通力合规评论——2024 年 10 月

如何用好《网络数据安全管理条例》，布局 2025 网安数据合规工作

2024 年 9 月 30 日，《网络数据安全管理条例》（“《网数条例》”）由国务院令第 790 号正式公布，将于 2025 年 1 月 1 日起正式施行。自网信办于 2021 年 11 月公布征求意见稿以来，《网数条例》经历 3 年的等待终于“靴子落地”。我们认为《网数条例》是对《网络安全法》《数据安全法》及《个人信息保护法》这网安数据领域三法生效以来的监管和执法总结，其出台标志着我国网络安全与数据领域的合规监管逐渐成熟，并将正式迈入新的阶段。

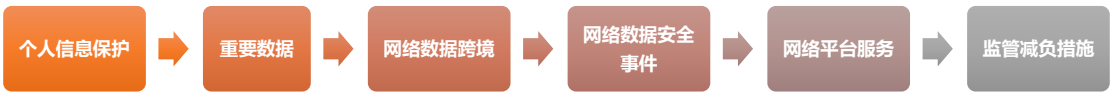
正因如此，《网数条例》整体并非全新的法律，所以监管部门并没有为企业预留太多准备时间——目前距离 2025 年 1 月 1 日仅 3 个月。基于同样的原因，我们预计《网数条例》正式生效后，监管部门的执法也不会有太长的“过渡期”。因此，我们特准备本快讯，帮助企业更好地理解《网数条例》相较现行法律体系需要注意的“新”义务，从而在明年到来之前做好相应的合规准备工作，更好地应对新阶段的监管挑战。

一、适用范围

《网数条例》适用于“网络数据处理活动”和“网络数据处理者”。但请不要被“网络”一词迷惑，以为它仅仅适用于互联网和电信公司。正如《网络安全法》下“网络运营者”几乎涵盖了所有使用互联网的公司。此外，考虑到目前绝大部分数据以电子形式存在，从实务角度出发，《网络数据条例》下的“网络数据”基本等同于数据，而“网络数据处理者”基本等同于数据控制者。这意味着，《网数条例》适用于几乎所有企业。

二、《网数条例》下，企业应关注的 2025 年合规工作

《网数条例》的内容基本承袭了“数据三法”的框架，但其中对于“数据三法”进行重申或补充的部分，很可能成为未来监管部门关注和执法的重点。为此，我们认为企业现阶段宜对以下特殊场景的合规要求予以重点关注：



《网数条例》下的主要合规义务

(一) 个人信息保护

1. 启动个人信息合规审计准备工作

《个人信息保护法》要求个人信息处理者定期开展合规审计，《网数条例》第 27 条从行政法规层面对网络数据处理者重申这一要求，并明确了审计的开展方式——“**自行或者委托专业机构**”。

结合去年公布的《个人信息保护合规审计管理办法（征求意见稿）》、今年 7 月公布的国家标准《数据安全技术 个人信息保护合规审计要求（征求意见稿）》，这进一步预示个人信息审计相关法律或标准即将正式出台。

我们建议，企业应及时启动个人信息合规审计的准备措施，以免在正式法案出台后被个人信息合规审计庞大的工作量与复杂的细则拖垮合规管理效率。此外，还可参考我们近期发表的专题指引，我们通过视频与图表形式简要分析了相关细则：

- *《个人信息合规审计太复杂？——图都帮你画好了！》*

2. 指定境内专门机构/指定代表并报送信息（仅限境外企业）

对于在中国境外处理中国境内个人信息的企业而言，《网数条例》第 26 条重申了《个人信息保护法》下境外个人信息处理者在境内设立专门机构或指定代表的信息报送要求，进一步明确报送对象为"所在地设区的市级网信部门"，并要求"网信部门应当及时通报同级有关主管部门"。

这一重申与细化或预示报送制度将正式在监管实践中落地，我们建议境外相关企业**尽快明确决定由何种类型的实体或个人担任其境内的代表**。可以考虑的因素包括：代表对于中国法律和监管体系的熟悉程度；代表对境外企业的个人信息处理情况和跨境传输情况的了解程度；代表与境外企业之间的关系（关联实体、高管/员工，或独立第三方）及沟通效率和顺畅程度；以及对代表的指定和任命是否会对境外企业带来额外风险。

3. 完善个人信息转移请求配套机制

《网数条例》第 25 条首次明确了个人行使其《个人信息保护法》下"**转移权**"的具体条件，很有可能增加用户请求企业转移其个人信息的频次。

我们建议：

- 及时更新隐私政策有关转移权的内容（例如，补充企业受理个人信息转移请求的审核标准、强调企业有权对不合理的转移请求收取必要费用）；
- 及时与技术部门同事沟通协作，确保隐私专线等沟通渠道畅通、个人信息转移与收费机制能够有效运行；
- 还可参考 2024 年 4 月发布的国家标准《数据安全技术 基于个人请求的个人信息转移要求（征求意见稿）》中有关行使转移权的具体细则，完善具体的转移机制。

4. 处理 1000 万人以上个人信息的企业

《网数条例》第 28 条要求处理 **1000 万人以上**个人信息的网络数据处理者应当参照遵守重要数据处理者的部分义务。这意味着《网数条例》首次在一般法规的层面，将满足一定数量级的个人信息界定为重要数据。

我们提醒符合这一数量条件的企业，及时关注以下新增义务：

- 明确网络数据安全负责人和网络数据安全管理机构，履行相应网络数据安全保护责任；
- 因合并、分立、解散、破产等可能影响 1000 万人以上个人信息安全的，应当：
  - (a) 采取网络数据安全保障措施；
  - (b) 报告：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；主管部门不明确的，向省级以上数据安全工作协调机制报告。

根据目前《网数条例》的规定，其他有关重要数据的义务暂时不适用于处理 1000 万以上个人信息的企业，例如专项风险评估和年度风险评估和报送（但个人信息的提供、

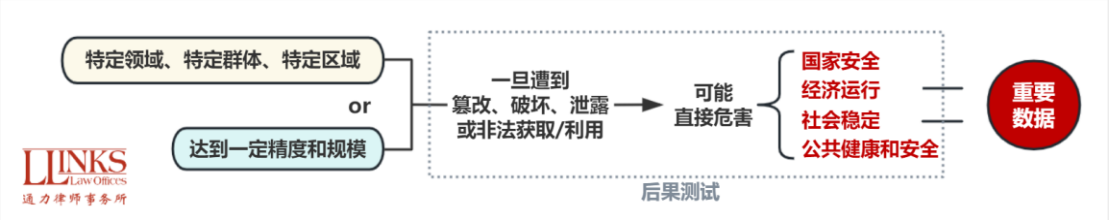
委托处理和共同处理在现行法律下也需要进行安全影响评估）。

(二) 重要数据

1. 及时识别并申报重要数据

《网数条例》第 29 条重申了《数据安全法》有关国家部门制定重要数据目录的内容，并且继《促进和规范数据跨境流动规定》后再次强调网络数据处理者**识别、申报**重要数据的义务。

重要数据的识别无疑是后续合规义务履行的基石。由于《数据安全法》《网络安全法》均无重要数据的定义，部门规章《数据出境安全评估办法》《汽车数据安全管理若干规定（试行）》以及国家标准《数据安全技术 数据分类分级规则》（GB/T 43697-2024）曾在实践中起重要参考作用。本次《网数条例》首次从行政法规层面明确了重要数据的定义（如下图），对此前部门规章与国家标准中的识别规则进行整合，将有助于企业攻克识别重要数据这一难题。



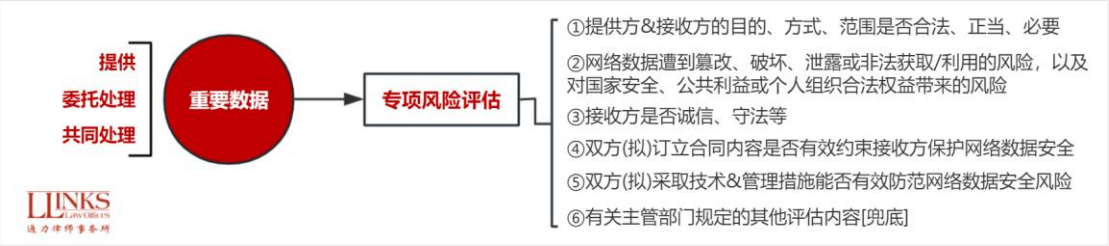
《网数条例》对重要数据的定义

值得注意的是，《网数条例》第 37 条还特别明确——如上述申报的数据未被相关地区、部门告知或公开发布为重要数据的，则**不需要**将其作为重要数据申报数据出境安全评估，相信将有效降低具有出境需求企业的合规成本。

虽然法律规定重要数据将由政府部门确定，但实践中，政府部门通常会组织其管辖范围内的企业对重要数据的识别进行研讨，并要求相关企业申报自行识别的重要数据类型。因此，我们建议重点企业参照重要数据等各类数据识别规则，尽快完善数据分类分级工作，并及时与主管部门沟通重要数据目录的制定进度，从而减轻后续合规成本。我们也将持续关注重要数据目录的制定动态并予以提示。

2. 重要数据专项风险评估

《网数条例》第 31 条新增了重要数据的“专项风险评估”要求——除履行法定职责或者法定义务外，重要数据的处理者应当在**提供、委托处理、共同处理**重要数据前进行风险评估（对比而言，个人信息的影响评估还包括处理敏感个人信息和数据出境。但由于重要数据本身均属于“敏感数据”，且其出境需要经过安全评估，因此《网数条例》将风险评估的范围限于上述三种情形）。重点评估内容包括：

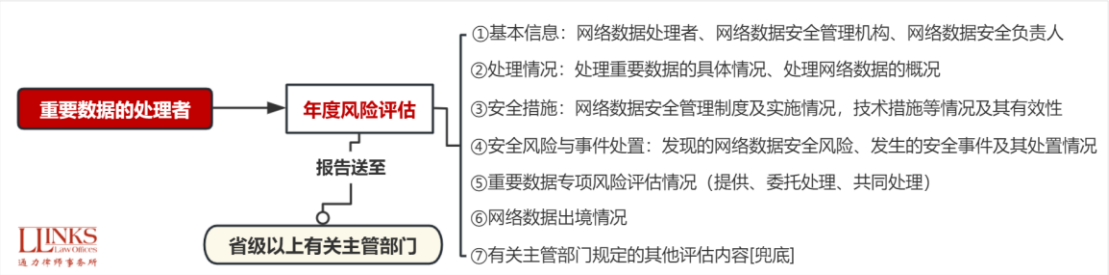


重要数据的专项风险评估要求

我们建议，对于可能掌握重要数据的企业，应积极参照个人信息的影响评估的相关经验，做好专项风险评估的准备，例如评估整体项目风险、起草或审阅提供/委托处理/共同处理重要数据相关合同、完善网络数据安全保障措施等。

3. 重要数据处理者的年度风险评估与报送

对于处理重要数据的网络数据处理者，《网数条例》第 33 条新增了“年度风险评估”与报送要求：



重要数据处理者的年度风险评估与报送要求

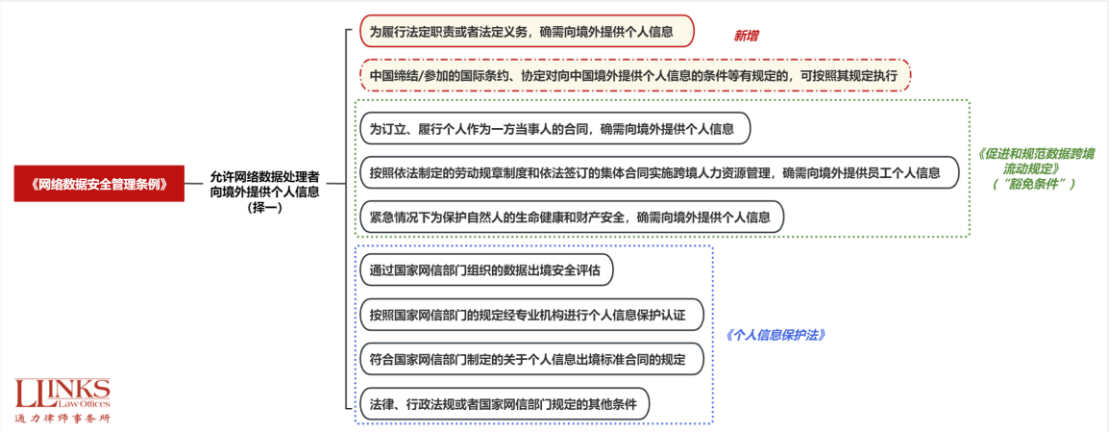
重要数据的年度风险评估和报送在特定行业已经成为一项常规工作（例如汽车行业）。因此，其他行业的企业可以积极借鉴该等特定行业的评估和报送经验。

(三) 网络数据跨境

本次《网数条例》并未对网络数据的跨境流通施加实质性的新义务，其新增内容主要以扩充与细化为主：

1. 个人信息出境路径的拓宽

《网数条例》不仅重申了《个人信息保护法》下的个人信息出境路径，更从行政法规层面将《促进和规范数据跨境流动规定》规定的 3 种豁免条件（可参阅我们此前的解读回顾具体要求*《博观约取、厚积薄发——简评<促进和规范数据跨境流动规定>》*）确立为出境路径。



《网数条例》下的个人信息出境路径总结

此外，结合今年 6 月中国网信办与德国数字化和交通部签订的《关于中德数据跨境流动合作的谅解备忘录》，我们相信未来中国将继续在促进数据跨境流通方面加深国际合作，也期待**本次新增的路径**（如上图）将能够为跨境金融数据监管核查等外资客户的切实需求带来更优解。

2. 数据出境安全评估时需明确出境规模

此前《数据出境安全评估办法》规定，如数据处理者出境数据的目的、方式、范围与种类发生变化的，则需重新申报数据出境安全评估（完整解读可参阅*《尘埃落定！一文详解<数据跨境传输安全评估>重点规定》*）。

对此，《网数条例》进一步增加了对"**规模**"的限制条件。即，要求网络数据处理者仅能按照其已通过数据出境安全评估的出境目的、方式、范围和种类、规模等向境外提供个人信息和重要数据。

为避免重新申报评估带来的合规成本，我们建议有相关需求的企业在开展评估时即明确划定出境数据的规模。

(四) 网络数据安全事件应对

1. 24 小时内上报网络产品重大风险

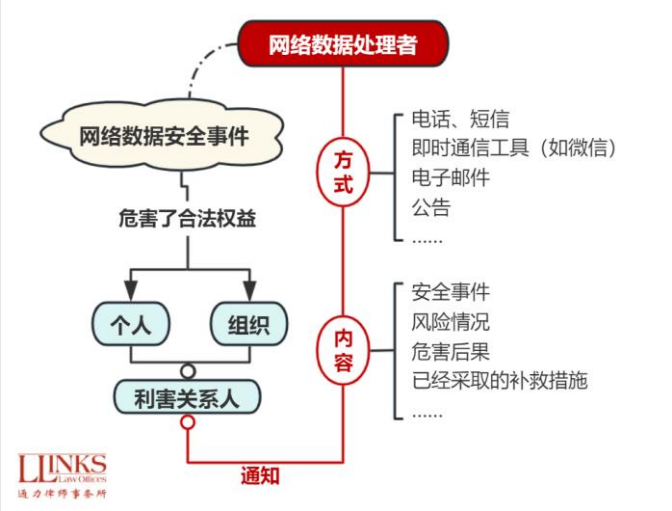
《网数条例》第 10 条新增有关网络产品或服务危害国家安全、公共利益的上报要求——当网络数据处理者发现其提供的网络产品、服务**涉及危害国家安全、公共利益时**，其应在 **24 小时**内向有关主管部门报告。考虑到实践需求，我们期待相关部门能在后续明确该报告所需的具体内容与报告渠道。

此外，相较此前工业和信息化部等部门发布《网络产品安全漏洞管理规定》要求的 2 日上报期限，该条款或许侧重于保护国家安全与公共利益，而采取了更短的期限。

2. 网络数据安全事件的上报与通知义务

《网数条例》第 11 条重申了《数据安全法》《网络安全法》中网络安全事件的上报义务，要求网络数据局处理者在发生网络数据安全事件时"按照规定向有关主管部门报告"。由于该条款仍未对法律依据、主管部门、报告内容与时限等细节予以明确，考虑到实践中网络安全事件的紧迫与严重性，我们建议企业事先参照网信办 2023 年 12 月发布的《网络安全事件报告管理办法（征求意见稿）》做好相应准备。

此外，第 11 条还新增了网络数据安全事件的**通知义务**——除法律、行政法规另有规定外，当网络数据安全事件对个人、组织合法权益造成危害时，网络数据处理者应及时以**特定方式**将**特定内容**通知利害关系人，具体要求如下图：



网络数据安全事件的通知要求

(五) 网络平台服务

1. 加强对接入平台的第三方产品/服务提供者的监督

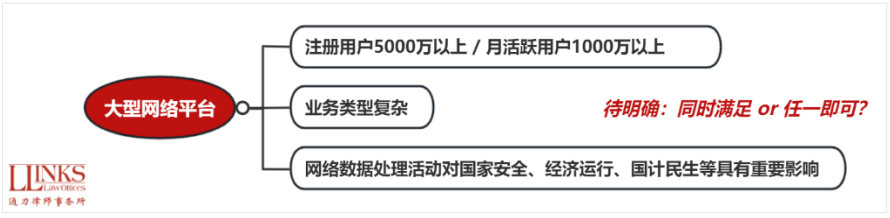
《网数条例》第 40 条强调网络平台服务者对接入其平台的第三方产品和服务提供者具有监督义务并负有相应连带责任:

- 应通过**平台规则或者合同**等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务
- 应**督促**第三方产品和服务提供者加强网络数据安全管理（如因该第三方违法违规或违约开展网络数据处理活动，对用户造成损害的，网络平台服务提供者与该第三方产品和服务提供者将承担相应责任）

此外，该条款还特别强调"**预装应用程序的智能终端等设备生产者**"同样需适用上述规定。我们提醒，涉及生产智能家电、医疗化工器械（例如，检测仪预装分析程序）等设备的企业也应予以注意，及时更新相应合作协议、加强监督工作，还可考虑投保网络数据损害赔偿相关责任险种。

2. "大型网络平台"的认定和义务?

《网数条例》首次从行政法规层面明确了"大型网络平台"的**量化标准**（如下图，但未明确 3 项条件之间的关系是"并"还是"或"，有待于后续监管过程中进一步明确（我们倾向于理解为"或"）。此外，现有资讯也尚未明确企业是需要自行开展认定，还是后续会由主管部门公布相应名单。



大型网络平台的认定标准

如企业初步判断认定其服务涉及大型网络平台，则需注意《网数条例》的新增义务：

- 每年度发布**《个人信息保护社会责任报告》**（说明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内容）
- 跨境提供网络数据的，应遵守国家数据跨境安全监管要求
- 不得利用网络数据、算法以及平台规则等损害用户合法权益
- 处理重要数据的，还应在其**年度风险评估报告**（见上文"重要数据处理者的年度风险评估与报送"）充分说明关键业务和供应链网络数据安全等情况

此外，待《个人信息保护合规审计管理办法》正式出台后，相关企业还需注意履行大型互联网平台运营者**特有的个人信息审计义务**，例如成立主要由外部成员组成的独立监督机构、重点审计大型互联网平台规则与《个人信息保护社会责任报告》内容等。

(六) 监管减负

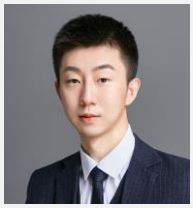
值得注意的是，为合理衔接此前网络安全与数据合规领域的既有监管规则，《网数条例》第 52 条特别强调了监管层面的"减负原则"，具体而言：

- 主管部门开展网络数据安全监督检查时，应**避免不必要的检查和交叉重复检查**
- 个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等应当加强衔接，**避免重复评估、审计**
- 重要数据风险评估和网络安全等级测评的内容重合的，**相关结果可以互相采信**

我们期待上述要求将在《网数条例》实施后有效减轻企业的合规负担，也将持续关注各监管部门后续的执法动向。

如您希望就相关问题进一步交流，请联系：

潘永建 | 合伙人
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳 | 合伙人
+86 21 3135 8683
nigel.zhu@llinkslaw.com