

公司上市与数据合规(下篇)

作者：潘永建 | 邓梓珊 | 胡鑫超

近年来,中国逐步公布若干新法律、法规、规范性文件和司法解释,对网络安全、数据保护的范围和力度逐步增强。根据公开资料统计,2020 年共有至少 32 家拟上市企业在上市过程中收到监管机构有关网络安全与数据合规方面的问询,可见在融资场景下企业的网络安全与数据合规情况也日益受到监管部门的重点关注。

企业在网安数据领域的违法违规可能招致“能力罚”,即不仅仅是罚款的事情,而事关企业可否继续经营。兹事体大,融资企业和投资人应当充分关注。

我们检索了 2020 年与网安数据合规相关的行政处罚决定书、上市公司招股书、法律意见书、问询函,《上篇》已经从“上市前”“上市后”两个时间段,并从“执法部门关注重点”“监管机构关注重点及发行人如何答复”两个角度为您罗列了与上市企业相关的网安数据合规问题。在本《下篇》中,我们为您总结不同行业的拟上市企业可能面临的网安数据合规问题类型及相关法律依据。

一. 政策变化

典型问题:

- 请发行人说明:《个人信息安全规范》《数据安全法》(草案)等法规的出台对发行人业务的具体影响,发行人及其原料数据采集供应商是否存在违反上述规定的情形,请发行人就相关监管政策出台对行业可能产生的影响进行重大事项提示和风险揭示。
- 请发行人说明:充分说明日益加强的数据行业监管及个人隐私保护政策,包括但不限于《个人信息安全规范(征求意见稿)》主要变化、《网络生态治理规定(征求意见稿)》等对发行人业务的潜在影响及相关应对措施,并进行重大事项提示。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

该问题聚焦于网安数据政策变化、行业监管规定对于发行人业务持续性的影响，属于监管机构较为关注的问题。该问题常见于大数据分析行业以及重度依赖用户数据的企业。

二. 网络与信息系统安全

典型问题:

- 发行人是否需要已开展网络安全等级保护等安全保护措施，是否需要测评?¹
- 发行人主营产品是否需要取得中国网络安全审查技术与认证中心出具的认证证书?
- 发行人主营产品安全技术的具体情况，防范交易外挂、黑客攻击等的具体措施及实际效果，是否达到与行业平均技术水平?²
- 发行人是否出现过安全事件(类型、原因、发生概率统计)，是否存在纠纷或潜在纠纷；是否受到主管部门调查(调查内容、原因、结果)；相比同行业遇到的网络攻击频率和影响，发行人产品在抗击网络攻击方面是否存在更大风险?²
- 发行人与客户的服务协议中对于潜在安全泄露的责任约定与免责条款?
- 发行人若发生安全事故，应承担何种具体责任(法定+合同约定)，表现方式及对生产经营的影响，有针对性地揭示可能存在的风险。
- 发行人主营产品，在使用过程中是否出现了存在外挂程序、被黑客攻击、软件漏洞、设备故障等安全问题(具体过程、解决方法、对产品的影响、目前解决情况、后期应对措施)?

¹ 与等保相关的问题属于监管机构较为关注的问题，常见于金融、物联网、大数据分析行业。

² 该类问题聚焦于产品/服务的安全性能以及发行人就客户网络安全所采取的技术措施及实施效果，属于监管机构较为关注的问题，常见于通信、支付、云计算行业。

主要法律依据与违法后果

- 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。(《网络安全法》第 25 条)
- 关键信息基础设施运营者未按要求制定网络安全事件应急预案的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。(《网络安全法》第 59 条)
- 未实现网络安全等级保护制度，采取安全技术措施的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。(《网络安全法》第 59 条)
- 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。(《网络安全法》第 23 条)
- 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。(《网络安全法》第 71 条)

三. 数据内控体系

典型问题:

- 发行人是否就业务所涉及的个人隐私信息、数据等建立了完整的制度有效确保系那个管信息的合规使用(数据备份机制、防范数据窃取及泄露的措施、对用户隐私数据加密措施以及对于到期数据的处理机制等)?¹
- 发行人信息安全系统是否安全稳定可靠,中介机构是否对发行人进行IT审计?
- 发行人是否建立了相关制度保证原始数据的准确性、及时性、不可修改性及成本核算的有效性、准确性?²
- 请发行人说明从电商平台通过函证获取的发行人相关财务与业务数据的具体方法和内容,是否存在数据受限的情形,是否可以从其他渠道验证相关数据的真实性、有效性,从而保证披露数据真实、准确、完整?
- 发行人数据获取、使用、处理等内部控制制度及执行情况。¹
- 发行人是否建立完善的防泄漏和保障网络安全的内部管理制度(特别是行业内常见的攻击手段,例如第三方支付中的“隔空盗刷行为”);制度是否有效(是否符合《网络安全法》规定)?¹
- 发行人是否发生过数据泄露事件(类型、原因、发生概率统计),是否存在纠纷或潜在纠纷?³

¹ 数据内控制度是否有效完备,属于监管机构重点关注的问题,各行各业均有涉猎,应引起拟上市企业的重点关注。

² 该问题涉及到数据的基本三性,属于监管机构较为关注的问题,主要见于通信行业与金融行业。金融行业参照相关国标,落实数据安全管理制度。

³ 该问题属于监管机构较为关注的问题。该问题常见于大数据分析行业以及重度依赖用户数据的企业。

主要法律依据与违法后果

- 未制定内部安全管理制度和操作规程,确定网络安全负责人,未制定网络安全事件应急预案,未采取数据分类、重要数据备份和加密等措施,由有关主管部门责令改正,给予警告;拒不改正或者导致危害网络安全等后果的,处一万元以上十万元以下罚款,对直接负责的主管人员处五千元以上五万元以下罚款。(《网络安全法》第59条)
- 有本法规定的违法行为的,依照有关法律、行政法规的规定记入信用档案,并予以公示。(《网络安全法》第71条)
- 开展数据活动应当依照法律、行政法规的规定和国家标准的强制性要求,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。重要数据的处理者应当设立数据安全负责人和管理机构,落实数据安全保护责任。(《数据安全法(草案)》第25条)
- 开展数据活动的组织、个人不履行本法第二十五条、第二十七条、第二十八条、第二十九条规定的数据安全保护义务或者未采取必要的安全措施的,由有关主管部门责令改正,给予警告,

可以并处一万元以上十万元以下罚款，对直接负责的主管人员可以处五千元以上五万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。（《数据安全法(草案)》第42条）

四. 数据来源及大数据应用

典型问题:

- 发行人开展业务所需数据主要来源(分类)、规模、所有权归属、数据内容或者标签、数据存储方式及管理、数据分析功能实现路径、数据获取方式是否属于行业惯例?¹
- 针对不同的数据来源，发行人收集收据、采购数据时，是否均取得了信息主体明确的授权或许可文件？
- 发行人开展业务所获取的数据的合法性，是否侵犯了第三方的合法权益，是否存在违法情形？
- (券商)发行人开展业务所需数据是否存在侵权及欺诈等损害客户利益的情况，有无潜在纠纷？
- 发行人开展业务所需数据是否采用现金购买、购买成本占比?²
- 发行人开展业务过程中是否获取或有可能获取国家秘密、保密信息、个人信息；是否存在泄露的情况？
- 发行人可以基于用户画像和行为分析实现推荐，依据用户不同的标签组合出不同的应用场景，实现资讯和广告内容的精准推荐和个性化营销服务。请发行人说明数据的形成过程，使用权限及其合法合规性；以及报告期各期发行人大数据团队的研发费用投入、研发项目、研发成果、员工人数、薪酬水平及合理性。³
- 针对爬虫技术：根据申请文件，发行人储备技术及在研项目中，存在利用爬虫技术对第三方网站、新媒体平台等进行数据爬取，且通过相关技术可以突破第三方网站、新媒体平台等对爬虫功能的限制和封锁。请发行人代表说明：(1)发行人是否存在未经许可突破第三方平台协议或限制搜集第三方平台数据的情况；(2)上述业务和技术是否涉嫌构成《反不正当竞争法》《网安法》《计算机信息安全保护条例》及《刑法》所规定的不正当竞争、非法侵入网络、危害计算机信息系统安全，非法获取计算机信息系统数据，是否存在侵犯第三方知识产权、商业秘密等风险。

¹ 该问题聚焦于数据来源、数据应用的整体合法性问题，属于监管机构重点关注的问题，各行各业均有涉猎，应引起拟上市企业的重点关注。

² 该问题主要关注从数据供应商获取数据的合法合规性，属于监管机构较为关注的问题，常见于需要大量行业资讯用于自身决策制定或提供资讯服务的企业。

³ 使用大数据生成用户画像、用于日常经营与商业决策已成为数字时代的经营常态，大数据甚至已经成为产品。该问题属于监管机构较为关注的问题，常见于大数据分析传媒行业。

主要法律依据与违法后果

- 数据获取和使用侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处

一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。（《网络安全法》第 64 条）

- 数据获取可能构成对第三人著作权和商业秘密的侵犯。侵犯商业秘密，由监督检查部门责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处五十万元以上五百万元以下的罚款。给商业秘密的权利人造成重大损失的，需承担相应的刑事责任。（《反不正当竞争法》第 21 条）
- 禁止非法复制、记录、存储国家秘密。禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密。禁止在私人交往和通信中涉及国家秘密。（《保守国家秘密法》第 26 条）
- 非法获取、持有国家秘密载体的；非法复制、记录、存储国家秘密的；在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的；将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的；在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的，依法给予处分；构成犯罪的，依法追究刑事责任。（《保守国家秘密法》第 48 条）
- 侵犯著作权或者与著作权有关的权利的，侵权人应当按照权利人的实际损失给予赔偿；实际损失难以计算的，可以按照侵权人的违法所得给予赔偿。赔偿数额还应当包括权利人为制止侵权行为所支付的合理开支。权利人的实际损失或者侵权人的违法所得不能确定的，由人民法院根据侵权行为的情节，判决给予五十万元以下的赔偿。（《著作权法》第 49 条）
- 侵犯商业秘密，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金。（《刑法》第 219 条）
- 经营者以及其他自然人、法人和非法人组织侵犯商业秘密的，由监督检查部门责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处五十万元以上五百万元以下的罚款。（《反不正当竞争法》第 21 条）
- 网络运营者、网络产品或者服务的提供者侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。（《网络安全法》第 64 条）
- 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年

以上七年以下有期徒刑，并处罚金。单位犯前罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。（《刑法》第 285 条）

五. 业务直接涉及个人信息的合规问题

典型问题:

- 发行人具体哪些业务需要使用客户数据或个人信息?¹
- 请发行人结合过往的纠纷，说明个人信息收集、使用是否存在侵犯第三方合法权益的情形(客户、客户的用户、APP 具体使用者、其他第三方的商业秘密及个人隐私)，是否有潜在纠纷。¹
- 发行人获取个人信息授权过程是否完备，是否明确告知收集信息的范围和用途，是否符合法律规定?²
- 请发行人说明获取用户数据及标签的过程、手段及方式，是否对用户有明示提示，是否合法合规。开展业务中使用个人信息是否存在不符合《信息安全技术 个人信息安全规范》的情况，如存在，请说明发行人内部的整改及规范情况。²
- 发行人所运营的 APP 是否曾受 APP 专项治理工作组点名?目前已曝光违法违规收集使用个人信息的 APP 是否涉及发行人及其客户?如是，请说明整改情况，是否获得认可，是否有被罚风险。
- 发行人员工是否曾涉及侵犯公民个人信息犯罪，该犯罪行为是否涉及发行人;该员工是否利用发行人设备、数据、软件等进行上述犯罪行为;结合上述违法、犯罪行为，说明公司的内控制度是否有效，发行人是否有相应机制保证展业的合法合规性。
- 发行人使用用户数据手段是否合法合规，尤其是商业化变现的合规性，是否有潜在纠纷?
- 发行人业务模式是否存在协助或变相协助客户侵犯第三方商业秘密或个人信息安全的行为?
- 第三方数据提供商及相关技术人员在发行人开展业务过程中是否会接触、获得、记录、存储及应用个人敏感信息?
- 发行人开展业务所收集的个人信息是否存在转授权或流转给第三方使用的情况?如存在，是否经过了个人信息主体的明示同意，是否经过了充分的脱敏，相关授权流程是否完备;将涉及信息收集的业务外包给第三方，是否具有合规性?
- 发行人所在行业是否允许第三方机构处理相关数据，是否需取得有权主管部门批准?

¹ 该类问题聚焦于开展业务过程中收集使用的个人信息类型、来源合法性、全流程的使用合规，属于监管机构重点关注的问题，各行各业均有涉猎，应引起拟上市企业的重点关注。

² 该类问题聚焦于获取个人信息主体授权过程的合规性，与个人信息来源的合法性有关，属于监管机构较为关注的问题。实践当中，获取个人信息的手段繁多，如通过用户主动填写获取、通过爬虫、接入第三方 SDK 或在应用程序中进行埋点。不同的收集手段所对应的合规风险是不一样的，比如爬虫技术，会涉及到公开个人信息的获取合规问题，用户授权是否充分、是否绕开反爬技术等。此外，我们注意到《信息安全技术 个人信息安全规范》这一推荐性国标作为企业应参照的个人信息保护体系标准被多次提及，足见该国标的重要性。

主要法律依据与违法后果

- 违反个人信息收集与使用的相关规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。（《网络安全法》第 64 条）
- 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。（《网络安全法》第 71 条）
- 信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。（《民法典》第 1038 条）
- 违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。（《个人信息保护法(草案)》第 62 条）
- 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。（《个人信息保护法(草案)》第 63 条）
- 违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。（《刑法》第 253 条之一）

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

北京市建国门北大街 8 号
华润大厦 4 楼
T: +86 10 8519 2266
F: +86 10 8519 2929

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 2021