

北京国枫律师事务所
关于云从科技集团股份有限公司
申请首次公开发行股票并在科创板上市的
补充法律意见书之三

国枫律证字[2020]AN332-54 号



GRANDWAY

北京国枫律师事务所

Grandway Law Offices

北京市东城区建国门内大街 26 号新闻大厦 7 层 邮编：100005
电话 (Tel): 010-88004488/66090088 传真 (Fax): 010-66090016

北京国枫律师事务所
关于云从科技集团股份有限公司
申请首次公开发行股票并在科创板上市的
补充法律意见书之三
国枫律证字[2020]AN332-54号

致：云从科技集团股份有限公司（发行人）

根据本所与重庆云从签订的《律师服务协议》及本所与重庆云从、发行人签订的《三方协议》，本所接受发行人的委托，担任发行人本次发行上市的专项法律顾问。

本所律师已根据《公司法》《证券法》《注册管理办法》《证券法律业务管理办法》《证券法律业务执业规则》等相关法律、法规、规章和规范性文件的规定并按照律师行业公认的业务标准、道德规范和勤勉尽责精神，对发行人提供的文件和有关事实进行了查验，并就发行人本次发行上市事宜出具了《北京国枫律师事务所关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的法律意见书》（以下称“法律意见书”）、《北京国枫律师事务所关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的律师工作报告》（以下称“律师工作报告”），并根据“上证科审（审核）[2020]1072号”《关于云从科技集团股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》（以下称“《第一轮问询函》”）出具了《北京国枫律师事务所关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的法律意见书之一》（以下称“补充法律意见书之一”），根据“上证科审（审核）[2021]176号”《关于云从科技集团股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函》（以下称“《第二轮问询函》”）出具了《北京国枫律师事务所关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的法律意见书

之二》（以下称“补充法律意见书之二”）。

根据“上证科审（审核）[2021]363号”《关于云从科技集团股份有限公司首次公开发行股票并在科创板上市的审核中心意见落实函》（以下称“《落实函》”）及发行人的要求，本所律师在对发行人与本次发行上市相关情况进行进一步查验的基础上，出具本补充法律意见书，对本所律师已经出具的法律意见书、律师工作报告的有关内容进行修改、补充或作进一步的说明。

本所律师同意将本补充法律意见书作为发行人本次发行上市所必备的法定文件随其他材料一起上报，并依法对本补充法律意见书承担相应责任；本补充法律意见书仅供发行人本次发行上市的目的使用，不得用作任何其他用途。

本所律师在法律意见书和律师工作报告中的声明事项亦适用于本补充法律意见书。如无特别说明，本补充法律意见书中有关用语的含义与法律意见书和律师工作报告中相同用语的含义一致。

本所律师根据《公司法》《证券法》《注册管理办法》《证券法律业务管理办法》《证券法律业务执业规则》等相关法律、行政法规、规章及规范性文件的要求和中国证监会、证券交易所的相关规定，并按照律师行业公认的业务标准、道德规范和勤勉尽责精神，现出具补充法律意见如下：

一、《落实函》问题二

请发行人进一步说明：（1）发行人软件产品销售涉及系统升级的相关约定、实际执行情况和会计核算情况；（2）结合应收账款逾期比例较高、坏账计提比例较低等，进一步说明应收账款违约的具体情况；（3）结合境内外法律法规和行业规范，进一步说明公司在保证人工智能技术可控、符合伦理规范的措施和规划，以及对客户隐私数据的保护措施。

请保荐机构核查并发表明确意见，请申报会计师就问题（1）（2）核查并发表明确意见，请发行人律师就问题（3）核查并发表明确意见。

回复：

（一）核查方式和手段

本所律师履行了以下核查程序：

1、查阅了境内外关于人工智能技术可控、伦理规范及隐私数据保护相关的主要法律法规和行业规范；

2、审阅发行人在保障人工智能技术的安全可控以及客户隐私数据安全方面的内部规章制度；

3、审阅发行人数据脱敏流程图、系统日志、软件升级记录；

4、访谈发行人相关技术人员，了解发行人为保障人工智能技术的安全可控、客户个人隐私数据的保护所采取的技术措施；

5、审阅发行人数据安全组织架构图；

6、审阅发行人伦理审查记录；

- 7、审阅发行人与上海市汇业律师事务所签订的律师服务协议；
- 8、审阅发行人员工培训记录；
- 9、审阅发行人员工保密协议及个人信息保护承诺书；
- 10、审阅发行人参与制定的相关标准制度文件；
- 11、审阅发行人环境管理体系认证证书；
- 12、审阅发行人部分业务合同、承诺书。

(二) 核查结论

1. 境内外相关法律法规和行业规范

我国及境外关于人工智能技术可控、伦理规范及隐私数据保护相关的主要法律法规和行业规范如下：

名称	发布主体	主要内容
人工智能伦理风险分析报告	国家人工智能标准化总体组织	<p>人工智能伦理准则：</p> <p>(1) 人类根本利益原则，指人工智能应以实现人类根本利益为终极目标；</p> <p>(2) 责任原则，指在人工智能相关的技术开发和应用两方面都建立明确的责任体系。</p>
新一代人工智能治理原则——发展负责任的人工智能	国家新一代人工智能治理专业委员会	<p>人工智能发展相关各方应遵循以下原则：</p> <p>(1) 和谐友好。人工智能发展应以增进人类共同福祉为目标；应符合人类的价值观和伦理道德，促进人机和谐，服务人类文明进步；应以保障社会安全、尊重人类权益为前提，避免误用，禁止滥用、恶用。</p> <p>(2) 公平公正。人工智能发展应促进公平公正，保障利益相关者的权益，促进机会均等。通过持续提高技术水平、改善管理方式，在数据获取、算法设计、技术开发、产品研发和应用过程中消除偏见和歧视。</p> <p>(3) 包容共享。人工智能应促进绿色发展，符合环境友好、资源节约的要求；应促进协调发展，推动各行各业转型升级，缩小区域差距；应促进包容发展，加强人工智能教育及科普，提升弱势群体适应性，努力消除数字鸿沟；应促进共享发展，避免数据与平台垄断，鼓励开放有序竞争。</p> <p>(4) 尊重隐私。人工智能发展应尊重和保护个人隐私，充分保障个人的知情权和选择权。在个人信息的收集、存储、处理、使用各环节应设置边界，建立规范。完善个人数据授权撤销机制，反对任何窃取、篡改、泄露和其他非法收集利用个人信息的行为。</p>

		<p>(5) 安全可控。人工智能系统应不断提升透明性、可解释性、可靠性、可控性，逐步实现可审核、可监督、可追溯、可信赖。高度关注人工智能系统的安全，提高人工智能鲁棒性及抗干扰性，形成人工智能安全评估和管控能力。</p> <p>(6) 共担责任。人工智能研发者、使用者及其他相关方应具有高度的社会责任感和自律意识，严格遵守法律法规、伦理道德和标准规范。建立人工智能问责机制，明确研发者、使用者和受用者等的责任。人工智能应用过程中应确保人类知情权，告知可能产生的风险和影响。防范利用人工智能进行非法活动。</p> <p>(7) 开放协作。鼓励跨学科、跨领域、跨地区、跨国界的交流合作，推动国际组织、政府部门、科研机构、教育机构、企业、社会组织、公众在人工智能发展与治理中的协调互动。开展国际对话与合作，在充分尊重各国人工智能治理原则和实践的前提下，推动形成具有广泛共识的国际人工智能治理框架和标准规范。</p> <p>(8) 敏捷治理。尊重人工智能发展规律，在推动人工智能创新发展、有序发展的同时，及时发现和解决可能引发的风险。不断提升智能化技术手段，优化管理机制，完善治理体系，推动治理原则贯穿人工智能产品和服务的全生命周期。对未来更高级人工智能的潜在风险持续开展研究和预判，确保人工智能始终朝着有利于人类的方向发展。</p>
<p>网络安全标准实践指南——人工智能伦理安全风险防范指引</p>	<p>全国信息安全标准化技术委员会秘书处</p>	<p>(1) 应符合我国社会价值观，并遵守国家法律法规。</p> <p>(2) 应以推动经济、社会、生态可持续发展为目标，致力于实现和谐友好、公平公正、包容共享、安全可控的人工智能。</p> <p>(3) 应尊重并保护个人基本权利，包括人身、隐私、财产等权利，特别关注保护弱势群体。</p> <p>(4) 应充分认识、全面分析人工智能伦理安全风险，在合理范围内开展相关活动。</p> <p>(5) 研究开发者、设计制造者、部署应用者应积极推动人工智能伦理安全风险治理体系与机制建设，实现开放协作、共担责任、敏捷治理。</p> <p>(6) 研究开发者、设计制造者、部署应用者应积极推动人工智能伦理安全风险以及相关防范措施宣传培训工作。</p> <p>(7) 谨慎开展具备自我复制或自我改进能力的自主性人工智能的研究开发，持续评估可能出现的失控性风险。</p> <p>(8) 应设置事故信息回溯机制和事故应急处置机制，包括人工紧急干预机制、中止应用机制等，明确事故处理流程，确保在人工智能伦理安全风</p>

		<p>险发生时作出及时响应。</p> <p>(9) 使用人工智能作为直接决策依据并影响个人权利时，应具有清晰、明确、可查的法律法规等依据。</p> <p>(10) 应向用户说明人工智能相关系统、产品或服务的功能、局限、风险以及可能的影响，解释相关应用过程及应用结果。</p>
中华人民共和国民法典	全国人民代表大会	<p>(1) 个人信息基本原则：自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。</p> <p>(2) 个人信息处理过程中的原则：处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理。</p> <p>(3) 不得泄露、篡改原则：信息处理者不得泄露、篡改、向他人非法提供个人信息，并应当采取必要措施确保个人信息安全，防止信息泄露、篡改、丢失。</p> <p>(4) 个人隐私保护的基本原则：自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。</p>
中华人民共和国网络安全法	全国人民代表大会常务委员会	<p>(1) 保密原则：网络运营者应当对其收集的用户信息严格保密，并建立保护制度。</p> <p>(2) 收集和存储：网络运营者应当以合法、正当、必要为原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得收集与其提供的服务无关的个人信息，应当遵守法律规定和约定处理其保存的个人信息。</p> <p>(3) 不得泄露、篡改原则：网络运营者不得泄露、篡改、毁损其收集的个人信息，未经同意不得向他人提供个人信息，并应当采取必要措施确保个人信息安全。</p> <p>(4) 不得非法出售或提供个人信息。</p>
信息安全技术 个人信息安全规范	国家市场监督管理总局 国家标准化管理委员会	<p>(1) 个人信息控制者作为有能力决定个人信息处理目的、方式等的组织和个人，在个人信息收集、存储、使用、共享、转让、公开披露及删除数据全生命周期应当遵守的原则和承担主要的信息保护义务。</p> <p>(2) 个人信息的受托处理者应当按照个人信息控制者的要求处理个人信息，并应履行协助个人信息控制者响应个人信息主体权利请求。</p> <p>(3) 个人信息的受托处理者在委托关系解除时不再存储相关个人信息等</p>

		义务。
中华人民共和国数据安全法（尚未施行，自 2021 年 9 月 1 日起施行）	全国人民代表大会常务委 员 会	<p>(1) 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。</p> <p>(2) 开展数据处理活动应当依照法律、法规的规定，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。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。</p> <p>(3) 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。</p> <p>(4) 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。</p> <p>(5) 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。</p> <p>(6) 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。</p>
北京共识——人工智能与教育	联合国教育、科学及文化组织	<p>(1) 人工智能的开发应当为人所控、以人为本；</p> <p>(2) 人工智能的部署应当服务于人并以增强人的能力为目的；</p> <p>(3) 人工智能的设计应合乎伦理、避免歧视、公平、透明和可审核；</p> <p>(4) 应在整个价值链全过程中监测并评估人工智能对人和社会的影响。</p>
可信赖人工智能伦理准则 (Ethics guidelines for trustworthy AI)	欧洲联盟	<p>(1) 人工智能技术须符合法律规定。</p> <p>(2) 人工智能技术须满足伦理道德原则及价值。</p> <p>(3) 人工智能在技术和社会层面应具有可靠性。</p> <p>(4) 可信赖人工智能应满足以下要求：保障人的能动性和监督能力、安全性、隐私数据管理、透明度、包容性、社会福祉、问责机制，以确保人工智能足够安全可靠。</p>

人工智能准则（AI PRINCIPLES）	美国国防创新委员会	<p>人工智能伦理准则包括：</p> <p>(1) 负责任；</p> <p>(2) 公平公正；</p> <p>(3) 可溯源；</p> <p>(4) 可信赖；</p> <p>(5) 可控。</p>
以人为本的人工智能社会原则（Social Principles of Human-Centric AI）	日本以人为本的人工智能社会原则委员会	<p>人工智能应当以下社会原则：</p> <p>(1) 以人为本；</p> <p>(2) 教育/扫盲原则；</p> <p>(3) 隐私保护原则；</p> <p>(4) 确保安全原则；</p> <p>(5) 公平竞争原则；</p> <p>(6) 公平、问责制和透明度原则；</p> <p>(7) 创新原则。</p>

2.发行人在保障人工智能技术可控方面的措施

发行人在人工智能技术可控方面，主要从制度层面、技术层面和内控机制进行保障，加强人工智能技术的安全性、可控性。

（1）制度层面

根据发行人提供的内部制度文件，为确保公司人工智能技术的安全可控，公司制定了一系列内部规章制度，以从制度层面保障公司人工智能技术的安全可控，具体如下：

制度名称	具体措施
网络安全保护总则	<p>①确立发行人网络安全的总体要求；</p> <p>②设立网络安全专门部门和岗位；</p> <p>③设置专项网络安全预算；</p> <p>④支持创新网络安全管理方式，促进网络新技术开发，推动公司网络技术创新，提高网络安全保护水平；</p> <p>⑤制定员工个人信息安全培训规范；</p> <p>⑥对拟运营的网络产品、服务设置安全性、合规性审查机制；</p> <p>⑦技术支撑部门等应采取防范、保护网络安全的技术措施，保障公司网络运行的物理和环境安全；</p>

	<p>⑧建立并不断完善网络设备管理制度，明确设备配备、领用、使用、变更等行为准则；</p> <p>⑨制定网络与信息安全应急预案、并采取应急演练等措施，监测、防御、处置来源于公司内外的网络安全和威胁；</p> <p>⑩建立并不断完善用户权利响应机制。</p>
信息安全奖惩管理办法	<p>①明确信息安全奖惩与违规行为处罚的操作原则；</p> <p>②明确奖励和处罚等级和措施。</p>
网络与信息安全应急预案	<p>①建立信息安全应急处理机制；</p> <p>②明确信息安全事件类型和等级；</p> <p>③建立应急组织架构并明确工作职责；</p> <p>④明确应急处置措施和程序。</p>

除上述制度规范外，发行人还制定了《机房安全管理制度》《备份与恢复管理办法》《恶意代码防范管理制度》《信息安全红线管理规定》《信息安全漏洞管理办法》《账号与口令管理办法》《云从科技三方开源软件管理办法》《云从科技技术研发流程管理办法》《数据分类识别规范》《个人信息安全影响自评估规范》《对外数据安全管理制度》《对内数据安全管理制度》《用户个人信息权利保障制度》等制度，保障发行人人工智能技术的安全可控。

(2) 技术层面

根据发行人提供的数据脱敏流程图、系统日志、软件升级记录并经访谈发行人相关技术人员，发行人为保障人工智能技术的安全可控，从技术层面针对数据、算法、网络平台和产品四个维度提供安全支持，具体采取了以下措施：

类别	具体措施
数据安全	<p>①采用数据脱敏与数据隐私计算技术确保数据的敏感标签从采集时及进行分离；</p> <p>②采用数据数字水印技术对数据使用的全流程进行全过程可追踪溯源；</p> <p>③采用数据的分级分类严格规范数据的使用授权与使用范围；</p> <p>④采用数据安全等级评测技术，确定数据的存储与使用环境的网络与存储安全；</p>
算法安全	<p>①采用底层代码自动化编译技术，实现算法的完全自主性，保障算法的安全可靠；</p> <p>②采用多层异构神经网络，确保算法的鲁棒性与可泛化性增强，实现技</p>

	<p>术的不同场景使用可控性安全；</p> <p>③采用产品系统多级日志与痕迹留存，实现算法的运行有记录可追溯，实现技术的运行可监控，可控制；</p>
平台与网络安全	<p>①采用边界防护技术，建立了网络安全纵深防御体系，生产网络与开发测试网络物理隔离。其中生产网络依据不同业务划分不同区域，不同区域间根据“最小”、“必须”的原则，通过防火墙进行访问控制实现逻辑安全隔离；</p> <p>②采用定期的漏洞扫描和安全评估机制，及时升级数据库和应用软件安全补丁，保障第三方开源软件使用安全。建立了常态化的渗透测试机制，重要信息系统在上线前必须通过安全评估后，才可上线；</p> <p>③采用 IDS、IPS、WAF、堡垒机、日志审计服务器等各项安全产品设备，实现了对网络安全攻击的实时检测和及时阻断及告警，提升网络安全应急响应水平；</p>
产品与业务安全	<p>①采用端侧产品数据不可逆加密技术，从数据获取源头实现对数据的脱敏与加密传输；</p> <p>②采用代码加壳编译技术，确保产品与算法不可被破解从而进行恶意攻击与使用；</p> <p>③采用产品终端监控与审计机制，对生产过程文件等行为进行管控与审计，并定期进行病毒查杀及补丁升级，且通过域控实现办公系统的统一认证，杜绝弱口令，有效提升产品生产环境的安全性。</p>

(3) 内控机制

根据发行人提供的数据安全组织架构图，发行人感知研究院和数据研究院作为公司的技术研发机构，在技术的研发以及管理过程中始终贯彻技术安全可控的宗旨，此外发行人还建立了信息安全委员会，对公司的技术和产品的研发进行安全、可追溯、可追责等法律、伦理方面的审查和监督，信息安全委员会与感知研究院、数据研究院一起构成了发行人人工智能技术安全可控的内部决策机构。

根据发行人提供的数据安全制度文件并经访谈发行人相关负责人，信息安全委员会作为网络安全和个人信息保护的最高决策机构，负责统筹、部署和决策网络安全和个人信息保护以及人工智能技术可控相关的管理、监督等工作。信息安全委员会下设信息安全工作小组和法务部，其中信息安全工作小组负责具体执行信息安全委员会决议，并负责在职权范围内监督和审批公司个人信息流动、人工

智能技术可控性管理相关业务等日常工作，法务部在信息安全工作小组的领导下执行具体的工作并共同保障公司人工智能技术安全可控。

3.发行人在保证人工智能技术符合伦理规范方面的措施

人工智能技术的复杂性决定了其会涉及法律、伦理、道德等多方面的问题，发行人高度认同人工智能伦理规范对于人工智能技术发展的重要性，坚持和谐友好、公平公正、包容共享、尊重隐私、安全可控、共担责任、开放协作、敏捷治理的价值取向，并以此作为人工智能技术发展的基本原则，提倡“以人为本”，倡导“多样化、公平化、透明化”的人工智能技术，并以“定义智能生活、提升人类潜能”作为公司使命。为实现这一目标，发行人在公司内部和外部均建立了伦理审查机制，并积极加强员工在人工智能伦理方面的培训和管理，并在开放协作、绿色环保等方面积极落实人工智能伦理准则的要求。

(1) 建立伦理审查机制

根据发行人提供的数据安全组织架构图并经访谈发行人相关负责人，发行人严格遵循人工智能发展的基本原则，建立了信息安全委员会、信息安全小组、法务部三层组织架构，与感知研究院、数据研究院共同组成了伦理审查机制。

根据发行人提供的伦理审查记录，发行人在技术、产品的研发立项、测试、验收以及应用等环节进行相应的伦理审查，包括但不限于：是否符合社会主义核心价值观，是否有利于推动经济、社会、生态的可持续性发展，是否有利于提升社会价值，是否充分尊重个人权利、保护个人隐私、关注弱势群体，是否满足数据安全、技术安全可控等，并对于审查中发现的问题及时进行整改、完善。例如：在项目立项阶段，会就产品全生命周期中或技术解决方案实施和使用过程中的伦理风险进行梳理、研究并制定相应的管控方案；在产品设计及使用优化阶段，充分评估审查产品设计应用的伦理风险（如歧视、偏见等）；在业务阶段，会要求客户保护用户权利、尊重用户隐私并保障用户数据不泄露。

根据发行人提供的律师服务协议，发行人不仅在公司内部建立了伦理审查机制，还聘请了上海市汇业律师事务所作为发行人人工智能伦理外部专家顾问，为发行人在遵守人工智能伦理规范方面提供合规建议和指导。

（2）员工培训与管理

根据发行人提供的员工培训记录、部分员工保密协议及个人信息保护承诺书，发行人定期对员工进行数据安全和个人隐私保护等相关人工智能伦理相关的培训，此外公司要求员工签署保密协议，重点岗位员工还会要求签署重要数据及个人信息保护承诺书，以便提升员工的数据合规意识以及社会责任感。

（3）发行人在开放协作、绿色环保等方面积极落实人工智能伦理准则的要求

根据发行人提供的相关标准制度文件并经访谈发行人相关技术负责人，报告期内，发行人高度重视开放协作的精神，一方面，积极参与国家层面的人工智能相关政策研究，并受邀参与了人工智能国家标准、公安部行业标准等 30 项国家和行业标准制定工作，为人工智能治理原则中的安全可控、多样性、公平性、包容性、可追踪等提供行业标准；另一方面，发行人与多个高校和研究机构进行了人工智能技术的前沿算法学术交流与分享活动，确保算法始终保持非歧视及公平性，实现技术的安全可控，符合人工智能治理原则中包容共享、共担责任、开放协作的具体要求。

根据发行人提供的环境管理体系认证证书，发行人积极倡导绿色环保的发展理念，并取得了符合“GB/T24001-2016/ISO14001:2015”标准的环境管理体系认证，符合人工智能治理原则中绿色友好的具体要求。

4.发行人在保护客户隐私数据方面的措施

发行人在客户隐私数据方面，主要从制度层面、技术层面和执行管理层面进行保障，加强对客户隐私数据的保护。

（1）制度层面

根据发行人提供的内部制度文件，针对在业务过程中获取的个人信息，发行人制定了《网络安全保护总则》，从原则上建立了个人信息保护的统领性制度，同时，发行人制定了《数据分类识别规范》《个人信息安全影响自评估规范》《对外数据安全管理制度》《对内数据安全管理制度》《用户个人信息权利保障制度》

等制度，从个人信息的分类识别、安全评估、权利保障、信息的收集、存储和处理等方面全面保障客户隐私数据的安全，具体如下：

制度名称	具体措施
数据分类识别规范	根据《信息安全技术 个人信息安全规范》对个人信息及数据按照敏感性程度和数量级两个维度确立分级保护机制。
个人信息安全影响自评规范	①针对不同场景建立个人信息安全影响自我评估机制； ②确立一般审查程序和特别审查程序，并根据审查程序的不同，采取不同的审查方式。
对外数据安全管理制度	①建立间接收集个人信息安全管理规范，明确个人信息间接获取的各项操作与审批流程； ②建立对外提供个人信息安全管理规范，明确对外提供个人信息（包括委托处理/共享/转让的情形）的各项操作与审批流程； ③建立个人信息公开披露处理规范，明确发行人个人信息公开披露流程； ④建立外部人员访问管理规范，明确外部人员访问发行人物流环境或通过网络通道进行访问的流程和注意事项； ⑤建立个人信息跨境传输规范，明确个人信息跨境传输的禁止情形和安全评估要求； ⑥建立政府数据协助管理规范，明确发行人向政府机关提供数据信息的范围及流程等相关事宜。
对内数据安全管理制度	①建立数据存储规范，明确对个人信息的分类存储、分级保护、加密措施； ②建立内部访问控制规范，明确内部个人信息访问的原则和控制措施； ③建立个人信息删除、账户注销操作规范，明确用户个人信息删除、账户注销操作流程； ④建立停止运营之个人信息处理规范，明确发行人产品或服务停止运营前后的个人信息处理流程。
用户个人信息权利保障制度	建立隐私政策的制定、发布、实施流程，并明确发行人用户权利申诉事件的响应处理程序。

（2）技术层面

经访谈发行人相关技术负责人，发行人对客户隐私数据进行全生命周期保护，包括数据采集、数据传输、数据存储、数据使用、数据销毁五个方面，在数

据生命周期中的每个环节均提供相应的安全技术保障措施，确保数据安全：

①数据采集方面，数据采集设备端采用数据特征降维技术，且采集系统获取的数据标签（个人信息）与数据主体采取分离式生成，分开加密，分开传输，采集系统本身具备权限体系与日志审查功能，可以确保采集人员的操作权限与数据采集的所有操作具备可追溯性；

②数据传输方面，数据通过加密，完成安全通信传输，且系统收到数据后需要有特定的身份进行认证，密钥进行解密；

③数据存储方面，认证凭据（如口令/私钥等）和敏感个人数据均进行加密，并设置访问权限，并通过网络策略限制其他服务或接口对敏感数据的调用，同时设置数据备份存储，降低因系统故障、操作失误以及安全问题而导致数据丢失的风险；

④数据使用方面，发行人在数据使用设置了包括访问授权、访问限流、数据分级、数据脱敏、数据水印和数据表列行级等权限管理；

⑤数据销毁方面，发行人会对所使用的数据在其数据生命周期结束时做数据销毁，通过软件销毁和硬件销毁两种方式达到数据销毁的目的。

（3）执行管理层面

根据发行人提供的业务合同、承诺书，并经访谈发行人业务负责人，发行人在与上下游客户、供应商的业务往来中，通过合同、承诺函等方式保证其符合客户隐私数据保护的相关要求，具体如下：

一方面，发行人会要求部分客户出具承诺书，具体内容为：“我司（即发行人客户，下同）承诺并保证：我司已向用户明确告知且获得用户的授权将向云从科技申请个人信息处理服务，用户对此表示同意，且已经向我司出具了法律授权文件，授权我司向云从科技提供用户个人信息。鉴于我司已经获得前述第一款所载明之客户的充分、真实的授权及转授权的权利，我司在此授权并同意：云从科技有权将我司提交的用户个人信息进行处理，并向我司提交上述个人信息处理结果。”

另一方面，发行人在与涉及个人信息数据传输、存储、运用业务的客户签订合同时，会将下列条款列为合同通用条款：甲方（即发行人客户，下同）应确保

使用乙方（即发行人，下同）的服务应用于合同约定之事项，不得用于违反法律、法规及规范性文件规定的经营活动；甲方应确保其已经取得权利人的合法授权，授权其向乙方提供相关的用户信息并进行相应的比对、核查；甲方承诺不以任何违反法律或侵犯第三方合法权益（包括但不限于知识产权、隐私权、肖像权）的方式使用本合同项下产品/服务；甲方应依据相关法律法规使用乙方产品或服务，甲方应对自身业务合法性、合规性负责。如因甲方违规或不合理使用乙方产品或服务而产生的不良法律后果，由甲方承担。

5.发行人在人工智能技术可控和符合伦理规范方面的规划

经访谈发行人业务负责人，一方面，发行人将不断提高相关技术水平和先进性，并通过 AI 工程化手段，逐步构建低风险机器学习模型与平台，建立机器学习算法模型安全性的流程与评估体系；发行人拟构建人工智能风险与安全综合测试平台，建设自动检测与评估平台，针对数据与算法的安全性、公平性、可追溯性、风险类型、影响程度与影响范围等方面，对人工智能产品及应用进行风险与安全综合检测与评估。另一方面，发行人将通过继续不断加强员工在人工智能伦理规范方面的培训、优化内控决策结构和程序等手段，培养员工正确的人工智能伦理意识；不仅如此，发行人还将根据国际国内不断发展变化的人工智能技术可控、伦理规范方面的理念、规定和制度，不断发展、完善公司相关内部制度文件，积极落实先进管理理念和宗旨；最后，发行人将继续与有关部门、科研机构、行业组织、社会团体等开展合作与交流，研究符合人类伦理道德的智能自主学习模型，实现人工智能行为与人类价值观的融合。

6.结论意见

综上所述，本所律师认为：发行人为保障人工智能技术的安全可控、符合伦理规范和客户隐私的数据安全，已在制度、技术、内控等方面采取了相应措施，并制定了相应规划，相关措施和规划符合相关法律法规及行业规范的规定。

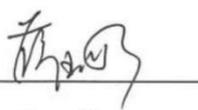
本补充法律意见书一式叁份。

（此页无正文，为《北京国枫律师事务所关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之三》的签署页）



负责人 
张利国

经办律师 
臧欣


薛玉婷

2021年7月10日