijing.gov.cn/zhengce/zhengcefagui/202211/t20221110_2855591.html

[8] 北京市人民政府网。

9. 深圳发改委就《深圳市数据交易管理暂行办法》《深圳市数据商合数据流通交易第三方服务机构管理暂行办法》征求意见

11 月 18 日，深圳市发改委发布通告，就《深圳市数据交易管理暂行办法（征求意见稿）》（下称《交易管理暂行办法》）、《深圳市数据商和数据流通交易第三方服务机构管理暂行办法（征求意见稿）》（下称《数据商和第三方机构管理暂行办法》）公开征求意见，意见反馈截止时间为 2022 年 12 月 18 日。主要内容如下：

- **交易标的类型**：包括数据产品、数据服务、数据工具及经主管部门同意的其他交易标的。

- **交易准入要求**：数据交易标的在数据交易场所上市前，数据商应当提交关于数据来源、数据授权使用目的和范围、数据处理行为等方面的说明材料以及第三方服务机构出具的数据合规评估报告。数据交易主体可委托第三方服务机构开展数据资产价值评估、数据质量评估认证、数据安全检测评估认证等服务。

- **交易流程**：数据交易包括交易准备、交易磋商、交易合同签订、交付结算、争议处理等行为。需特别注意的是，数据商应提前进行合规审查，对其开发、发布、销售的交易标的进行严格审查，确保交易标的来源合法、内容真实、质量可靠。涉及跨境交易向境外提供交易标的，应当符合国家数据出境安全管理规定。

- **交易安全要求**：数据交易场所运营机构、数据卖方、数据买方、数据商和第三方服务机构应依照法律、法规、规章和国家标准的强制性要求，建立健全全流程数据安全管理制度，组织开展安全教育培训，落实数据安全保护责任，采取相应的技术措施和其他必要措施，保障数据安全。[9]

《交易管理暂行办法》《数据商和第三方机构管理暂行办法》征求意见稿全文请参见：http://fgw.sz.gov.cn/hdjlpt/yjzj/answer/24960

[9] 深圳市发展改革委员会官网。

10. 江西省发布《江西省数字经济领域反垄断合规指引》

11 月 17 日，江西省市场监督局发布《江西省数字经济领域反垄断合规指引》（下称《指引》），助力推进本省数字经济做优做强“一号发展工程”，建立健全数字经济公平竞争监管制度，引导数字经济领域的经营者增强反垄断合规意识，建立反垄断合规管理制度。

《指引》共七章三十条，规定了合规风险识别、合规重点事项、合规制度建设等内容，主要从垄断协议、滥用市场支配地位、经营者集中三个方面结合数字经济特性和应用场景分级描述了数字经济领域的违法行为以及具有数字经济特性的高风险行为；从承诺合规、配合调查、提出与撤回承诺、积极举证、豁免和适用除外、申请适用简易程序、投诉和举报等七个方面梳理了数字经济领域的经营者合规重点事项；并规定了倡导合规文化、引导行业合规、建立合规制度、开展合规培训、评估合规风险、寻求合规咨询与指导、处置合规风险和合规数字管理等相关内容。[10]

《江西省数字经济领域反垄断合规指引》全文请参见：

http://amr.jiangxi.gov.cn/art/2022/11/17/art_22493_4225088.html

11. 印度就新《数字个人数据保护法案》草案发起公众咨询

印度电子和信息技术部（下称“MeitY”）于 2022 年 11 月 18 日在公布了新的《2022 年数字个人数据保护法案》草案，并就此发起公众咨询，反馈时间截止 2022 年 12 月 17 日。自 2018 年 7 月首次提出以来，这是印度政府第四次修改该草案。该法案旨在确保个人数据的安全，在用户同意的情况下，表明收集信息的目的并确切分类。

具体而言，该法案适用于：在印度境内对数字个人数据的处理，如果这些个人数据是在网络上从数据委托人处收集的，或这些离线收集的个人数据被数字化；以及在印度境外处理的数字个人数据，如果

[10] 江西省市场监督管理局官网。

这种处理与向印度境内的数据委托人提供商品或服务的任何分析或活动有关。

该法案规定了个人数据的处理方式，承认用户保护其个人数据及合法处理个人数据的权力。目前的立法要求公司（即数据处理者）遵循足够的安全保障措施来保护用户信息，在发生数据泄露时提醒用户，并在个人选择删除账户时停止保留用户数据。此外，该草案还规定了数据最小化的要求，以及公司必须采取的额外防护措施，以防止未经授权收集或处理个人数据。

值得注意的是，该法案不再强制要求数据本地化，允许将个人数据传输到印度境外的某些被指定的国家和地区；但是，在发出指定通知之前，中央政府将对相关因素进行评估。此外，该法案规定，由中央政府设立的印度数据保护委员会将负责执行其规定。该法案还规定，如果出现未能遵守该法案的严重情形，该委员会可以施加不超过 500 亿印度卢比（约 5,900 万欧元）的罚款。[11]

《2022 年数字个人数据保护法案》全文请参见：

https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

12. 沙特阿拉伯就《个人数据保护法》拟议修正案发起公众咨询

11 月 20 日，沙特阿拉伯数据和人工智能管理局（下称“SDAIA”）就其对《个人数据保护法》的拟议修正案发起了公众咨询，咨询期截止到 2022 年 12 月 20 日。该法由 2021 年 9 月 17 日的第 M/19 号皇家法令批准，并由 2021 年 9 月 14 日的第 98 号决议（下称“PDPL”）执行。就此次修订，拟议的修正案主要包括以下内容：

在数据主体有权以可读和清晰的格式获得个人数据方面，第 4 条被修订后已包括数据可携权，即如果技术上可行，数据主体有权要求将其个人数据转移至另一个控制者。

[11] The Hacker News.

在数据处理的合法性依据方面，第 10 条进行了有关修订，将控制者或任何其他方的合法利益作为新情形，如果个人数据不是敏感的，可以允许在没有获得数据主体同意的情况下进行处理。

在营销方面，第 26 条修改后允许出于营销目的处理个人数据，但要有明确的机制，该机制必须允许目标接收者随时要求停止处理，并且必须允许仅仅在下述情形处理敏感的个人数据，即直接从数据主体处收集，而且数据主体对出于营销目的进行这种处理作出明确同意。

在数据跨境传输方面，第 28 条此前涉及身份证明文件的复印，现在修订为允许在特定情况下根据某些条件将数据转移到国外；第 29 条此前是禁止向国外转移数据的，现在规定，主管部门应是负责监督 PDPL 及其《执行条例》执行情况的实体，可以将其部分责任委托至其他公共机构，且控制者可能被要求协助主管部门确保遵守 PDPL。

在个人数据记录的保存方面，第 30 条作出了控制者应保存对个人数据进行操作的记录，并应制定相应的规则以限制对这些数据的访问的补充规定。[12]

更多内容请参见：https://www.dataguidance.com/news/saudi-arabia%C2%A0sdaia-launches-public-consultation

[12] DataGuidance 官网。

环球律师事务所
GLOBAL LAW OFFICE

监管动态

1. 北京市通管局通报 22 款问题 App

北京市通信管理局（以下简称“通管局”）依据《网络安全法》《数据安全法》《个人信息保护法》《网络产品安全漏洞管理规定》《电信和互联网用户个人信息保护规定》等法律法规，按照工业和信息化部《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》等工作部署，持续开展 APP 隐私合规和网络数据安全专项整治。11 月 24 日，通管局通报 20 款需整改 App 与 2 款整改不合格下架 App。

此次通告所反映的违规问题包括：（1）违反必要原则，未明示收集使用个人信息的目的、方式和范围，违规向他人提供个人信息，未经用户同意收集使用个人信息，账号注销难，App 频繁自启动和关联启动；（2）应用数据任意备份风险；（3）在网站或移动应用程序前后端数据传输过程中，为对敏感个人信息进行加密；（4）具有用户信息验证、营销活动推广等跨平台用数据提供场景的业务，企业未在提供数据前征得用户明示同意；（5）强制用户使用定向推送功能；（6）更正、删除个人信息及注销账号难，未公布个人信息安全投诉、举报渠道等；（7）Zip 文件解压目录遍历漏洞、Janus 签名机制漏洞、Webview 远程代码执行漏洞、未移除有风险的 Webview 系统隐藏接口漏洞。[13]

2. 北京市市监局公布十一件网络交易执法领域典型案例

11 月 9 日，北京市市场监督管理局（以下简称“市监局”）发布十一件网络交易执法典型案例，涉及虚假广告、价格欺诈、商标侵权、不正当竞争等违法行为，以更好警示违法者，提醒消费者，充分发挥社会舆论监督作用。案例情况总结如下：

（一）北京新运动电子商务有限责任公司在微信公众号上发布促销广告，内容为“今天除了疫情，战争，坠机，还有促销！淘宝新势力周活动，跨店满（199-20），不封顶”。此种借机蹭热度进行营销

[13] 北京市通信管理局官网。

的行为违背了社会公序良俗，造成了不良社会影响，违反了《广告法》。执法机关责令其停止违法行为，并罚款 20 万元。

（二）北京中航天使教育科技集团有限公司在其发布的互联网广告中漏绘我国南海诸岛，严重损害了国家尊严和利益，误导社会公众，扰乱市场秩序，违反《广告法》。执法机关责令其停止违法行为，并罚款 40 万元。

（三）北京西美医疗美容门在大众点评店铺销售美容商品，2021 年 10 月 10 日至 2022 年 7 月 11 日期间价格展示为“¥17940 已优惠 8060”，未表明折价、减价的计算基准，违反《价格法》。执法机关责令其责令停止违法行为，并罚款 6 万元。

（四）北京早春二月餐饮管理有限公司未按要求在网上真实公示菜品主要原材料，误导消费者，违反《网络餐饮服务食品安全监督管理办法》。执法机关责令其责令改正违法行为，并罚款 5000 元。

（五）北京易捷顺达汽车租赁有限公司未经“e 代驾”许可，使用与其注册商标相同或者近似的商标，违反《商标法》。执法机关责令其责令停止侵权行为，并罚款 12.5 万元。

（六）北京七月麦香餐饮管理有限公司未及时更新平台公示主体信息案，且未按照要求改正违法行为，违反了《电子商务法》。执法机关责令其责令改正违法行为，并罚款 7000 元。

（七）北京森之脉生物科技有限公司未经授权擅自使用“同仁堂”商标，在其店铺名称前突出使用，属于足以引人误认为与他人存在特定联系的混淆行为，违反了《反不正当竞争法》。执法机关责令其责令改正违法行为，并罚款 3 万元。

（八）北京翰海辰星商业有限公司为提升商品销售量，通过虚假交易的方式，在某电商平台完成订单 54 单，完成交易 1.296 万台，完成商品虚假评价 1280 条。该行为构成对商品的销售状况、用户评价作虚假或者引人误解的商业宣传的行为，违反《反不正当竞争法》。执法机关责令其责令停止违法行为，并罚款 40 万元。

（九）北京乐纯悠品食品科技有限公司在其天猫旗舰店对所售的乐纯儿童乳酪棒进行宣传时称，其竞争对手公司出品的百吉福成长奶酪含有大量的添加剂，吃多了会影响孩子身体发育，暗示选择该款成长奶酪等类似奶酪棒是错误的选择。该行为属于损害竞争对手商品声誉的商业诋毁行为，违反了《反不正当竞争法》。执法机关责令其责停止违法行为，并罚款 10 万元。

（十）谦的朋友（北京）文化传媒有限责任公司为了吸引点击量，在抖音平台账号展示的视频含有“直到今天我公司的销售额从零到破亿”“抖音四个月赚了 2 个亿”“变现了两个亿”等内容，属于虚假宣传的违法行为，违反了《反不正当竞争法》。执法机关责令其停止违法行为，并罚款 30 万元。

（十一）成都抖咖文化传播有限公司旗下某主播在为某品牌螺蛳粉进行直播带货过程中，将该品牌螺蛳粉与其他品牌螺蛳粉并列摆放，并使用“那个是什么鬼，我真的不明白那个是什么鬼”“它连及格线都不到”等言语，通过贬低其他品牌螺蛳粉的方式进行引人误解的商业宣传，违反了《反不正当竞争法》。执法机关责令停止违法行为，并罚款 20 万元。[14]

3. 江苏省市监局公布八件互联网领域反不正当竞争典型案例

11 月 9 日，江苏省市监局官方微信发布互联网领域反不正当竞争典型案例，涉及篡改伪造销售量、虚构商品交易记录、实施混淆行为、商业诋毁、虚假宣传、虚假交易、生产销售不合格产品等不正当竞争行为。下文摘录部分典型案例：

（一）在无锡某商贸有限公司篡改**伪造销售量案**中，为营造其网店在售商品销量巨大的假象，诱导消费者购买其商品，公司雇佣他人对部分商品宣传页面中的销量数据进行篡改，篡改后的累计销量数据均为“10 万+”，远高于商品实际的销售数据。其行为违反了《反不正当竞争法》第八条第一款，被处于 5 万元罚款。

[14] 北京市市场监督管理局官方微信公众号。

（二）在睢宁某商贸有限公司**虚构商品交易记录**案中，公司在某接单平台充值 123093.50 元，主要用于对专营店销售的带挂钩超市货架进行刷单，对商品的销售数量、用户评价作虚假宣传。上述商品成交量共计 231 件，交易金额 97541 元，其中，虚构交易量 85 件，金额 35099 元。该行为违反了《反不正当竞争法》第八条的规定，被处于 2 万元罚款。

（三）在苏州某商贸有限公司**实施混淆行为**案中，公司在短视频平台账号中多处使用“戎美”字样，并在消费者提出“是淘宝那个戎美？”等问题时，给予肯定的答复。其行为足以使消费者误以为当事人，与“戎美”商标持有者日禾戎美股份有限公司及其经营的品牌服饰存在特定联系，违反了《反不正当竞争法》第六条第一项、第二项的规定，被处以 5 万元的罚款。

（四）在常州某汽车销售服务有限公司**商业诋毁及虚假宣传**案中，汽车销售公司在其短视频平台账号发布宣传广告视频称“它的用料比奥迪好十倍，是 SUV 圈里之光，品控、用料，比奥迪好十倍，……”对比的为奥迪 Q3 和 Q5 车型。公司无法提供“用料比奥迪好十倍”的相关证据。截止案发，该视频播放量为 17.3 万。该公司使用不实宣传用语，构成虚假宣传，并且将本店商品与奥迪汽车相比较，构成损害竞争对手商品声誉的违法行为，被处于 20 万元的罚款。

（五）在南通某纺织科技有限公司**虚假宣传、生产销售不合格产品**案中，纺织科技有限公司的一款商品在直播间购物车内的链接名称为“纯棉澳棉长绒棉磨毛四件套”，线下商品实际名称为“100 支珍珠磨毛高定刺绣四件套”。公司直播宣传该商品为“全棉”、“100 支纯棉磨毛”，棉是“澳洲进口”。经过技术检测，公司在直播间的宣传内容与其实际情况不符。执法部门认为该公司使用不实标语欺骗、误导消费者，违反了《反不正当竞争法》与《产品质量法》，没收违法所得 0.76 万元，并处以罚款 20 万元。

（六）在李某军**虚假交易**案中，李某军使用其本人及配偶居民身份证注册两个网店销售童鞋。当事人通过后台批发采购程序多次利用他人及本人名义在上述两个网店下单购买童鞋，实际并未发货。当事人通过上述方式在其中一家网店分 12 次增加了 116500 双的销量记

录，在另一家网店分 6 次增加了 300000 双的销量记录。该行为违反了《反不正当竞争法》第八条第一款，被处以 4 万元罚款。[15]

4. 内蒙古通管局下架 16 款未按要求完成整改的问题 App

11 月 11 日，内蒙古自治区通信管理局（下称“通管局”）发布《关于下架侵害用户权益 App 名单的通报》（2022 年第 2 批，总第 2 批）。通管局针对 9 月 26 日公开通报的 47 款侵害用户权益的 App 进行了复检，发现其中仍有 16 款问题 App 未按要求完成整改，依然存在“违规收集个人信息”、“App 强制、频繁、过度索取权限”、“超范围收集个人信息”、“强制用户使用定向推送功能”的问题。

通管局依据《网络安全法》《电信和互联网用户个人信息保护规定》《移动智能终端应用软件预置和分发管理暂行规定》等法律法规和规范性文件要求，决定对上述 16 款问题 APP 予以下架处置。[16]

5. 工信部通报 2022 年第三季度电信服务质量

11 月 16 日，工业和信息化部官网公布的 2022 年第三季度电信服务情况显示，已组织对重点应用商店及分发平台进行检查，推动在架 APP 抽测合格率整体环比提升 14.4%。其中，vivo、华为应用商店的合格率名列前茅。

三季度，工业和信息化部组织检测 66.5 万款 APP，责令整改 222 款，公开通报 47 款。各地通信管理局加强监督执法。其中，对存在携号转网服务问题的企业，约谈提醒 36 家次，责令整改 32 家次，通报批评 4 家次，行政处罚 7 家次；对存在垃圾信息问题的企业，约谈提醒并责令整改 53 家次，通报批评 87 家次，行政处罚 12 家次。30 家企业因受到行政处罚被列入电信业务经营不良名单。

此外，对于用户的申诉与投诉，工业和信息化部公示了 2022 年第三季度用户申诉主要涉及的移动转售企业名单和互联网信息服务

[15] 江苏省市场监督管理局微信公众号。
[16] 内蒙古自治区通管局官网。

投诉处理及时率未达标的企业名单。工业和信息化部已督促相关企业改进服务，解决用户反映的问题，不得侵害电信用户的合法权益。

与此同时，工业和信息化部还作出了两点经营和消费提示：（一）要求各基础电信企业要进一步规范经营行为，明示资费标准、服务内容、适用范围等重点事项，让用户明明白白消费。各互联网企业要持续提高服务热线的人工接听率和用户投诉处理及时率，积极回应用户诉求，优化服务体验；（二）提醒广大用户，通过电子商务或网络直播等互联网渠道购买电话卡、流量充值或办理其他电信业务时，要选择基础电信企业自营或授权（有统一的网络渠道电子标识牌公示）的正规渠道，不要轻信“0 元”、“免费送”等营销陷阱，谨防自身权益受到损害。[17]

相关企业名单请参见：
https://www.miit.gov.cn/zwgk/zcwj/wjfb/tg/art/2022/art_5e7b0a3f341944b38971daed080eb89a.html

6. 多省网信办开展 2022 年度汽车数据安全管理情况报送工作

近期，根据《汽车数据安全管理若干规定（试行）》，北京、天津、四川、浙江、江西和湖南等地的网信办组织开展了 2022 年度北京市汽车数据安全管理情况报送工作，要求开展重要数据处理活动的汽车数据处理者，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业编制《2022 年度汽车数据安全管理情况报告》，加盖企业公章，向所属地区的网信办报送。报送截止日期为 2022 年 12 月 15 日。

同时，各地网信办将依据报送情况，选择部分重点企业进行实地走访调研，指导排查数据安全风险隐患。[18]

汽车数据安全管理情况报告（参考模板）下载地址：https://pan.baidu.com/s/1xxXmN1trreqMPY1ZFJkw1g；提取码：lyh9

[17] 工业与信息化部官网。
[18] 各地网信办微信公众号。

7. 英国信息专员办公室就信息自由投诉的优先次序问题开展咨询

近日，英国信息专员办公室（下称“ICO”）就处理其收到的有关公共机构处理信息自由（下称“FOI”）请求的投诉的优先次序问题向公众征求意见。由于近年来 FOI 服务的需求增加，加上资金有限，ICO 需要更好地选择如何将资源分配给那些重要的问题。ICO 提议将优先处理那些被要求提供的信息中存在明显公共利益的投诉。公共利益包括与公共利益有关的广泛价值观和相应原则，或符合社会最佳利益的事物。

此次意见征求中提出了新的优先次序标准，将涵盖根据《信息自由法》和《环境信息条例》提出的投诉。新标准包括应用以下测试：

- 所申请的信息是否具有高度公共利益？它是否提出了一个新的或具备受瞩目的问题，以至于应该被迅速查看？
- 申请者是否是旨在提高信息权意识、支持弱势群体或旨在提高对潜在重大公共利益问题认识的个人或团体？
- 弱势群体或个人是否有可能受到所申请信息的重大影响？
- 优先次序的确定是否会产生显著的实际利益或支持那些被监管者？

确定优先次序并不意味着 ICO 将预先确定投诉的结果。ICO 可能支持投诉，也可能不支持。在可能的情况下，ICO 将根据其收到的信息通过决定或诉讼来解决一个投诉。上述做法能够尽快为申请者提供关于 ICO 决定的监管确定性。申请者或政府机构也可以随后按照其意愿继续推进投诉，以获得包括向法庭申诉在内的其他救济。[19]

[19] 英国信息专员办公室官网。

8. 欧洲数据保护监督员就网络安全要求条例发表意见

11 月 15 日欧洲数据保护监督员（下称“EDPS”）宣布，其已于 2022 年 11 月 10 日发布了关于拟议的《对具有数字要素产品的横向网络安全要求的条例建议》的第 23/2022 号意见，旨在为广泛的硬件和软件产品及其远程数据处理解决方案制定欧盟范围内的网络安全要求。可能受到拟议条例影响的产品包括浏览器、操作系统、防火墙、网络管理系统、智能电表或路由器等。

监督员 Wojciech Wiewiórowski 表示：“具有数字要素的产品的网络安全对于有效保护数字时代个人的基本权利至关重要，包括他们的隐私权和数据保护权。”EDPS 乐于接受拟议条例的措施，即将安全原则和数据最小化原则作为欧盟范围内网络安全要求的重要组成部分。然而，EDPS 也建议将数据保护设计原则和默认数据保护原则作为这些要求的组成部分。

此外，EDPS 建议澄清包括欧洲数据保护委员会在内的相关机构和组织之间设想的协同作用的类型，EDPS 同时强调，根据网络安全标准化和某些数字要素产品的认证情况，拟议的欧洲网络安全证书不应作为《通用数据保护条例》认证的替代品。

最后，EDPS 建议澄清拟议条例和欧盟数据保护法律之间的关系，特别是这些法律及条例在市场监督和执法领域将如何互动。EDPS 认为，拟议条例不应影响或试图影响现有的欧盟法律，这些法律已经规范了个人数据的处理以及独立数据保护机构的任务和权力。[20]

[20] 欧盟数据保护监督员官网。

环球律师事务所
GLOBAL LAW OFFICE

相关新闻

1. 2022 年世界互联网大会在浙江乌镇举办

11 月 9 日至 11 月 11 日，2022 年世界互联网大会乌镇峰会在浙江乌镇举办。乌镇峰会已连续成功举办九年。此次峰会亦是世界互联网大会国际组织成立后的首次年会。峰会围绕“共建网络世界 共创数字未来——携手构建网络空间命运共同体”的主题，采用“线上线下”相结合的方式举办，受到国际社会的广泛关注。

本届世界互联网大会围绕全球发展倡议数字合作、数字经济、数据治理、疫情下的数字社会、人工智能与数字伦理、弥合数字鸿沟、网络传播与和平发展、网络法治、网络安全技术发展和国际合作等议题深入交流、热烈讨论，在加强数字合作互利共赢、数字经济创新发展、数字生态安全治理等方面形成广泛共识，“携手构建网络空间命运共同体”“走出一条全球数字发展之路”获得与会各方的高度认可和热烈响应。

本届大会从全球 100 多个国家申报的 210 余项案例中，精选 12 项案例在此次峰会期间集中发布。全方位生动讲述网络基础设施建设、网络文化交流、数字经济创新发展、网络安全保障、网络空间国际治理五大领域美美与共的动人故事。

同时，大会还发布了“世界互联网领先科技成果”，评选出来自高通、华为、北京大学等企业和机构的 15 项代表性科技成果，展现了全球数字技术的强大活力，成为展示全球前沿技术、激发数字创新思想的重要窗口。

而在 11 月 10 日上午，峰会还举行了“网络空间国际规则：实践与探索”论坛。论坛就“围绕促进数字基础设施普惠接入加强国际合作”“加快构建数字规则体系，加强数字发展国际合作”“构建网络空间国际治理新秩序”等进行交流探讨、发表看法，并发布了《“构建网络空间命运共同体”系列国际研讨会成果汇编》。

成果汇编全文请参见：https://cn.wicinternet.org/pdf/《“构建网络空间命运共同体”系列国际研讨会成果汇编》(中文版).pdf。[21]

2. 世界互联网大会发布中国与世界的《互联网发展报告》

11 月 9 日，《中国互联网发展报告 2022》和《世界互联网发展报告 2022》蓝皮书在乌镇峰会上发布。蓝皮书由中国网络空间研究院牵头编撰、国内外互联网领域高端智库和研究机构支持参与，充分展现互联网发展的新进展、新成就、新趋势，已连续发布六年。

《中国互联网发展报告 2022》立体全面呈现中国互联网发展的新探索、新实践、新成就。一年来，中国信息基础设施建设全球领先，一体化大数据中心完成布局；数字经济赋能作用凸显，数据要素市场加速培育；数字化公共服务效能增强，社会治理向智慧化方向发展；网络文明建设稳步推进，网络综合治理体系更加健全；数据安全保护体系初步建立；网络法治建设逐步完善；网络空间国际交流合作务实高效，数字合作展现新作为。

而《世界互联网发展报告 2022》立足全球视野，充分反映各国互联网建设新举措、新进展。一年来，全球信息基础设施优化升级，卫星互联网商用部署加快；数字技术发展驶入快车道，人工智能技术应用场景拓宽；数字经济助力全球经济复苏，地区间“数字鸿沟”加大；数字政府建设水平提升，各国差距明显；互联网媒体多元化发展，社交媒体成舆论主战场；网络安全漏洞频现，网络攻防对抗加剧；网络立法进程加快，数字市场监管日益强化；网络空间国际竞争加剧。[22]

3. 最高检发布 2019 年以来检察机关办理个人信息保护领域公益诉讼案件数据统计

11 月 10 日，最高人民检察院发布检察机关办理个人信息保护领域公益诉讼案件数据分析。数据显示，2019 年以来，全国检察机关共立案办理个人信息保护领域公益诉讼案件 8361 件，其中，2019 年立

[21] 2022 年世界互联网大会官网。
[22] 国家互联网信息化办公室官网。

案 147 件，2020 年立案 750 件，2021 年立案 2276 件，2022 年 1 月至 9 月立案 5188 件，案件数量逐年上升。其中，2022 年 1 月至 9 月批捕 1199 人、起诉 6223 人，较 2018 年同期分别下降 47.2%、上升 87.9%。

最高检第一检察厅厅长苗生明表示，对侵犯公民个人信息案件的起诉人数逐年上升，说明检察机关持续加大打击犯罪力度。批准逮捕人数大幅下降，说明检察机关在办案中严格落实少捕慎诉慎押刑事司法政策。在侵犯公民个人信息案中，大部分犯罪嫌疑人主动认罪认罚，对他们采取非羁押监管措施能够保证诉讼顺利进行，也体现了在惩罚犯罪的前提下，加强人权司法保障、促进社会和谐的理念。

最高检第八检察厅副厅长邱景辉认为，《个人信息保护法》出台后，检察机将聚焦严重侵害社会公共利益的侵犯个人信息违法行为，充分发挥公益诉讼制度在个人信息安全溯源治理方面的优势，积极履职。随着相关工作的不断深入，检察机关办理的个人信息保护领域公益诉讼案件数量逐年增长，也在该领域探索创新了一些独具特色的办案方法。

同时，党的二十大报告提出“完善公益诉讼制度”。在个人信息保护领域，检察机关将做好公益诉讼检察工作与其他保护机制的制度衔接，检察机关对内不断强化“四大检察”协同发力，对外加强与公安、网信、市场监管、工信等行政机关的协作配合，形成保护公民个人信息合力。[23]

4. 公安公安侦破涉及 27 个省份特大系列侵犯公民个人信息案件

近日，黑龙江鸡西市公安局成功侦破一起特大系列侵犯公民个人信息案件，共计抓获犯罪嫌疑人 322 名，涉及全国 27 个省份。

今年 2 月，鸡西市公安局发现辖区内有居民大量收租微信号、QQ 号，并以从中赚取差价的方式进行牟利。鸡西市公安局组织 100 余名

[23] 中华人民共和国最高人民检察院官网。

警力，先后辗转湖南、河南、云南等 7 省份 12 地，共抓获犯罪嫌疑人 50 名，捣毁窝点 10 处，缴获全部涉案工具。

经查，该犯罪团伙组织严密，分为“客服、中介、粉商、号商、租号人员”五个层级，通过境外聊天软件互相勾连，层层转包、加价。以发布招嫖信息等诱导性信息吸粉引流，再通过租收的微信号进行登录，发布虚假信息，以达到获取巨额不法利益的目的。

今年 9 月 22 日，警方再次抽调警力，一举全链条摧毁该犯罪团伙，共抓获犯罪嫌疑人 322 名，依法扣押涉案资金 560 余万元，扣押电脑 78 部，手机 412 部，涉案银行卡 638 张。目前案件进一步办理中。[24]

5. 中国在联合国提交《中国关于加强人工智能伦理治理的立场文件》

11 月 16 日，中国裁军大使李松率团出席在日内瓦举行的联合国《特定常规武器公约》2022 年缔约国大会，并向大会提交了《中国关于加强人工智能伦理治理的立场文件》。李松大使指出，人工智能，伦理先行。作为最具代表性的颠覆性技术，人工智能在给人类社会带来潜在巨大发展红利的同时，其不确定性可能带来诸多全球性挑战，甚至引发根本性的伦理关切。

李松表示，中国的立场文件系针对国际社会的广泛关注而提出。中国始终致力于在人工智能领域构建人类命运共同体，积极倡导“以人为本”和“智能向善”理念，主张增进各国对人工智能伦理问题的理解，确保人工智能安全、可靠、可控，更好赋能全球可持续发展，增进全人类共同福祉。为实现这一目标，中国呼呼各方秉持共商共建共享理念，推动国际人工智能伦理治理。

在结合了中国在科技伦理领域的政策实践，参考了国际社会有益成果后，中方在文件中就人工智能生命周期监管、研发及使用等一系列问题提出以下主张：一是人工智能治理应坚持伦理先行，通过制度

[24] 央视财经微信公众号。

建设、风险管控、协同共治等推进人工智能伦理监管；二是应加强自我约束，提高人工智能研发过程中算法安全与数据质量，减少偏见歧视；三是应提倡负责任使用人工智能，避免误用、滥用及恶用，加强公众宣传教育；四是应鼓励国际合作，在充分尊重各国人工智能治理原则和实践的前提下，推动形成具有广泛共识的国际人工智能治理框架和标准规范。[25]

6. 上海嘉定法院发布首批 10 个数字经济司法典型案例

11 月 17 日，上海市嘉定区人民法院（下称“上海嘉定法院”）举行新闻发布会，发布上海法院数字经济司法研究及实践（嘉定）基地首批典型案例。此次发布的首批典型案例以上海嘉定法院近两年的生效案例为主，还有来自江苏昆山法院、江苏太仓法院等上海法院数字经济司法研究及实践（嘉定）基地（以下简称基地）首批战略合作单位推荐的案例。

首批典型案例根据数据流通、相关主体权益及市场秩序保护的需要，结合数据所涉客体、主体、法律关系特征，以基地对数字经济案件分类体系为基础，聚焦四大方面，包括：

一、 涉个人信息处理或利用网络侵害其他人格权典型案例

1. 微博大 V 网络言论自由与侵害名誉权边界
2. 电子商务平台经营者处理个人信息合法性基础的认定

二、 涉数据形态财产权益及市场竞争秩序保护典型案

3. 网络游戏账号限制自由转让约定的效力及虚拟财产价值认定
4. 设置网页推广关键词侵害商标权及不正当竞争竞合的处理

三、 涉平台经营者/数据算法运用者法定义务及相关主体权益保护典型案

5. 网络接入服务提供者网站备案信息真实性核验义务的认定
6. 网络货运平台司机提供劳务受损赔偿责任的认定

[25] 中华人民共和国常驻联合国日内瓦办事处和瑞士其他国际组织代表团官网。

7. 平台在网约顺风车交易中的安全保障义务及侵权责任的认定

四、 涉侵害数据形态权益、利用数据技术实施网络犯罪及灰黑产业防治典型案例

8. 买卖公民个人信息的刑事责任及相关灰黑产业链的规制

9. 非法搭建“第四方支付平台”为商户提供收付款服务的认定

10. 切断分时租赁汽车定位系统逃避租金行为的定性

具体案例内容请见：[26]

https://mp.weixin.qq.com/s/rmP7ZGqQH-6WjE3YY33gdA

7. 香港个人资料私隐专员公署发表两份案例调查报告

11 月 14 日，香港个人资料私隐专员公署发表两份与个人信息安全及数据安全相关的调查报告：（一）医思健康透过统一系统互用旗下品牌客户的个人资料；及（二）快图美（远东）有限公司（快图美）数据库遭勒索软件攻击。

在第一个案例中，个人资料私隐专员发现医思健康在收购汇儿及纽约医疗后，将后两者客户的个人资料储存与其系统中，并将客户的部分个人资料在医思健康旗下使用该系统的 28 个品牌之间互用，使有关资料可被不同品牌的前线职员查阅。客户在投诉过程中也表示，他们本来只向个别品牌提供的个人资料，在不知情的情况下，被披露及转移给其他品牌的职员。在此情况下，私隐专员认为 EC Healthcare 违反了《个人资料条例》附表 1 中《保障资料原则》第 3(1)条关于使用（包括披露和传输个人数据）的规定。因此，私隐专员向 EC Healthcare 送达了执行通知书，指示其补救及防止再次发生相关违规行为。

在第二个案例中， 2021 年 11 月 1 日公署收到快图美的资料泄露事故通报，表示其网上商店的数据库于 2021 年 10 月 26 日遭勒索软

[26] 上海最高人民法院官方微信公众号。

件攻击及恶意加密。事件共影响 54 万余名会员及 7 万余名曾在 2020 年 11 月 16 日至 2021 年 10 月 26 日期间于快图美网上商店订购产品及/或接受服务的客户。隐私专员发现 Fotomax 在风险意识和个人数据安全措施方面存在严重缺陷，导致数据库遭到勒索软件攻击。私隐专员认为，Fotomax 没有采取所有切实可行的步骤来确保所涉及的个人资料受到保护，免遭未经授权或意外的访问、处理、删除、丢失或使用，因此违反了《个人资料条例》第 4(1)条关于个人资料安全的规定。隐私专员已向 Fotomax 发出执行通知，指示 Fotomax 采取补救措施。[27]

两个案例的完整调查报告请参见：

https://www.pcpd.org.hk/english/news_events/media_statements/press_20221114.html

8. 西班牙数据保护局对 BBVA 违反 GDPR 原则罚款 80,000 欧元

西班牙数据保护局（下称“AEPD”）于 2022 年 11 月 10 日公布了其在第 PS/00419/2022 号诉讼案中的决定，根据个人控诉，AEPD 对毕尔巴鄂比斯卡亚阿根廷银行（下称“BBVA”）违反《通用数据保护条例》（欧盟第 2016/679 号条例）（下称“GDPR”）第 5 条(1)款(f)项和第 32 条的行为处以 80,000 欧元罚款，随后降为 48,000 欧元。

AEPD 提到，原告要求 BBVA 提供其账户的所有权证明时，收到的却是一份第三方合同的副本。另外，AEPD 还确认原告已告知 BBVA，其仍可通过与 BBVA 的对话记录获取该文件，且该文件未被删除。在调查结果中，AEPD 认为上述情况造成了个人数据安全泄露事件，并将此归类为违反保密性原则的情形，因为其向原告提供的合同中含有第三方个人数据。就此，AEPD 决定根据 GDPR 第 5 条(1)款(f)项，对 BBVA 违反完整性和保密性原则的行为处以 50,000 欧元罚款。

AEPD 进一步强调道，在违法行为发生时，BBVA 没有足够的技术和组织措施来预防第三方合同出现的状况。AEPD 于是另外决定对 BBVA 违反 GDPR 第 32 条的行为处以 30,000 欧元的处罚。因此，

[27] 香港个人资料私隐专员公署官网。

AEPD 对 BBVA 违反 GDPR 第 5(1)(f)条和 32 条的行为共处以 80,000 欧元的罚款。此外，根据相关规定，BBVA 可在提出指控的期限内主动承担责任，这将使处罚程序中实施的罚款减少 20%。同样，在此程序执行之前，BBVA 都可以自愿支付处罚，这也将导致处罚金额减少 20%。于是，80,000 欧元的罚款随后将被减少到 48,000 欧元。[28]

9. 美国 40 位州检察长与谷歌达成 3.915 亿美元的和解

11 月 14 日，美国 40 位州总检察长一起宣布与谷歌就其位置跟踪做法达成和解协议，谷歌需要为此支付 3.915 亿美元。该和解协议由俄勒冈州检察官 Rosenblum 和内布拉斯加州检察官 Doug Peterson 牵头，是有史以来规模最大的消费者隐私和解。

位置数据是谷歌数字广告业务的重要组成部分。谷歌使用它收集的个人和行为数据来建立详细的用户档案和目标广告。但同时，位置数据也是最敏感和最有价值的个人信息之一，即使是有限数量的位置数据也会暴露一个人的身份和日常生活，并可用于推断个人详细信息。根据各州检察长的调查，至少从 2014 起，谷歌通过账户与设备账号设置的设计，误导用户认为他们已经在账户设置中关闭了位置跟踪，而事实上，谷歌仍在继续收集他们的位置信息，并将这些信息提供给广告商。

除了数百万美元的和解协议外，作为谈判的一部分，谷歌还同意从 2023 年开始大幅改进其位置跟踪披露和用户控制。谷歌需要做到每当用户将与位置相关的帐户设置“打开”或“关闭”时，向用户显示附加信息；将有关位置数据的关键信息明确向用户展示；向用户提供有关 Google 收集的位置数据类型以及如何在增强的“位置技术”网页上使用这些数据的详细信息。[29]

[28] 西班牙数据保护局官网。
[29] 美国俄勒冈州司法部官网。

环球律师事务所
GLOBAL LAW OFFICE

环球解读

1. 个人信息出境合规指引之三——《网络安全标准实践指南 个人信息跨境处理活动安全认证规范》

引言

2022 年 11 月 8 日，全国信息安全标准化技术委员会（以下简称“信安标委”）再次发布《网络安全标准实践指南 个人信息跨境处理活动安全认证规范（v2.0 征求意见稿）》（以下简称“《认证规范 v2.0（征求意见稿）》”），并向社会公开征求意见。半年前，信安标委于 2022 年 4 月 29 日发布了《网络安全标准实践指南 个人信息跨境处理活动认证技术规范（征求意见稿）》，成为首个探索个人信息跨境处理活动认证制度，并且为《中华人民共和国个人信息保护法》（以下简称“《个保法》”）第三十八条“个人信息保护认证制度”提供了落地支撑。此后两个月，信安标委于 2022 年 6 月 24 日正式发布《网络安全标准实践指南 个人信息跨境处理活动安全认证规范》（以下简称“《认证规范 v1.0》”）。然后尚未组织正式认证，在发布《认证规范 v1.0》正式稿不到五个月时间，信安标委又将 1.0 版本升级到了 2.0 版本，并两次征求社会广泛意见，结合这半年中陆续发布《个人信息出境标准合同规定（征求意见稿）》（以下简称“《标准合同规定征求意见稿》”）和实施《数据出境安全评估办法》，足以看出监管部门针对《个保法》第三十八条能够实施落地的良苦用心和谨慎态度。

相较于《认证规范 v1.0》，《认证规范 v2.0（征求意见稿）》修订的内容主要包括删除了对“适用情形”的具体限定、新增了第三板块“术语定义”、细化了与境外接收方签署的具有法律约束力的协议应包含的具体内容、新增了个人信息保护机构的具体职责、增加了个人信息保护影响评估的相关要求，以及进一步细化并完善了个人信息处理者和境外接收方的责任义务等。本文将通过梳理和总结《认证规范 v2.0（征求意见稿）》中关于个人信息保护认证制度的适用情形、认证方式、基本原则、处理规则等内容，以期通过初步解读为企业了解个人信息出境安全认证机制提供参考。

一、 体系定位：个人信息跨境保护机制之一

根据国际标准化组织（ISO）对“认证”的通用定义，“认证”是指由独立机构提供书面证书，证明相关产品、服务或系统符合特定要求。在个人信息保护领域，适用认证机制可以提高保护个人信息主体权益的透明度，也可以促使企业间的合作关系更加可靠。譬如，根据《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）序言第 100 条，建立认证机制可以提高透明度和遵守法规的程度。GDPR 没有强制要求控制者和处理者进行认证，根据 GDPR 第 42 条第 3 款，认证是一个自愿过程，旨在帮助组织证明其符合 GDPR 的各项要求。换言之，认证的对象包括很多，例如中小企业的数据处理过程、数据跨境传输等都可以作为被认证的对象。这也是为什么 GDPR 关于认证的条款（第 42 条和第 43 条）没有被放在第 V 章跨境传输中的原因。

并且，根据 GDPR 第 46 条，认证（Certification）和签署标准合同条款（Standard Contractual Clauses）、约束性公司规则（Binding Corporate Rules，以下简称“BCR”）等同被作为合法跨境传输的前提和机制之一。因此，企业如需进行跨境传输，选择认证自然也是一种证明合规的措施。根据欧盟数据保护委员会（European Data Protection Board，以下简称“EDPB”）于 2022 年 6 月 30 日发布的《关于认证作为传输工具的指南 07/2022》（Guidelines 07/2022 on certification as a tool for transfers），在跨境传输场景下，申请认证的主体是位于欧盟境外的数据接收方。而数据提供方则需要满足其在 GDPR 下的合规要求，对认证结果的有效性等问题进行验证和核查。根据 GDPR 第 42 条，认证证书可由成员国数据保护机构（Supervisory Authority）、成员国认可的认证机构（Certification Body）颁布，认证标准可以由 EDPB 批准，也可由成员国监管机构批准。认证有效期最长 3 年，但如果符合认证的条件在届满时未发生变化，认证有效期可延长。

而在我国，认证同样被作为个人信息跨境传输的机制之一。根据《个保法》第三十八条，个人信息处理者向境外提供个人信息时，需满足以下四个条件之一：（1）依照本法第四十条的规定通过国家网信部门组织的安全评估；（2）按照国家网信部门的规定经专业机构进行个人信息保护认证；（3）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（4）法律、行政法规或者国家网信部门规定的其他条件。

对于《个保法》第三十八条第一款第一项所提出的安全评估，2022

年 7 月 7 日，国家互联网信息办公室（以下简称“网信办”）发布了《数据出境安全评估办法》最终版，该办法已于 2022 年 9 月 1 日生效并实施。我们此前已发布《环球合规与风控 | 数据出境合规指引之二——依规开展数据出境安全评估》进行解读。对于《个保法》第三十八条第一款第三项所提出的标准合同，2022 年 6 月 30 日，网信办发布了《标准合同规定征求意见稿》，并公开向社会征求意见。我们的解读请详见《环球合规与风控 | 个人信息出境合规指引之一——签署“中国版”个人信息出境标准合同》。本文文首提及的信安标委于 2022 年度对《认证规范》的草案形成到几次修订均属于落实《个保法》第三十八条第一款第二项提出的个人信息保护认证制度。

二、 适用情形

从比较的角度先对《认证规范 v1.0》和《认证规范 v2.0（征求意见稿）》适用情形的区别进行概括：

《认证规范 v1.0》	《认证规范 v2.0（征求意见稿）》
本文件作为认证机构对个人信息跨境处理活动进行个人信息保护认证的基本要求，适用于以下情形： a) 跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动； b)《中华人民共和国个人信息保护法》第三条第二款适用的个人信息处理活动。	本文件作为认证机构对个人信息跨境处理活动进行个人信息保护认证的认证依据，适用于个人信息处理者开展个人信息跨境处理活动。

《数据出境安全评估办法》和《标准合同规定征求意见稿》规定的适用哪套保护个人信息出境的机制，通过下述四方面来判断：（1）个人信息处理者是否被认定为关键信息基础设施运营者（以下简称“CIIO”）；（2）处理的个人信息所对应的主体是否超出 100 万人；（3）累计向境外提供的个人信息所对应的主体是否达到 10 万人以上（自上年 1 月 1 日起）；（4）累计向境外提供的敏感个人信息对应的主体是否达到 1 万人以上（自上年 1 月 1 日起）。如果上述四个问题中有一个答案为“是”，则个人信息向境外传输前必须通过申报出境安全评估后方能进行，无法采用订立标准合同的方式作

为个人信息跨境传输的保护措施。如果上述问题的答案均为“否”，则通过与境外接收方签署标准合同后可以合规地向境外接收方提供个人信息。虽然《个保法》第三十八条是要求个人信息处理者任选其一方式，但其实在选择顺序上需要先评估是否符合申报出境安全评估，不适用时才能考虑适用出境标准合同的机制。

《认证规范 v1.0》的适用情形是“**跨国公司或者同一经济、事业实体下属子公司或关联公司之间**”传输数据和“**《中华人民共和国个人信息保护法》第三条第二款适用的个人信息处理活动**”（即在我国境内运营过程中产生的个人信息直接采集并存储于境外服务器）。因此，此前普遍认为只有发生上述两种数据处理活动的，才可以申请认证，并且可能发生于（1）符合出境安全评估条件的，应当申请安全评估的同时可再申请认证（通常为对自身合规要求基准高且内部预算比较充足的企业），认证为可选项、加分项，安全评估为必须项；（2）不符合出境安全评估条件的，应当签署出境标准合同并可申请出境安全认证（通常亦属于对自身合规要求基准高的企业）；或者只选择申请出境安全认证（标准合同与认证二选一）。

“跨国公司及同一实体下的子公司和关联公司间的个人信息处理活动”作为出境安全认证的适用条件这点，比较类似于 GDPR 下的 BCR 规定。BCR 也是通过对跨国公司内部对数据跨境传输设置内部规则的方式实现自我约束，从而满足合规要求。GDPR 规定 BCR 应当经过**由欧盟成员国数据保护监管机构认可**（approve）。EDPB 也在官网上对于经过认可实施 BCR 的组织进行了公示。如果跨国集团获得了经认可的 BCR，则该公司无需得到另行批准即可直接将欧盟境内的个人数据传输到同一集团内欧盟境外的其他公司，即使其他公司位于没有按照 GDPR 要求为个人数据提供足够保护的国家。总之，BCR 可以保证公司在 GDPR 的总体框架下通过其内部制度保证集团内部适用统一的标准来实现对数据主体的保护，并达到防范数据跨境可能引发潜在风险的目的。与 BCR 不同，我国的跨境处理活动认证并非由监管机关认可，而由认证机构实施认证。相较于 GDPR，对于跨国公司内部的个人信息跨境传输，我国《个保法》并未进行特殊规定。此外，除了两类跨境数据处理活动外，其他跨境数据处理活动能否适用《认证规范 v1.0》，均是企业重点关注的问题。

《个保法》第三条第二款**适用的**个人信息处理活动，包括：（一）以向境内自然人提供产品或者服务为目的[30]；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。因此，如果境外个人信息处理者**直接收集**中国境内的个人信息，理应遵守《个保法》的要求。例如国外的某跨境电商平台直接收集中国境内用户的个人信息，并将其存储在位于境外的服务器。《认证规范 v1.0》认为处于境外的个人信息处理者在境外"直接采集"产生于中国境内的个人信息属于"个人信息跨境处理"活动，可以选择认证机制作为个人信息跨境的前提条件。

本次《认证规范 v2.0（征求意见稿）》的适用情形删除了具体的两类数据跨境处理活动，扩大到所有的个人信息处理者开展的跨境数据处理活动。但《认证规范 v2.0（征求意见稿）》仍然对《认证规范 v1.0》规定的两类数据跨境活动，即"跨国公司或者同一经济、事业实体下属子公司或关联公司"和"《中华人民共和国个人信息保护法》第三条第二款规定的境外个人信息处理者"的认证申请主体在《认证规范 v2.0（征求意见稿）》第二条中进行了特别提示，可见其特殊性。

三、 认证申请主体：境内主体

对于申请认证的主体，《认证规范 v2.0（征求意见稿）》相较于《认证规范 v1.0》，增加了一项总体要求，即申请认证的个人信息处理者应取得**合法的法人资格**、正常经营且具有良好的信誉、商誉，这也排除了个人和其他非法人组织申请认证的可能。

其他内容与《认证规范 v1.0》并无区别，基本上都应当由**境内主体提交认证申请**，并承担相应法律责任，无法由境外接收方申请认证。就上节中提到的当涉及两类特殊的数据跨境活动，其申请认证的主体具体如下：

适用情形	申请主体（同时也是责任主体）

[30] 对于如何判断"以向境内自然人提供产品或服务为目的"，鉴于现行生效法规未作明确解释，目前可以参考《信息安全技术 数据出境安全评估指南（征求意见稿）》中对于"境内运营"的解释，即判断是否向中华人民共和境内提供产品或服务的参考因素包括但不限于：使用中文、以人民币作为结算货币、向中国境内配送物流等。

跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动	**境内**一方
境外个人信息处理者**直接收集**中国境内的个人信息	境外个人信息处理者在**中国境内**设置的**专门机构或指定代表**

GDPR 序言第 80 条提及，如数据控制者未在欧盟境内设立实体，但根据适用条件需要适用 GDPR，则应当指定一名代表。该代表应由控制者书面授权明确指定，代表其履行 GDPR 下的义务。此类代表的指定不影响控制者在 GDPR 下的责任或义务。如果控制者不遵守规定，指定代表应接受强制执行程序。第 27 条第 4 款也规定，控制者指定代表不影响可能对控制者本身提起的法律诉讼。根据上述要求，GDPR 下的当地代表可能被引入诉讼执行程序中，但不影响控制者本身应当承担的责任。

根据我国《个保法》第五十三条，《个保法》第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立**专门机构或者指定代表，负责处理个人信息保护相关事务**，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。对于在我国境内设立的专门机构或者指定代表，《个保法》虽然并未对其应当承担的法律责任进行专门规定，但仍应当适用《个保法》第七章对于违法处理个人信息或未履行个人信息保护义务行为的一般法律规定。《认证规范 v2.0（征求意见稿）》也规定申请认证的主体须承担法律责任，我们认为此处的法律责任即应当参考《个保法》第七章，情节严重的，将由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

同时，如前所述，GDPR 下跨境传输场景中由数据接收方申请认证，而《认证规范 v2.0（征求意见稿）》则要求境内出境方或境外个人信息处理者在境内设置的专门机构或指定代表进行认证，这

无形中给境内主体施加了监督压力。规定由境内主体申请认证主要可能是为了便于开展认证工作的实施、就认证活动而言方便监管以及追究法律责任。我们认为，虽然规定法律责任的直接承担方为境内主体，但并不能理解为**境外主体不受认证机制的监管**，即参与个人信息跨境处理的相关方均应受认证机制的监管。

此外，《个保法》规定应“按照国家网信部门的规定经过专业机构进行认证”，《认证规范 v2.0（征求意见稿）》虽然对认证的申请主体做了明确规定，但并未明确有资格开展认证业务的机构名单，也未明确成为个人信息跨境活动的安全认证机构须满足何等条件，但确定了认证机构有权对境外接收方做出的承诺进行监督。同时，《认证规范 v2.0（征求意见稿）》写到，本规范由中国网络安全审查技术与认证中心与中国电子技术标准化研究院等单位提供技术支持，我们推断这两家机构很大概率会是跨境安全认证的专业机构，但具体机构名录还将等待官方进一步公布。

四、 术语定义

较《认证规范 v1.0》而言，《认证规范 v2.0（征求意见稿）》新增了第三章“术语定义”，具体列明了文中所涉“个人信息主体”“个人信息处理者”及“境外接收者”的定义。

“个人信息主体”是指“个人信息所标识或者关联的自然人”，此定义与《标准合同规定征求意见稿》中的定义一致；“个人信息处理者”是指“在个人信息处理活动中自主决定处理目的、处理方式的组织、个人”，此定义与《个保法》第七十三条的定义一致；《认证规范 v2.0（征求意见稿）》对“境外接收者”的定义为“位于中华人民共和国境外并自个人信息处理者处接收个人信息的组织或个人”，该定义与《标准合同规定征求意见稿》中的“境外接收方”定义相一致。

可见，《认证规范 v2.0（征求意见稿）》提及的相关术语都来源于既有的法律和部门规章，并未提出新的概念或是术语。企业在适用《认证规范 v2.0（征求意见稿）》时，只需要与《个保法》和相关法律法规保持一致进行判断即可，没有增加新的难度。

五、 基本原则

《认证规范 v2.0（征求意见稿）》提出了关于个人信息保护认证活动的六项基本原则，其中部分原则与《个保法》下的基本原则相同，但也有本次《认证规范 v2.0（征求意见稿）》新增的原则性规定。相较于《认证规范 v1.0》，《认证规范 v2.0（征求意见稿）》对基本原则做了更为详尽的补充，进一步细化了个人信息处理者和境外接收方应遵守的基本原则的具体内涵。例如在公开、透明原则中，《认证规范 v1.0》规定个人信息处理者需要向个人信息主体告知“个人信息跨境提供的目的、范围和处理方式”，而《认证规范 v2.0（征求意见稿）》要求个人信息处理者和境外接收方需要及时向个人信息主体告知“境外接收方的名称、联系方式，个人信息跨境处理的目的、范围和处理方式，以及权利、行使权利的方式和程序等”，增加了加粗标红字体部分的告知范围。各项原则的具体区别如下：

原则	《认证规范 v1.0》	《认证规范 v2.0（征求意见稿）》	《个保法》
1. 合法、正当、必要和诚信原则	个人信息处理者在跨境处理个人信息时应当满足法律法规的规定，严格按照约定目的并采取对个人信息权益影响最小的方式处理个人信息，严守合同、协议等具有法律效力文件的约定和承诺，不得违背约定和承诺损害个人信息主体的合法权益。	个人信息处理者和境外接收方在跨境处理个人信息时应满足法律法规的规定，按照约定目的并采取对个人信息权益影响最小的方式处理个人信息，遵守合同、协议等具有法律效力文件的约定和承诺，不得违背约定和承诺损害个人信息主体的合法权益。	处理个人信息应当遵循**合法、正当、必要和诚信**原则，不得通过误导、欺诈、胁迫等方式处理个人信息。（第五条） 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，**采取对个人权益影响最小**的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。（第六条）
2. 公开、透明原则	个人信息处理者在跨境处理个人信息时应当满足处理规则公开、处理过程透明要求，及时向个人信息主体告知个人信息跨境提供的目	个人信息处理者和境外接收方在跨境处理个人信息时应满足处理规则公开、处理过程透明要求，及时向个人信息主体告知境外接收方	处理个人信息应当遵循公开、**透明**原则，公开个人信息处理规则，明示处理的目的、方式和范围。（第七条）

	的、范围和处理方式，确保个人信息主体了解自身个人信息的跨境处理情况。	的名称、联系方式，个人信息跨境处理的目的、范围和处理方式，以及权利、行使权利的方式和程序等，确保个人信息主体了解自身个人信息的跨境处理情况。	
3. 信息质量保障原则	个人信息处理者和境外接收方在跨境处理个人信息时应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响	个人信息处理者和境外接收方在跨境处理个人信息时应保障个人信息的质量，**避免因个人信息不准确、不完整对个人权益造成不利影响**。	处理个人信息应当保证**个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响**。（第八条）
4. 同等保护原则	个人信息处理者和境外接收方在跨境处理个人信息时应当采取必要措施，确保个人信息跨境处理活动达到中华人民共和国个人信息保护相关法律法规规定的个人信息保护标准。	个人信息处理者和境外接收方在跨境处理个人信息时均应采取必要措施，保护所处理个人信息的安全，确保个人信息跨境处理活动达到《中华人民共和国个人信息保护法》规定的个人信息保护标准	个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。（第三十八条）
5. 责任明确原则	个人信息处理者和境外接收方在跨境处理个人信息时应当采取必要措施，保护所处理个人信息的安全，保障个人信息主体权益，并指定境内一方、多方或者境外接收方在境内设置的机构承担法律责任。	个人信息处理者和境外接收方在跨境处理个人信息时应保障个人信息主体权益，并指定境内一方、多方或者境外接收方在境内设置的机构对境外接收方的个人信息违规处理活动承担法律责任。	个人信息处理者应当对其个人信息处理活动负责，并**采取必要措施保障所处理的个人信息的安全**。（第九条）

6. 自愿认证原则	个人信息跨境处理活动认证属于国家推荐的自愿性认证，鼓励符合条件的个人信息处理者和境外接收方在跨境处理个人信息时自愿申请个人信息跨境处理活动认证，充分发挥认证在加强个人信息保护、提高个人信息跨境处理效率方面的作用。	个人信息跨境处理活动认证属于国家推荐的**自愿性认证**，鼓励符合条件的个人信息处理者在跨境处理个人信息时自愿申请个人信息跨境处理活动认证，充分发挥认证在加强个人信息保护、提高个人信息跨境处理效率方面的作用。	N/A

以上可见，《认证规范 v2.0（征求意见稿）》回归了与《个保法》相一致的要求，删除了《认证规范 v1.0》中超出《个保法》原则的部分内容，与上位法的要求更为贴合。但是，《认证规范 v2.0（征求意见稿）》比《个保法》多增加了“自愿认证”的原则，即个人信息跨境处理活动认证属于国家推荐的自愿性认证，鼓励符合条件的个人信息跨境活动相关方自愿申请个人信息跨境处理活动认证。因为本标准正是为认证活动而制，将认证的性质与作用提到原则位置也无可厚非。就“自愿认证”而言，涉及个人信息跨境传输活动的个人信息处理者，是否选择认证完全出于自愿：如果选择认证，也需要判断是否符合数据出境安全评估而同时申请安全评估；不选择申请跨境处理活动认证，但必须满足《个保法》第三十八条规定的其他保护措施后，方可进行个人信息跨境传输。

六、 基本要求

对于开展个人信息跨境处理活动，《认证规范 v2.0（征求意见稿）》从具有法律约束力的协议、组织管理、个人信息跨境处理规则、个人信息保护影响评估等四个方面对个人信息处理者与境外接收方提出了基本要求。这些要求不仅可以作为认证机构实施个人信息跨境处理活动认证的相关依据，也可以为个人信息处理者规范其个人信息跨境处理活动提供参考。下面，我们将对此具体展开介绍：

（一）具有法律约束力的协议

《认证规范 v2.0（征求意见稿）》在“具有法律约束力的协议”部分较《认证规范 v1.0》做出了较大改动，新增了数条与境外接收方签署的具有法律约束力和可执行文件的具体内容，此修订可帮助个人信息处理者和境外接收方在签订相关协议时更加明确协议应涵盖的内容，同时也对协议双方提出了更高的合规要求，确保个人信息主体权益得到充分的保障。在该文件中应当明确的重点内容如下：

a) 个人信息处理者和境外接收方的基本信息，包括但不限于名称、地址、联系人姓名、联系方式等；
b) 个人信息跨境处理的目的、范围、类型、敏感程度、数量、方式、保存期限、储存地点等；
c) 个人信息处理者和境外接收方保护个人信息的责任与义务，以及为防范个人信息跨境处理可能带来安全风险所采取的技术和管理措施；
d) 个人信息主体的权利，以及保障个人信息主体权利的途径和方式；
e) 救济、合同解除、违约责任、争议解决等；
f) 境外接收方承诺并遵守同一个人信息跨境处理规则，并确保个人信息保护水平不低于中华人民共和国个人信息保护相关法律、行政法规规定的标准；
g) 境外接收方承诺接受认证机构监督；
h) 境外接收方承诺接受中华人民共和国个人信息保护相关法律、行政法规管辖；
i) 明确在中华人民共和国境内承担法律责任的组织，并承诺履行个人信息保护义务；
j) 个人信息处理者和境外接收方均承诺对侵害个人信息权益行为承担法律责任，法律责任不明确的，由个人信息处理者承担法律责任；
k) 其他应遵守的法律、行政法规规定的义务。

较《认证规范 v1.0》而言，《认证规范 v2.0（征求意见稿）》新增了《标准合同规定征求意见稿》中第六条第（三）、（五）、（六）项[31]规定的标准合同应包括的主要内容，与个人信息出境相关法规间

[31] 第六条 标准合同包括以下主要内容：（一）个人信息处理者和境外接收方的基本信息，包括但不限于名称、地址、联系人姓名、联系方式等；（二）个人信息出境的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点等；（三）个人信息处理者和境外接收方保护个人信息的责任与义务，以及为防范个人信息出境可能带来安全风险所采取的技术和管理措施等；（四）境外接收方所在国家或者地区的个人信息保护政策法规对遵守本合同条款的影响；（五）个人信息主体的权利，以及保障个人信息主体权利的途径和方式；（六）救济、合同解除、违约责任、争议解决等。

达成了更好的协调性，更有利于对个人信息跨境处理活动的规范，提升个人信息保护水平。

企业在与境外接收方订立的具有法律约束力的文件（如《数据跨境传输协议》）时，一方面可根据《标准合同规定征求意见稿》，参考“个人信息出境标准合同”模板，将跨境处理个人信息的目的以及个人信息的类别、范围以附录形式进行列明；另一方面，还应当考虑重点补充或强调如下内容：（1）境外接收方承诺并遵守同一个人信息跨境处理规则，并确保个人信息保护水平不低于中华人民共和国个人信息保护相关法律、行政法规规定的标准；（2）境外接收方承诺接受认证机构监督；（3）境外接收方承诺接受中华人民共和国个人信息保护相关法律、行政法规管辖；（4）个人信息处理者和境外接收方均承诺对侵害个人信息权益行为承担法律责任，法律责任不明确的，由个人信息处理者承担法律责任；以及（5）其他应遵守的法律、行政法规规定的义务。

其中，第（4）点正表达了本文第三节中提及的参与个人信息跨境处理的相关方均应受认证机制的监管。关于接受监督的具体方式，包括答复询问、配合检查、服从采取的措施或做出的决定、提供已采取必要行动的书面证明等均由《认证规范 v2.0（征求意见稿）》第 6.2 点进一步明确。关于“个人信息主体权益保护措施”的具体内容，可以参照《认证规范 v2.0（征求意见稿）》第 6 点对个人信息主体权益保障的要求（具体详见下文第七节）。关于“同一个人信息跨境处理规则”具备所指的内容，《认证规范 v2.0（征求意见稿）》第 5.3 点也作了相应规定（具体详见下文第六节第 3 点“处理规则”部分）。

但是，当出现《个保法》第三条第二款的场景时，境外个人信息处理者于境外处理境内自然人个人信息并委托在境内设置的专门机构或指定代表申请认证的情况下，《认证规范 v2.0（征求意见稿）》第 5.1 点提及的“开展个人信息跨境处理活动的个人信息处理者和境外接收方”具体分别是指哪些主体，是否由境内专门机构/指定代表和境外个人信息处理者签署具有法律约束力的文件，存在一定的不确定性；抑或《认证规范 v2.0（征求意见稿）》第 5.1 点不适用《个保法》第三条第二款的场景，还需要《认证规范 v2.0》定稿版进一步解明。

（二）组织管理：指定个人信息保护负责人、设立个人信息保护机构

《认证规范 v2.0（征求意见稿）》明确要求，开展个人信息跨境处理活动的个人信息处理者和境外接收方均需要既指定个人信息保护负责人，又要设立个人信息保护机构。《认证规范 v2.0（征求意见稿）》对于个人信息保护负责人和个人信息保护机构的产生方式、基本要求以及具体职责进行了较为详细的规定，具体内容如下：

	个人信息保护负责人	个人信息保护机构
产生方式	开展个人信息跨境处理活动的个人信息处理者和境外接收方**均应指定**	开展个人信息跨境处理活动的个人信息处理者和境外接收方**均应设立**
基本要求	1. 具备个人信息保护专业知识和相关管理工作经历； 2. 由本组织的决策层成员承担。	1. **履行个人信息保护义务**； 2. **防止未经授权的访问以及个人信息泄露、篡改、丢失等**。
工作职责	1. 明确个人信息保护工作的主要目标、基本要求、工作任务、保护措施； 2. 为本组织的个人信息保护工作提供人力、财力、物力保障，确保所需资源可用； 3. 指导、支持相关人员开展本组织的个人信息保护工作，确保个人信息保护工作达到预期目标； 4. 向本组织的主要负责人汇报个人信息保护工作情况，推动个人信息保护工作持续改进。	1. 依法制定并实施个人信息跨境处理活动计划； 2. 组织开展个人信息保护影响评估； 3. 监督本组织按照约定的个人信息跨境处理规则处理跨境个人信息，保护个人信息权益； 4. 采取有效措施保证按照约定的处理目的、范围、方式处理跨境个人信息，履行个人信息保护义务，保障个人信息安全； 5. 定期对本组织处理个人信息遵守中华人民共和国法律、行政法规的情况进行合规审计； 6. 接受和处理个人信息主体的请求和投诉； 7. 接受认证机构对个人信息跨境处理活动的监督，包括答复询问、配合检查等。

1. 个人信息保护负责人

从上述工作职责来看，个人信息保护负责人主要承担领导决策职责并提供总体性保障支持，以便具体工作人员的个人信息保护工作达到预期目标，同时也具备管理权限和资源配置能力，能够为个人信息保护工作的开展提供人财物保障。关于主要负责人具体是由 CEO、CTO 还是其他决策层 VP 成员担任，取决于每个企业内部的不同治理结构，哪个具体决策层人员具备相关专业背景、知识储备和管理技能，《认证规范 v2.0（征求意见稿）》没有规定。

与《认证规范 v2.0（征求意见稿）》只要涉及个人信息跨境活动均需要指定个人信息保护负责人要求不同的是，《个保法》第五十二条第一款仅规定“处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人”。关于“国家网信部门规定数量”还有待《个保法》的相关配套规定加以明确。《信息安全技术 个人信息安全规范》（GB/T 35273-2020）（以下简称“《个人信息安全规范》”）对个人信息保护负责人的设立标准（满足以下条件之一）为：1.主要业务涉及个人信息处理，且从业人员规模大于 200 人；2.处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；3.处理超过 10 万人的个人敏感信息的。

如果《认证规范 v2.0》最终稿与目前的征求意见稿保持一致，那么根据 5.2.1 条，意味着只要开展个人信息处理活动，符合条件申请出境认证的，认证主体应当指定个人信息保护负责人，不论涉及处理个人信息的主体数量多少。

同时，值得关注的是，对于《个保法》第三条第二款的情况，即发生个人信息处理者在境外处理境内自然人个人信息的情形，如何指定个人信息保护负责人才能满足要求，《认证规范 v2.0（征求意见稿）》并没有明确说明，这是否意味着境外个人信息处理者需要在境内指定个人信息保护负责人？还是在境外指定也可以，只要符合《个保法》第五十三条在中国境内设置专门机构或指定代表申请认证；抑或由该境内设置的专门机构派员担任或者由指定代表一并担任？以上问题仍然需要《认证规范 v2.0》最终稿或操作指引进行厘清。

当然，还应当提醒的是，如果相关企业已经设置了个人信息保护负责人，并且涉及个人信息跨境传输，以及符合条件申请出境认证的，则应当在本企业的岗位职责说明或其他类似制度中进一步补充个人信息保护负责人需要监督、指导合规的个人信息跨境活动，并且对选

择跨境传输认证发挥决策作用，并了解相关的内容以支持认证工作的开展。

2. 关于个人信息保护机构

《认证规范 v2.0（征求意见稿）》要求开展个人信息跨境处理活动的个人信息处理者和境外接收方均应设立个人信息保护机构，针对具体合规要求（如个人信息保护影响评估）进行落实和执行。《个保法》虽然没有直接规定企业应当设立个人信息保护机构，但我们认为企业履行《个保法》规定的各方面义务显然需要通过专门工作机构来完成。与此同时，《个人信息安全规范》也明确指出，企业应当设立个人信息保护机构，与个人信息保护负责人一起承担数据保护和合规管理工作，特别是确保能够及时应对和处理个人信息泄露、篡改和丢失事件，这与《认证规范 v2.0（征求意见稿）》中对个人信息保护机构的基本要求一致。

与《认证规范 v1.0》相比，《认证规范 v2.0（征求意见稿）》在“个人信息保护机构”部分增添了一些机构的具体职责，具体来说：

第（4）项“采取有效措施保证按照约定的处理目的、范围、方式处理跨境个人信息，履行个人信息保护义务，保障个人信息安全”要求处理者和境外接收方的个人信息保护机构应当履行安全保障义务，回应了《认证规范 v2.0（征求意见稿）》第 4 点基本原则中的要求。

第（5）项“定期对本组织处理个人信息遵守中华人民共和国法律、行政法规的情况进行合规审计”。审计工作作为个人信息保护机构的重要职责之一，也是《个保法》第五十四条的明确要求，需要企业切实落实，以应对相关部门的监管要求。

在一般情况下，企业内的法律合规部门、大数据部门、各产品线、运维和 IT 部门与个人信息保护工作最密切相关，如果可以由其中一个部门的负责人牵头（如果符合条件，既可以被认定为个人信息保护负责人，亦可被委任为数据保护岗位负责人、网络安全负责人），从各相关部门抽取核心人员（经签署专项保密协议后）共同组建企业个人信息保护机构，各司其职，履行各项《个保法》下的

义务，包括符合个人信息跨境传输的合规措施，以及《认证规范 v2.0（征求意见稿）》要求的各项具体内容。

根据《认证规范 v2.0（征求意见稿）》，需要再次强调，境内个人信息处理者和境外接收方均需分别委任个人信息保护负责人和设立开展个人信息保护工作的专门机构，方可满足要求。如一旦开始认证工作，认证机构可能会要求企业提供此类任命和签发的内部文件。

（三）处理规则：遵守同一个人信息跨境处理规则

在处理规则方面，《认证规范 v2.0（征求意见稿）》较《认证规范 v1.0》，仅调整了一些措辞，规定参与个人信息处理的相关方遵守同一个人信息跨境处理规则的，应至少包括下列事项：

a) 明确跨境处理个人信息的基本情况，包括个人信息数量、范围、种类、敏感程度等；
b) 明确跨境处理个人信息的目的、方式和范围；
c) 明确个人信息境外存储的起止时间及到期后的处理方式；
d) 明确跨境处理个人信息需要中转的国家或者地区；
e) 明确保障个人信息主体权益所需资源和采取的措施；
f) 明确个人信息安全事件的赔偿、处置规则。

此处的“个人信息跨境处理规则”为上述第六节第 1 点（f）项提到的“同一个人信息处理规则”，即个人信息跨境处理各方制定的具有法律约束力的文件中，应包含上述个人信息跨境处理规则，并由个人信息处理者和接收方在签署后遵守并适用。如未覆盖上述规则或缺失部分内容的，例如未约定到期后的处理方式，则可能导致认证无法通过，影响整体数据出境的计划。

（四）影响评估：进行个人信息保护影响评估

《认证规范 v2.0（征求意见稿）》要求个人信息处理者应对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。相较于《认证规范 v1.0》，《认证规范 v2.0（征求意见稿）》新增了多项评估报告应包括的事项，并强调评估后需形成评估报告，且评估报告至

少保存 3 年，与《个保法》的要求进行了衔接。

目前，企业一方面可参考《认证规范 v2.0（征求意见稿）》对于个人信息保护影响评估的要求，另一方面还可以参考《数据出境安全评估办法》和《标准合同规定征求意见稿》对于个人信息保护影响评估的要求，此外，还可以部分参考《信息安全技术 个人信息影响评估指南》（GB/T 39335-2020）的指引，对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。但整体而言，评估内容不应少于《认证规范 v2.0（征求意见稿）》的要求，即个人信息保护影响评估至少包括下列评估事项：

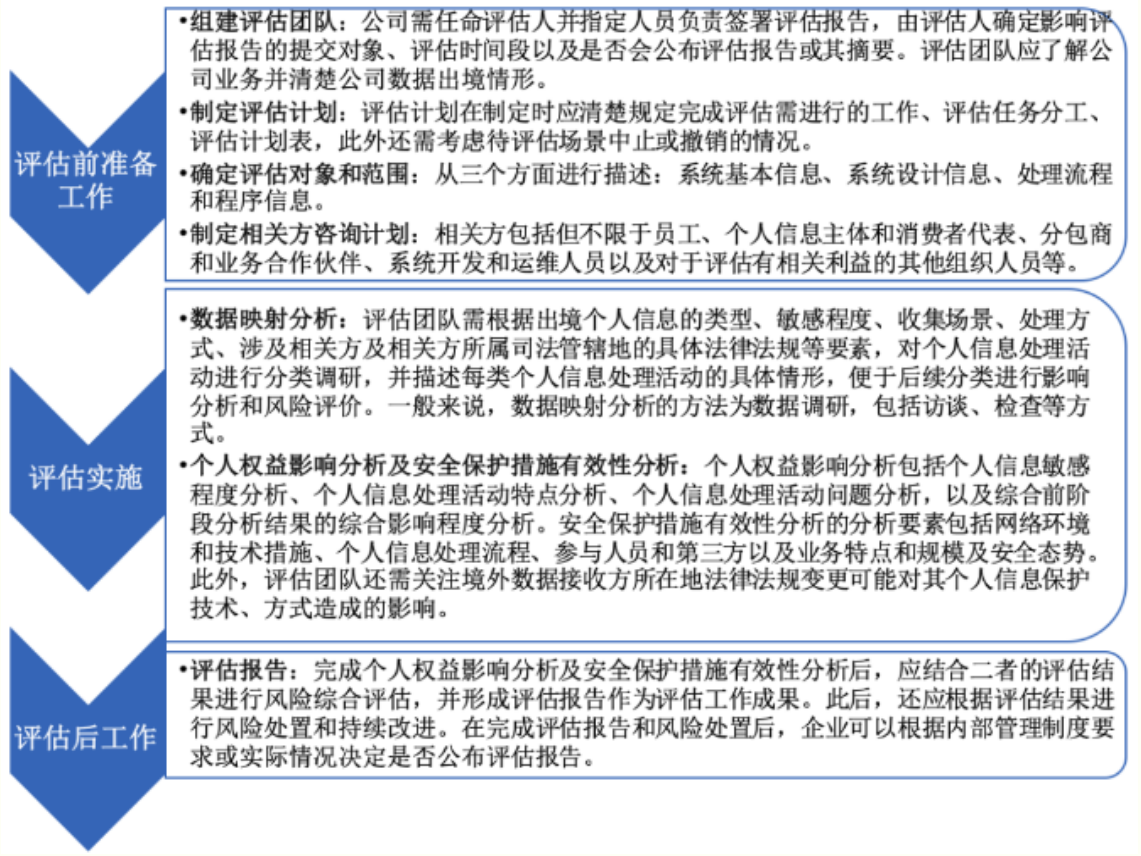
a) 个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；
b) 跨境处理个人信息的规模、范围、类型、敏感程度、频率，个人信息跨境处理可能对个人信息权益带来的风险；
c) 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障跨境处理个人信息的安全；
d) 个人信息跨境处理后泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等；
e) 境外接收方所在国家或者地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响，包括但不限于：
   - 境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生数据安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息请求及境外接收方应对的情况；
   - 该国家或地区现行的个人信息保护法律法规、普遍适用的标准情况，及与我国个人信息保护相关法律法规、标准情况的差异；
   - 该国家或地区加入的区域或全球性的个人信息保护方面的组织，以及所做出的具有约束力的国际承诺；
   - 该国家或地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。
f) 其他可能影响个人信息跨境处理安全的事项。

《认证规范 v2.0（征求意见稿）》还提到个人信息处理者应当评

估境外接收方所在国家和地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响，具体如何才算是对个人信息主体权益带来影响，实践中目前还未形成统一标准，甚至对于境外法律环境评估到何等颗粒度企业也还存在困惑。

结合上述，除了通用的评估项外，我们认为数据出境场景下个人信息保护影响评估还应重点衡量以下方面问题：（1）相关数据是否为国家禁止向境外提供的字段；（2）个人信息处理者和境外接收方的安全保护能力、安全措施和环境（境外国家和地区的网络安全环境等对个人信息主体权益的影响）等；和（3）其他可能严重影响个人信息和重要数据安全的风险或维护个人信息权益所必需的事项。

在评估步骤上，可以根据《个人信息影响评估指南》第五部分“评估实施流程”，将个人信息影响评估分为三个部分，即评估前准备工作、实施评估、评估后工作，具体内容如下：



结合《认证规范 v.2.0》《个保法》以及《个人信息影响评估指南》，我们建议企业在开展个人信息保护影响评估时，针对自身的个人信息

处理活动及合规实践，建立并落实适合实际情况的个人信息保护影响评估机制，包括由谁执行、如何执行、如何决策等内容。考虑到开展个人信息保护影响评估的专业性和复杂性，企业也可以引入外部第三方机构予以协助。

七、 个人信息主体权益的保障

在《个保法》的基础上，《认证规范 v2.0（征求意见稿）》对个人信息主体权利进行了完善与补充，同时也明确了个人信息处理活动相关方需承担的责任与义务，具体内容如下：

个人信息主体权利	个人信息处理者和境外接收方的责任和义务
1. 个人信息主体是个人信息处理者和境外接收方签订法律文件中的第三方受益人，有权要求个人信息处理者和境外接收方提供法律文本中涉及个人信息主体权益部分的副本，并向个人信息处理者和境外接收方主张权利； 2. 个人信息主体对其个人信息的处理享有知情权、决定权、限制或拒绝他人对其个人信息进行处理的权利、查阅权、复制权、更正与补充的权利、删除权，有权撤回对其个人信息跨境处理的同意； 3. 个人信息主体行使上述权利时，个人信息主体可请求个人信息处理者采取适当措施实现，或直接向境外接收方提出请求。个人信息处理者无法实现的，应通知并要求境外接收方协助实现。个人信息主体有权要求个人信息处理者和境外接收方对其个人信息跨境处理规则进行解释说明； 4. 个人信息主体有权拒绝个人信息处理者仅通过自动化决策的方式作出决定；	1. 以电子邮件、即时通信、信函、传真等方式告知个人信息主体开展个人信息跨境处理活动的个人信息处理者和境外接收方的基本情况，以及向境外提供个人信息的目的、类型和保存时间，并取得个人信息主体的单独同意； 2. 如果境外接收方所在国家或地区法律或政策发生变化，导致境外接收方无法履行本认证所提出的要求，境外接收方应在知道前述变化后立即通知个人信息处理者及认证机构； 3. 按照已签署的具有法律效力文件约定的处理目的、处理方式、保护措施等跨境处理个人信息，不得超出约定跨境处理个人信息； 4. 境外接收方承诺不将所接收的个人信息提供给第三方。如确需提供的，应满足中华人民共和国有关法律、行政法规要求，并采取必要措施确保第三方个人信息跨境处理活动达到《中华人民共和国个人信息保护法》规定的个人信息保护标准； 5. 为个人信息主体提供查阅其个人信息的途径，个人信息主体要求查阅、复制、更正、补充或者删除其个人信息时，

5. 个人信息主体有权对违法个人信息处理活动向中华人民共和国履行个人信息保护职责的部门进行投诉、举报； 6. 个人信息权益受到损害时，个人信息主体有权向个人信息处理者、境外接收方的任何一方提出赔偿要求； 7. 个人信息主体有权在其经常居住地所在法院向开展个人信息跨境处理活动的处理者和境外接收方提起司法诉讼； 8. 法律、行政法规规定的其他权利等。	应当及时予以响应，拒绝其请求的，应当说明理由； 6. 客观记录开展的个人信息跨境处理活动，保存记录至少 3 年；按照相关法律法规要求向中华人民共和国履行个人信息保护职责的部门提供相关记录文件； 7. 当出现难以保证跨境个人信息安全的情况时，应当及时中止跨境处理个人信息，并通知对方； 8. 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者及境外接收方应当立即采取补救措施，并通知对方，报告中华人民共和国履行个人信息保护职责的部门，按照相关法律法规要求通知个人信息主体，记录并留存所有与个人信息泄露、篡改、丢失有关的事实及其影响，包括采取的所有补救措施。通知、报告包含以下内容： 1）个人信息泄露、篡改、丢失的原因； 2）泄露的个人信息种类和可能造成的危害；并通知履行个人信息保护职责的部门和个人； 3）已采取的补救措施； 4）个人可以采取的减轻危害的措施； 5）负责处理个人信息泄露、篡改、丢失的负责人或负责团队的联系方式。 9. 应个人信息主体的请求，提供法律文本中涉及个人信息主体权益部分的副本； 10. 境外接收方的境内法律责任承担方承诺为个人信息主体行使权利提供便利条件，当发生个人信息跨境处理活动损害个人信息主体权益时，承担法律赔偿责任； 11. 承诺接受中华人民共和国认证机构对个人信息跨境处理活动的监督，包括答复询问、配合检查、服从采取的措施

	或做出的决定等，并提供已采取必要行动的书面证明； 12. 承担证明相关责任义务已履行的举证责任； 13. 承诺遵守中华人民共和国个人信息保护有关法律、行政法规，接受中华人民共和国司法管辖；承诺与个人信息跨境处理有关的纠纷适用中华人民共和国相关法律法规。

（一）个人信息主体权利

相较于《个保法》，《认证规范 v2.0（征求意见稿）》第 6.1 点提出了更具可操作性的保护要求。例如：个人有权要求个人信息处理者和境外接收方提供法律文本中涉及个人信息主体权益部分的副本；有权向国内监管部门进行投诉、举报；有权在经常居所地所在法院向个人信息处理者和境外接收方提起司法诉讼。《认证规范 v2.0（征求意见稿）》还提出，个人信息主体是个人信息处理者和境外接收方签订法律文件中的第三方受益人。虽然《标准合同规定征求意见稿》的标准合同模板中也提及了“受益人”的表述，但《个保法》并未明确提及“受益人”的概念，出境相关方对个人信息主体的个人信息进行保护，个人信息主体究竟是否为受益人？当出现个人信息泄露时，个人信息主体往往成为被侵权人而非受益人。综上，此处“受益人”的概念可能值得进一步探讨。

《认证规范 v2.0（征求意见稿）》规定，个人信息主体有权撤回对其个人信息跨境处理的同意；发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者及境外接收方应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。这也呼应了《个保法》第三十九条要求个人信息出境时应当获得单独同意的要求，即个人信息出境场景下适用单独同意，无法适用《个保法》第十三条第一款第（二）项至第（七）项。

此外，相较于《认证规范 v1.0》，《认证规范 v2.0（征求意见稿）》还补充规定，个人信息主体可以向个人信息处理者或者直接向境外接收方提出行权请求；当个人信息权益受到损害时，个人信息主体有权向个人信息处理者、境外接收方的任何一方提出赔偿要

求。如果赔偿请求得不到主张的，还可以向权利人经常居住地所在法院请求司法救济。前述规定构建起了完整的个人信息主体权利行使链条，从具体的权利内容到行权方式、途径，再到权利受损时的赔偿请求权和司法救济权，《认证规范 v2.0（征求意见稿）》做出了更为细化的规定。

（二）个人信息处理者和境外接收方责任与义务

《认证规范 v2.0（征求意见稿）》要求，个人信息处理者和境外接收方以电子邮件、即时通信、信函、传真等方式告知个人信息主体开展个人信息跨境处理活动的个人信息处理者和境外接收方的基本情况，以及向境外提供个人信息的目的、类型和保存时间，并取得个人信息主体的单独同意。此处对于单独同意的形式进行了明确，包括电子邮件、即使通信、信函、传真，但这些方式在很多场景下相对较难实现，例如在电商、云服务等场景下，如果还需要通过电子邮件、信函、传真这类方式，那么往往可能最终无法获得个人信息主体的单独同意。

《认证规范 v2.0（征求意见稿）》要求个人信息处理者和境外接收方在发现难以保证跨境个人信息安全的情况时，及时停止跨境处理活动，并通知对方。这要求个人信息处理者和境外接收方对个人信息跨境处理活动进行实时监督和监控，具体如何发现问题，如何恢复跨境传输，是否需要重新认证一次，目前《认证规范 v2.0（征求意见稿）》均未予以明确。

《认证规范 v2.0（征求意见稿）》第 6.2 点（i）项规定，应个人信息主体的请求，个人信息处理者和境外接收方应当提供法律文本中涉及个人信息主体权益部分的副本。就这一点，在企业实际落实过程中，可以参考《标准合同规定征求意见稿》标准合同模板中的规定，即在为保护商业秘密或其他机密信息（例如受保护的知识产权内容等）所必需的范围内，可以在提供副本之前对法律文本的相关内容进行适当遮蔽，但承诺向个人信息主体提供有效摘要以助其理解相关内容。

相较于《认证规范 v1.0》，《认证规范 v2.0（征求意见稿）》也对个人信息处理者和境外接收方提出了更多新的、细化的要求，具体包括：

【境外接收方通知义务】如果境外接收方所在国家或地区法律或政策发生变化，导致境外接收方无法履行本认证所提出的要求,境外接收方应在知道前述变化后立即通知个人信息处理者及认证机构；

【不得将个人信息提供给第三方】境外接收方承诺不将所接收的个人信息提供给第三方。如确需提供的，应满足中华人民共和国有关法律、行政法规要求，并采取必要措施确保第三方个人信息跨境处理活动达到《个保法》规定的个人信息保护标准；

【记录及保存要求】客观记录开展的个人信息跨境处理活动，保存记录至少 3 年；按照相关法律法规要求向中华人民共和国履行个人信息保护职责的部门提供相关记录文件；

【安全事件的通知报告义务（细化）】发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者及境外接收方应当及时通知对方和个人信息主体，并报告中国履行个人信息保护职责的部门。通知、报告包含以下内容：（1）个人信息泄露、篡改、丢失的原因；（2）泄露的个人信息种类和可能造成的危害；（3）已采取的补救措施；（4）个人可以采取的减轻危害的措施；（5）负责处理个人信息泄露、篡改、丢失的负责人或负责团队的联系方式。

此外还要求个人信息处理者和境外接收方需要承担已履行责任义务的举证责任，并承诺与个人信息跨境处理有关的纠纷适用中华人民共和国相关法律法规。

八、 结语

《认证规范 v2.0（征求意见稿）》的出台，为落实《个保法》第三十八条第一项第二款的个人信息保护认证制度提供了法律依据，规定了什么情形需要申请个人信息保护认证，适格的申请认证的主体有哪些，认证申请的具体要求有哪些，个人信息主体的权利以及相关方的责任义务是什么等内容。同时，《认证规范 v2.0（征求意见稿）》也解答了境外接收方是否需要履行个人信息跨境传输的义务以及应当如何履行的问题。

尽管《认证规范 v2.0（征求意见稿）》对个人信息保护认证相关

内容做了较为详细的规定，但并未规定实施认证的具体机制与流程（包括：认证机构有哪些以及需要何种资质、申请认证需要提交何种资料、结果有哪些、认证有效期、重新申请认证的情形、个人信息主体行使查询更正等权利的方式和个人信息处理者和境外接收方的响应时限、对于认证结果不服时的救济手段等），也未明确个人信息主体权益受损时的赔偿标准指导。同时，我们也期待后续出台的法律法规以及《认证规范 v2.0》正式稿可以进一步明确认证机制相关事项，为个人信息保护认证制度的落地提供更明确的指引。

2022 年 第十期 /总第四十四期

数据合规时事速递
NEWSLETTERS

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

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

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