瀚一律师事务所
HAN YI LAW OFFICES
上海市中山西路 2020 号华宜大厦 1 座 1801 室 邮政编码: 200235 电话: (86-21) 6083-9800
www.hanyilaw.com

《网络数据安全管理条例（征求意见稿）》速评

— 网络数据安全迎来强监管时代

2021 年 11 月 14 日，国家互联网信息办公室（“网信办”）发布《网络数据安全管理条例（征求意见稿）》（“网络数据安全条例草案”或“条例草案”）并向社会公开征求意见。网络数据安全条例草案对《网络安全法》、《数据安全法》、《个人信息保护法》等上位法中关于数据安全管理的规定在网络空间的落实进行了细化和补充。

条例草案适用范围很广，包括中国境内利用网络开展数据处理活动、网络数据安全的监督管理，也包括部分在中国境外处理中国境内个人和组织数据的活动[1]。本文将主要从网络数据安全条例草案对企业赴境外上市、并购重组以及日常运营涉及的数据处理等方面的潜在影响和立法亮点进行简要地梳理和总结，以供有兴趣的人士参考。

1. 对赴境外上市的企业的影响

(1) 网络安全审查的要求对赴“国外上市”和“香港上市”进行了区分

2021 年 7 月，网信办公布了《网络安全审查办法（修订草案征求意见稿）》（“安审征求意见稿”）向社会公开征求意见，其在现行有效的《网络安全审查办法》基础上，将网络安全审查的适用范围由关键信息基础设施运营者采购网络产品和服务影响或可能影响国家安全的情形，扩展至包括数据处理者开展数据处理活动影响或可能影响国家安全的情形，并特别规定“掌握超过 100 万用户个人信息的运营者赴国外上市”应申报网络安全审查。

安审征求意见稿中“国外上市”的表述是否包括赴香港上市曾引起社会广泛讨论。值得注意的是，网络数据安全条例草案特将“处理 100 万人以上个人信息的数据处理者赴国外上市”与“数据处理者赴香港上市，影响或可能影响国家安全的”列为了两种分别需要申报网络安全审查的情形。从文字表述可以看出，条例草案意图将赴“香港上市”排除在赴“国外上市”之外，作为单独的情形予以处理。而就赴香港上市的企业而言，网络数据安全条例草案要求该等企业在“存在影响或可能影响国家安全的情况”下，方有义务在上市前进行网络安全审查申报。然而，网络数据安全条例草案并未对“影响或可能影响国家安全”的判断标准提供具

[1] 包括在中国境外处理中国境内个人和组织数据的以下活动（自然人因个人或者家庭事务开展数据处理活动的除外）：
(1) 以向境内提供产品或者服务为目的；
(2) 分析、评估境内个人、组织的行为；
(3) 涉及境内重要数据处理；
(4) 法律、行政法规规定的其他情形。

体指引。在初步参考条例草案中对重要数据[2]的定义和列举的基础上，我们理解，如相关企业涉及重要数据、核心数据[3]的处理行为的，则该等企业赴香港上市可能被认定为影响或可能影响国家安全，从而被要求进行网络安全审查的可能性将相对较大。

对于如何判断“存在影响或可能影响国家安全的情形”，我们也与网信办进行了初步的电话咨询，相关工作人员表示，在网络数据安全条例草案、安审征求意见稿及相关细则正式生效前，网信办尚无法对赴香港上市的企业在哪些情形下需要进行网络安全审查给出明确答复。

(2) 赴境外上市的数据处理者需履行年度数据安全评估及报告义务

根据网络数据安全条例草案，赴境外上市的数据处理者（从字面意思看，此处的赴“境外上市”应包括赴国外上市和赴香港上市的情况）应当自行或委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告上报设区的市级网信部门。

条例草案暂未明确上述评估和报告义务是否也适用于处于上市过程中的数据处理者。如果网络数据安全条例草案按目前规定生效，处于境外上市过程中的数据处理者，除应考虑可能适用的网络安全审查义务外，也应与主管部门保持密切联系，以确认是否应履行数据安全评估及报告义务。

2. 对企业合并、重组及解散的影响

根据网络数据安全条例草案，数据处理者发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告；数据处理者发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。

如果是汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的，数据处理者还应当履行网络安全审查申报义务。

---

[2] 重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。包括以下数据：

(1) 未公开的政务数据、工作秘密、情报数据和执法司法数据；
(2) 出口管制数据，出口管制物项涉及的核心技术、设计方案、生产工艺等相关的数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争实力有直接影响的科学技术成果数据；
(3) 国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；
(4) 工业、电信、能源、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；
(5) 达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等人口与健康、自然资源与环境国家基础数据；
(6) 国家基础设施、关键信息基础设施建设运行及其安全数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；
(7) 其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。

[3] 核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据。

3. 企业日常数据处理的有关要求

(1) 个人信息保护

个人信息的保护是网络数据安全监管的重点之一。与 2021 年 8 月颁布的《个人信息保护法》相比，网络数据安全条例草案在个人信息保护方面有如下几个亮点：

- *个人信息处理规则的展示*。数据处理者处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。

- *单独同意的定义以及举证责任*。条例草案重申了《个人信息保护法》对特定情况下处理个人信息应当取得个人单独同意的有关规定，且对“单独同意”进行了明确的定义，即单独同意是指数据处理者在开展具体数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意。该等定义要求数据处理者不得在一次弹框中同时对多项个人信息、多种处理活动同时征求个人同意。此外，条例草案还特别规定，对个人同意行为有效性存在争议的，数据处理者负有举证责任。

- *个性化推荐需单独同意*。条例草案规定互联网平台运营者利用个人信息和个性化推送算法向用户提供信息的，应当对推送信息的真实性、准确性以及来源合法性负责，并应就收集个人信息用于个性化推荐事项取得个人单独同意，相较《个人信息保护法》提出了更高的要求（*《个人信息保护法》仅要求提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式，并未明确要求取得个人单独同意*）。若未来正式稿中确认了该要求，则企业非经用户个人明确单独同意将不得向用户进行个性化推荐，这也将在一定程度上限制企业采取自动化营销的手段。

- *生物特征信息的收集的限制*。条例草案规定，数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。

- *对个人信息的重点保护*。条例草案进一步明确国家对个人信息权益进行重点保护。若数据处理者处理 100 万人以上个人信息的，还应当遵守网络数据安全条例草案相关章节对重要数据处理者的规定。

(2) 重要数据安全

网络数据安全条例草案沿袭了《数据安全法》中建立数据分类分级保护制度的有关规定，按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护，并对重要数据的处理者提出了如下需履行的主要义务：

- *重要数据的定义*。《数据安全法》未对“重要数据”进行明确定义，而网络数据安全条例草案则对“重要数据”的定义进行了概括性描述及重点列举。但对于重要数据的细化，我们理解，将主要依赖于各地区、各部门按照国家有关要求和标准，逐步制定的本地区、

本部门以及相关行业、领域重要数据和核心数据目录。在相关目录未制定并公开之前，如企业对自己所处理的数据是否构成重要数据不确定的，亦可以主动与相关主管部门进行个案沟通，进行识别和确认。

- *信息识别后的备案义务*。重要数据的处理者，应当在识别其重要数据后的 15 个工作日内向设区的市级网信部门备案。数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等（但不包括数据内容本身）。

- *专人负责、建立培训制度以及年度数据安全评估义务*。处理重要数据的数据处理者应当委派明确的数据安全负责人、制定数据安全培训计划，并应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门。

- *共享需取得同意*。数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。

(3) 数据跨境安全管理

- *建立数据出境全面监管制度*。条例草案意图建立全方位的数据出境监管制度，除数据处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息的，或者为了保护个人生命健康和财产安全而必须向境外提供个人信息情况外，数据处理者因业务等需要，确需向中华人民共和国境外提供数据的均需符合条例草案规定条件之一（如进行出境数据安全评估，或按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同等）。如前述规定予以生效，则意味着，除特定情形外，境内企业因业务需要向境外或境外机构提供数据的行为均需符合条例草案规定的条件，但对于各项条件的适用对象和要求，尚有待主管部门的进一步解释。

- *数据出境安全评估*。出境数据中包含重要数据、关键信息基础设施运营者和处理一百万人以上个人信息的数据处理者向境外提供个人信息等情况的，应通过网信办组织的数据跨境安全评估。

- *个人信息的单独同意*。数据处理者向中国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。但收集个人信息时已单独就个人信息出境取得个人同意，且按照取得同意的事项出境的，无需再次取得个人单独同意。

- *年度报告义务*。向境外提供个人信息和重要数据的数据处理者，应当在每年 1 月 31 日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况。

- *禁止非法提供 VPN 服务*。国家建立数据跨境安全网关，对来源于中国境外、法律法规禁止发布或者传输的信息予以阻断传播。任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线路等，也不得提供为穿透、绕过数据跨境安全网关的各种服务。境内用户访问境内网络的，其流量不得被路由至境外。

(4) 互联网平台运营者

- *境外运营的报告义务*。大型互联网平台运营者（指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者）在境外设立总部或者运营中心、研发中心，应当向网信办和行业主管部门报告。

- *算法策略公开*。互联网平台运营者应当建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定程序、裁决程序。就平台规则、隐私政策制定或者对用户权益有重大影响的修订，互联网平台运营者应当面向社会公开征求意见，并充分采纳公众意见，修改完善相关规则和政策；日活用户超过一亿的大型互联网平台运营者还应当经网信办认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。

- *对第三方责任先行赔偿*。互联网平台运营者应对接入其平台的第三方产品和服务承担数据安全管理责任，通过合同等形式明确第三方的数据安全责任义务，并督促第三方加强数据安全管理，采取必要的数据安全保护措施。若第三方产品和服务对用户造成损害的，用户可以要求互联网平台运营者先行赔偿。

(5) 关键信息基础设施运营者

除向境外提供个人信息的情况外，关键信息基础设施运营者采购的云计算服务，也应当履行相应的安全评估义务。

* * *

虽然网络数据安全条例草案、安审征求意见稿等仍处于草拟以及征求意见阶段，相关规定中的部分内容以及概念如何解读和实施尚处于探讨阶段，最终出台的规定与草案是否存在差异仍具有一定的不确定性，但条例草案已经在网络数据安全监管的基本制度、监管原则、执法重点等方面为数据处理者指明了方向，希望以上简要小结可以有助于相关企业提前完善内部的数据安全管理制度，以便对即将到来的新的监管要求采取及时的应对措施。

我们将密切关注相关立法的动态，并及时向有兴趣的客户更新相关信息。

瀚一律师事务所
2021 年 11 月 17 日