通力合规评论 —— 2024 年 12 月(年终特辑)
2025 年了，网数合规工作还要做啥?

时光荏苒，不知不觉 2024 年已经来到尾声。对于网安数据领域的合规人来说，2024 年是精彩纷呈的一年。这一年中，1 月，《未成年人网络保护条例》正式生效，成为未成年人网络保护领域的首部全面性法规；3 月，《促进和规范数据跨境流动规定》为绝大多数企业的数据出境合规义务松了绑；4 月，工信部发布公告，启动增值电信业务扩大对外开放试点；5 月，《欧盟人工智能法案》通过，为国内 AI 监管和治理提供了重要的借鉴；同月，上海、天津等自贸区发布数据跨境清单，为数据跨境提供了新的合规路径；7 月，国标草案《个人信息保护合规审计要求》为个人信息合规审计开启了预热；9 月，《网络数据安全管理条例》重磅发布，重申并细化了多项重要数据合规义务；12 月，《银行保险机构数据安全管理办法》正式发布，为银保机构数据合规定下了基调。

执法方面，2024 年呈现以下特点：移动应用程序等互联网产品的全方位监管趋于常态化。例如，工信部定期对 APP(SDK)进行检测，并公开通报违法违规情况；在全球范围内，数据跨境传输的安全日益受到重视。7 月，某中国实体在韩平台因违规跨境传输消费者个人信息，遭到约 20 亿韩元的罚款；数据安全领域的执法处罚数量显著上升，“一案双查”成为常见的执法模式，即在处理数据安全事件时，既要追究攻击者的责任，也要对未履行数据安全保护义务的相关企业进行追责；算法治理领域成为监管部门的关注重点。11 月，网信办等四部委厅局联合决定开展“清朗·网络平台算法典型问题治理”专项行动，旨在解决算法滥用问题、保护用户权益。

网络安全与数据合规领域的立法和执法活动让人应接不暇，也让网数合规人的学习常学常新，甚至对于新的合规义务有些疲于应对。那么，来到 2025 年，有哪些新的合规义务需要履行，又有哪些既有的合规义务需要查漏补缺?通力网络安全与数据合规团队特此为您带来 2025 年网络安全与数据合规工作的展望。

1. 数据合规工作更重视“内功”

距离个保法的生效已经过去了三年多，个保法的相关执法活动也成为常态。但根据我们的观察，过去几年，无论是监管机关还是企业，关注的都主要是个人信息合规的“外在”。例如，许多企业都在过去几年完善了其网站和 APP 的隐私政策，也对网站和 APP 涉及个人信息的功能根据法律的要求进行了整改和提升，而监管部门也着重在这一领域重点进行执法，例如，工信部今年以来已经发布了 10 批关于侵害用户权益行为的 APP(SDK)的通报。

但大家也都知道，数据合规的内涵还包括诸多对于“内功”的要求。随着近几年网信及其他行业主管部门执法经验的积累，执法机构已经不再将目光局限在外部可查的部分。近三年以来，针对数据“内部”相关义务的执法呈逐年上升的趋势。执法针对的违规内容包括：未履行数据安全保护技术、未经扫描和修复的漏洞、未按照法律进行数据安全应急处置，以及违法向境外提供重要数据等。

为了应对该等趋势，我们建议企业:

1) 从组织架构、管理流程和技术措施等方面入手，构建全面的数据安全管理体系。体系应覆盖数据生命周期的各个环节，确保数据在采集、存储、传输、处理、共享、删除等过程中严格遵守个保法及其他相关法律法规的要求;
2) 定期对员工进行数据安全意识教育，并合理确定个人信息处理的操作权限，以减少因人为因素导致的不合规事件;
3) 建立完善的数据安全应急响应机制，并进行定期演练，以确保企业在突发事件中的应变能力。确保在安全事件(如数据泄露)发生时，能够迅速采取有效应对措施，并及时按照法律要求与监管部门或受影响的个人沟通;
4) 开展数据盘点与数据分类分级、个人信息保护审计、重要数据、AI 合规与治理、数据出境等重点专项工作(详见下文)。

2. 数据盘点与数据分类分级

数据盘点与数据分类分级并不是 24 年甚至 23 年的新合规义务，但我们在服务客户的过程中发现，都快 25 年了，仍然有许多需要履行数据合规义务的企业没有做过数据盘点，遑论数据分类分级。

数据盘点与数据分类分级是几乎所有数据合规义务的基础和出发点。如果企业都不知道自身有哪些数据，不同数据分别是什么级别和敏感程度，那么无论是隐私政策的制订，数据出境，还是个人信息合规审计，这些工作都无法有效推进。而数据盘点和数据分类分级工作比较完善的企业，往往也能够以这些工作为基础，高效地完成其他数据合规工作。

因此，所有的数据处理者(尤其是处理个人信息与重要数据的企业)，无论其需要履行何种数据合规义务，都建议尽快进行数据盘点与数据分类分级工作。

相比数据盘点，许多企业感觉数据分类分级比较抽象，往往无从下手，这里我们给大家一些建议:

1) 完成数据盘点工作，形成以字段为最小单位的数据清单;
2) 结合企业所在的行业和企业的具体业务，制订数据分类分级的逻辑。分类分级的逻辑可以参考企业所在行业适用的国家标准或者行业标准。例如，金融行业的企业可以参考《金融数据安全 数据安全分级指南》；医药行业企业可以参考《信息安全技术 健康医疗数据安全指南》；所在行业还没有特定分类分级指南的企业可以参考《工业数据分类分级指南(试行)》《网络安全标准实践指南-网络数据分类分级指引》等;
3) 利用数据分类分级的自动化工具，将数据清单中的字段导入工具中，形成初步的分类分级清单。如果数据字段数量不多的，也可以用手动的方式根据既定的分类分级逻辑，进行分类分级工作并形成清单;
4) 对初步形成的分类分级清单进行复核，针对不符合法律和企业要求的数据分类分级结果，调整分类分级的逻辑；此后，再重复上述第 3)步;
5) 形成最终的数据分类分级清单，并定期对清单进行维护和更新。

3. 个人信息保护审计

个人信息审计在个保法中被正式确立为一项法律义务。此后，随着《个人信息保护合规审计管理办法》《数据安全技术 个人信息保护合规审计要求》等法规、国标草案的公布，具有了落地执行的可行性。而随着网数条例对个人信息审计的重申，2025 年内个人信息审计已经成为了一项“箭在弦上”的义务。

所有的个人信息处理者至少两年需要进行一次个人信息审计，以下两类个人信息处理者需要每年进行一次个人信息审计：(i)处理超过 100 万人个人信息的个人信息处理者；及(ii)处理未成年人个人信息的处理者。

本文第 2 部分提到的数据盘点与数据分类分级将会是个人信息审计工作开展的基础。通过全面盘点数据，明确数据的类型和等级，可以为审计工作提供明确的方向，确保审计工作有的放矢，也可以减少审计的工作量。

审计的重点内容包括：

1) 个人信息处理活动的合法性基础：同意?履行合同必要?履行法定义务?...
2) 个人信息处理规则：形式与内容、是否履行告知义务
3) 特殊情形的个人信息处理活动：共同处理个人信息、委托处理个人信息、对外提供个人信息、合并/分立等情形下的个人信息转移、自动化决策处理个人信息、公开个人信息、处理公开个人信息、处理敏感个人信息、处理未满十四岁未成年人的个人信息、向境外提供个人信息
4) 个人信息主体权利的保障：具体权利的保障、对权利要求的响应
5) 个人信息保护制度和组织架构的完善程度
6) 个人信息保护所采取的技术措施
7) 对于个人信息安全事件的应对：应急预案、响应情况
8) 针对大型互联网平台运营者的特殊审计要点：独立机构、平台规则、对平台内运营者的监督、社会责任报告

建议企业尽早规划个人信息审计工作，因为针对审计发现问题的整改往往耗时较长，而企业如果未及时整改，或在整改期间遇到监管机关的调查或执法，仍然面临着被认定为未履行数据合规义务的风险。

4. 重要数据识别与合规义务

重要数据的定义和相关的合规义务相信读者都已经有所了解，所以此处我们不再赘述。此处主要给大家介绍下，为什么大多数企业需要在 25 年开始进行重要数据和规定相关工作。

首先，数安法、网数条例等法律法规已经明确了，重要数据由地区、行业主管部门确定重要数据目录，再由数据处理者根据目录进行重要数据的识别、申报和保护。因此，理论上来说，只有企业所在的行业主管部门制定并公布了相关行业的重要数据目录，企业才有义务识别并保护重要数据。

但基于以下理由，我们建议企业至少应当开始着手进行重要数据合规相关的准备工作:

1) 企业一旦被认定掌握重要数据，将有诸多相关的合规义务，包括设立网络安全管理机构与网络安全负责人、进行重要数据处理的专项风险评估和年度风险评估，以及重要数据的本地化存储以及数据出境安全评估义务。这些义务的履行都需要长时间的准备和一定的资金投入，因此如果等到重要数据目录公布后才开始准备相应的合规义务准备，可能会面临很长时间的合规“真空期”。

   以数据本地化存储为例，目前大部分跨国企业都是使用的境外的 IT 系统，业务数据通常也都直接出境而不在境内存储。如果企业掌握重要数据，要实现重要数据的境内存储，甚至有些重要数据可能不再可以出境，那么必然会面临 IT 系统和业务结构的大调整。以我们在项目中了解到的 IT 系统调整为例，整体而言需要的时间至少在 6 个月以上，投入的资金至少在数百万元人民币。因此，如果不提前进行 IT 系统的调整，如果政府重要数据目录发布后，企业一旦发现跨境传输的数据中包括重要数据，那么就会面临要么继续违法出境重要数据，或者停止出境重要数据而导致业务中断的两难境地。

2) 目前已经有一些强监管的行业的主管部门，通过内部会议等方式向行业内企业发布了重要数据目录。虽然此类未公开发布的重要数据目录理论上没有法律强制力，但监管部门已经要求企业按照内部的目录申报重要数据，并重点要求企业履行相关重要数据的出境安全评估义务。

因此，基于上述理由，我们建议企业在现阶段应当至少对企业是否可能掌握重要数据进行初步摸排(可在进行上述数据盘点与数据分类分级工作的过程中同步进行)，以判断企业后续是否可能会需要履行重要数据的相关义务。

对于企业初步梳理是否掌握重要数据的，我们的建议如下:

1) 至少先完成企业的数据盘点工作，在数据清单的基础上开展重要数据的识别工作;
2) 根据重要数据的判断标准(“后果测试”)，以及重要数据的相关国标和指南(包括此前发布的草案)(包括但不限于《信息安全技术 重要数据识别指南(草案)》《信息安全技术 数据出境安全评估指南》《数据安全技术 数据分类分级规则》附录 G“重要数据识别指南”)中列举的示例，评估企业的数据在发生安全事件时是否可能危害国家安全或社会公共利益;
3) 除针对单一字段的后果测试外，也需要考虑企业的数据经过聚合、融合后是否会形成重要数据;
4) 在重要数据的后果测试中，企业需要结合自身的业务和数据情况，确定将特定数据界定为重要数据所需的“可能性”的阈值。例如，如果将这一阈值界定为 50%，那么对于危害后果发生可能性低于 50%的数据，就暂不列为潜在的重要数据。如果对于可能性无法定量分析的，也建议至

少做定性分析，判断可能性的大小；

5) 在初步识别重要数据的过程中，如有必要，可以咨询行业主管部门的建议。

如果企业初步审慎判断认为不掌握重要数据的，那么可以合理判断暂时不需要履行重要数据相关义务，也无需提前为未来可能出现的重要数据目录提前规划。但如果企业经初步评估认为可能掌握重要数据的，需要及时制定预案，为后续因履行重要数据合规义务而需要进行的 IT、企业架构、业务流程等变更做准备。

5. AI 合规与治理

随着越来越多的企业入局大语言模型、AIGC 等赛道，以及企业积极拥抱和介入 AI 产品，AI 的合规与治理已经成为企业数据合规工作中不可忽视的一环。AI 的合规与治理分为服务提供者与使用者两个方面，具体的合规建议如下：

1) 作为 AI 服务提供者

- 如果对公众提供 AI 服务，应履行算法备案手续，并按照国家有关规定开展安全评估；此外，如底层技术基于第三方大模型或算法，需确保供应商已完成相应备案与评估；
- 定期审核、评估、验证算法机制机理、模型、数据和应用结果，确保其不危害国家安全或公共利益，扰乱经济秩序和社会秩序，侵犯他人合法权益；
- 参照《关于加强科技伦理治理的指导意见(征求意见稿)》明确的科技伦理治理的基本原则，并结合自身商业模式，制定科技伦理审查规则；
- 加强用户实名制管理，并参考《网络信息内容生态治理规定》等相关法律要求，落实用户发布内容的治理；
- 公示 AI 服务的基本原理、目的意图和主要运行机制，提供便捷关闭 AI 服务的选项，并允许用户选择或删除用于 AI 推荐的个人标签；
- 不应滥用大数据分析等技术手段，例如：基于用户消费记录、偏好等设置不公平的交易条件等。

2) 作为 AI 使用者

- 手动筛查并验证 AI 的输入和输出内容，确保其使用符合相关法律规定；
- 在引入 AI 供应商前，审查其是否具备相应的资质和安全技术能力；
- 原则上不向公众发布 AI 生成内容，如需发布，应经过适当的内部审查；
- 制定相关 AI 管理制度和使用手册，教育员工避免在使用 AI 服务时输入公司商业秘密等敏感数据；
- 建立监控和报告机制，记录员工对于 AI 工具的使用情况；
- 使用境外 AI 服务时，如需应用 VPN，应选用有资质的企业提供的 VPN 服务。

6. 数据出境

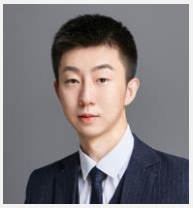
自今年 3 月《促进和规范数据跨境流动规定》正式生效以来，我国数据出境的监管体系已基本成型。大部分涉及数据出境的企业也已经都按照法律的要求，完成了数据出境的安全评估或标准合同备案。

对于尚未完成数据出境法律义务，但又有数据合规出境需求的企业，建议在 25 年的合规工作中，对企业是否需要，以及如何履行数据出境法律义务进行评估，包括:

1) 第一步: 判断数据出境是否落入法定的“履行合同所必要”“跨境人力资源管理”等豁免情形。如果全部出境场景都可以落入豁免情形的，则可以免予数据出境法律义务；如果不能完全落入豁免情形的，则进行以下第二步;
2) 第二步: 判断不落入豁免情形的数据出境场景是否可以落入各自贸区发布的“正面清单”(例如上海自贸区临港片区的一般数据清单)；如果落入“正面清单”的，则可以根据正面清单规定的场景和相应的合规要求进行出境。如果不落入的，则进行以下第三步;
3) 第三步: 判断不落入豁免情形的出境场景中，企业自当年 1 月 1 日起累计向境外提供个人信息数量是否超过 10 万人，或向境外提供任何敏感个人信息；如果不满足的，则可以免予数据出境法律义务；如果满足的，则进行以下第三步;
4) 第四步: 判断不落入豁免情形的出境场景中，企业自当年 1 月 1 日起累计向境外提供个人信息数量是否超过 100 万人，或向境外提供超过 1 万人的敏感个人信息。如是，则需要进行个人信息出境安全评估；如否，则需要进行个人信息出境标准合同备案或个人信息保护认证;
5) 第五步: 如企业所在行业主管部门或其他政府部门已发布适用于企业的重要数据目录的，对照重要数据目录识别企业是否掌握以及出境重要数据，如是，则需要进行重要数据的出境安全评估。

我们希望本期合规评论能帮助您更好地规划 2025 年的数据合规工作。如果您希望了解有关更多数据盘点与数据分类分级、个人信息保护审计、重要数据、AI 合规与治理、数据出境等重点专项工作的信息，或者希望了解我们有关网安数据领域的其他法律服务，欢迎与我们取得联系:

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



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

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: **master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野