企业境外上市中的网络安全和数据合规问题(三)
——个人信息保护、APP 合规与内控体系建设

作者：张征轶 | 朱晓阳 | 韩政

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。在《企业境外上市中的网络安全和数据合规问题(二)》一文中总结了网络安全审查和数据出境合规的监管要点。本文将延续这个系列，围绕境内企业在筹备及推进境外上市过程中，如何系统性地应对数据合规中的个人信息保护、APP 合规要求，以及如何建立企业完善的网络安全和数据合规内部控制体系等问题展开探讨，力求为相关企业提供一份清晰、实用的行动指南。

一. 个人信息保护合规要点

个人信息保护的合规性，无疑是企业境外上市审核流程中，境内外监管机构共同关注的焦点。监管部门会仔细检视企业处理个人信息的方式、政策及具体实践，判断其是否全面符合相关法律法规。以下是企业在此方面需重点履行的几项核心义务:

(一) 单独同意

根据《个人信息保护法》，在处理敏感个人信息、向第三方提供、公开个人信息或将个人信息跨境传输等特定场景下，企业必须获得个人的“单独同意”。

“单独同意”的核心法律内涵在于强调用户同意的“具体”与“特定”。这意味着，企业不能再依赖冗长隐私政策中的一揽子授权来模糊处理，而是必须针对每一项需要“单独同意”的个人信息处理行为，设计清晰、独立的交互界面(例如，专门的弹窗或非默认勾选框)。同时，需

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

辅以简明扼要、无歧义的说明，让用户充分了解其同意的具体内容、潜在后果以及拒绝的权利与途径，确保用户在完全知情的前提下，主动、明确地对特定事项进行授权。

(二) “最小必要”原则

《个人信息保护法》明确，个人信息处理应遵循“最小必要”原则。简而言之，企业收集和处理个人信息，目的必须明确、合理，且范围严格限定在实现该目的所必需的最小限度内，不得进行与处理目的无关的个人信息收集。

具体操作上，企业需要针对其产品或服务的核心功能，逐项审慎评估个人信息收集的必要性。对此，可参考《常见类型移动互联网应用程序必要个人信息范围规定》等指引性文件，这些文件为不同类型 APP 的基本功能及其对应的必要个人信息范围提供了参照。例如，即时通信类 APP 的核心功能是“提供文字、图片、语音、视频等网络即时通信服务”，其必要个人信息仅包括注册用户的手机号和账号信息(含联系人列表)。在产品设计和功能开发阶段，企业必须将“最小必要”原则作为前置合规审查的关键环节，否则将面临监管处罚风险。

(三) 第三方数据交互

商业活动中，企业与第三方的数据交互(如委托处理、对外提供、转让等)涉及复杂的法律关系和严格的合规义务。

《个人信息保护法》规定，企业委托第三方处理个人信息的，双方应明确约定处理目的、期限、方式、信息种类、保护措施及各自的权利义务，并对受托方的处理活动进行监督。若向其他个人信息处理者提供其处理的个人信息，企业则需向个人告知接收方的具体信息(名称/姓名、联系方式、处理目的、处理方式和个人信息种类)，并取得个人的单独同意。

实践中，未能准确区分“委托处理”与“对外提供”，是企业常见的违法雷区。例如，若企业将用户数据提供给第三方后，接收方对数据拥有独立控制权或使用目的，这通常构成“对外提供”。此时，企业必须就此行为获取用户的明确单独同意，仅仅在隐私政策中概括提及则可能违反《个人信息保护法》等法规。

(四) 未成年人个人信息保护

《个人信息保护法》对不满十四周岁的未成年人(下称“儿童”)的个人信息，设定了更为严格的特殊保护标准。

企业必须制定专门的儿童个人信息保护规则，详细说明收集、使用、存储、共享、转让、披露儿童个人信息的目的、方式、范围、期限以及相应的安全保障措施。在处理任何儿童个人信息前，企业必须依法获得其父母或其他监护人的明确同意。

(五) 合规审计

《个人信息保护法》第六十四条明确规定了个人信息处理者的定期合规审计义务。根据《个人信息保护合规审计管理办法》，处理千万级别以上用户个人信息的企业需每两年进行一次审计，其他类型企业亦需定期开展；而《未成年人网络保护条例》则要求以未成年人为主要服务对象的企业每年进行审计。

合规审计旨在全面、客观地评估企业个人信息保护措施的合规性与有效性，及时发现并修正潜在法律风险。这不仅是履行法定义务，更是企业在境外上市过程中向境内数据监管机关、境内外证券监管部门证明其持续履行个人信息数据保护责任的关键一环。

二. APP 合规

APP 作为企业与用户互动的主要窗口，往往是监管执法的重点关注对象，也是对于依赖 APP 开展日常经营的企业申请境外上市时证券监管部门的关注重点。

(一) APP 备案

根据工信部发布的《工业和信息化部关于开展移动互联网应用程序备案工作的通知》等相关规定，自 2023 年 9 月起，在中国境内通过应用商店分发、小程序、快应用等任何形式向公众提供互联网信息服务的 APP，其运营者都必须依法履行备案手续。未按要求备案的 APP，将面临网络接入受限、应用商店下架等法律后果，严重影响其服务的持续性。

特别值得注意的是，对于从事新闻信息、网络出版、网络文化(如游戏、直播、音乐)、网络音视频、在线教育、互联网医疗等特定服务的 APP，在进行备案前，必须首先取得相关行业主管部门核发的许可证或批准文件，如《互联网新闻信息服务许可证》、《网络出版服务许可证》等。

(二) APP 场景下个人信息保护的精细化要求

APP 是个人信息收集与处理最为集中的场景，因而成为个人信息保护法规执法的重点监控区。针对 APP 个人信息收集中常见的强制索取权限、超范围收集、默认勾选、诱导提供非必要信息及未成年人保护不足等问题，国家网信办、工信部、公安部、市场监管总局等多部门已联合或单独出台系列规范，如《App 违法违规收集使用个人信息行为认定方法》和《常见类型移动互联网应用程序必要个人信息范围规定》，对 APP 个人信息保护提出了具体而严格的要求。企业需逐条对照，确保在每一个细节上都符合规定。

三. 数据治理内控体系建设

构建一套设计科学、执行严格且持续优化的数据治理内控体系，是企业全面履行《网络安全法》、《数据安全法》及《个人信息保护法》等法律法规所规定的数据安全与个人信息保护义务的保障；境内外证券监管部门也会在企业申请境外上市过程中，重点审查企业是否建立完善的数据合规相关内控制度。这些内控体系建设通常需要包括以下方面:

(一) 完善组织架构与制度建设

1. 组织架构层面

数据治理的法律责任最终需落实到具体组织和人员。企业应建立由高管层直接领导的数据安全与个人信息保护决策监督机构(如数据合规委员会)，负责制定并批准企业整体数据合规战略和重大政策，确保资源投入与组织保障，并对整体合规状况负最终领导责任。

在此之下，要明确界定法务、合规、IT、业务、内审、人力资源等各部门在数据治理中的具体职责和协作流程。例如，法务合规部负责法规解读、政策制定与更新、主导个人信息保护影响评估；IT 部门负责技术防护与安全监控；业务部门则需在具体业务场景中严格执行合规政策。

对于数据处理规模庞大、业务风险较高的企业，可考虑设立数据保护官(DPO)或组建独立的数据合规团队，专职负责日常合规监督、政策落地、内部培训、用户请求响应、影响评估组织及监管沟通。

2. 制度建设层面

完备的内部制度是确保数据处理活动符合法律规定的基础。企业需要依据《网络安全法》、《数据安全法》、《个人信息保护法》及其配套的法规、部门规章、国家标准(如 GB/T 35273《信息安全技术个人信息安全规范》等)，并结合自身业务活动和数据处理的实际情况，建立、实施一套全面、系统且具有可操作性的覆盖全生命周期的内部管理制度和标准操作程序。同时，通过培训、考核等方式，确保全体相关员工知晓、理解并严格执行这些制度，将抽象的法律要求转化为具体的日常工作指引，并辅以监督和问责机制。

相关制度至少应包括但不限于:

1) 《数据安全管理总章程/政策》：纲领性文件，明确合规承诺、目标、原则与核心要求。
2) 《数据分类分级管理规范与实施细则》：明确数据分类(如个人信息、重要数据、核心数据)与分级(如敏感、秘密级)标准、流程，并据此实施差异化保护。

3) 《个人信息保护影响评估(PIA)管理办法与操作流程》：规范 PIA 的触发条件、评估内容、方法、风险判定、处置措施及报告要求。
4) 《数据安全事件应急响应预案与演练制度》：明确事件定义、分级、报告流程、应急处置、调查问责及事后改进，并定期演练。
5) 《第三方(供应商、合作伙伴)数据安全管理规定》：规范对第三方的尽职调查、合同约定(含数据保护责任、保密、审计、违约责任)及持续监督评估。

(二) 实施全流程技术防护措施

《网络安全法》、《数据安全法》、《个人信息保护法》均明确要求数据处理者采取必要的技术措施，保障所处理个人信息和数据的安全。企业应在数据获取、内部流转、对外传输、存储、使用、加工直至销毁的各个环节，综合运用多种技术手段，部署与数据规模、敏感度及风险等级相匹配的技术保障措施，构建多层次、多维度的纵深防御体系。

(三) 通过评估与审计实现动态合规

数据合规并非一劳永逸，而是需根据法律法规变化和业务发展，进行持续监控、评估与动态改进的长期过程。企业必须建立常态化的内外部评估与审计机制，确保数据治理体系能持续有效履行法定义务，并及时适应新的合规挑战。

四. 寻求监管与第三方“背书”

境外上市过程中，企业在构建内部数据合规体系、努力满足法律要求的基础上，若能进一步主动与监管部门沟通获取指导，并借助权威第三方机构的评估认证来客观展现合规水平，将极大增强其在境外上市时向交易所和证券监管机构证明自身数据处理活动合法合规的说服力。

(一) 主动与监管部门沟通，以获取对其合规理解的确认和指导

企业应根据自身业务性质、数据处理特点(如是否涉及大量敏感信息、跨境传输、特定行业等)及行业特殊监管要求，主动识别并与具有管辖权或重大影响力的各级监管部门进行必要沟通。这些部门可能包括但不限于：国家和地方网信部门、工业和信息化主管部门、公安机关(特别是网络安全保卫部门)、相关行业的特定监管机构(例如人民银行、卫健委、测绘局等)。

与监管部门建立并维持专业的沟通，有助于企业更准确地把握法律底线，降低因对法律理解偏差而导致的合规风险。对于某些原则性规定或存在解释空间的关键合规事项，可在审慎评估后，尝试通过正式咨询、会谈纪要等方式，就具体法律要求的满足情况(如某项数据出境活动的合法性)请求指导意见或确认(尽管监管机构对出具普适性“合规证明”通常持谨慎态度)。

(二) 借助第三方专业机构的评估与认证，提供中立客观的合规佐证

聘请在数据安全与个人信息保护领域享有良好声誉的第三方机构(如国家认可的信息安全测评机构)，对企业数据安全管理体系、个人信息保护措施的合法性与执行有效性、APP 隐私合规等进行独立客观的评估、检测或审计，是向境外监管机构和资本市场证明企业自身数据合规的有效途径。

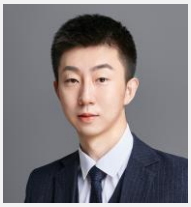
此外，如果企业能够积极获取并维持一些国际上广泛认可的数据保护相关认证(如 ISO/IEC 27001 信息安全管理体系、ISO/IEC 27701 隐私信息管理体系、DSMM 等)，也能在一定程度上证明企业在数据保护管理上的成熟度和持续投入。其他如针对云服务商的 SOC 2 审计报告(尤其关注安全、保密和隐私目标的 Type II 报告)、支付卡行业数据安全标准(PCI DSS)认证(若涉及处理支付卡信息)等，可根据业务适用性和拟上市地监管需要酌情申请认证取得。

结语

对计划申请境外上市的境内企业而言，数据合规已非可有可无的选项，而是贯穿上市申请、审核、发行及上市后持续信披与运营全过程的硬性法律要求。因此，企业应将数据合规深度融入公司治理与日常运营，通过持续强化内控与必要的外部验证，全面履行各项法定数据保护义务，为境外上市及长远发展奠定坚实的法律基石。

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	北京	深圳
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	伦敦	
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	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