君合研究简讯

JUNHE

2024 年 10 月 9 日

数据安全法律热点问题

网数新义务亟待评估——《网络数据安全管理条例》合规义务重点综述

2024 年 9 月 24 日，国务院公布《网络数据安全管理条例》（以下简称“**《条例》**”），自 2025 年 1 月 1 日起施行。《条例》是一部针对个人信息、数据安全、网络安全等方面的综合性行政法规，对《网络安全法》《数据安全法》《个人信息保护法》等上位法相关制度规定予以细化、补充、完善。**尽管涉及范围较广，《条例》的立法思路是以问题为导向，聚焦个人信息、重要数据、网络数据跨境流动等方面的突出重点问题，有针对性的健全制度措施，**例如个人信息处理规则描述要求、个人信息转移请求实现途径、境外处理者专门机构或者指定代表信息报送、重要数据（包括 1000 万人以上个人信息）风险评估及报送制度、大型网络平台责任义务、个人信息跨境传输的法定情形。

考虑到《条例》规定的广度及复杂度，我们将在本文**介绍《条例》中对于企业合规有较大影响的、建议企业在《条例》生效前尽快评估适用性、进行合规提升的新规定、新义务**。从重大方面而言，企业亟需特别考虑的是：

- 是否需要根据《条例》满足或提升**个人信息保护相关**已落地的合规措施；
- 是否属于**重要数据处理者**，若属于，需落地重要数据处理者的法律义务；以及
- 是否属于**网络平台服务提供者**，是否符合相关法律义务。

此外，企业还需结合《条例》其他关于网络数据安全保护的各项细化性规定考虑自身的细化合规义务、目前实践是否需调整或完善。

一 个人信息保护合规义务

《条例》重点细化了《个人信息保护法》中的部分规定，并针对处理 1000 万人以上个人信息的处理者增设了新的申报义务。如下新规定值得企业重点关注：

1. **明确境外处理者应向市级网信办报送专门机构或者指定代表信息**。《个人信息保护法》第五十三条规定了落入管辖范围的境外个人信息处理者应当在境内设立专门机构或者指定代表并将有关机构的名称或者代表的姓名、联系方式等报送给履行个人信息保护职责的部门。此前实践中具体报送流程及通道尚待明确和落地。《条例》首次明确了应向相关机构所在地设区的市级网信部门报送上述信息。（*第二十六条*）但有关境内专门机构或者代表的具体职责及义务、信息报送的具体流程仍有待进一步澄清。

2. **要求处理 1000 万人以上个人信息应参考重要数据处理者规定，设立、报送网络数据安全负责人和网络数据安全管理机构，以及向主管部门报送合并、分立、解散、破产情况下数据处置方案**。《条例》规定处理 1000 万人以上个人信息的网络数据处理者，还应当遵守《条例》第三十条、第三十二条对处理重要数据的网络

数据处理者作出的规定，即设立并向主管部门申报网络数据安全负责人和网络数据安全管理机构；因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案等信息。（*第二十八条*）

3. **明确隐私政策中关于保存期限、收集个人信息、共享个人信息等方面的描述规则**。《条例》对个人信息处理规则的发布和披露要求进行了补充和完善。特别的，要求个人信息处理规则在说明个人信息保存期限时，如果“保存期限难以确定的，应当明确保存期限的确定方法”。网络数据处理者应当**以清单等形式**予以列明收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息。（*第二十一条*）企业需根据《条例》核查自身个人信息处理规则是否符合该等要求。

4. **细化行使个人信息转移权的具体条件**。《个人信息保护法》第四十五条原则性规定，个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。《条例》首次规定了行使个人信息转移请求权应满足的条件，即：（1）能够验证请求人的真实身份；（2）请求转移的是本人同意提供的或者基于合同收集的个人信息；（3）转移个人信息具备技术可行性；（4）转移个人信息不损害他人合法权益。（*第二十五条*）

5. **新增需要删除或匿名化个人信息的情形**。根据《条例》规定，因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，网络数据处理者应当删除个人信息或者进行匿名化处理。（*第二十四条*）上述两种情形是现行法律法规新增明确的应当对所收集个人信息删除或匿名化处理的具体情形。例如，企业可能会利用自动化采集技术（如爬虫、传感器等）进行数据收集，而在这一过程中，可能会不可避免地收集到一些并非业务所必需的个人信息。这些信息可能并不是企业主动寻求收集的，而是由于技术限制或环境因素导致的。如果确实无法避免地收集到了非必要个人信息，企业应当尽快采取措施进行删除或匿名化处理。

6. **强调定期合规审计的要求**。《条例》强调了网络数据处理者应当定期自行或者委托专业机构对其处理个人信息遵守法律、行政法规的情况进行合规审计。（*第二十七条*）可以预见与合规审计相关的规则和指引也将逐步落地。

二　重要数据处理者安全合规义务

《条例》延续了《数据安全法》对重要数据监管的整体思路，对于《数据安全法》中规定的重要数据处理者的内部管理机构、风险评估、主管部门报送等义务进行了进一步细化和扩展。重要数据处理者的主要义务总结如下：

1. **设立并向主管部门申报网络数据安全负责人和网络数据安全管理机构**。重要数据的处理者应当明确数据安全负责人和管理机构，并需每年通过年度风险报告向主管部门报送。网络数据安全管理机构的责任包括：（一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；（二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；（三）受理并处理网络数据安全投诉、举报。《条例》还细化了网络数据安全负责人的背景审查、任职要求等方面的要求。（*第三十条*、*第三十三条*）

2. **提供、委托处理、共同处理重要数据需进行风险评估并向主管部门报送**。重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估（属于履行法定职责或者法定义务的除外），且每年通过年度风险报告向主管部门报送。《条例》并规定了风险评估的重点评估内容。（*第三十一条*、*第三十三条*）

3. **进行年度风险评估并向主管机关报送**。重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门将通报同级网

信部门、公安机关。《条例》并详细列举了风险评估报告应当包括的内容。存在可能危害国家安全的重要数据处理活动的，主管部门有权要求重要数据的处理者进行整改或者停止处理重要数据。（*第三十三条*）

4. **合并、分立、解散、破产情况下需合规并向主管机关报送**。重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等。（*第三十二条*）

三　网络数据处理者的数据跨境合规义务

就数据跨境传输的监管，一方面，《条例》融合了《数据安全法》、《个人信息保护法》和《促进和规范数据跨境流动规定》等法规中的规定，明确了个人信息和重要数据跨境提供的具体条件。另一方面，《条例》强化了数据跨境流动中的安全管理要求。网络数据处理者的网络数据跨境合规义务具体总结如下：

1. **对于个人信息出境，应满足八种情形之一**。网络数据处理者向境外提供个人信息的，《条例》第三十五条提供了八种情形，除了《个人信息保护法》明确列举的（1）数据出境安全评估、（2）个人信息保护认证、（3）订立个人信息出境标准合同和（4）法律、行政法规或者国家网信部门规定的其他条件之外，《条例》延续了《促进和规范数据跨境流动规定》中的规定，增加了以下三种情形供网络数据处理者考虑：（1）为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；（2）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；（3）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。

   虽然“关键信息基础设施运营者以外的数据处理者自当年 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）”这一情形未被《条例》明确列为出境情形之一，但企业可依据于“法律、行政法规或者国家网信部门规定的其他条件”这一情形开展个人信息出境活动。

   此外，《条例》专门将“为履行法定职责或者法定义务，确需向境外提供个人信息”明确列为个人信息出境的条件之一。但对于履行法定职责及法定义务的内涵外延仍需在实务之中了解主管部门的监管要求。

2. **对于重要数据出境，应通过数据出境安全评估**。《条例》对重要数据出境的规定，与《数据出境安全评估办法》和《促进和规范数据跨境流动规定》保持一致。一方面，网络数据处理者应就其确需传输出境的重要数据开展数据出境安全评估；另一方面，未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。

3. **通过安全评估的数据出境活动不应超出原评估范围**。《条例》基于《数据出境安全评估办法》第十四条的规定，明确要求网络数据处理者在通过数据出境安全评估后向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。其中“规模”为《条例》新增内容。

此外，《条例》强化了数据跨境流动中的安全管理要求，规定国家采取措施防范、处置数据跨境风险和威胁，禁止提供专门用于破坏、避开技术措施的程序、工具等，为数据跨境流动提供安全保障。

四　网络平台（包括大型网络平台）的合规义务

网络平台，尤其是大型网络平台已经成为网络空间治理的关键节点。此外，实践中存在网络平台服务提供者滥用数据优势、侵害用户个人信息及其他合法权益的行为。大型网络平台的规模效应及其利用数据优势进行的不正当行为特别是不正当竞争行为对平台内经营者及终端用户将产生更大影响。《条例》设置专章对网络平台、特别是大型网络平台义务进行规定，落实网络平台主体责任。

1. **强调网络平台服务提供者主体责任，保护网络数据安全**。该项规定也适用于预装应用程序的

智能终端等设备生产者。该等提供者需通过平台规则明确第三方产品和服务提供者的网络数据安全保护义务，并依法对用户损害承担责任（*第四十条*）。应用程序分发平台需建立核验规则对应用程序开展网络数据安全相关的核验，并对违规应用程序进行相应处置（*第四十一条*）。

此前《移动互联网应用程序信息服务管理规定》等 app 管理规定已要求应用程序分发平台制定平台管理规则，加强对在架应用程序的日常管理，对存在数据安全风险隐患，违法违规收集使用个人信息，损害他人合法权益等的，不得为其提供服务。此条规定进一步将此义务明确扩展到所有网络平台服务提供者及预装 app 的智能终端设备生产者。

2. **网络平台的其他合规义务**。除上述规定外，本章针对网络平台的大部分义务是对数据处理者或者网络运营者现有数据、网络安全保护义务在网络平台场景下的重述及强调。例如：

   - 针对个性化推送，设置易于理解、便于访问和操作关闭选项（*第四十二条*）。
   - 鼓励使用国家网络身份认证公共服务登记、核验真实身份信息（*第四十三条*）。
   - 跨境提供网络数据，应当遵守国家数据跨境安全管理要求（*第四十五条*）。

3. **明确大型网络平台定义**。《个人信息保护法》第五十八条规定了“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”的相关法律义务。《条例》规定“大型网络平台”为“注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台”。（*第六十二条第（八）款*）。上述定义在一定程度上明确了《个人信息保护法》第五十八条规定的用户数量巨大的情况。但是，对于“业务类型复杂”，“网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响”如何认定仍有待进一步在实践之中明确。另外，对于大型网络平台的认定是否需完全满足上述用户数标准、性质标准、影响标准三个标准，还是仅需满足其中一个标准也待进一步澄清。

4. **大型网络平台发布年度个人信息保护社会责任报告义务**。大型网络平台应当每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。（*第四十四条*）这是针对《个人信息保护法》规定的大型网络平台定期发布个人信息保护社会责任报告的义务的细化。

5. **限制大型网络平台与网络数据相关的不正当行为**。大型网络平台服务提供者不得利用网络数据、算法以及平台规则等通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据，不得无正当理由限制用户访问、使用其数据，不对用户实施不合理的差别待遇等（*第四十六条*）。

   上述大部分要求大部分可散见于《个人信息保护法》、《互联网信息服务算法推荐管理规定》、《反垄断法》、《网络反不正当竞争暂行规定》等法律法规。《条例》着重强调了大型网络平台的上述义务，在一定程度上考虑了大型网络平台的规模效应及其利用数据优势进行的不正当行为特别是不正当竞争行为对平台内经营者及终端用户的破坏力。

   特别值得注意的是，“不得无正当理由限制用户访问、使用其数据”的要求，不但包含了现有法规下个人对其个人信息的访问权，可能还包含了平台内商家用户对其数据的访问权、使用权。但目前《条例》中的规定仍然较为笼统，访问、使用相关数据的边界及范围有待进一步澄清。

五　网络数据保护的一般性义务

1. **明确帮助非法网络数据处理活动的具体表现形式**。《条例》第八条第二款明确列明了关于支持、

帮助利用网络数据从事非法活动及从事非法网络数据处理活动方面的禁止性行为，可供企业按照该项规定进行自查自身业务活动是否涉及。

2. **涉及国家安全、公共利益安全缺陷漏洞应在 24 小时内报告**。《网络产品安全漏洞管理规定》要求网络产品提供者应当在 2 日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息。《条例》第十条进一步规定，发现网络产品、服务存在安全缺陷、漏洞等风险，且涉及危害国家安全、公共利益，网络数据处理者应当在 24 小时内向有关主管部门报告。但仍待明确该义务的主体除网络产品、服务的提供者外，是否还包括任何其他使用者等第三方主体。

3. **建立健全网络数据安全事件应急预案**。《条例》第十一条要求网络数据处理者建立健全网络数据安全事件应急预案，并规定了发生网络数据安全事件时，立即启动预案、向有关主管部门报告以及通知利害关系人的义务。

4. **明确向其他方提供、委托处理个人信息和重要数据的法律要求**。对于向其他网络数据处理者提供、委托处理个人信息和重要数据的，网络数据处理者需要与接收方签署合同、并对接收方履行义务的情况进行监督，同时还需对共享、委托处理的处理情况记录至少保存 3 年。对于网络数据接收方而言，《条例》也明确规定其履行安全保护的义务。

5. **重述数安领域国家安全审查的原则**。《条例》第十三条规定网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查，这与《数据安全法》第二十四条及《网络安全法》第三十五条的要求保持一致。

6. **细化网络数据处理者为国家机关、关键信息基础设施运营者（以下简称“关基运营者”）提供服务时在网络数据处理方面的禁止性活动**。《条例》第十六条规定，网络数据处理者为国家机关、关基运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的，未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析。

   对于受托方的数据处理行为而言，不仅受到委托方与其之间协议的约束，本条款还从行政法规的层面进一步明确了禁止性要求。

7. **配合主管部门监督检查的义务**。网络数据处理者应配合相关主管部门开展的监督检查，具体包括：配合主管部门对网络数据安全进行的监督检查工作（*第五十条*）；及时整改网络数据处理活动存在的较大安全风险（*第五十一条*）。

六　明确《条例》适用范围

需说明的是，《条例》的规制对象是“网络数据处理活动”，即收集、存储、使用、加工、传输、提供、公开、删除通过网络处理和产生的各种电子数据的活动。《条例》的主要义务主体是“网络数据处理者”，即在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。其认定逻辑基本与《个人信息保护法》中的“个人信息处理者”相类似，只是处理的对象更广，包括所有“网络数据”。

《条例》对适用地域范围的界定，基本延续并融合了《网络安全法》《数据安全法》和《个人信息保护法》的规制路径，具体分为三种情形：（1）在中国境内开展网络数据处理活动及其安全监督管理；（2）在境外处理境内自然人个人信息的活动，且以向境内自然人提供产品或者服务为目的，或涉及分析、评估境内自然人的行为的；（3）在境外开展网络数据处理活动，且损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的。（*第二条*）

七　细化法律责任

针对《条例》部分条款的违规行为，《条例》专门设定了明确具体的责任追究机制，包括责令改正，警告，没收违法所得，罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处以罚款。例如，未履行国家安全审查义务

在严重情况下可能导致双罚，包括违规实体 1000 万元以下罚款、以及其直接负责的主管人员和其他直接责任人员 100 万元以下罚款。

鉴于《条例》系依据上位法《网络安全法》、《数据安全法》及《个人信息保护法》制定，《条例》第五十八条原则性规定：对于违反本《条例》其他条款的行为，将由相关主管部门依据上述法律的规定，追究相应的法律责任。这意味着，在严重情况下，主管部门仍可依据上述法律追究违规行为的法律责任。

此外，《条例》第五十九条还规定“首次违规轻微不罚”的情形，即：网络数据处理者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，从轻、减轻或者不予行政处罚。类似规定此前已出现在《网信部门行政执法程序规定》和《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》中。

八　我们的观察

《条例》作为网络安全、数据安全、个人信息保护方面的综合性立法，总结了近年来基本大法执法情况及产业发展，以问题为导向，起到了落地细化、更新完善的作用。

首先，《条例》明确了部分此前缺乏具体标准或实施指引的法律原则性要求，如个人信息转移权、境外个人处理者应向市级网信办报送境内专门机构或者指定代表信息、大型网络平台责任义务等，将直接推动这些要求的执行落地。

其次，针对重要数据理者及 1000 万人以上个人信息的个人信息处理者，《条例》规定了更为严格的安全组织管理、风险评估、政府申报等义务，将推动这些数据处理者的进一步合规强化。

再次，对网络平台服务提供者，《条例》在法规层面明确了相关的网络数据安全的特殊保护责任及主体责任，强化全链条数据安全保护。

结合企业各自不同的情况，我们建议企业进行相应的合规评估，密切关注上述合规要求及其实施细则及指引的落地，为上述合规要求在不久的生效做好准备。

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
郭超　律　师　电话：86 10 8553 7733　邮箱地址：guoch@junhe.com
冯毅捷　律　师　电话：86 10 8540 8723　邮箱地址：fengyj@junhe.com

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”。