

一文详解企业境外上市网安数据合规

作者：潘永建 | 黄文捷

2021 年 6 月 30 日，网约车巨头“滴滴出行”于美国首次公开募股。2021 年 7 月 2 日，网络安全审查办公室宣布按照《网络安全审查办法》，对“滴滴出行”启动网络安全审查，审查期间停止“滴滴出行”新用户注册。2021 年 7 月 5 日，“运满满”“货车帮”“BOSS 直聘”同样被启动网络安全审查。随后，以网络安全审查为核心的网络安全与数据合规问题引起了拟境外上市主体更为广泛的关注。

目录

- 一、何为境外发行上市
- 二、境外上市网安数据合规法律规定
 - (一) 主要制度
 - (二) 重点实务问题
 - (三) 境外上市地法规
- 三、境外上市网安数据合规案例
- 四、境外上市网安数据合规工作方案

一、何为境外发行上市

境外发行上市是指境内的股份有限公司向境外投资者发行证券并在境外证券交易所公开上市，发行的证券种类包括股票、存托凭证、可转换为股票的公司债券或者其他具有股权性质的证券。境外发行上市分为境外直接发行上市和间接发行上市两种。

境外直接发行上市指注册在境内的股份有限公司在境外发行证券或者将其证券在境外上市交易，即以境内公司的名义在境外发行上市；境外间接发行上市指主要业务经营活动在境内的企业，以境外企业的名义，基于境内企业的股权、资产、收益或其他类似权益在境外发行证券或者将证券在境外上市交易，¹境外公司一般通过收购、股权置换的方式取得国内资产的控制权。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

¹ 《国务院关于境内企业境外发行证券和上市的管理规定(草案征求意见稿)》第二条。

一般而言,“境外”包括中国香港、澳门、台湾地区,“赴境外上市”包括赴香港上市。不过,在讨论企业境外上市网络安全与数据合规时,有必要厘清“赴境外上市”是否仍然包括赴香港上市。2021年11月14日发布的《网络数据安全条例(征求意见稿)》明确区分了“赴国外上市”和“赴香港上市”,符合以下情形的应当申报网络安全审查:处理一百万人以上个人信息的数据处理者赴国外上市的;以及数据处理者赴香港上市,影响或者可能影响国家安全的。然而,2021年12月28日发布的《网络安全审查办法》则规定,申报网络安全审查的情形为“赴国外上市”。因此,业内普遍认为,从立法进程来看,正式生效的《网络安全审查办法》使用的“赴国外上市”这一措辞不包含赴香港上市的情形。即便《网络数据安全条例(征求意见稿)》作为条例,其法律位阶高于《网络安全审查办法》,两者的起草单位均为国家互联网信息办公室,可以合理认为《网络安全审查办法》和《网络数据安全条例(征求意见稿)》中“赴国外上市”具有相同的含义。另一方面,从立法目的来看,上市场景下的网络安全审查目的在于评估上市活动中关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险,香港政府引起监管部门这一担忧的可能性较低。综上,“赴境外上市”包括赴香港上市,但《网络安全审查办法》中的“赴国外上市”不包括赴香港上市。

二. 境外上市网安数据合规法律规定

(一) 主要制度

1. 境外发行上市管理规定

2021年12月24日,证券监督管理委员会发布《国务院关于境内企业境外发行证券和上市的管理规定(草案征求意见稿)》,规定经国务院有关主管部门依法审查认定,境外发行上市威胁或危害国家安全的,不得境外发行上市;同时强调境外发行上市应严格遵守网络安全、数据安全等国家安全法律法规和有关规定。

2. 保密和档案管理规定

2022年4月2日,证券监督管理委员会发布《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定(征求意见稿)》,强调加强监管在境内企业境外发行证券和上市活动中的以下活动:涉及国家秘密、机关单位工作秘密的文件保密和档案管理,并履行保密相关审批备案义务;证券公司、证券服务机构的工作底稿应当存放在境内,不得未经批准向境外提供;向境外提供重要会计档案或复制件的应依法履行相应程序。

3. 网络安全审查

中国的网络安全审查制度由《国家安全法》《网络安全法》确立,由《网络安全审查办法》具体实施。根据《网络安全审查办法》,网络安全审查包括两种触发机制:依申报审查及依职权审查。(详见我们之前发表的文章 [《2022 版<网络安全审查办法>重点问题评析》](#))

(1) 依申报审查

根据《网络安全审查办法》，符合以下情形的，当事人应当按照《网络安全审查办法》申报进行网络安全审查：

- (i) 关键信息基础设施运营者采购网络产品和服务，影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查；
- (ii) 掌握超过 100 万用户个人信息的网络平台运营者赴国外上市的，应当向网络安全审查办公室申报网络安全审查。

(2) 依职权审查

在《网络安全审查办法》下，除在上述第(i)和第(ii)项所述情形下当事人应当主动申报进行网络安全审查外，如果网络安全审查工作机制成员单位认为“网络产品和服务”以及“数据处理活动”影响或可能影响国家安全的，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依职权进行网络安全审查。

4. 数据安全合规

境外上市过程中，拟上市主体向境外监管机构、中介机构提供数据的行为属于数据出境，受到《数据安全法》《网络安全法》等数据出境法律法规约束。

(1) 向境外监管机构提交数据

拟上市主体向境外监管机构提交数据受到严格规制。《数据安全法》第三十六条明确要求，非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。《个人信息保护法》亦强调，非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定(征求意见稿)》中有类似规定，甚至更为严格，直接要求证券公司、证券服务机构的工作底稿存储在境内。这一规定与部分境外上市地关于信息披露、审计的规定相冲突，详见以下第 5 点。

(2) 数据出境安全评估

个人信息和重要数据出境应满足数据出境安全评估要求。关键信息基础设施运营者进行数据出境的，应当向国家网信部门申报数据出境安全评估；其他数据处理者进行数据出境的，具体出境细则几经发布但尚未生效，根据 2021 年 10 月 29 日发布的《数据出境安全评估办法(征求意见稿)》，重要数据出境、处理 100 万人以上的个人信息处理者进行个人信息出境、累计出境 1 万人以上敏感个人信息等情况应向国家网信部门申

报数据出境安全评估,且所有数据出境均应事先开展数据出境风险自评估(详见我们之前发表的文章[《一图读懂数据出境规则》](#))。

(3) 个人信息出境其他合规要求

个人信息出境还应满足《个人信息保护法》提出的合规要求,处理个人信息应取得相关个人的授权同意,除非处理个人信息属于《个人信息保护法》第十三条规定的例外情形。对于个人信息的跨境传输,个人信息处理者应向个人告知境外接收方的名称或者姓名、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接收方行使本法规定权利的方式和程序等事项,并取得个人的单独同意;进行个人信息保护影响评估,评估个人信息出境是否合法、正当、必要等。

在境外上市情境下,交易记录、交易合同等数据出境的过程中很有可能涉及个人信息出境,除非出境前相关个人信息进行了匿名化处理(例如,在数据出境的过程中不传输直接标识符或将间接标识符采用符合国家标准的加密算法进行加密),否则必须遵守上述合规要求。

(二) 重点实务问题

1. 何为网络平台运营者?

尽管《网络安全审查办法》并未明确网络平台运营者的具体含义,但参考《电子商务法》等生效法律,以及《网络数据安全条例(征求意见稿)》等法律草案,可以推导“网络平台运营者”的大致内涵和外延。我们将相关现行有效法律和法律草案中与“网络平台运营者”相类似的概念总结如下:

法律法规	概念	定义
《电子商务法》	电子商务平台经营者	本法所称电子商务平台经营者,是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务,供交易双方或者多方独立开展交易活动的法人或者非法人组织。(第9条)
《网络交易监督管理办法》	网络交易平台经营者	网络交易平台经营者,是指在网络交易活动中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务,供交易双方或者多方独立开展网络交易活动的法人或者非法人组织。(第7条)
《国务院反垄断委员会关于平台	平台经营者	互联网平台,是指通过网络信息技术,使相互依赖的双边或者多边主体在特定载体提

经济领域的反垄断指南》		供的规则下交互，以此共同创造价值的商业组织形态。 平台经营者，是指向自然人、法人及其他市场主体提供经营场所、交易撮合、信息交流等互联网平台服务的经营者。(第 2 条)
《网络数据安全 管理条例(征求意见稿)》	互联网平台运营者	互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。(第 73 条)

通过上表的相近概念，我们认为，《网络安全审查办法》下的网络平台运营者是向自然人、法人等市场主体提供网络平台服务的主体，而网络平台服务又包括信息发布、社交、交易、支付、视听等类型。典型的网络平台服务面向广大公众用户，例如电商平台、线上支付平台，形式包括但不限于网站、软件、APP、小程序。传统的 2B 企业在日常运营中一般不涉及提供网络平台服务，其搭建的供内部员工使用的平台(商业合作伙伴可能有接入权限)作用并非为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务。

2. 100 万用户个人信息

此处“100 万用户”与上述网络平台相对应，应理解为使用信息发布、社交、交易、支付、视听等网络平台的公众用户。企业内部员工、商业合作伙伴员工可能也有权限接入网络平台，其是否应当算作“100 万用户”，有待监管机构的进一步澄清。

3. 网络安全审查的评估要点及审查条件

评估对象	评估要点	依申报审查条件	依职权审查条件
网络产品和服务	- 产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险; - 产品和服务供应中断对关键信息基础设施业务连续性的危害; - 产品和服务的安全性、开放性、透明性、来源的多样性,供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险;	关键信息基础设施运营者采购网络产品和服务,影响或者可能影响国家安全(由企业先行预判风险)	《网络安全审查办法》第二条限定网络安全审查适用情形包括:关键信息基础设施运营者采购网络产品和服务,网络平台运营者开展数据处理活动。 - 网络安全审查工作机制成员单位认为影响或者可

	- 产品和服务提供者遵守中国法律、行政法规、部门规章情况; - 上市存在关键信息基础设施被外国政府影响、控制、恶意利用的风险,以及网络信息安全风险。		能影响国家安全的网络产品和服务以及数据处理活动,由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后,依照《网络安全审查办法》的规定进行审查。
数据处理活动	核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险。	/	
上市活动	上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险,以及网络信息安全风险。	掌握超过 100 万用户个人信息的网络平台运营者	

综上,按照目前生效的法律法规,在境外上市情景下,“网络平台运营者”在符合“掌握超过 100 万用户个人信息”并“赴国外上市”的情景下方有义务主动申报网络安全审查。

然而需注意,在境外上市过程中,监管部门亦可能从网络产品和服务以及数据处理活动安全性、可能带来的国家安全风险方面对拟上市主体依职权主动发起网络安全审查。

(三) 境外上市地法规

以美国为例,拟在美国上市主体受限于美国证券法下的披露要求:美国《2002 年萨班斯·奥克斯利法案》(the Sarbanes-Oxley Act of 2002)要求发行人接受美国公众公司会计监督委员会(the Public Company Accounting Oversight Board's (“PCAOB”))的审查。审查程序之一即为 PCAOB 审查发行人的审计机构的审计工作底稿,工作底稿内容一般包括:²

- (1) 总账和摘要:总账,重要合同总结或摘要,备忘录(会计立场或分析文件),第三方确认函,信件往来,账户或交易明细表,审计计划,保证信等;
- (2) 账户或交易明细表:审计师通常将账户或交易明细表与发票、提单、采购订单、银行对账单、支票、电汇等支持性证据进行比对,审计师可以选择是否在工作底稿中保留这些支持性证据对应的文件;
- (3) 组织结构图,投资者和所有权信息,与客户、供应商、借贷机构的重要合同信息等;
- (4) 支持审计师对可能影响公司所有权的股权交易以及管理层对该等交易的预测、判断、审计的评估的证据:交易性质、条款概要、交易金额、交易合同等;及

² 详见 <https://www.sec.gov/news/speech/fischer-remarks-international-council-securities-associations-052422>

- (5) 有关公司财务报告内部控制有效性的信息：公司的财务内控制度，公司的操作系统如何确保正确处理金融交易等(例如，显示设置选项的系统菜单屏幕截图)。

已经或拟在美国上市的发行人及其审计机构面临中国《数据安全法》《个人信息保护法》等法律法规下关于网络安全和数据安全的合规要求及美国证券法律下信息披露法律要求的冲突，且这一冲突未见缓解迹象。

2020 年，美国通过《外国公司问责法》(the Holding Foreign Companies Accountable Act)，以贯彻审计机构在《2002 年萨班斯法案》下的义务。具体而言，《外国公司问责法》要求：

- (1) PCAOB 确定审计机构所在司法管辖区当局采取的立场是否导致 PCAOB 无法对该等审计机构进行审查；
- (2) SEC 确定提交年度报告的发行人，该等年度报告包含由 PCAOB 决定所涵盖的审计机构编制的审计报告；
- (3) 某一发行人被 SEC 根据上述程序连续三年确定后，SEC 应当对这些发行人的证券实施交易禁令。

自《外国公司问责法》通过以来，PCAOB 已确定中国和香港两个司法管辖区的当局阻止 PCAOB 对审计机构进行审查；截止 2022 年 5 月，SEC 已确定 40 个年度报告中包含由这些无法接受审查的审计机构编制的审计报告的发行人，这些发行人面临潜在的退市风险。³

三. 境外上市网安数据合规案例

根据证监会官网发布的境外证券发行反馈意见，⁴我们总结梳理如下相关案例。

发行人	反馈意见	反馈意见发布时间
阳光保险	十、请说明你公司开发、运营的 APP、小程序等产品情况，并说明是否涉及提供信息内容，如果提供，说明信息内容的类型，以及信息内容安全保护的措施。请律师核查并出具明确的法律意见。	2022 年 4 月 18 日—2022 年 4 月 22 日
	十一、请说明你公司收集及储存的用户信息规模，数据收集使用情况，上市前后保护个人信息和数据安全的安排，是否符合《中华人民共和国数据安全法》等法律法规要求。请律师核查并出具明确的法律意见。	
中联航运	四、请说明你公司及下属公司业务经营过程中收集及使用数据的情况，并说明是否符合《数据安全法》《关键信息基础设施安全保护条例》等法律法规的相关要求。请律师核查并出具明确的法律意见。	2022 年 2 月 21 日—2022 年 2 月 25 日

³ 详见 <https://www.sec.gov/news/speech/fischer-remarks-international-council-securities-associations-052422>

⁴ 详见 http://www.csrc.gov.cn/csrc/c100098/common_list.shtml

珠海万达	六、请说明你公司 收集及储存的个人信息规模 ，是否适用 网络安全审查 ，是否符合 个人信息保护法、信息安全法 规定。请律师核查并出具明确的法律意见。	2021年11月1日—2021年11月5日
圆心科技	七、请说明你公司 收集及储存的医疗数据、个人信息规模 ，并对照网络安全审查管理办法(征求意见稿)自查，说明是否适用 网络安全审查 。请律师核查并出具明确的法律意见。	2021年10月11日—2021年10月15日
鹰瞳科技	一、请补充说明你公司经营风险分析中所披露的 关于业务受制于与数据保护相关法律法规的详细情况 ，是否符合 个人信息和重要数据等相关法律法规规定 ，并提供依据。请律师核查并出具法律意见。	2021年6月28日—2021年7月2日
蚂蚁集团	六、请补充说明你公司及各下属公司业务有关情况:.....(二)落实《网络安全法》等有关规定，加强信息跨境流动合规管理的情况;.....。	2020年9月7日—2020年9月11日

上述案例表明，证监会目前的关注点主要集中于网安数据合规领域的传统重点，包括收集及储存的个人信息规模、收集及使用数据的情况、个人信息合规、重要数据合规、数据出境合规等；并且，自《网络安全审查管理办法(征求意见稿)》发布后，证监会明确问询两个发行人其上市活动是否适用网络安全审查。拟境外上市主体可以比照自身和上述发行人的行业、业务模式、处理的数据类型等情况借鉴参考，并寻求数据专业律师的支持。

四. 境外上市网安数据合规工作方案

为满足境外上市网安数据合规，我们建议拟上市主体可以从以下方面着手：

1. 开展数据合规体检

简而言之，数据合规体检首先是对企业收集处理的数据进行摸排，厘清核心数据、重要数据、个人信息等数据类型；其次，明确各类数据合规义务，根据法律法规要求评估企业对各类数据的保护是否达到基本合规要求。

开展数据合规体检，不仅有利于为境外上市网安数据合规的后续工作方案(健全网安数据合规制度、评估网络安全审查、评估数据出境风险)做铺垫；还有利于拟上市主体对其持有的数据“摸家底”，对不同重要和敏感程度的数据采取不同的管控和保护措施，建立、完善数据风险管理内部流程，对企业控制、处理的数据采取恰当的分类措施，应对上市以外其他各类业务场景下的网安数据合规义务(详见我们之前发表的文章[《能力越大，责任越大——数据分类分级制度评述》](#))。

2. 建立健全网络安全和数据合规制度

除网络安全审查外，证监会对于拟境外上市主体的网络安全和数据合规审查重点与对境内上市主体的重点相比并无显著差别(详见我们之前发表的文章[《公司上市与数据合规\(上篇\)》](#)及[《公司上市与数据合规\(下篇\)》](#))，拟上市主体应注意根据企业实际情况建立健全网络安全、数据安全、个人信息保护、重要数据等合规制度，包括但不限于：

- 个人信息安全事件应急预案制度
- 个人信息安全影响评估制度
- 个人信息安全负责人制度
- 数据分类分级制度
- 数据共享制度
- 数据出境制度
- 权限管理制度
- 数据合规审计制度
- 国家秘密及重要数据识别指南

3. 就赴国外上市情形，评估是否应当进行网络安全审查

《网络安全审查办法》明确规定了赴国外上市应当进行网络安全审查的条件，建议拟境外上市主体审慎评估：

- 自身是否构成“掌握超过 100 万用户个人信息的”“网络平台运营者”“赴国外上市”，以明确是否因境外上市情景而触发网络安全审查；
- 企业自身是否构成关键信息基础设施运营者，采购的网络产品和服务的安全性、开放性、透明性等；
- 企业的数据出境情况，尤其是企业的数据处理活动是否涉及核心数据、重要数据或者大量个人信息非法出境的风险；
- 企业的其他数据处理活动，包括核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用的风险；在评估重要数据时，注意企业的主要商业合作伙伴是否构成关键信息基础设施运营者、企业是否从关键信息基础设施运营者处接收重要数据。

4. 评估数据出境风险

企业在境外上市过程中，尤其应注意梳理向境外传输的数据类型、数据量、是否涉及受监管数据。境外上市情境下关于数据出境的不同合规义务交织，不仅涉及上述网络安全审查，还涉及数据出境安全评估、获取个人同意、个人信息保护影响评估等严格的合规要求。

此外，还需结合境外上市地的证券披露法律法规要求，明确拟上市主体、中介机构披露义务的具体内容、涉及的数据类型，是否受制于中国数据安全或数据出境等法律法规。以审计底稿为例，其包含的数据量较大且数据类型复杂，很有可能涉及个人信息、重要数据或其他受到特别监管的数据，拟上市主体在向境外中介机构提供此类底稿的过程中需符合数据出境合规义务，境内中介机构向境外监管机构提供此类底稿则需进行前置审批。

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2022