

个人信息保护法律热点问题

《网络数据安全条例（征求意见稿）》要点解读之数据安全保护专题

2021年11月14日，国家互联网信息办公室（以下简称“**国家网信办**”）发布《网络数据安全条例（征求意见稿）》（以下简称“**《数安条例草案》**”），并向社会公开征求意见至2021年12月13日。

《数安条例草案》以《网络安全法》、《数据安全法》、《个人信息保护法》作为上位法依据，共九章七十五条。其中要点诸多，针对数据跨境安全传输、个人信息权利保护、数据安全保护、赴国外上市与赴港上市的网络安全审查标准、互联网平台运营者义务等内容均分别做出细致规定。我们将分批次与主题对《数安条例草案》进行解读，本文为“数据安全保护”专题。

一、**数据分类分级保护制度**

《数安条例草案》第五条第一款落实了《数据安全法》中第二十一条已规定的国家数据分类分级保护制度，同时在此基础上做出补充：（1）将数据分为一般数据、重要数据、核心数据；（2）明确了重要数据与核心数据的概念，可分别参照《数安条例草案》第七十三条第三款与第四款。

“核心数据”的概念与《数据安全法》第二十

一条制定的概念完全一致，即核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的的数据。

“重要数据”是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。包括以下数据：（1）未公开的政务数据、工作秘密、情报数据和执法司法数据；（2）出口管制数据，出口管制物项涉及的核心技术、设计方案、生产工艺等相关的数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争实力有直接影响的科学技术成果数据；（3）国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；（4）工业、电信、能源、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；（5）达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等人口与健康、自然资源与环境国家基础数据；（6）国家基础设施、关键信息基础设施建设运行及其安全数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；（7）其他可能影响国

家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。

此次提出的“重要数据”的概念相较于国家网信办于2019年5月发布《数据安全管理办法（征求意见稿）》¹，有了很大程度上的细化²，但具体的数据范围还有待进一步澄清。

二、网络安全审查申报义务

《数安条例草案》第十三条对网络安全审查申报义务做出规定。该条第一款第一项规定：汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的，需要申报网络安全审查。该条规定相较于国家网信办于2021年7月10日公布的《网络安全审查办法（修订草案征求意见稿）》³中规定的网络安全审查触发情形，对掌握大量数据资源的互联网平台运营者提出了额外要求。而对于这部分互联网平台运营者的划分届时是否可以参照《互联网平台分类分级指南（征求意见稿）》生效后的规定仍待进一步观察。另外，该条第二款还规定：大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。该款为大型互联网平台运营者的境外部署运营中心、研发中心增设了报告义务。

该条第一款第二项和第三项涉及境外上市，详情请参见本系列相关专题：《网络数据安全条例》（征求意见稿）对企业上市影响十问十答。⁴

三、数据安全应急处理机制

网络安全事件的报告义务具体要求散落在公

安部、网信部门、工信部等各个主管部门的行政法规、部分规章文件中。例如《中华人民共和国计算机信息系统安全保护条例》规定，对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告。《数安条例草案》第十一条进一步提高了网络安全事件与数据安全事件中报告义务的时间要求：数据处理者应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知。安全事件涉嫌犯罪的，数据处理者应当按规定向公安机关报案。

当数据安全事件涉及到“重要数据”到达“十万人”门槛时，数据处理者还需：（1）在发生安全事件的八小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等；（2）在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。

四、共享、交易、委托处理重要数据

《数安条例草案》第十二条针对数据共享与委托处理做出进一步规定，尤其是明确了共享、交易、委托处理重要数据的，应当遵守以下规定：（1）与数据接收方约定处理数据的目的、范围、处理方式、数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；（2）留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。此外，第三十三条还规定共享、交易、委托处理重要数据的还应获得

¹ 中华人民共和国司法部，《数据安全管理办法（征求意见稿）》，http://www.moj.gov.cn/pub/sfbgw/zlk/202102/t20210207_174015.html。

² 《数据安全管理办法（征求意见稿）》第三十八条第五款：（五）重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

³ 中华人民共和国国家互联网信息办公室，《网络安全审查办法（修订草案征求意见稿）》，http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm。

⁴ 《君合法评 | <网络数据安全条例>（征求意见稿）对企业上市影响十问十答》，<https://mp.weixin.qq.com/s/cIPStfxzPrxJEA3Ugexzkw>。

政府部门审批。

五、重要数据等保三级要求与密码保护要求

《数安条例草案》第九条第一款重申了《网络安全法》第二十一条与《个人信息保护法》第五十一条，针对数据处理器应当采取的数据安全必要措施的规定。

《数安条例草案》第九条第二款对重要数据处理器提出等保层级上的具体规定：处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，且处理核心数据的系统依照有关规定从严保护。第三款进一步提出使用密码进行保护的要求：数据处理器应当使用密码对重要数据和核心数据进行保护。

六、重要数据处理器备案、报告、年度评估、审批义务

《数安条例草案》为重要数据处理器设定了一系列报告、备案、年度评估、接受审批义务，主要包括以下几个方面。

（一）重要数据处理器合并、重组、分立的报告义务

《数安条例草案》第十四条规定，当重要数据处理器发生合并、重组、分立等情况的，数据接收方应当向设区的市级主管部门报告。《数安条例草案》未明确规定报告义务的具体要求及其与上述备案义务的关系。

（二）重要数据处理器备案义务

《数安条例草案》第二十九条规定重要数据的处理器，应当在在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括：

（1）数据处理器基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；（2）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身；（3）国家网信部

门和主管、监管部门规定的其他备案内容。处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。实践中如何判断数据处理器具体明确的“识别”日期有待进一步观察。我们注意到，2019年发布的《数据安全管理办法（征求意见稿）》⁵第十五条有类似规定：网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

（三）涉及境外上市重要数据处理者的年度安全评估义务

《数安条例草案》第三十二条针对涉及重要数据及赴境外上市的数据处理器规定了年度数据安全评估的义务，关于赴境外上市数据处理器义务的分析，可参考本系列其他专题，以下分析仅针对重要数据处理器。

《数安条例草案》第三十二条第一款规定了重要数据处理器应当自行或者委托数据安全服务机构每年开展一次数据安全评估。提交上一年度数据安全评估报告的时间节点为次年的1月31日，负责的网信部门级别是设区的市级网信部门。报告的具体内容应当包括：（1）处理重要数据的情况；（2）发现的数据安全风险及处置措施；（3）数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；（4）落实国家数据安全法律、行政法规和标准情况；（5）发生的数据安全事件及其处置情况；（6）共享、交易、委托处理、向境外提供重要数据的安全评估情况；（7）数据安全相关的投诉及处理情况；（8）国家网信部门和主管、监管部门明确的其他数据安全情况。

《数安条例草案》第三十二条第二款规定：数据处理器应当保留风险评估报告至少三年。此处的“风险评估报告”与上一款的“数据安全评估报告”

⁵ 中华人民共和国司法部，《数据安全管理办法（征求意见稿）》，http://www.moj.gov.cn/pub/sfbgw/zlk/202102/t20210207_174015.htm

tml.

应该指向一致，但使用不同的名词仍会引起歧义。

（四）共享、交易、委托处理重要数据接受审批义务

《数安条例草案》第三十三条规定，数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。

七、重要数据处理者其他义务

（一）明确数据安全负责人

《数安条例草案》第二十八条规定，重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：（1）研究提出数据安全相关重大决策建议；（2）制定实施数据安全保护计划和数据安全事件应急预案；（3）开展数据安全风险监测，及时处置数据安全风险和事件；（4）定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；（5）受理、处置数据安全投诉、举报；

（6）按照要求及时向网信部门和主管、监管部门报告数据安全情况。数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。

（二）安全教育培训时长要求

针对重要数据的处理者，《数安条例草案》规定其应当制定数据安全培训计划，每年组织开展全员

数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。具体的“二十小时”标准此前并未在《网络安全法》第三十四条、《数据安全法》第二十七条、《个人信息保护法》第五十一条关于培训的要求中体现，此条新增要求为重要数据处理者提供了非常明确的合规要求。

八、国家建立健全数据交易管理制度

《数安条例草案》第七条第二款规定：国家建立健全数据交易管理制度，明确数据交易机构设立、运行标准，规范数据流通交易行为，确保数据依法有序流通。

该条款作为国家建立健全数据交易管理制度的宣示性条款，在此之前，《山东省大数据发展促进条例》已于2021年9月30日通过，《上海市数据条例》也已于2021年11月25日通过，广东省人民政府于2021年7月5日印发《广东省数据要素市场化配置改革行动方案》的通知。可见各地政府都在加快推进数据要素的市场化配置效率，积极落实数据交易管理制度。

除上述针对数据安全保护制定的具体规定外，《数安条例草案》在个人信息权益的保护方面，赴国外上市与赴港上市的网络安全审查标准方面，以及互联网平台运营者义务的规定方面均有细致的补充。我们将会在其他专题另行介绍。

董 潇 合 伙 人 电 话：86 10 8519 1718 邮 箱 地 址：dongx@junhe.com
郭静荷 律 师 电 话：86 10 8553 7947 邮 箱 地 址：guojh@junhe.com
李硕颖 律 师 电 话：86 21 2208 6242 邮 箱 地 址：lishuoying@junhe.com



本文仅为分享信息之目的提供。本文的任何内容均不构成君合律师事务所的任何法律意见或建议。如您想获得更多讯息，敬请关注君合官方网站“www.junhe.com”或君合微信公众号“君合法律评论”/微信号“JUNHE_LegalUpdates”。