NEWSLETTER 数据合规

2019 第四期 /总第四期

数据合规时事速递

北京市环球律师事务所

2019 年 7 月 4 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、新法速递

1.《个人信息出境安全评估办法》解读[1]

发布背景

2019 年 6 月 13 日,国家互联网信息办公室发布了《个人信息出境安全评估办法（征求意见稿）》（以下简称“办法”）。本次发布的《办法》主要有以下几方面的内容：第一，界定了个人信息出境的行为；第二，明确了网络运营者和个人信息接收者的职责；第三，细化了个人信息出境安全评估的内容。

《办法》对于目前我国已经出台的与个人信息保护相关的法律法规进行了细化和延伸。例如，2017 年生效的《网络安全法》第三十七条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。”而本次《办法》正是对个人信息出境安全评估的具体规定。

此外，《办法》也将为我国个人信息出境提供法律参考，填补了目前该领域法律的空白。纵观国外，部分国家及国际组织出台了各自的法律和政策文件，来管理以个人信息为代表的跨境数据，如欧盟的《一般数据保护条例》（GDPR）、英国的《数据保护法案》、亚太经合组织的《跨境隐私规则体系》、日本的《个人信息保护法》等，以保障个人信息跨境流动的安全。而我国目前仍没有出台有关法律与国外接轨。我国数据出境数量巨大，建立一个适用我国国情的个人信息出境管理办法，对在数据出境中的个人信息安全保护有着重要的意义。

评估对象

人们一直关心《办法》是否会将普通个人用户也纳入评估的对象范围，在此次《办法》的第二条明确规定了“网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息，应当按照《办法》进行安全评估”。可见，《办法》里评估对象

[1] 澎湃问政，网信天津，《个人信息出境安全评估办法》解读。

针对的是“网络运营者”，包括网络的所有者、管理者和网络服务提供者。

在我国，网络运营者收集、持有和使用大量的个人信息。因此对网络运营者进行有效的监管，能更大程度上对个人信息安全进行保障。

评估主体

此次《办法》规定安全评估的工作由各省级网信部门负责，这是由其所担负的网络安全管理职能决定的。具体的评估流程为，网络运营者先向所在地省级网信部门申报个人信息出境安全评估，省级网信部门会组织专家或技术力量进行安全评估，经过认定个人信息出境不会对国家安全、社会公共利益造成损害的，可以准许出境。

《办法》将安全评估的时间规定在了 15 个工作日内，主要是为了不影响网络运营者的正常业务时间。网络运营者对评估结论存在异议的，可以向国家网信部门提出申诉，此规定增加了网络运营者对数据评估结论不认可时的一项救济权。

评估内容

有一种观点是，安全评估实施过程中可能会有个人信息泄露的风险。其实这一担心是完全不必要的。一方面，从网络运营者所需提供的材料来看，根据《办法》第四条，提供的材料包括申报书、网络运营者与接收者签订的合同、个人信息出境安全风险及安全保障措施分析报告等。另一方面，根据《办法》第六条，在安全评估时，省级网信部门重点评估的内容包括：是否符合法律法规、是否能保障个人信息主体合法权益等。可以看出，安全评估过程中并不需要提供具体的用户个人信息。也就是说，评估的是网络运营者是否能够对拟出境的个人信息提供充分的安全保障，而非具体的个人信息本身。

出境后保障措施

个人信息出境后，由于数据持有者发生了变化，数据的保护能力、适用的法律法规也会发生改变，个人信息主体维护自身合法权益将面临一定的困难。《办法》充分考虑了这一难题，第十三至十五条要求境内网络运营者与境外个人信息接收者签订合同，保护个人信息主体合法权益，同时第十六条还对接收者将所接收到的个人信息传输给其他第三方的行为进行了限制。

总结

《个人信息出境安全评估办法》明确了网络运营者在个人信息出境方面的责任和义务，在做好个人信息出境安全工作方面，对网络运营者提出了更高的要求。针对个人信息脱离控制流向境外的情况，《办法》设计了一项强有力的制度，以最大限度地保障个人信息主体的合法权益。

二、监管动态

1. 工业和信息化部发布 2019 年一季度电信服务质量情况

整改问题

工业和信息化部近日通报 2019 年一季度电信服务质量情况。工信部指出，在用户个人信息保护方面，某美妆平台、某外卖平台、某海淘购物平台均有不达标情况。该三款 App 均存在误导用户授权同意收集个人信息等问题。

整改背景

一季度，工信部对 100 家互联网企业 106 项互联网服务进行抽查，发现 18 家互联网企业存在未公示用户个人信息收集使用规则、未提供账号注销服务等问题。这些不达标企业均接到责令整改的通知。

其中某美妆平台、某外卖平台、某海淘购物平台、某金融平台等 App 不仅未经用户同意收集个人信息，还存在误导用户同意收集使用个人信息的问题；某租车平台、某在线教育平台等 8 个 App 未公示用户个人信息收集、使用规则；某音乐音频软件、某在线教育平台等 6 个 App 则未提供账号注销服务。

专项治理

今年初，中央网信办、工信部、公安部、市场监管总局四部门联合开展 App 违法违规收集使用个人信息专项治理， 并前后发布了《App 违法违规收集使用个人信息自评估指南》《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》。

截止到今年 6 月 11 号，App 专项治理工作组收到了 5500 多条举报信息，包括 1800 多条实名举报的信息。在这些举报信息里，有 19%是关于没有公开收集和使用个人信息的举报；没有提供注销账号的渠道，或注销账号后没有及时地删除个人信息的举报约占 16.3%；收集个人信息未取得用户同意，或者收集、上传个人信息后再提醒用户阅读隐私政策的投诉约占 8.1%。

可以由此看出，无论是对于头部 App 还是一般的 App，违法违规收集个人信息的行为仍然十分普遍。

软件检测

除此之外，工信部针对 50 家手机应用软件进行技术检测。发现了 33 款违规的软件，对强行捆绑推广其他应用，违法违规收集个人信息等内容，进行下架处理，责令其进行整改。

其中，因恶意“吸费”、强行捆绑其他应用软件，百度手机助手中 12 款应用软件被下架；因未经用户同意收集使用个人信息，应用宝中 5 款应用软件被下架；豌豆荚等多个应用商店的多款应用软件因强行捆绑并推广其他应用软件被下架。

投诉举报

关于骚扰电话， 12321 网络不良与垃圾信息举报受理中心（简称 12321 举报受理中心）第一季度受理用户举报投诉 209278 件，环比下降 9.3%。其中，95/96 号码骚扰电话被举报投诉量涨幅明显，环比上升 35.4%，贷款理财类居首位。关于垃圾短信，12321 举报受理中心受理 87203 件，环比下降 16.3%。其中，金融保险类、零售推销类、游戏推广类端口短信被举报投诉量居前三。

关于不良手机应用，12321 举报受理中心接到有效举报 81495 件次，同比下降 40.61%，环比下降 21.40%。通过行业自律，联合应用商店、安全检测厂商对存在问题的 277 款不良手机应用进行了下架处理。

2. 工业和信息化部发布《电信和互联网行业提升网络数据安全保护能力专项行动方案》

监管背景

近年来，国家大数据发展战略正在加快实施。与此同时，个人信息泄露、数据过度采集滥用、非法交易等数据安全问题日益凸显。为积极应对新形势新情况新问题，工业和信息化部办公厅关于印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，具体内容如下：

总体要求

严格落实《网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《互联网信息服务管理办法》等法律法规，坚持维护数据安全与促进数据开发利用并重，坚持数据分类分级保护，开展为期一年的行业提升网络数据安全保护能力专项行动（以下简称专项行动）。

工作目标

（一）通过集中开展数据安全合规性评估、专项治理和监督检查， 2019 年 10 月底前完成全部基础电信企业（含专业公司）、50 家重点互联网企业以及 200 款主流 App 数据安全检查。

（二）基本建立行业网络数据安全保障体系。形成行业网络数据保护目录，制定 15 项以上行业网络数据安全标准规范。

重点任务

（一）加快完善网络数据安全制度标准

1、强化网络数据安全管理制度设计。加快建立网络数据分类分级保护、数据安全风险评估、数据安全事件通报处置、数据对外提供使用报告等制度，健全完善

企业内部网络数据全生命周期安全管理制度。

2、完善网络数据安全标准体系。推动出台行业《网络数据安全标准体系建设指南》，指导中国通信标准化协会成立网络数据安全标准专项工作组。

（二）开展合规性评估和专项治理

1、开展网络数据安全风险评估。出台网络数据安全合规性评估要点，针对物联网、车联网、卫星互联网、人工智能等新技术新应用带来的重大互联网数据安全问题，及时开展行业评估和跨部门联合评估工作。

2、深化 App 违法违规专项治理。组织开展应用商店安全责任专项部署，督促应用商店落实 App 运营者真实身份信息验证、应用程序安全检测、违法违规 App 下架等责任。

3、强化网络数据安全监督执法。将企业网络数据安全责任落实情况、数据安全合规性评估落实情况作为重点内容。

（三）强化行业网络数据安全管理

1、稳步实施网络数据资源“清单式”管理。形成行业网络数据保护目录，指导督促试点企业建立内部网络数据清单和数据分类分级管理制度。

2、明确企业网络数据安全职能部门，推动设立或明确网络数据安全管理责任部门和专职人员。

3、强化网络数据对外合作安全管理，落实《工业和信息化部关于加强基础电信企业数据安全管理规范清理数据对外合作工作的通知》。

4、加强行业网络数据安全应急管理，落实工业和信息化部相关应急预案要求。

（四）创新推动网络数据安全技术防护能力建设

1、加强网络数据安全技术手段建设。

2、推动网络数据安全技术创新发展。

3、加强专业支撑队伍建设。成立行业网络数据安全专家委员会，委托中国信息通信研究院、中国电子信息产业发展研究院、中国电子技术标准化研究院、中国互联网协会、中国通信标准化协会等单位开展面向行业的网络数据安全法律法规和政策标准宣贯、技能培训和测试检查。

（五）强化社会监督和宣传交流

1、强化社会监督和行业自律。
2、加强宣传展示和国际交流。

工作安排

（一）工作部署阶段（2019 年 7 月）。部制定印发专项行动方案，组织开展宣贯部署，向各单位、各企业制定印发工作任务清单，明确各项任务时间节点和工作要求。

（二）重点保障阶段（2019 年 8-10 月）。指导完成各省级基础电信企业和重点互联网企业重点环节数据安全合规性评估，持续开展 App 违法违规收集使用个人信息专项治理。

（三）长效建设阶段（2019 年 11 月-2020 年 5 月）。建立网络数据安全管理长效机制。

（四）总结提升阶段（2020 年 6-7 月）。对典型经验做法进行推广，巩固相关工作成效。

工作要求

（一）加强组织领导。
（二）明确任务分工。
（三）强化监督检查。
（四）加强宣传通报。

3. 四部委联合开展互联网网站安全专项整治[2]

2019 年 5 月至 2019 年 12 月，中央网信办、工信部、公安部、市场监管总局四部委联合在全国范围内开展互联网网站安全专项整治工作。专项整治工作特别针对未备案或备案信息不准确的网站进行清理，并对一些违法犯罪行为，例如攻击网站等，进行打击，以及对违法违规网站进行处罚和曝光。

治理背景

据国家计算机网络应急技术处理协调中心（简称"CNCERT"）有关负责人介绍，我国目前互联网网站安全受到较大威胁，攻击篡改、植入后门、数据窃取等等危害网络安全的行为呈增长态势。据 CNCERT 提供数据，2019 年 1 月至 4 月我国境内被篡改的网站达 8,231 个，被植入后门的网站达 10,010 个。此外，由于运营者不重视网络和数据安全问题，特别是中小网站安全管理和防护能力较低，缺乏有效安全保障措施，一些企业的数据库都没有相应防护措施，导致了大量用户个人信息泄露事件。

治理特点

本次专项整治加大了对未履行网络安全义务、发生网络安全事件的网站运营者或开办者的处罚力度，督促网络运营者切实落实安全防护责任，加强网站的安全管理与安全保障措施。各地方的通讯管理局与公安机关将根据《网络安全法》，对发生网页篡改、被植入后门木马、大量公民个人信息被窃取等网络安全事件，或存在非法获取、出售或提供个人信息等行为，以及落实网络安全义务不到位的网站，依据情节严重程度，采取约谈主要负责人、停业整顿、关闭网站、注销备案等措施并公开曝光，涉企行政处罚信息将依法纳入市场监管总局国家企业信用信息公示系统予以公示。专项整治期间，有关部门还将责令未按照有关规定进行 ICP 备案、联网备案或备案信息不准确的网站限期整改，对拒不整改的网站采取清理措施。公安机关还计划对非法入侵控制网站牟取利益或从事非法活动，非法提供入侵控制网站工具，买卖网站数据和控制权限，窃取买卖个人信息等违法犯罪活动和网络黑产行为进行打击。各地网信部门统筹协调本地区专项整治工作。

[2] 新华网《中央网信办等四部委联合开展互联网网站安全专项整治 将处罚并曝光违法违规网站》。

防护手段

国家工业信息安全发展研究中心检查评估所副所长于盟指出，对于网络安全保障与数据保护，可以利用云防护方式提高网站的防护能力。云防护一般利用 DNS 流量牵引将网站访问量引流至分布式的云防护清洗中心进行安全检测与拦截，再将通过检验的流量引回网站服务器端，而不需部署硬件设备和调整业务结构及网络拓扑，具有部署快速简便、及时防护最新漏洞、全网协同防御等特点，而且费用比较经济。对于云防护技术，国家信安标委组织制定了《信息安全技术网站安全云防护平台技术要求》等标准对云防护服务商进行规范引导。

4. 花钱购买 1000 多个企鹅号，苍南经营者被罚款 10 万元[3]

处罚动态

据苍南县公安局消息，6 月 3 日，苍南警方对当地一位企业经营者林某处以罚款 10 万元的处罚。据称，林某涉嫌花 1600 多元购入 1000 多个他人注册的企鹅号，被认为以非法方式获取侵犯个人信息，违反《中华人民共和国网络安全法》。

具体案情

苍南警方网安部门根据线索，发现有人在网络上非法大量购入企鹅号。随后，根据网安部门所提供的线索及指导，苍南警方开展调查，并迅速锁定苍南某网络公司老板林某。在林某所在公司现场，警方查获了涉案电脑及 1000 多个含个人身份证、手机号等信息的企鹅号。

经查，林某为了发展业务，自 2018 年 2 月以来，先后花了 1600 多元，分多次向他人购买 1000 多个企鹅号账号及密码，并以公司主体形式进行运营。“每个企鹅号账号发布的数量是有限的，想发布更多的信息，就要大量购买账号。”林某交代，她通过在网络上购买企鹅号账号，用以帮助客户在该平台上发布信息，赚取更多的广告费。为了盈利并且推广公司业务，林某购入关注量较大的企鹅号进行运营，关注量越大，则可获得的利润也更多。

根据民警的介绍，注册企鹅号需要收集申请人的身份证，手机号码等个人信息，注册成功之后可以用来在某平台上发布信息。即使发布的内容符合法律规定，但林某的行为侵犯了他人个人信息，违反了《网络安全法》，被公安机关处以 10 万元的行政处罚。

警方提醒

办案的警方提醒相关的从业人员，网络仍属法律监管之地，企业和公民要培养法律和自律的意识，不侵犯他人的个人信息，日常的经营活动也要遵守相关的法律法规。

[3] 温州日报《花钱购买 1000 多个企鹅号 苍南经营者被罚款 10 万元》。

5. 中国首次发放 5G 商用牌照[4]

发放情况

6 月 6 日，中国电信、中国移动、中国联通和中国广电正式获得工信部发放的 5G 商用牌照，这标志着我国正式进入了 5G 时代。值得关注的是，除了三大基础电信的运营商，此次中国广电也获得了 5G 的商用牌照。

开启 5G 元年

工信部部长苗圩谈到，在 5G 时代下，我们将从移动互联网时代转为移动物联网时代，新一代的信息基础设施将会更加高速和安全。不仅如此，5G 时代还会为数字化转型带来很多机遇，如发展工业互联网、车联网等。这些新的机会都将会给数字经济带来飞速的发展。

中国信通研究院发表文章《5G 产业经济贡献》，预计在未来的五年内，在我国，5G 商用将会直接带动高到 10.6 万亿的经济总产出，带来超过 300 万个工作岗位。

但是在 5G 时代，虽然生活发生了快速转变，变得方便快捷，但其产生的大量的流动的数据也会对我们的个人信息和隐私安全带来很大的影响。因此，在新的技术与时代面前，我们不仅要关注 5G 带来的发展动力，也要注重保护 5G 时代下的个人信息安全。

专家视角

中国电信集团公司技术部网络与信息安全领域业务督导王爱宝谈到，在 5G 和物联网时代，网络和信息安全领域也会面临更多的挑战。随着互联网发展越来越快，其中所包含的价值越来越多，在万物互联的时代，个人信息数量急剧增长，也会面临更多的数据泄露的风险。

[4] 新华网《我国正式发放 5G 商用牌照》。

三、相关案例

1. 某浏览器被诉违法收集个人隐私 法院裁定：立即停止[5]

案情介绍

2019 年 6 月，一位用户在法院起诉了某浏览器 App 的运营方，起诉理由为该浏览器 App 获取了该用户社交账户的头像、生日、性别、好友和地区等个人信息。该用户提起了行为保全申请，要求该运营方停止收集其前述个人信息的侵权行为。

根据北青报报道，该用户在日常使用这款浏览器时发现浏览器存在上述的问题，并且该浏览器没有为用户提供任何渠道来删除这些违法收集的个人信息，也没有提供任何方式让用户取消个人信息的授权。于是该用户决定起诉这款浏览器的 App 运营方。请求被申请人立即停止通过浏览器 App 收集申请人帐号的头像、地区、生日、好友、性别等个人信息。

法院判决

法院最终判决被告立即停止通过浏览器 App 获取申请人个人信息的行为。

[5] 观察者网《某浏览器被诉违法收集个人隐私 法院裁定：立即停止》。

2. 全国首例“暗刷流量”案宣判[6]

具体案情

经人介绍，许某和常某成为网友。据常某说，2017 年 9 月许某在网上聊天中与常某达成约定，要求常某为某游戏的 App 移动端暗刷流量，每千次点 UV 的价格为 1 元左右，双方以第三方统计平台 CNZZ 对流量进行统计的结果为标准。

许某称，其受马某的请求找到常某让其来刷流量，并且明确告诉过常某只要真量，不能通过机刷。

2017 年 9 月 15 日至 10 月 8 日，双方进行了三轮交易。10 月 9 日至 10 月 23 日间，许某对常某刷出的约 2800 万 UV 产生怀疑，认为有 40%的数据是掺假的，因此仅同意支付对应价款 16293 元。

而常某则认为许某应按照 2800 万 UV 对应的价款进行支付，即 30743 元，遂将许某诉至北京房山法院，索赔剩余钱款，后又撤诉，诉至北京互联网法院。

庭审情况

根据常某诉讼代理人的介绍，案件涉及的点击量需要在 15 天中实现，并且需要每天超百万手机用户点击。常某本人也是中间商，为完成案件所涉点击量，需经过层层分包。

“我下面有代理，将代码发送给代理，每个点击都是真实的人在点。”常某称其代理还拥有下级代理微信群，“链接是一串代码，我的下家做成吸引用户点击的图片。”

庭审中，技术调查官季晓辉将常某叙述的 js 暗刷流程归纳为“借助其他 APP 或广告的点击量，在其中植入 js 暗刷点击，通过搭其他广告便车的方式来刷其自身游戏的访问量，并且不被相关用户知晓。”此说法获得了诉讼当事双方的认可。

法院判决

经审理，北京互联网法院认为，网络产品的真实流量能在一定程度上反映网络

[6] 北京青年报，《“暗刷流量”首案宣判 庭审揭开玄机》。

产品的受欢迎程度甚至质量优劣情况，因此，流量是网络用户选择网络产品的决定因素之一。虚假流量会使网络用户的决策受到营销，扭曲决策机制。涉案合同当事人通过作弊造假行为进行欺诈性点击，违反了商业道德底线，违背诚信原则。这一行为亦可能侵害社会公共利益，既侵害了不特定市场竞争者的利益，又会欺骗、误导网络用户选择与其预期不相符的网络产品，侵害了广大网络用户的福祉。

根据我国《合同法》，合同如损害社会公共利益，则该合同无效。涉案合同违反社会公共利益、违反公序良俗，应属绝对无效的范畴。

此外，双方通过虚假流量交易获益，违背任何人不得因违法行为获益的基本法理。同时，考虑到此案呈现的技术复杂性、“刷流量”行为的隐蔽性，以及由此产生的对社会公共利益的严重损害，需通过个案的查处表明司法对此类行为的否定态度。因此，对双方在合同履行过程中的获利，法院将另行制作决定书予以收缴。同时，将涉案其他违法行为线索转交相关部门依法查处。

专家点评

中国人民大学助理教授熊丙万在《法学苑》直播间表示，数据造假作为一种行业潜规则，在造假的过程出现纠纷时很少会选择诉诸法律手段，导致这种现象一直被深藏。而这些数据的真实性认定也存在一定的现实困难。

此外，熊丙万教授认为，数据暗刷也侵犯了消费者的权益。一方面诱骗消费者点击的行为侵犯了知情权；另一方面，商家通过数据造假，给潜在消费者营造出一种商品很受欢迎的错觉，也是对消费者的一种欺诈。

四、合规前沿

1. 苹果新登录选项或对Facebook和谷歌屏蔽更多个人信息 [7]

合规举措

2019 年 6 月 5 日据路透社报道，根据此前发布的设计指南，苹果公司将要求开发者在 iPhone 和 iPad 应用中放置一个新的“使用苹果帐号登录”（Sign in with Apple）按钮，并要求将该按钮置于竞争对手谷歌和 Facebook 的登录按钮之上。

毫无疑问，此举意味着将苹果帐号放在有利位置上，其意义重大，因为用户经常在应用中选择默认选项或顶部选项。如果开发者要在应用中提供使用 Facebook 或谷歌帐号登录选项，则苹果也将要求应用开发者提供“使用苹果帐号登录”按钮。

当前，许多消费者选择使用谷歌或 Facebook 帐号登录到其他应用，省去了为多个不同应用创建不同账号的麻烦。

但登录按钮可以将用户的使用习惯等数据发回给应用开发者。为此，苹果软件主管 Craig Federighi 表示，苹果正寻求为用户提供一个更私密的选择，在允许用户快速登录的同时，又不向其他公司发送数据。

官方回应

苹果表示，其登录按钮将在年末正式推出。需要指出的是，对于那些拥有自己的专属登录系统、不使用谷歌或 Facebook 第三方按钮的应用，苹果的这份开发指导方针似乎并未做出要求。

[7] 陆家嘴时报《苹果公司新登录选项或对 Facebook 和谷歌屏蔽更多个人信息》。

五、环球评论

1. 深度解读《数据安全管理办法（征求意见稿）》十大重点内容

2019 年 5 月 28 日，国家互联网信息办公室颁布《数据安全管理办法（征求意见稿）》（“《办法（征求意见稿）》”），引起各界关注。普遍认为，《办法（征求意见稿）》承袭了《网络安全法》等法规保护数据安全、推动数据发展的宗旨，从个人信息、重要数据两个角度出发，在实操层面对我国数据安全保护工作做出了规定。

总体而言，对于个人信息，《办法（征求意见稿）》规定了网络运营者的具体义务，特别在收集个人信息需要公开透明且不得过度、收集儿童信息需获监护人同意、确立数据安全责任人制度、提供个人信息原则上需征得信息主体同意、网络运营者的继受者需承继数据安全责任等规则上与之前颁布的《网络安全法》《信息安全技术 个人信息安全规范》（GB/T 35273-2017）（“《个人信息安全规范（征求意见稿）》”）等规定大致相当，同时也提出了敏感信息备案等新的制度。

对于重要数据，《办法（征求意见稿）》进一步细化了重要数据的定义，同时提出了收集重要数据需提请备案以及向境外提供重要数据需提请批准的新要求。我们理解，《办法（征求意见稿）》体现的个人信息与重要数据平行保护的立法趋势，符合现阶段国家在数据安全保护问题上的一贯立场，具有重要意义。

就《办法（征求意见稿）》的十大主要内容，我们介绍分析如下。

数据收集规则应严格遵守公开透明

《办法（征求意见稿）》第九条规定，如果收集使用规则包含在隐私政策中，应相对集中，明显提示，以方便阅读。另仅当用户知悉收集使用规则并明确同意后，网络运营者方可收集个人信息。第十条规定，网络运营者应当严格遵守收集使用规则，网站、应用程序收集或使用个人信息的功能设计应同隐私政策保持一致，同步调整。

《App 违法违规收集使用个人信息自评估指南》（“《自评估指南》”）评估点 4，要求企业的隐私政策应该易于阅读。而《办法（征求意见稿）》也强调了隐私政策的内容应当方便阅读，且进一步强调了收集使用个人信息的内容应当便于阅读。这包括两个维度：第一，收集使用个人信息的规则应当集中，能让用户清晰、系统地了解到收集使用了哪些信息；第二，收集使用的规则应当明显提示，能让用户直观、方便地知道个人信息如何被收集和使用。

此外，《办法（征求意见稿）》还强调，收集个人信息前必须取得用户明确同意。《个人信息安全规范（征求意见稿）》已规定，网络运营者收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围，并获得个人信息主体的授权同意；《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》（“《认定方法》”）规定，App 未经同意就开始收集个人信息属于违法违规收集使用个人信息。可见，《办法（征求意见稿）》的此条内容，与前述法规对收集使用个人信息的规定是一脉相承的。

《办法（征求意见稿）》第十条是对第九条规定的补充和强化，目的在于要求网络运营者规范收集和使用用户个人信息的行为，并严格遵守隐私政策的内容。本条要求隐私政策应与其相关的产品功能同步调整，也就是要求隐私政策应该随着业务功能的变化随时进行更新。《个人信息安全规范（征求意见稿）》5.5 条对隐私政策的更新做出了同样的要求，在收集、使用个人信息的业务功能或个人信息收集方式等出现变更时，应及时更新隐私政策并重新告知个人信息主体。

提供个人信息应征得信息主体同意

《办法（征求意见稿）》第二十七条规定了网络运营者对外提供个人信息的需进行风险自评估以及获得个人信息主体同意的义务。但是在第二十七条中，《办法（征求意见稿）》并未将本条适用的场景描述为 “共享、公开披露”等，而使用了“向他人提供”这一表达。不得而知立法者是否试图与《刑法》第二百五十三条之一侵犯公民个人信息罪，以及《网络安全法》第四十二条中使用的表达保持一致。那么，能否将此处“向他人提供”理解为适用于共享、转让、公开披露、向境外提供等的场景，还需要进一步讨论。

《办法（征求意见稿）》第二十七条要求网络运营者在向他人提供个人信息之前，应征得个人信息主体的同意。这一规定也与《网络安全法》相互呼应，但《办法（征求意见稿）》列举了五种例外情形，对比《网络安全法》而言有所增加。《网络安全法》仅规定，向他人提供经过处理无法识别特定个人且不能复原的信息，不用征得个人信息主体的同意；而《办法（征求意见稿）》中增加了（1）合法公开渠道获取，（2）个人信息主体主动公开，（3）执法机关依法履行职责所必需，（4）维护国家安全、社会公共利益、个人信息主体生命安全所必需，四种例外情形。《办法（征求意见稿）》增加对提供个人信息征得同意的例外情形，实际上扩大了无需征得个人信息主体同意的情形范围，能够一定程度上减轻网络运营者的压力，做到一种立法的平衡。

获取儿童个人信息，需要获得监护人同意

《办法（征求意见稿）》第十二条规定收集 14 周岁以下未成年人个人信息的，应当征得其监护人同意。

我国《民法总则》将未成年人的年龄界限设置为 18 周岁以下。在个人信息保护领域，我国现行《信息安全技术 个人信息安全规范》（以下简称“《个人信息安全规范》”）第 5.5 条 c）款设定了特殊规则，即收集不满 14 周岁的未成年人的个人信息，需要征求其监护人的明示同意。在年龄界限方面，《办法（征求意见稿）》第十二条与《个人信息安全规范》第 5.5 条 c）款以及最新出台的《儿童个人信息网络保护规定（征求意见稿）》（以下简称“《规定》”）的要求是一致的。但是，对于同意的方式，《个人信息安全规范》要求必须取得监护人的明示同意，即监护人需要通过书面声明或主动做出肯定性动作，对个人信息进行特定处理做出明确授权的行为，第十二条却降低了监护人同意的门槛，对监护人同意要求上并没有要求需要明示同意。结合《儿童个人信息网络保护规定》第七条“监护人的同意应当明示同意，并且需要具体、清楚、明确和基于自愿”。对此，我们认为，《办法（征求意见稿）》可能还会做出调整与改善。另外，笔者认为《个人信息安全规范》第 5.4 条 c）款是值得借鉴的，对于 14 周岁以上的未成年人，对于一些特殊复杂的场景，并不能独立做出判断的，监护人的明示同意应该被视为保护手段之一，而《儿童个人信息网络保护规定》又不管这一段，因此，如果《办法（征求意见稿）》第十二条可以再增加半句话“收集 14 周岁（含）以上未成年人的个人信息的，应当征得未成年人的明示同意或者其监护人的明示同意”可能会更加完整地保护未成年人权益，也与《个人信息安全规范》相衔接。

此外，为保护未成年人，部分企业根据我国法律法规实施了防沉迷和实名认证，有些企业还推出了青少年模式。我们认为实践中可能出现更为复杂的问题，例如企业如何有效地识别未成年人、企业如何设置验证监护人同意的机制。对于这些问题，期待后续出台更为详细的实施办法，为企业提供更为细致的操作指引。

获取儿童个人信息应获监护人同意

《办法（征求意见稿）》第十六条规定，实施该类行为不得妨碍网站的正常运行，如严重影响网站运行，网站有权要求停止自动化访问收集，该行为即应停止。《办法（征求意见稿）》同时明确，自动化访问收集流量超过网站日均流量三分之一，即构成严重影响网站运行。

我们理解，爬虫技术是互联网社会利用数据资源的重要方式，但滥用爬虫技术也会损害数据主体的利益。实践中，爬虫技术引起的核心问题是企业之间的商业利益纠纷，主要体现在以下方面：爬取方的频繁访问，对被爬取方服务器造成压力；爬虫会破坏网站或 APP 运营的方式和逻辑，侵害数据方未来的价值；爬虫的搭便

车行为可能会让企业的一些盈利模式不能再继续下去，比如电商的竞价排名等。

因此，国家在维护合理爬虫行为的同时，有必要去打击侵害他人利益的滥用行为，此次《办法（征求意见稿）》正是我国立法首次对该问题做出的回应。在判断此类行为的损害大小时，实践中往往会考虑爬取数据的公开程度高底、数量多少、行为人是否潜入数据方的计算机信息系统、被爬取方是否有 Robots 协议等因素。另外，关于如何证明爬取方占用流量超过网站日均流量的三分之一，目前尚无明确的指引，还有待进一步的立法或司法解释进行完善。

不因用户授权范围差异而歧视用户

《美国加州消费者隐私法》第 1798.125 （a）条规定，“企业不得因为消费者行使本标题下任何消费者的权利而歧视消费者，包括但不限于：（A）拒绝向消费者提供产品或服务。…（D）提示消费者将获得不同价格或费率的商品或服务，或者将向消费者提供不同水平或质量的商品或服务。”8

本次《办法（征求意见稿）》第十三条在一定程度上借鉴了美国 CCPA 的规定，首次明确提出，网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等方面的歧视。这表明我国法律在个人信息主体自主选择权保护方面更进了一步。

定向推送应做好适当合规控制措施

本次《办法（征求意见稿）》第二十三条对网络运营者定向推送的行为作出规制，即事前要求允许信息主体 opt- in，事中要求运营者明示“定推”字样，事后要求为用户提供停止接收定向推送信息的功能，以充分保障个人信息主体对于定向推送的自主选择权。同时，《办法（征求意见稿）》还要求用户选择停止接收定向推送信息时，网络运营者删除已经收集的设备识别码等用户数据和个人信息，从深层基础上严格控制网络运营者对用户画像的使用界限。

本条在实践中颇有争议，有观点质疑同时进行事前、事中及事后规制的必要性与合理性；有观点认为定向推送的定义目前仍缺乏明确界定；另有观点指出新闻信息与商业性信息有时不能完全区分识别，两者推送的基础逻辑不同，为用户设置简单的拒绝功能并不能很好地反映用户需求；完全删除用户数据如设备识别码等也

[8] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375，最后访问于 2019 年 7 月 4 日。

不利于未来提供用户需要的其他服务推荐等。

个人敏感信息和重要数据应备案

本次《办法（征求意见稿）》第十五条规定， 网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则、收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

个人信息与重要数据备案制度最开始由《天津市数据安全管理办法（暂行）》提出，该规定要求网络运营者对收集到的用户个人信息与重要数据需要进行备案。本次《办法（征求意见稿）》将备案范围中的个人信息范围限定为个人敏感信息，同时备案内容的要求相较于天津市也更为概括。另外，鉴于《办法（征求意见稿）》第十四条明确了网络运营者从第三方间接收集个人信息与直接收集个人信息需履行同等的保护责任，所以网络运营者即便不直接向个人信息主体收集其个人敏感信息，而是从第三方处获得个人敏感信息的，也可能需要履行相应的备案义务。

然而，尽管备案制度利于政府发挥监管作用，但是实务界仍不乏有质疑之声。实践中，网络运营者搜集的数据往往范围广泛、数量众多，且数据常具有动态性和时效性的特点，如要逐一备案，势必将大幅增加企业在数据合规运行的成本，同时对地方网信部门的备案管理要求也会显著增加。

个人信息与重要数据应分别监管

《办法（征求意见稿）》第二十八条规定，网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。向境外提供个人信息按有关规定执行。第三十八条规定，重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

本次《办法（征求意见稿）》出台之前，我国立法对重要数据的保护规定并不明晰，且未明确与个人信息的保护分割。相关规定主要涉及：2016 年颁布的《网络安全法》对于关键信息基础设施运营者的重要数据提出本地化要求；2017 年颁布的《个人信息和重要数据出境安全评估办法（征求意见稿）》对重要数据进行了定义，指与国家安全、经济发展，以及社会公共利益密切相关的数据；随后 2017 年全国信息安全标准化技术委员会在《信息安全技术 数据出境安全评估指南(征求

意见稿)》中提出了《重要数据识别指南》，列举了各行业各领域涉及的重要数据范围。

本次《办法（征求意见稿）》第三十八条对重要数据的定义更为细致，在一般性陈述之外列举了部分示例，又明确排除了企业生产经营和内部管理信息及个人信息作为重要数据的可能。更为关键的是，第二十八条要求个人信息和重要数据保护执行各自的办法，暗示了重要数据将和个人信息并行、两者将有独立的出境安全评估办法的立法趋势。不久前出台的《个人信息安全评估办法（征求意见稿）》也正好印证了这一趋势。因为个人信息与重要数据的不同特质，各自需对应不同的规制方式，我们可以期待未来关于重要数据更为细致的规定出台。此外，第二十八条只说了行业主管监管部门不明时报省级网信部门批准。但实践中，有些企业可能面临两个以上的行业主管部门，实现报审的相关规定可能使网络运营者面临多头部门管理的现象，当多部门意见不一致时如何处理，还有待进一步的指引。

平台方应与第三方应用明确责任

《办法（征求意见稿）》第三十条规定，网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。

本条加重网络运营者的责任，要求其对接入平台第三方的数据安全问题也承担责任，除非其能证明自己无过错。实践中有观点认为，平台应当于第三方应用之间通过合同约定各自需要承担的责任，如果让平台承担无过错责任，对平台来说责任较重可能并不合理，并且平台应当承担的是未遵守行政法规而产生的网络安全责任，而非侵权责任法中的无过错责任。比如像云服务平台，数据的直接收集是云服务提供方的客户本身，平台根本没有对数据活动进行任何处理活动。当然可以通过合同约定双方的数据安全要求和责任，平台方也需要督促第三方应用运营者加强数据安全管理。另外，如果接入平台的第三方一直变化，可能会使问题更加复杂，需要企业合规人员密切关注这些动态变化。

统一规则并全方位监督违法行为

《办法（征求意见稿）》第三十三至三十七条分别规定了具体的数据安全监管形式，包括：约谈整改、安全认证、安全事件报告、数据报送、行政处罚和法律责任，整体上对“数据安全监督管理”进行了全方位的规定，形成了一定的“数据安全监督管理”闭环。

第三十三条规定，网信部门在履行职责中，发现网络运营者数据安全管理责任落实不到位，应按照规定的权限和程序约谈网络运营者的主要负责人，督促整改。结合近年来网络安全和数据保护相关执法行动，网信部门的约谈整改已成为监管的主要措施之一。例如，2019 年 1 月，国家网信办正式启动网络生态治理专项行动，已经有不少企业受到了国家或地方网信部门的约谈和敦促整改，快速有效地达成了一定的“净网”效果。此外，结合近年来网络安全和数据保护相关执法行动，网信部门的约谈整改已成为监管的主要措施之一。约谈虽然仅作为一种软性的监管手段，但是也起到了良好的震慑作用，与《网络安全法》关于约谈的相关规定一脉相承，往往企业会从顾及自身的企业形象与声誉考虑，提前做好合规措施防止企业直接负责面临被约谈。

第三十四条规定的安全认证以及国家网信部门会同国务院市场监督管理部门对安全认证的组织和指导职权，与之前 2019 年 3 月 13 日市场监管总局和中央网信办联合发布《关于开展 App 安全认证工作的公告》决定开展 App 安全认证工作相衔接。其中，通过“国家鼓励 App 运营者自愿通过 App 安全认证”引导 APP 运营者履行安全保护义务，通过“鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的 App”引导消费者选用安全的 App 产品，从而对违法违规收集个人信息的 APP 进行市场劣汰和净化。

第三十五条规定的个人信息泄露等安全事件的通知和报告，借鉴吸收了欧盟的 GDPR 第三十三条（将个人数据泄露向监管机构报告）和第三十四条（将个人数据泄露向数据主体传达）。除了规定报告的及时性要求之外，未来还应当借鉴 GDPR 进一步细化规定向监管机构报告的最迟期限、数据处理者向数据控制者的及时告知义务、明确告知内容范围（泄露数据的类型与数量、数据保护官的具体情况、泄露后果的描述、已采取的应对措施或者制定的处理计划、满足及时性下的分阶段提供相关信息等）以及监管机构对泄露事件的记录责任和报告信息的核实责任。

第三十六条规定的网络营运者的数据报送义务与主管部门的安全保护责任，与《网络安全法》第二十八、三十八条，《电子商务法》第二十五、二十八条，《网络交易监督管理办法(征求意见稿) 》第二十五、二十六、四十、四十一、四十二条相衔接。

第三十七条规定，网络运营者违反本办法规定的，由有关部门依照相关法律、行政法规的规定，根据情节给予公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。该条确立了所有违反规定的统一处罚机制，这与以往《网络安全法》规定不同违法行为可能触发不同行政法责任的立法例有所不同。

2. 各国个人信息出境实况——兼评《个人信息出境安全评估办法（征求意见稿）》

2019 年 6 月 13 日凌晨，国家网信办发布《个人信息出境安全评估办法（征求意见稿）》（以下简称“《新评估办法（征求意见稿）》”），在其 2017 年发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称“《旧评估办法（征求意见稿）》”）的基础上进行了很大的变动。本文主要以个人信息安全影响评估的整体步骤为脉络，梳理《新评估办法（征求意见稿）》的相关规定和重要变化。

出台背景

随着跨境业务的不断增加，数据在全球范围的流动已成为了企业间经营活动的重要特征之一。早在《网络安全法》出台之时，我国就对数据出境的问题，提出了安全评估的要求，认为关键信息基础设施运营者在境内运营过程中所收集或产生的业务数据，原则上应该在境内进行存储，如果因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。推荐性国家标准 《信息安全技术 个人信息安全规范 》 也对个人信息跨境转移做出相关规定：在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应符合国家网信部门会同国务院有关部门制定的办法和相关标准的要求。这里的办法，我们认为指的是《旧评估办法（征求意见稿）》，相关标准指的是《信息安全技术 数据出境安全评估指南（征求意见稿）》（以下简称“《评估指南（征求意见稿）》”）。2017 年，国家发布《旧评估办法（征求意见稿）》，针对个人信息与重要数据的出境评估，做出了较为细致的要求。而此次《新评估办法（征求意见稿）》把《旧评估办法（征求意见稿）》中的个人信息出境部分单独抽出来进行规制，意味着原来将“个人信息”与“重要数据”的统一评估路径，拆分成了两条不同的监管轨道，设定了更加清晰和严格的评估标准，将个人信息的出境传输行为纳入更全面的监管系统中。

如上所述，相较于《旧评估办法（征求意见稿）》同时规定了“个人信息”与“重要数据”的出境评估要求，《新评估办法（征求意见稿）》只针对“个人信息”的出境评估作出了相应规定，其最主要的原因在于， “个人信息”是对公民个人权益的保护，而“重要数据”则更加强调维护国家安全与社会利益。也意味着，未来国家应该还会对“重要数据”的出境评估做出单独的规定。这一趋势也体现在此前出台的《数据安全管理办法（征求意见稿）》中，虽然其第一条仍然强调是保障个人信息和重要数据安全，但在具体的条文中，也对个人信息和重要数据的规定做了一定区分，比如第 28 条规定重要数据出境需评估风险加报请主管部门同意。

评估主体

在《旧评估办法（征求意见稿）》中，规定行业主管或监管部门负责本行业数据出境安全评估工作，行业主管或监管部门不明确的，由国家网信部门组织评估。而在此次《新评估办法（征求意见稿）》中，规定个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。省级网信部门在收到个人信息出境安全评估申报材料并核查其完备性后，应当组织专家或技术力量进行安全评估。安全评估原则上需要在 15 个工作日内完成。此次新规将评估主体直接确定为省级网信部门来对评估事项负责，化解了对监管部门不够明晰的情况。同时，将评估机构统一为网信部门，有利于管理和网络运营者申诉上的统一。这种做法，虽然加强了监管对个人信息出境的审查与把控，但问题是省级网信部门的人力资源是否已经足够充裕到对本省范围内企业所报审的申报材料可以在 15 日内逐一审查完毕并反馈。如果不能够在规定时间内完成实质性审查的话，要么《新评估办法（征求意见稿）》最后落入空文，要么该条款的思路最终会在征求意见结束后得以改变。

评估对象

我国《网络安全法》第三十七条明确规定，对于关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据明确要求应在境内存储。而在《旧评估办法（征求意见稿）》第二条规定，网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。此条规定将数据境内储存的义务从关键信息基础设施的运营者拓展到了所有的网络运营者。而在此次《新评估办法（征求意见稿）》删除了此条内容，对数据的本地化储存没有再作出相应规定。但同时，对于数据出境要进行评估的主体，相较于《网络安全法》,《新评估办法（征求意见稿）》规定的范围则更广。《网络安全法》只将数据出境评估的主体限定为关键信息基础设施运营者，而《新评估办法（征求意见稿）》与《旧评估办法（征求意见稿）》类似，则要求所有涉及个人信息出境的网络运营者，都需要进行安全影响的评估，并且需要报请网信部门做实质性审查。

考虑到将所有网络运营者都纳入审查的范围，势必会加重政府部门的审查成本。有关学者提出建议考虑是否对评估主体增加豁免（即例外）的条件，如对有关数据极少且偶发的个人信息出境行为和跨国企业内部经营管理涉及到的数据等是否可以免于评估。其次，对于网络运营者，学者也建议进行角色的区分，将控制者与处理者相关的评估义务进行一定的区别，这样能使得法规在具体落实时更加合理并且能提升效率。

评估流程

1. 自评估流程非唯一要件

《旧评估办法（征求意见稿）》中规定，网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。对于含有或累计含有 50 万人以上的个人信息，数据量超过 1000GB 等可能影响国家安全和社会公共利益的网络运营者，要求其必须报请行业主管或监管部门进行评估。也就可以看出，在《旧评估办法（征求意见稿）》中包含了运营者自评估以及符合特定条件情况下方才报请监管部门评估两种模式。而《新评估办法（征求意见稿）》对于所有网络运营者，无论其规模大小，也不论行业类型，只要涉及个人信息出境，都要求其必须在企业自行评估后向所在地省级/市网信部门申报并进行安全评估，即企业在自评估或者委托第三方评估后，都需要报请网信部门批准。可以看出，新规对个人信息出境的评估要求比以前更加严格了。

2. 评估具体流程

根据《新评估办法》规定，网络运营者在个人信息出境前，应当向所在地省级网信部门申报个人信息出境安全评估，同时提交以下材料：

（一）申报书；

（二）网络运营者与接收者签订的合同；

（三）个人信息出境安全风险及安全保障措施分析报告；

（四）国家网信部门要求提供的其他材料。

《新评估办法（征求意见稿）》同时规定，省级网信部门在收到个人信息出境安全评估申报材料并核查其完备性后，应当组织专家或技术力量进行安全评估。安全评估应当在 15 个工作日内完成，情况复杂的可以适当延长。在《旧评估办法》中，规定行业主管或监管部门组织的安全评估，应当于六十个工作日内完成。此次新规将评估的时间在原来的基础上进行了大大缩短。这也是考虑到在具体实践中，许多企业依靠数据的流动创造市场价值，而对其审查评估的时间过长，会对企业经营活动造成很多影响甚至是延误。对评估时间的缩短，将有助于提高数据流转的效率，有利于创造更多价值。但是，因为此次评估的主体扩大，要求所有网络运营者都进行相关评估，评估渠道有出现拥挤的可能。因为法律中规定情况复杂的可以适当延长评估时间，但没有说明情况复杂的具体情形，也没有细化说明可延长的最大

期限是几何，对于企业来说仍然存是潜在的不确定性风险。

《新评估办法（征求意见稿）》第七条规定，省级网信部门在将个人信息出境安全评估结论通报网络运营者的同时，将个人信息出境安全评估情况报国家网信部门。网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的，可以向国家网信部门提出申诉。相较于《旧评估办法（征求意见稿）》，《新评估办法（征求意见稿）》对于个人信息出境安全评估情况的流向没有做太大变动，都要求评估的主体将结论通报网络运营者的同时，也将评估情况报国家网信部门。但在《新评估办法（征求意见稿）》中，增加了网络运营对评估结论存在异议时申诉的权利。这样的规定不仅使得网络运营者在面对自己不利的评估结果时多了一种救济措施，也会促使省级网信部门在进行安全影响评估时更加客观公正。

评估内容

《新评估办法（征求意见稿）》第六条，规定了在进行个人信息出境安全评估时应当重点评估的内容，包括：

（一）是否符合国家有关法律法规和政策规定；

（二）合同条款是否能够充分保障个人信息主体合法权益；

（三）合同能否得到有效执行；

（四）网络运营者或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件；

（五）网络运营者获得个人信息是否合法、正当；

（六）其他应当评估的内容。

对比《旧评估办法（征求意见稿）》的重点评估内容，《新评估办法（征求意见稿）》对这一部分作了较大的改动。其中最主要的一个变动是在重点评估的内容中，不仅增加了对网络运营者与境外数据接收方之间“合同”的评估，而且首次对网络运营者与境外数据接收者的合同进行了相关要求：如《新评估办法（征求意见稿）》细致地规定了双方签订的合同具体应该包含的具体内容，包括个人信息出境的目的、类型和保存时限等的规定，还包含了网络运营者以及境外接收者各自相应的义务。为了防止合同流于形式或者出现阴阳合同的情况，《新评估办法（征求意见稿）》还在评估的标准中，加入了对双方合同内容和执行的双重审查。

这一点与 GDPR 下标准合同条款的相关规定也有着类似之处。GDPR 规定，如果采用标准合同条款等适当保障措施，监管机关则不需要再对数据的跨境传输进行个案审批，但同时，欧盟委员会需要事先对标准合同条款本身进行批准。虽然标准合同条款针对的是数据传输方与数据接收方之间的合同，但其却主要是对非合同一方的数据主体提供了相应的保护机制。因为数据转移双方则可以通过其他

的商务条款约定商务合作的其他权利义务，但标准合同条款机制（SCC）则是通过落实数据转移双方对数据主体的民事赔偿责任来倒逼其切实保护个人信息主体的权利，防止合同的中的标准合同条款流于形式。鉴于此，既可以降低企业评估的成本，也能节省政府部门的评估资源。

对此，相关学者对《新评估办法（征求意见稿）》也提出一些建议，对不同的领域，如金融，医疗等是否可以拟制不同版本的标准合同条款，以应对实践中的不同情形。其次，对于合同能否单方面终止的问题，此次《新评估办法（征求意见稿）》中并没有涉及，这关涉到终止合同后数据出境方是否可以将数据追索回来的问题。

除此之外，《新评估办法（征求意见稿）》还规定了，个人信息主体有权获取合同的副本，这在保障个人信息主体实现相关权利的同时，有利于促进合同条款的透明与合理。但反过来，有些企业也会产生担心，如果出境方与接收方之间的数据转移涉及到商业秘密，那么个人信息主体的副本获取权利是否会使数据出入境企业之间显得有些尴尬？从这个问题引发得出的思考，也许我国的标准制定的组织可以比照欧盟的 SCC，制定标准化的数据出境合同。涉及商业秘密的部分，企业可以再拟定其他商务合同做出安排，标准合同一方面方便网信部门快速进行审批，也方便个人信息主体迅速读懂数据出境的主要内容。至于中国与欧盟企业之间的数据转移，究竟应当适用中国版的 SCC 还是欧盟版的 SCC，那就让企业自己去谈吧。

评估周期

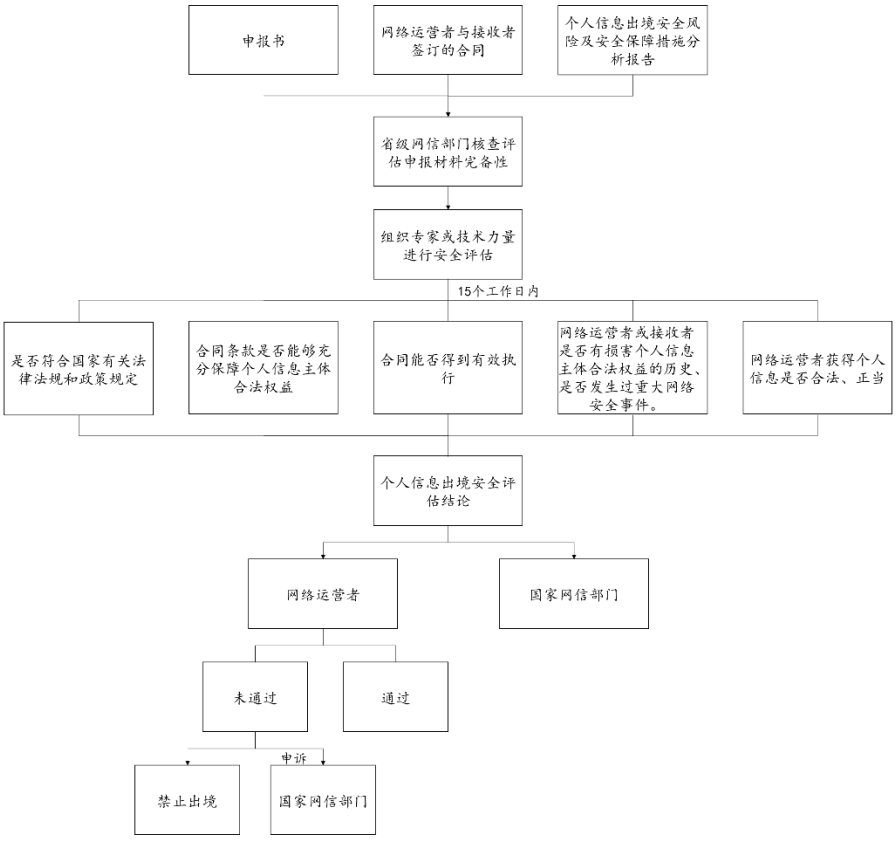
在《旧评估办法（征求意见稿）》中，规定网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时应当重新进行评估。而此次《新评估办法（征求意见稿）》规定，网络运营者应当每 2 年或者个人信息出境目的、类型和境外保存时间发生变化时应当重新评估。相较于以前的规定，此次新规将数据出境评估的周期延长到了两年，并对应当进行重新评估的场景进行了具体说明，取消了《旧评估办法（征求意见稿）》中用“等”字进行概括的做法，让要求网络运营者进行重新评估的情形更加清晰和明确。

同时，《新评估办法（征求意见稿）》也规定， 向不同的接收者提供个人信息应当分别申报安全评估，向同一接收者多次或连续提供个人信息无需多次评估。也就意味着，接收者的具体情形也成为了影响网络运营者个人信息出境的安全影响评估周期的一个因素。

持续监管

《新评估办法（征求意见稿）》规定了，网络运营者应当每年 12 月 31 日前将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门。这意味着网络运营者即使在通过了个人信息出境安全影响评估，也需要每年向所在地省级网信部门汇报出境情况以及合同履行情况，类似一种工商年审的情况。且根据《新评估办法（征求意见稿）》的规定，网络运营者应当建立个人信息出境记录并且至少保存 5 年。由此可见，出境安全评估并不是一劳永逸的措施，后续企业仍然需要对个人信息的出境情况进行持续监管，并且有义务留存好所有的出境记录，以备核查之需。

评估流程图



小结

可以看出，此次《新评估办法（征求意见稿）》的出台，无论对评估的主体、评估的内容，以及后续监管的要求，都做出了更严格和细致的规定。这样的规定势必会对相关网络运营者带来较大的影响与压力。综合个人信息出境安全影响评估的成本，以及企业可能面临评估失败后的风险，许多企业可能会由此选择增加个人信息本地化储存的策略。同时，要求所有涉及个人信息出境的网络运营者，无论业务和规模如何，都必须将评估情况向网信部门申请报批，一定程度上也会加大国家对于评估所投入的成本。如何在保障个人信息安全的同时，增加数据流动所带来的发展价值，也是各方对此《新评估办法（征求意见稿）》提出建设性意见的基本落脚点。

附件一：其他国家对于数据出境评估的相关规定

国外立法实践中也存在关于个人信息跨境数据传输的相关法律或判例。 对于国内所称的“个人信息”，国外也有类似定义。 一般而言，外国当局依靠评估来决定一个组织是否可以进行跨境数据传输。 除此之外，国外也规定了其他替代规则来评估是否允许跨境数据传输。主要内容如下。

（一）GDPR

在欧盟，关于规范数据保护的最重要的法律为 《一般数据保护条例》，（简称“GDPR”）。 GDPR 规定，在转移个人数据时，不应低于 GDPR 所规定的对自然人的保护水平，即向国外传递的个人信息应由第三国提供“足够的保护”。

根据上述规则，个人信息向第三国或地区的转移将通过以下方式加以规范 。

第三国或地区的评估应由欧盟委员会（ 以下简称 “欧委会”）进行。 它将评估数据输入国或地区的法律，确认该国家或地区对于尊重人权和基本自由、个人信息的保护水平是否充分。欧委会建立了一个“白名单”，列举其认可的国家或地区。目前，欧委会认可的有 12 个国家和地区，即美国，加拿大，安道尔共和国，瑞士，法罗群岛，根西岛，不列颠群岛，泽西岛，以色列，新西兰，阿根廷和乌拉圭。

此外，GDPR 允许组织在跨境数据传输实践中使用标准合同条款来证明其数据保护能力。 此外，适用有约束力的公司准则（以下称为“BCR”）也可以满足跨境数据传输期间数据保护的要求。 对于传输数据的组织的 BCR 的评估应该由主管部门进行。对于 BCR 的评估内容包括：组织结构，要传输的数据类型，准则对于企业内部和外部的有效性，数据保护的适用原则，赋予个人信息主体的权利及实施，组织的责任，投诉机制，DPO 的设置，以及向主管当局汇报的制度等。经过评估后，跨国公司各实体之间传输数据均适用同一标准。

除了评估，GDPR 还规定，当且仅当个人信息控制者提供适当的保障措施时，个人信息控制者可以将个人数据传输到第三国。 这些保障措施包括：

（1） 具有公共当局或机构之间具有法律约束力和可执行的文书;

（2） 具有由委员会根据审查程序审核通过的标准数据保护条款，以及监管机构通过并经欧委会批准的标准数据保护条款 ;

（3） 具有经批准的企业行为准则，以及第三国的个人信息控制者或处理者做出的具有约束力和可执行的适当的保障措施的承诺;

（4） 具有相应认证证书，以及第三国个人信息控制者或处理者作出的具有约束力和可执行的适当的保障措施的承诺。

（二）APEC 的 CBPR 体系

除了对跨境数据转移评估制定统一规定外，各国和各地区还制定双边或多边条约以对评估进行规定。 APEC 跨境隐私规则系统（以下简称“CBPR 体系”）是此种方式的最佳实践之一。

2012 年，CBPR 体系投入使用。 它为成员国之间提供跨境数据传输规则，要求在 APEC 国家内加入 CBPR 系统的成员国之间传输公民的个人信息应符合 CBPR 的要求。 到目前为止，美国、日本、墨西哥、加拿大、新加坡和韩国加入了 CBPR 体系。

CBPR 体系由四部分组成：自我评估，合规审查，承认/接受，争议解决和执行。各成员国在将个人信息传输到国外之前，应进行以下两个步骤。

首先，组织应根据 APEC 认可的 CBPR 调查问卷进行自我评估。 该问卷将由相应的 APEC 认可的代理机构提供。问卷主要用于评估组织保护数据的能力。 它所涉及的问题包括以下方面：

（1）通知。 组织是否向个人提供关于其个人信息传输的清晰且易于访问的陈述。
（2）信息收集的限制。 收集个人信息是否仅限于所述目的。
（3）个人信息的使用。个人信息的使用是否仅限于实现收集目的和其他兼容或相关的目的。
（4）选择。 组织是否向个人提供与其个人信息的收集、使用和披露相关的权利。
（5）个人信息的完整性。个人信息控制者是否保持个人信息记录的准确性和完整性。
（6）安全保障。 组织是否以合理的安全措施保护个人信息 。
（7）访问和更正。组织是否为个人提供访问和更正其信息的权利。
（8）责任制。该组织是否有责任遵守实施 CBPR 体系的措施。

再者，组织应当将完成的问卷和任何相关文件提交给 APEC 认可的代理机构。代理机构根据 CBPR 项目中建立的基本标准进行保密审查。

（三）隐私盾

隐私盾也是关于个人信息跨境转移条约的一种实践做法。 2016 年 2 月 2 日，美国和欧盟达成了一项名为“隐私盾”的协议。 该条约适用于美国和欧盟之间的跨境数据传输。 它主要规定了组织自我评估规则和美国监管机构的监督，并试图建

立一个灵活的区域内数据自由流动的机制。

（四）加拿大

加拿大联邦隐私专员办公室规定，数据转让人在通过合同和其他措施将个人数据转移到国外时应对其安全承担保护责任。 它要求数据传输者：（1）避免未经授权使用或披露任何第三方转移到国外的个人信息; （2）确保转移数据后的第三国有完善的政策或数据保护程序; （3）定期评估第三国境内处理或存储个人信息的行为是否足够安全。

（五）新加坡

在新加坡“个人资料保护法”（以下简称“PDPA”）中，新加坡个人资料保护委员会规定，转让人与受让人之间签订跨境数据转移合同，合同中应该设置条款要求数据收集者所提供的保护数据能力不低于 PDPA 要求的保护水平。对于跨国组织，他们可以适用有约束力的公司准则来保护跨境数据传输过程中的数据。

（六）结论

如上所述，对于个人信息的跨境转移 ，常见的做法是对跨境数据传输进行评估。 然而，由于目前各国对于评估的要求各有不同，例如，某些国家或地区要求组织进行自我评估，而其他国家或地区则要求由监管部门进行评估。

此外，除了评估之外的其他规则也适用于监管个人信息的跨境转移。 一般来说，这些规则包括：（1）数据传输合同模板，包括标准合同条款和可变动的合同条款; （2）有约束力的公司准则; （3）认证或审核等监督方法; （4）保证转让人的数据安全。这些，这对于我国而言也都是值得借鉴的。

附件二：新旧评估办法（征求意见稿）对比表

《旧评估办法（征求意见稿）》	《新评估办法（征求意见稿）》	变动之处
第一条 为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。	**第一条** 为保障数据跨境流动中的个人信息安全，根据《中华人民共和国网络安全法》等相关法律法规，制定本办法。	《新评估办法（征求意见稿）》只针对个人信息进行评估，将保障的内容总结为了跨境流动中的个人信息安全。
第二条 网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。	**第二条**网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息（以下称个人信息出境），应当按照本办法进行安全评估。经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。 国家关于个人信息出境另有规定的，从其规定。	《新评估办法（征求意见稿）》取消了个人信息在境内储存的要求，但同时，将需要进行安全评估的范围扩大为所有的网络运营者。 同时，也新增了对于个人信息不得出境的情形。
第三条 数据出境安全评估应遵循公正、客观、有效的原则，保障个人信息和重要数据安全，促进网络信息依法有序自由流动。	/	《新评估办法（征求意见稿）》删除了此条规定。
/	**第三条** 个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。	《新评估办法（征求意见稿）》对个人信息出境的评估，规定了网络运营者应向省级网信部门申报，且根据接收者的数量为标准

	向不同的接收者提供个人信息应当分别申报安全评估，向同一接收者多次或连续提供个人信息无需多次评估。 每 2 年或者个人信息出境目的、类型和境外保存时间发生变化时应当重新评估。	来确定评估的次数，并对申报评估的频率进行了规定。
第四条 个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。	/	《新评估办法（征求意见稿）》删除了向个人信息主体说明数据出境相关信息的内容，也删除了未成年人个人信息出境须经其监护人同意的规定。
/	**第四条**网络运营者申报个人信息出境安全评估应当提供以下材料，并对材料的真实性、准确性负责： （一）申报书。 （二）网络运营者与接收者签订的合同。 （三）个人信息出境安全风险及安全保障措施分析报告。 （四）国家网信部门要求提供的其他材料。	《新评估办法（征求意见稿）》新增了对于网络运营者申报个人信息出境安全评估应当提供的材料。
第五条 国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估。	**第五条** 省级网信部门在收到个人信息出境安全评估申报材料并核查其完备性后，应当组织专家或技术力量进行安全评估。安全评估应当在 15 个工作日内完成，情况复杂的可以适当延	《新评估办法（征求意见稿）》将开展数据出境安全评估的部门具体到了省级网信部门，并对将评估的时间规定为了 15 个工作日。

	长。	
第六条 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。	/	《新评估办法（征求意见稿）》删除了此条。
第七条 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。	/	《新评估办法（征求意见稿）》删除了网络运营者对数据出境自行评估的规定。
第八条 数据出境安全评估应重点评估以下内容： （一）数据出境的必要性； （二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等； （三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等； （四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等； （五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险； （六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险； （七）其他需要评估的重要事项。	**第六条** 个人信息出境安全评估重点评估以下内容： （一）是否符合国家有关法律法规和政策规定。 （二）合同条款是否能够充分保障个人信息主体合法权益。 （三）合同能否得到有效执行。 （四）网络运营者或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件。 （五）网络运营者获得个人信息是否合法、正当。 （六）其他应当评估的内容。	《新评估办法（征求意见稿）》对个人信息出境安全评估的重点评估内容做了很大的改动，其中最主要的变动为增加了对个人信息转移双方之间签订的合同的评估。

第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估： （一）含有或累计含有50万人以上的个人信息； （二）数据量超过1000GB； （三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等； （四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息； （五）关键信息基础设施运营者向境外提供个人信息和重要数据； （六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。 行业主管或监管部门不明确的，由国家网信部门组织评估。	/	因为《新评估办法（征求意见稿）》中要求所有的网络运营者都应报请省级以上网信部门进行个人信息出境的安全评估，因此删除了对此条的规定。
第十条 行业主管或监管部门组织的安全评估，应当于六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。	**第七条** 省级网信部门在将个人信息出境安全评估结论通报网络运营者的同时，将个人信息出境安全评估情况报国家网信部门。 网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的，可以向国家网信部	《新评估办法（征求意见稿）》在第五条将《旧评估办法》此处的评估时间修改为了15天，并且增加了网络运营者对评估结果提出申诉的权利。

	门提出申诉。	
/	**第八条** 网络运营者应当建立个人信息出境记录并且至少保存 5 年，记录包括： （一）向境外提供个人信息的日期时间。 （二）接收者的身份，包括但不限于接收者的名称、地址、联系方式等。 （三）向境外提供的个人信息的类型及数量、敏感程度。 （四）国家网信部门规定的其他内容。	《新评估办法（征求意见稿）》新增对于个人信息出境记录保存的相关规定。
/	**第九条**网络运营者应当每年 12 月 31 日前将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门。 发生较大数据安全事件时，应及时报所在地省级网信部门。	《新评估办法（征求意见稿）》新增对网络运营者将个人信息出境情况，合同履行情况以及较大数据安全事件进行报告的相关规定
/	**第十条** 省级网信部门应当定期组织检查运营者的个人信息出境记录等个人信息出境情况，重点检查合同规定义务的履行情况、是否存在违反国家规定或损害个人信息主体合法权益的行为等。 发现损害个人信息主体合法权益、数据泄露安全事件等情况时，应当及时要求网络运营者整改，通过网络运营者督促接收者整改。	《新评估办法（征求意见稿）》新增了此条内容。

第十一条 存在以下情况之一的，数据不得出境： （一）个人信息出境未经个人信息主体同意，或可能侵害个人利益； （二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益； （三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。	**第十一条** 出现以下情况之一时，网信部门可以要求网络运营者暂停或终止向境外提供个人信息： （一）网络运营者或接收者发生较大数据泄露、数据滥用等事件。 （二）个人信息主体不能或者难以维护个人合法权益。 （三）网络运营者或接收者无力保障个人信息安全。	《新评估办法（征求意见稿）》除了在第二条规定了个人信息不得出境的情形，在此条也规定了要求网络运营者暂停或者终止向境外提供个人信息的情形。
第十二条 网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报行业主管或监管部门。 当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。	/	《新评估办法（征求意见稿）》对此条进行了修改，详见《新评估办法（征求意见稿）》第三条。
第十三条 对违反相关法律法规和本办法向境外提供数据的行为，任何个人和组织有权向国家网信部门、公安部门等有关部门举报。	**第十二条** 任何个人和组织有权对违反本办法规定向境外提供个人信息的行为，向省级以上网信部门或者相关部门举报。	《新评估办法（征求意见稿）》将受理举报的部门修改为了省级以上网信部门或者相关部门。
/	**第十三条** 网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件（统称合同），应当明确：	《新评估办法（征求意见稿）》新增对网络运营者与个人信息接收者签订合同的相关内容的规定。

	（一）个人信息出境的目的、类型、保存时限。 （二）个人信息主体是合同中涉及个人信息主体权益的条款的受益人。 （三）个人信息主体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。 （四）接收者所在国家法律环境发生变化导致合同难以履行时，应当终止合同，或者重新进行安全评估。 （五）合同的终止不能免除合同中涉及个人信息主体合法权益有关条款规定的网络运营者和接收者的责任和义务，除非接收者已经销毁了接收到的个人信息或作了匿名化处理。 （六）双方约定的其他内容。	
/	**第十四条** 合同应当明确网络运营者承担以下责任和义务： （一）以电子邮件、即时通信、信函、传真等方式告知个人信息主体网络运营者和接收者的基本情况，以及向境外提供个人信息的目的、类型和保存时间。	《新评估办法（征求意见稿）》新增此条，同上。

	（二）应个人信息主体的请求，提供本合同的副本。 （三）应请求向接收者转达个人信息主体诉求，包括向接收者索赔；个人信息主体不能从接收者获得赔偿时，先行赔付。	
/	**第十五条** 合同应当明确接收者承担以下责任和义务： （一）为个人信息主体提供访问其个人信息的途径，个人信息主体要求更正或者删除其个人信息时，应在合理的代价和时限内予以响应、更正或者删除。 （二）按照合同约定的目的使用个人信息，个人信息的境外保存期限不得超出合同约定的时限。 （三）确认签署合同及履行合同义务不会违背接收者所在国家的法律要求，当接收者所在国家和地区法律环境发生变化可能影响合同执行时，应当及时通知网络运营者，并通过网络运营者报告网络运营者所在地省级网信部门。	《新评估办法（征求意见稿）》新增此条，同上。
/	**第十六条** 合同应当明确接收者不得将接收到的个人信息传输给第三方，除非满足以下条件： （一）网络运营者已经	《新评估办法（征求意见稿）》新增此条，同上。

	通过电子邮件、即时通信、信函、传真等方式将个人信息传输给第三方的目的、第三方的身份和国别，以及传输的个人信息类型、第三方保留时限等通知个人信息主体。 （二）接收者承诺在个人信息主体请求停止向第三方传输时，停止传输并要求第三方销毁已经接收到的个人信息。 （三）涉及到个人敏感信息时，已征得个人信息主体同意。 （四）因向第三方传输个人信息对个人信息主体合法权益带来损害时，网络运营者同意先行承担赔付责任。	
/	**第十七条** 网络运营者关于个人信息出境安全风险及安全保障措施分析报告应当至少包括： （一）网络运营者和接收者的背景、规模、业务、财务、信誉、网络安全能力等。 （二）个人信息出境计划，包括持续时间、涉及的个人信息主体数量、向境外提供的个人信息规模、个人信息出境后是否会再向第三方传输等。 （三）个人信息出境风险分析和保障个人信息安全和个人信息主体合	《新评估办法（征求意见稿）》新增对网络运营者关于个人信息出境安全风险及安全保障措施分析报告内容的规定。

	法权益的措施。	
第十四条 违反本办法规定的，依照有关法律法规进行处罚。	**第十八条** 网络运营者违反本办法规定向境外提供个人信息的，依照有关法律法规进行处理。	《新评估办法（征求意见稿）》明确了网络运营者违反此办法规定会依照有关法律法规进行处理。
第十五条 我国政府与其他国家、地区签署的关于数据出境的协议，按照协议的规定执行。 涉及国家秘密信息的按照相关规定执行。	**第十九条** 我国参与的或者与其他国家和地区、国际组织缔结的条约、协议等对个人信息出境有明确规定的，适用其规定，我国声明保留的条款除外。	《新评估办法（征求意见稿）》对按照其他协议执行的情形中增加了我国参与的或与国际组织缔结的条约、协议，但强调我国声明保留的除外。
第十六条 其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。	/	《新评估办法（征求意见稿）》删除了此条内容。
/	**第二十条** 境外机构经营活动中，通过互联网等收集境内用户个人信息，应当在境内通过法定代表人或者机构履行本办法中网络运营者的责任和义务。	《新评估办法（征求意见稿）》新增了此条规定。
第十七条 本办法下列用语的含义： 网络运营者，是指网络的所有者、管理者和网络服务提供者。 数据出境，是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。 个人信息，是指以电子	**第二十一条** 本办法下列用语的含义： （一）网络运营者，是指网络的所有者、管理者和网络服务提供者。 （二）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件	《新评估办法（征求意见稿）》删除了对“数据出境”，“重要数据”的含义解释；同时增加了对“个人敏感信息”的含义解释。

或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。 重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。	号码、个人生物识别信息、住址、电话号码等。 （三）个人敏感信息，是指一旦被泄露、窃取、篡改、非法使用可能危害个人信息主体人身、财产安全，或导致个人信息主体名誉、身心健康受到损害等的个人信息。	
第十八条 本办法自 2017 年 月 日起实施。	**第二十二条** 本办法自 年 月 日起实施。	

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