以案说法：如何理解和应用《促进和规范数据跨境流动规定》

作者：杨建媛 邬丹 杨吕敏 魏依文 赵雅泽

引言

2024年3月22日，国家互联网信息办公室（“网信办”）发布*《促进和规范数据跨境流动规定》*（“《跨境新规》”），自公布之日起施行。2023年9月28日，网信办曾发布*《规范和促进数据跨境流动规定（征求意见稿）》*（“《征求意见稿》”）。历经半年，数据跨境流动新监管体系终于尘埃落定。

《跨境新规》对于便利数据跨境流动而言是绝对利好。一方面，强调“有限豁免”，从数据处理场景、敏感程度、处理规模等角度切入，为数据出境合规机制设置豁免情形，部分豁免情形甚至对关键信息基础设施（“关基”）运营者也适用；另一方面，强调“风险路径”，聚焦重要数据以及达到特定规模、敏感程度的个人信息，进行深度监管。

最受关注的遗留问题为如何认定敏感个人信息。根据《跨境新规》，出境1条敏感个人信息即需要订立标准合同或通过个人信息保护认证；若自当年1月1日起累计出境1万人以上敏感个人信息，则需申报数据出境安全评估。目前，通常参考GB/T 35273《信息安全技术 个人信息安全规范》（“35273标准”）划定敏感个人信息，部分字段对于企业影响较大，例如身份证号、银行卡号。

需要注意的是，《跨境新规》的豁免主要针对出境合规机制，即数据出境安全评估、个人信息出境标准合同、个人信息保护认证。在出境合规机制之外，企业出境个人信息仍需履行《个人信息保护法》规定的其他合规要求，典型包括：告知个人信息主体、取得个人单独同意或满足其他合法性基础、开展个人信息保护影响评估（即PIA）。

为协助企业更好地理解与应用《跨境新规》，我们梳理了系统性的理论工具，以便企业判断和选择适当的出境合规机制，并通过4个实践案例进一步分析新规的具体应用。

一、理论工具：出境合规机制的判断与选择

根据《跨境新规》，数据处理者在判断数据出境活动应当采取何种出境合规机制时，可以按照“豁免监管—强制监管—自由选择”的顺序进行评估。

（一）豁免监管的判断：如果不涉及受监管数据类型，或者满足特定的收集地、合法性基础或数据量要求，则数据出境无需采取任何出境合规机制。

（除下述第4点“数据量”的豁免条件外，其余豁免场景适用于全部数据处理活动，包括关基运营者的数据处理活动。）

1. 数据类型：出境数据是否不涉及受监管数据类型？

不包含个人信息或重要数据：受出境监管的数据主要为个人信息、重要数据系通识认知，其他数据的出境一般不受监管，除非存在外国司法或执法等特定场景。《跨境新规》进一步强调了在国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，如果不包含个人信息或者重要数据，则无需采取任何出境合规机制。

不属于自贸区负面清单：自由贸易试验区（“自贸区”）在国家数据分类分级保护制度的框架下，可自行制定区内需要纳入监管范围的数据清单（“负面清单”）。对于自贸区内的数据处理者，如果出境的数据并未落入负面清单，则无需采取任何出境合规机制。

2. 收集地：是否在境外收集、产生个人信息？

境外数据过境：如果拟出境的个人信息是在境外收集和产生，且在境内处理过程中没有引入境内个人信息或重要数据，则无需采取任何出境合规机制。

3. 合法性基础：是否满足特定的合法性基础（“场景豁免”）？

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，无需采取任何出境合规机制。《跨境新规》明示列举了跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等典型场景。

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，无需采取任何出境合规机制。

相较《征求意见稿》的“实施人力资源管理”，《跨境新规》强调该豁免场景仅适用于“实施跨境人力资源管理”所必需的情形，意味着一般人力资源管理场景可能无法适用该豁免条件，对跨境的必要性提出了更高的要求，从而收缩了适用范围。

紧急情况下为保护自然人的生命健康和财产安全等，确需向境外提供个人信息，无需采取任何出境合规机制。

4. 数据量：当年累计出境的一般个人信息是否不满10万人？

不满10万人一般个人信息：关基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的个人信息（不含敏感个人信息）如果不满10万人（以自然人为单位去重后计算），则无需采取任何出境合规机制。就数据量的计算范围，在计算10万人时，无需纳入上述已被豁免的个人信息。

（二）强制监管的判断：如果构成特殊的主体、数据性质或数据量，则数据出境应当适用安全评估。

1. 主体性质：是否构成特殊主体？

关基运营者：如果企业构成关基运营者，向境外提供个人信息或重要数据，且不符合前述豁免情形的，则应申报数据出境安全评估。

2. 数据性质：是否构成特殊数据？

官方认定的重要数据：如果出境的数据构成重要数据，则应申报数据出境安全评估。数据处理者有义务按相关规定识别、申报重要数据，但仅有经相关部门、地区告知或公开发布的重要数据才需要申报安全评估。

2024年3月15日，国家标准GB/T 43697-2024《数据安全技术数据分类分级规则》发布，其附录G《重要数据识别指南》对重要数据的识别具有参考价值，但重要数据的最终认定需以官方发布的重要数据目录为准。目前，天津等地区已经公开发布重要数据目录。行业重要数据目录未必会向社会公开，工信、能源、航空等行业目前均已存在行业内部的重要数据目录。

敏感个人信息：对于出境敏感个人信息，如果当年出境量累计达到1万人以上，则应申报数据出境安全评估；如果当年出境量不到1万人，则应订立个人信息出境标准合同或通过个人信息保护认证。

针对敏感个人信息的判定，各国监管都在探索之路上。美国最近发布的《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》将人类基因组数据、生物识别标识符、精确地理位置数据、个人健康信息、个人财务数据、受覆盖的个人识别符界定为敏感个人信息，仍较为宽泛。

尽量细化敏感个人信息的类型及定义，同时为不同类型的敏感个人信息设置不同的触发监管的数量门槛，并明确数据脱敏的法律效果，对于各国而言皆为具有实际价值、但必定纠结的重要课题。**中国监管现状如下：**

▶**敏感性质判定**：《个人信息保护法》规定的敏感个人信息包括：生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。网信办本次发布的《个人信息出境标准合同备案指南（第二版）》重申需参考35273标准判断出境敏感个人信息的类型。35273标准中判定敏感个人信息的因素较为宽泛，监管实践的把握尺度亦类似。

▶**数量门槛判定**：敏感个人信息以1万人为限，划分数据出境安全评估、和标准合同或认证；理论上即便出境1条敏感个人信息，亦需要采取出境合规机制。

▶**脱敏效果判定**：若通过技术手段降低敏感个人信息的敏感程度，则脱敏后的敏感个人信息是否可以降级为个人信息？目前并无明确答案。科技发展导致脱敏后重新识别个人的能力不断提升，料想各国监管均难以轻易作出判断。

3. 数据量：当年是否累计出境100万人以上一般个人信息或1万人以上敏感个人信息？

100万人以上一般个人信息：自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息），应申报数据出境安全评估。

1万人以上敏感个人信息：自当年1月1日起累计向境外提供1万人以上敏感个人信息，应申报数据出境安全评估。

就数据量的计算范围，在计算100万人或1万人时，无需纳入前述第一（一）部分第1-3项所述已被豁免的个人信息。

（三）出境合规机制的自由选择：对于豁免监管、强制监管之外的数据出境，数据处理者可以自行选择合适的出境合规机制。

1. 数据量：当年是否累计出境10~100万人一般个人信息或不满1万人敏感个人信息？

针对以下数据处理场景，关基运营者之外的数据处理者可以自行选择合适的出境合规机制，包括订立个人信息出境标准合同或通过个人信息保护认证。

10~100万人一般个人信息：自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）。

不满1万人敏感个人信息：自当年1月1日起累计向境外提供不满1万人敏感个人信息。

就数据量的计算范围，在计算时无需纳入前述第（一）部分第1-3项所述已被豁免监管的个人信息。

二、案例分析：《跨境新规》的理解与应用

对于《跨境新规》的上述规定，我们通过以下四个案例进一步分析新规的具体应用，以便企业参考。

（一）案例1：境外酒店预定场景

案例事实概况：某酒店位于中国境外，通过官方网站及App等线上渠道，面向全球（包括中国境内）的顾客提供酒店相关服务，涉及中国境内顾客超过100万人。

1. 境外个人信息处理者是否需要采取出境合规机制？

根据《数据出境安全评估申报指南（第二版）》《个人信息出境标准合同备案指南（第二版）》，以下情形属于数据出境行为：符合《个人信息保护法》第三条第二款（注：即域外管辖条款）情形，在境外处理境内自然人个人信息等其他数据处理活动。因此，**即使在中国境内没有数据出境方，境外的个人信息处理者如果符合《个人信息保护法》的域外管辖条件，且直接从中国境内用户处收集个人信息、并传输至境外处理，则也需要采取出境合规机制，除非可以被豁免。**

2. 境外酒店预定能否适用“履行个人合同所必需”的豁免？

《跨境新规》延续并完善了《征求意见稿》中的基于合法性基础的“场景豁免”，其中包括：为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息，则无需采取任何出境合规机制。“为订立、履行个人作为一方当事人的合同所必需”是《个人信息保护法》已明确规定的合法性基础，而《跨境新规》进一步列举的典型场景均属于客观必要的场景，即，不跨境传输相应的个人信息给境外服务提供方，则个人无法开展相关跨境活动。

本案例属于酒店预订场景，境外酒店可以为订立、履行个人合同所必需而出境个人信息，无需采取任何出境合规机制。此外，根据《跨境新规》，场景豁免应优先适用。因此，尽管该境外酒店每年在境外收集和处理超过100万中国境内个人的个人信息，但因其系跨境酒店预定所必需，该等个人信息可在数量计算中排除，不会触发基于数据量的监管，故无需采取任何出境合规机制。

（二）案例2：电子名片管理场景

案例事实概况：某境外公司为境内客户提供电子名片管理产品，客户可将其收集到的名片上传至系统，系统会自动识别名片上的姓名、职称、电子邮箱、手机号等信息，方便客户管理联系人信息。该境外公司的服务器位于东南亚，客户上传名片信息时相关个人信息即出境。

1. 该公司的中国境内客户是否因使用该系统而需采取出境合规机制？

若境内客户本身并非关基运营者，通常情况下可就该场景豁免出境合规机制：

数据性质：不涉及敏感个人信息出境。本案例中出境个人信息仅涉及名片上的姓名、职称、电子邮箱、手机号等非敏感个人信息，不会因敏感个人信息出境而触发出境合规机制。

数据量级：所涉联系人信息不满10万人。通常情况下，商业伙伴联系人的数量较为有限，即使大型公司，每年接触10万人以上商业伙伴联系人并将其信息上传系统的可能性也比较低。因此，境内客户不会单纯因为使用该境外电子名片管理产品而触发出境合规机制。

（三）案例3：人工智能训练数据出境场景

案例事实概况：某公司拟使用位于中国境外的算力基础设施进行人工智能训练，需要向境外传输大规模训练数据。该公司注册地不在任何自贸区，但服务器部署于上海自贸区临港新片区。

1. 该公司可否借助“自贸区负面清单”实现数据合规出境？

有观点认为，适用自贸区负面清单的前提是该公司注册于自贸区；也有观点认为，公司在自贸区内开展数据出境活动，即可适用自贸区负面清单。本案例中，公司在自贸区内仅有服务器、没有实体，该公司在自

贸区内的数据出境活动能否享受自贸区的优惠政策，仍有一定的不确定性。

跨境新规：《跨境新规》规定，“自由贸易试验区…可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单”“自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予…”——“区内”二字为新增，但仅从字面变化无法确定公司是否必须注册于自贸区内。

地方实践：上海自贸区和天津自贸区已就适用主体作出限定，但范围有所不同。

▶上海临港：2024年2月，《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》（“《上海办法》”）发布，允许数据处理者根据本片区的重要数据目录和一般数据清单对应采取安全评估、登记备案等措施，实现数据出境合规。《上海办法》的适用主体限于以下数据处理者：（1）在临港新片区内登记注册的；或（2）在临港新片区开展数据跨境流动相关活动的。

▶天津：2024年2月，《中国（天津）自由贸易试验区企业数据分类分级标准规范》（“《天津规范》”）发布，采用“定量与定性相结合”的方式将企业数据分为核心数据、重要数据、一般数据3个级别，并制定了重要数据的识别标准和清单。《天津规范》的适用主体仅限于天津自贸区内企业。

2. 借助“自贸区负面清单”是否可以实现大规模训练数据出境？

自贸区负面清单并非意味着监管完全放宽，通过该机制实现数据出境仍存在一些制约：

清单审批流程严格：根据《跨境新规》，负面清单须经省级网络安全和信息化委员会批准，并报国家网信部门、国家数据管理部门备案。一方面，这意味着最终出台的负面清单具备较强的权威性，但另一方面，这也可能会限制自贸区在负面清单制定上的自主权。

受限于分类分级框架：相较于《征求意见稿》，《跨境新规》强调负面清单须在国家数据分类分级保护制度框架下制定。一方面，站位国家安全和公共安全的重要数据大概率仍会落入“负面清单”从而适用安全评估。另一方面，涉及个体权益保护的敏感个人信息能否在“负面清单”得到降级甚至豁免，仍有待观察。

在特定语境下，重要数据和个人信息亦可能发生内涵交叉。例如，《天津规范》将“企业掌握的1000万人以上个人信息”“100万人以上个人敏感信息”“10万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息”均识别为重要数据。

落地时间并不确定：目前仅天津自贸区、上海自贸区在负面清单制定上动作较快，但负面清单机制何时才能切实落地并在实践中成熟运作，面临一定不确定性。

本案例中，人工智能研发需要海量训练数据，必然涉及大量数据出境。如果其中涉及重要数据，则即使通过自贸区仍然难以突破国家数据分类分级框架。如果涉及大量个人信息，则亦有可能落入重要数据的范畴。如何对待上述范围外的个人信息出境，将是衡量自贸区负面清单含金量的重要标准，解决方法亦如前

文所述：尽量细化敏感个人信息的类型及定义，同时为不同类型的敏感个人信息设置不同的、触发监管的数量门槛，并明确数据脱敏的法律效果。

（四）案例4：跨国公司人力资源管理场景

案例事实概况：某跨国公司的中国境内子公司统一使用全球总部的人力资源系统处理中国境内员工、求职者的个人信息，从而出境人力资源相关个人信息，其中涉及员工的身份证号、银行卡号等敏感个人信息。

1. 出境员工个人信息能否适用“跨境人力资源管理”的豁免？

《跨境新规》规定，“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的”，无需采取任何出境合规机制。相较于求职者，已经入职跨国公司的员工显然对于其个人信息出境至全球总部具备更为明确的预期，人力资源统一管理亦为跨国公司运作机制的应有之义。

本案例需关注以下两方面的制约因素，实践中的监管态度将决定该豁免场景的适用范围：

程序要件：《跨境新规》依然强调人力资源管理的依据为依法制定的劳动规章制度和依法签订的集体合同。根据《劳动合同法》，直接涉及劳动者切身利益的规章制度需要依法履行平等协商和公示程序，而集体合同需要依法履行平等协商和报送程序。实践中，订立集体合同的情况很少，若严格要求同时具备劳动规章制度和集体合同，必将对多数公司适用该豁免场景形成阻碍。

必要性限制：《跨境新规》依然强调出境员工个人信息的必要性，并将《征求意见稿》中的“人力资源管理所必需”改为“跨境人力资源管理所必需”。如果将其严格解释为个人信息不跨境即客观无法实现人力资源管理（例如，外企招聘CEO，需出境个人简历并由总部面试候选人），则将极大限制该豁免场景的适用性。

此外，在员工个人信息出境场景中，涉及身份证号、银行卡号等敏感个人信息出境的情况较为常见。若无法满足该豁免场景的程序要件和必要性，则需要纳入敏感个人信息的出境数量计算。即使出境1名员工的敏感个人信息，也需要订立标准合同或通过个人信息保护认证；如果结合员工之外的出境场景，当年累计出境敏感个人信息达到1万人，还应申报安全评估。

2. 出境求职者个人信息能否适用“订立个人合同所必需”的豁免？

《跨境新规》关于“跨境人力资源管理”的豁免场景仅适用于员工，不包括求职者。公司收集、出境求职者个人信息的目的为招聘员工，可以考虑适用“订立个人合同所必需”的豁免场景。

本案例中，即使求职者应聘境内公司的职位，在某些情况下，公司如果不出境个人信息确实难以完成招聘流程，例如：对于通过业务考核的求职者，全球总部为满足监管或内控要求而需对求职者进行合规审查、

背景调查，尤其是强监管行业的从业人员；对于应聘高级职位的求职者，全球总部需要直接对其进行考核。但是，在初步遴选阶段、或普通职位应聘场景，出境求职者个人信息的必要性论证则存在不确定性，有可能无法适用豁免情形。

2024-03-27