《网数条例》合规行动建议

作者：杨建媛 邬丹 魏依文

引言

历时3年，《网络数据安全管理条例》（下称“**《网数条例》**”）终将于2025年1月1日起生效。在数据保护领域的法规标准迭出、监管机构交错的大背景下，《网数条例》提出的关键词是**聚焦重点、合规减负、监管协同**。本文将着重介绍《网数条例》下需关注的合规行动。

一、重要数据：终于平稳落定

1. 企业如何履行“重要数据”的识别申报义务？

答：政府确定目录→企业自行识别→企业申报→政府确认。

重要数据一贯采取自上而下的路径，先由监管机构定调、再由企业落地。《网数条例》免除了其《征求意见稿》中的重要数据备案义务，但仍要求企业申报重要数据、由监管机构予以确认。**这一方面为企业增设了合规义务，另一方面则增加了重要数据的可确定性。**

保护重要数据的第一步是识别重要数据，而企业面临的老大难问题正是“什么是重要数据”。《网数条例》在重要数据的定义中提出了定性要件，至于具体标准，则交由各地区、各部门确定重要数据具体目录。其后，由企业据此识别自己掌握的重要数据，并向监管机构进行申报。最后，由监管机构确认重要数据，并告知企业或公开发布。

此外，《网数条例》提出，企业如果处理1000万人以上个人信息，则应遵守重要数据处理者的两类义务，但并未扩展至所有义务，也未将“1000万以上个人信息”与“重要数据”直接划等号。实践中，可能仍有赖于部门规定（如《汽车数据安全管理若干规定（试行）》）、地方规定（如《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》）进行细致的界定。

2. 谁可以担任“网络数据安全负责人”？

答：专业知识和管理工作经历+管理层成员+有权向主管机构汇报。

三大法均提及网络安全负责人、数据安全负责人、个人信息保护负责人，而企业的实践难题在于谁来担任这些负责人。《网数条例》要求重要数据的处理者设置“网络数据安全负责人”，且对该负责人提出了具体要求，包括：**（1）具备网络数据安全专业知识和相关管理工作经历，（2）属于企业的管理层成员，（3）有权直接向有关主管部门报告网络数据安全情况。**

由此可见，网络数据安全负责人必须由企业的管理层成员担任，例如，分管数据安全的高管。该负责人本身应具备相关知识与经历，向上应被赋权向监管机构汇报情况，向下应设置专业团队及人员共同支撑。

此外，**《网数条例》没有明确规定网络数据安全负责人的个人责任，**对于企业的违法行为，仍由“直接负责的主管人员”和“其他直接责任人员”承担相应的个人责任。

3. 重要数据生命周期管理中应重点关注哪些环节？

答：涉及第三方的流转环节：提供、委托处理、共同处理、出境、转移。

相较于企业内部的重要数据处理，当重要数据在企业与第三方之间流转，则天然增加了风险。因此，《网数条例》重点关注提供、委托处理、共同处理、出境、转移这些环节。

（1）提供、委托处理、共同处理：提供、委托处理、共同处理重要数据时企业应事先进行风险评估，除非是为履行法定义务。**风险评估的内容与数据出境风险自评估较为相似，但并不需要取得监管批准，而是需在向主管部门报送年度风险评估报告时包含相关风险评估情况。**评估内容具体对比如下表：

《网络数据安全管理条例》：提供、委托处理、共同处理重要数据的风险评估	《数据出境安全评估办法》：数据出境风险自评估
（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；	（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；
（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；	（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；
（三）网络数据接收方的诚信、守法等情况；	（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
（四）与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；	（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；
（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；	（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
（六）有关主管部门规定的其他评估内容。	（六）其他可能影响数据出境安全的事项。

此外，参考《个人信息保护法》（下称“**《个保法》**”）的规定，《网数条例》要求企业在提供、委托处理重要数据时，应与接收方进行合同约定，对接收方进行监督，并保留处理情况记录至少3年。

（2）出境：《网数条例》重申，企业出境重要数据前应通过国家网信部门的安全评估。此外，企业在向主管部门报送年度风险评估报告时，应包括网络数据出境情况。

（3）转移：企业如果发生合并、分立、解散、破产等事件，可能影响重要数据安全，则应向主管部门报告重要数据处置方案、接收方的名称/姓名和联系方式等，以免重要数据落入无人保障的真空状态。

4. 如何通过开展重要数据风险评估把握监管脉络？

答：自评估+合规整改+监管报送。

“自评估+监管报送”是数据保护领域常见的监管方式，履行报送义务后自然就知道如何保护重要数据。

《网数条例》细化了《数据安全法》关于重要数据的风险评估、报告内容及监管报送的要求。**企业开展风险评估、撰写报告，其实也是同步合规整改的过程，合规要点包括：**数据及处理活动的基本情况、企业采取的组织措施和技术措施、第三方数据流转情况、安全事件风险及处置；大型网络平台需额外注意关键业务和供应链安全。

二、网络平台：监管走向深入

1. 如何理解“网络平台服务提供者”的适用范围？

答：法规未明确，实践中应当具备外接第三方产品和服务、面向公众的属性。

《网数条例》未对“网络平台服务提供者”作出明确定义，其适用范围主要取决于对“网络”范围的解释。《网络安全法》项下的“网络”覆盖范围较为宽泛。本处的“网络”究竟采广义解释（互联网、局域网、内网等均被包含在内）还是狭义解释（仅涉及面向公众开放的互联网）已引发讨论，但从抓重点的立法本意而言不宜做扩大解释。

以下主体属于《网数条例》项下的“网络平台服务提供者”或需适用相关规定，且将受到特别关注：

- **大型网络平台服务提供者：**仅就字面解读，其需同时满足“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”三个要件。**实践中，用户量可能会成为判断企业是否落入“大型网络平台服务提供者”范围的主要因素。**一方面，用户量为量化标准，较容易判断；另一方面，达到用户量标准通常意味着其具有“重要影响力”，在平台功能日益聚合化的当下亦不难认定“业务类型复杂”。例如，即便是垂类的电商平台，亦融合了销售、广告、支付、物流等诸多业务。

放眼全球，欧盟的平台治理亦以较为限定的大型网络平台为主要抓手，对“守门人”和“超大型在线平台”进行重点监管。

- **预装应用程序的智能终端等设备生产者：**例如手机、车机、电脑等智能终端设备生产者将被视为网络平台服务提供者，督促第三方产品和服务提供者加强网络数据安全管理。

● **提供应用程序分发服务的网络平台服务提供者：**作为应用程序分发平台，需开展应用程序及网络数据安全相关核验，并在发现不符合强制要求时采取警示、不予分发、暂停分发或者终止分发等措施。

2. 为何对网络平台服务提供者施以额外的严格义务？

答：不履行网安义务+滥用数据优势+平台“力量”膨胀。

《网数条例》的官方解读对此作出答复，理解源于对网络平台服务提供者的监管实践：（1）基础原因：平台不履行网络数据安全义务；（2）进阶原因：平台滥用数据优势从事法律、行政法规禁止的活动。尤其是后者，可以看出监管部门已充分认识到平台的优势地位以及其对社会秩序的巨大影响。

法律、社群规范、市场、架构（技术）是社会控制的主要手段。在当今时代，平台通过网络技术手段深深嵌入（甚至是重塑）人们的生活，影响着人们衣食住行的各个维度。这一点在大型网络平台处展现得更为明显，正如《网数条例》第46条所道“三条路径”，**数据、算法和平台规则助推平台“力量”膨胀，自然也成为监管的主要切入点。**

相较于欧盟《数字市场法》和《数字服务法》等相对“大一统”的平台监管框架，我国现阶段的平台监管要求散落在不同立法之中。《网数条例》作为其中一块拼图，划定了网数角度针对平台监管的重点。

3. 网络平台服务提供者的哪些监管要求值得被特别关注？

答：（1）所有网络平台：第三方产品和服务的监督及责任承担+用户标签删除功能+网络身份认证。

（2）大型网络平台：社会责任报告+数据跨境管理+禁止滥用数据、算法和平台规则。

整体而言，《网数条例》对网络平台服务提供者的监管态度较为严格：

● **第三方产品和服务的监督及责任承担：**第三方产品和服务提供者违法违约处理数据，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。鉴于实践中平台往往会接入诸多第三方产品和服务，本项要求可能会扩大平台的责任范围。

此外，根据《民法典》第176条，民事主体依照法律规定或当事人约定承担民

事责任。因此，《网数条例》（仅为行政法规）规定的前述责任当指行政责任，而非民事责任。

● **针对个人特征的用户标签删除功能：**本处是对《个保法》第24条第二款（保障个人在自动化决策信息推送中的拒绝权）的延伸规定。此前，《互联网信息服务算法推荐管理规定》就曾要求算法推荐服务提供者为用户提供该等用户标签的选择或删除功能。但在实践中，本项要求存在一定落地阻力：既涉及技术困难，也包括可能会对精准营销业务产生重大影响。

● **网络身份认证：**我国早在《网络安全法》就已为网络运营者设置身份认证义务，《网数条例》将在此基础上按照“政府引导、用户自愿”的原则进一步推广网络身份认证。

除以上要求外，大型网络平台服务提供者将适用加重义务：

● **个人信息保护社会责任报告：**本处对《个保法》第58条第四款作出细化，将报告发布周期由“定期”明确为“每年度”，并规定了报告的主要披露事项，可见本项义务将切实走向落地。

● **数据跨境管理、禁止滥用数据、算法和平台规则：**本处主要是重复现有法律法规要求的宣示性规定，再次强调大型网络平台服务提供者的前述义务要求，表明监管部门日后可能会对其采取更为严厉的执法行动。

4. 如何看待网络数据安全保险的发展前景？

答：较为明朗，但受限于不能承保行政罚款。

基于网络数据对个人、企业、社会、国家安全的重要意义，一旦发生数据泄漏等安全事件，可能会引发较大规模的损害，网络平台服务提供者即面临承担巨额损害赔偿的风险，由此，事先购买网络数据安全保险的意义则凸显出来。《网数条例》亦明确提出鼓励保险公司开发相关险种、鼓励网络平台服务提供者等投保。

不过需注意的是，在现行中国法项下，责任保险的承保范围不包括行政罚款，可能会一定程度上限制网络数据安全保险的推广。

三、个人信息：强调、明确及优化

1. 已存在个人信息保护专项立法的情况下，个人信息保护章节意义何在？

答：“强调（突出监管重点）”“明晰（方便推进落地）”“优化（贴合实际情况）”。

《网数条例》系行政法规，基于《个保法》及其实施三年来的经验，对个人信息保护要求进行“**强调**”“**明晰**”及“**优化**”。具体而言：

（1）强调：通过重申、整合《个保法》及相关法律法规的重点内容，强调个人信息处理全生命周期中的重点监管环节及相应要求，包括**告知、同意、个人信息权利的行使**等；

（2）明确：明确个别事项的合规要求，以便企业推进落地，例如明确网络数据处理者响应个人信息转移请求的要求及限制，要求网络数据处理者落实信息收集/共享“双清单”；

（3）优化：在《个保法》的基础上，结合个人信息保护监管的实践经验，优化个别事项的合规要求，以使个人信息保护要求更加贴合实际，例如允许网络数据处理者在难以确定保存期限的情况下，向个人告知保存期限的确定方法。

2. 具体有哪些值得关注的亮点？

答：“同意”及相关要求、转移权的行使、“双清单”、保存期限披露方式。

（1）“同意”及相关要求

《网数条例》通过专门条款对同意及相关要求/概念（单独同意、重新同意、必要性）进行梳理、强调，突出了“同意”在各类合法性基础中的重要地位。

其中，以下要点值得提及：

- **即便在“同意”情形下，“必要性”仍是基本原则。**超出“提供产品或者服务所必需”而收集的个人信息，即便获得个人同意，仍有违“必要性”原则。即，同意不是万能的。

- **明确定义“单独同意”，但应如何获取单独同意仍有待观察。**《网数条例》将“单独同意”定义为“个人针对其个人信息进行特定处理而专门作出具体、明确的同意”。有观点认为通过“独立勾选框”获得单独同意的模式将成为过去式。但是，仅从文本层面，我们理解尚无法作出此类解释。

- **关注“同意”后的持续性义务。**获得个人同意后，网络数据处理者不得超出个人同意的范围处理个人信息。当个人信息的处理目的、方式、种类发生变更时，

网络数据处理者应重新取得个人同意。

（2）转移权的行使

在满足四项限制性条件的情况下，网络数据处理者应当响应个人信息转移请求：（一）能够验证请求人的真实身份；（二）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；（三）转移个人信息具备技术可行性；（四）转移个人信息不损害他人合法权益。

相较于保障个人权利，转移权对于消除锁定效应、促进市场竞争的意义将更为深远。作为我国数据基础制度建设的顶层设计，“数据二十条”明确提出“保障数据来源者享有获取或复制转移由其促成产生数据的权益”，与欧盟《数据法》项下用户的数据获取及利用权益异曲同工。因其自带的冲突性和使命感，料想转移权的落地将会是缓慢却又坚定的过程。

技术层面，个人行使转移权的范围，应仅包括网络数据处理者收集的、有关其个人的原始数据，而不包括经加工、处理后的衍生数据；主要针对面向个人直接收集的个人信息，即以同意或“为订立、履行合同所必需”作为合法性基础所收集的个人信息。

（3）“双清单”要求法定化

《网数条例》第21条第二款规定，“网络数据处理者按照前款规定向个人告知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的，应当以清单等形式予以列明。”

该款内容系对于《关于开展信息通信服务感知提升行动的通知》中个人信息保护“双清单”要求的法定化，使这一义务对网络数据处理者普遍适用，规范了收集、共享个人信息的披露形式要求。网络数据处理者需注意调整隐私政策等告知文本。

（4）保存期限披露方式

《网数条例》关注到部分场景下，要求网络数据处理者确定确切的个人信息保存期限可能存在困难，故允许仅明确保存期限的确定方式，如此将会更加贴合实践做法。

3. 境外网络数据处理者处理境内自然人个人信息，如何设立及向监管机关报送境内机构/代表信息？

答：首先判断是否符合《个保法》第53条要求；若符合，根据《网数条例》进行报送。

根据《个保法》及《网数条例》规定，境外网络数据处理者处理境内自然人个人信息，若属于“以向境内自然人提供产品或者服务为目的”，或为“分析、评估境内自然人的行为”，需在中国境内设立专门机构或指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门。

目前，符合条件的境外网络数据处理者完成机构设立和报送工作的时间线、具体规则尚不清晰。实践中，一些境外网络数据处理者可能持观望态度，特别是在中国境内所获实质利益有限的情况下。

2024-10-09