

企业境外上市中的网络安全和数据合规问题(二) ——网络安全审查及数据出境合规要点

作者：张征轶 | 朱晓阳 | 韩政 | 梁茜颖

前言

此前，我们在[《企业境外上市中的网络安全和数据合规问题\(一\)》](#)中梳理了网络安全和数据合规领域的主要法律法规和监管体系演变。随着法规建设和监管体系的日趋完善，无论是从监管的角度，亦或拟上市企业的角度，尤其是对于那些具备大量网络数据或个人信息的企业，其上市过程中的网络安全和数据合规问题被愈发重视。尤其在近一年多企业境外上市的热潮中，无论是本所服务的境外上市企业，还是市场公开项目，越来越多的企业在境外上市过程中聘请专业的数据合规顾问处理复杂的网络安全和数据合规问题。

本文作为“企业境外上市中的网络安全和数据合规问题”系列文章的第二篇，旨在总结本所“企业境外上市数据合规小组”过往诸多项目实务经验，梳理企业境外上市过程中涉及的网络安全审查和数据出境合规要点，以供相关企业或境外上市中介机构参考。

第一部分 境外上市中的网络安全审查

一. 触发网络安全审查的情形

目前，我国有关网络安全审查制度及具体实施要求主要由《网络安全法》《网络安全审查办法》规制。根据网络安全审查工作机制成员单位¹是否主动发起审查，网络安全审查的触发情形可被区分为两类，分别为依申报审查和依职权审查。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

¹ 指国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局十三家成员单位。

1. 依申报审查

依申报审查是指在符合以下任一情形时，由当事人按照《网络安全审查办法》进行网络安全审查自主申报：

- (1) **关键信息基础设施运营者**（“CIIO”）采购网络产品和服务，影响或者可能影响国家安全的；
- (2) **网络平台运营者**开展数据处理活动，影响或者可能影响国家安全的（此处的“数据处理活动”指网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动）；
- (3) **网络平台运营者**掌握超过 100 万用户个人信息，且赴国外上市。

根据《关键信息基础设施安全保护条例》，CIIO 是指“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统”。重要行业和领域的主管部门、监督管理部门将会自行认定运营者是否系 CIIO 并予以通知，运营者无需进行自行判断；换言之，若企业未曾收到监管机构认定其构成或可能构成关键信息基础设施运营者的通知，则可认为企业不属于关键信息基础设施运营者，有关关键信息基础设施运营者的网络安全审查申报义务不适用于该企业。

此外，《网络安全审查办法》及相关法律法规中并未对“网络平台运营者”作出明确定义，企业需要结合业务内容和数据处理活动内容来进行实质判断，实践中，通过互联网平台方式向大量 C 端个人消费者提供商品或服务的企业具有不小概率会被认定为“网络平台运营者”，常见的如从事电子商务、居民生活服务、互联网零售等业务的企业。

2. 依职权审查

网络安全审查工作机制成员单位认为影响或者可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，根据其职权主动发起网络安全审查。

二. 境外上市过程中的网络安全审查

国家互联网信息办公室在《网络安全审查办法》答记者中明确指出，网络平台运营者在向国外证券监管机构正式提出上市申请之前申报网络安全审查，尤其是当其业务涉及国家安全等重要领域时。这一要求旨在确保国家网络安全不受境外上市活动的影响。此外，在境外上市的相关申报文件准备过程中，企业和中介机构还需在提交给中国证监会的文件中，详细说明是否已经涉及并履行了相应的安全审查程序，以确保所有流程符合国家相关法律法规的要求。

在实践中，拟境外上市的企业除了需要初步梳理和掌握其已收集和处理的个人信息数量及具体情况外，中介机构也会积极协助企业进行更为深入和全面的梳理工作。这一步骤的目的是为了进一步分

析和评估企业是否具备充分的内部、外部依据确认自身是否需要进行网络安全审查申报。例如，虽然“赴香港上市”明确不属于《网络安全审查办法》第七条中规定的“赴国外上市”，但企业还可以通过向中国网络安全审查认证和市场监管大数据中心(简称“CCRC”)进行咨询，确认其境外上市是否属于《网络安全审查办法》第七条规定的应当进行网络安全审查申报的情形，从而借助官方意见对自身是否需要进行网络安全审查申报予以明确。尽管《网络数据安全条例(征求意见稿)》曾将“数据处理者赴香港上市，影响或者可能影响国家安全的”列为应当申报网络安全审查的情形，但今年 1 月 1 日最终生效的《网络数据安全条例》已将该情形删除。

第二部分 境外上市中的数据出境合规

一. 重要数据出境

《促进和规范数据跨境流动规定》第七条规定，针对重要数据出境，无论是 CII 或除 CII 外的数据处理者均需要通过所在地省级网信部门向国家网信部门申报数据出境安全评估。对于确需出境的重要数据，经数据出境安全评估认为不会危害国家和社会公共利益的，方可出境。

企业确保重要数据出境合规的前提是准确识别重要数据。《网络数据安全条例》规定，重要数据的范围由相关地区、行业部门的监管部门确定。目前实践中对于重要数据的确认主要有几种途径：(1) 部分行业、领域数据分类分级标准规范和重要数据识别申报规则已经公开发布，如工业领域的《工业领域重要数据识别指南》、电信领域的《电信领域重要数据识别指南》、自然资源领域的《地理信息数据分类分级工作指南(试行)》、统计领域的《统计数据安全管理条例》等；(2) 此外，还有主管部门通过召开会议、制发文件、一对一通知等形式告知到数据处理者。

和“关键信息基础设施运营者”的认定逻辑类似，《促进和规范数据跨境流动规定》第 2 条规定，数据处理者应当按照相关规定识别、申报重要数据；未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。国家互联网信息办公室发布的《数据出境安全管理政策问答(2025 年 5 月)》也曾对此特别予以说明，即如果相关行业没有发布行业、领域的数据分类分级标准规范和重要数据识别申报规则，数据处理者也没有被有关部门告知应当进行重要数据识别申报的，数据处理者不需要作为重要数据申报数据安全评估，相关数据出境活动不会被认定为违反违规出境重要数据，不会因此受到行政处罚。如果数据处理者掌握的数据公开发布或被告知为重要数据后，继续开展数据出境活动的，应当在数据公开发布或被告知后 2 个月内，及时履行数据出境安全评估。

二. 个人信息出境

根据《个人信息保护法》第三十八条的规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

- (1) 依照《个人信息保护法》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。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的, 可以按照其规定执行。

据此, 根据个人信息出境的类型和情形不同, 对于个人信息出境的监管类型可区分为豁免、与接收方订立个人信息出境标准合同、通过个人信息保护认证和数据出境安全评估。

企业主体	涉及情形	监管要求
CIIO	向境外提供任何个人信息 ²	数据出境安全评估
除 CIIO 外的数据处理器 (自当年 1 月 1 日起累计)	自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息(不含敏感个人信息 ³)	豁免
	向境外提供 10 万人以上、不满 100 万人个人信息(不含敏感个人信息)	与接收方订立个人信息出境标准合同/通过个人信息保护认证
	向境外提供 100 万人以上个人信息(不含敏感个人信息)	数据出境安全评估
	向境外提供不满 1 万人以上敏感个人信息	与接收方订立个人信息出境标准合同/通过个人信息保护认证
	向境外提供 1 万人以上敏感个人信息	数据出境安全评估

同时, 《促进和规范数据跨境流动规定》允许自由贸易试验区在国家数据分类分级保护制度框架下, 自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单(“负面清单”), 经省级网络安全和信息化委员会批准后, 报国家网信部门、国家数据管理部门备案。截至目前, 天津、北京、上海、海南和浙江的自贸区已制定负面清单, 就具体行业和数据出境场景进行细化规定。

三. 其他数据出境的监管豁免情形

除上文表格所述的“自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息”属于豁免监管的数据出境情形外, 根据《促进和规范数据跨境流动规定》之规定, 如下情形亦在豁免之列:

² 所谓“个人信息”, 是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息, 不包括匿名化处理后的信息。此处匿名化处理是指经过处理无法识别特定自然人且不能复原的过程。

³ 所谓“敏感个人信息”是指一旦泄露或者非法使用, 容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息, 包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息, 以及不满十四周岁未成年人的个人信息。

1. 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供, 且不包含个人信息或者重要数据的;
2. 数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供, 处理过程中没有引入境内个人信息或者重要数据的;
3. 为订立、履行个人作为一方当事人的合同, 如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等, 确需向境外提供个人信息的;
4. 按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理, 确需向境外提供员工个人信息的(企业对于自身相关行为是否属于“跨境人力资源管理”行为存在疑义的, 可通过中介机构咨询相关主管部门意见);
5. 紧急情况下为保护自然人的生命健康和财产安全, 确需向境外提供个人信息的。

结语

我们期望本文的梳理能够帮助相关方更迅速地了解企业境外上市过程中面临的网络安全审查和数据出境合规要点及其应对策略。随着国际地缘博弈不断加剧, 在当下及未来较长一段时间内, 可以预见各方对网络安全和数据出境的重视将不断加强; 加之国内网络安全和数据合规监管体系亦在不断动态更新或完善之中, 企业及相关专业机构应不断跟踪学习, 了解监管动态, 和主管部门进行适时沟通, 从而以最高效的方式应对企业境外上市过程中的相关合规风险。

如您希望就相关问题进一步交流，请联系：



张征轶
+86 21 3135 8727
zhengyi.zhang@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com



韩政
+86 21 3135 8684
ryan.han@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 2025