DOI: 10.54254/3049-7825/2025.25149

中欧敏感数据出境规则的合规冲突与制度衔接

牛小艾

（斯旺西大学，英国斯旺西，SA18FE；2419743@swasea.ac.uk）

摘　要：在数字经济跨境发展的背景下，敏感数据的出境合规问题引发多国立法关注。中欧在敏感数据定义、处理条件、跨境传输机制等方面均建立了相对完善的制度体系，但在具体适用上存在明显差异。本文以中国《个人信息保护法》及欧盟《通用数据保护条例》为基础，通过比较两者在制度设计上的侧重点与监管路径，梳理企业在双重合规过程中可能面临的实践困境，并尝试在有限知识基础上探讨中欧制度衔接的可能方向。

关键词：敏感数据；跨境传输；中欧比较；数据合规；制度衔接

引言

在数字经济快速发展的背景下，跨境数据流动已成为推动国际贸易与全球信息互联的重要基础。然而，随着数据所承载的信息价值日益凸显，数据跨境流动所引发的隐私保护、数据安全与主权冲突等问题，也逐渐成为各国关注的重点。特别是在涉及自然人身份、生物特征、健康记录等内容的“敏感数据”出境情形中，不同法域间在数据定义、处理条件及传输路径上的制度差异，使得企业在跨境合规实践中面临不小的挑战。

近年来，中国和欧盟分别通过《个人信息保护法》与《通用数据保护条例》，构建了较为系统的数据保护框架。其中，对于敏感数据的界定与跨境传输的规范成为重点内容。然而，由于两者在法律适用范围、风险评估标准、监管模式和制度目标上的侧重点存在明显差异，企业在同时面对中欧两套规则时往往难以找到稳定、可预期的合规路径。同时，从更广义的制度视角来看，这种差异也反映出当前国际数据治理秩序中尚未形成统一标准的问题。

本文尝试从中欧两地敏感数据出境规则出发，梳理两者在法律构成、制度逻辑与监管路径方面的主要差异，并结合实际合规场景，观察企业可能面临的困境与制度冲突。同时，在尊重不同法域制度独立性的基础上，探索中欧之间在敏感数据跨境管理中寻求制度衔接与协调的可能方向，期望能为后续相关研究提供一定参考。

1. 敏感数据的法律属性与合规特殊性

在个人信息保护的法律体系中，敏感数据因其具有更高的隐私风险与社会影响力，通常被各国立法机构设定为优先保护对象。中欧作为近年来推进数据立法较为积极的两个法域，分别通过《中华人民共和国个人信息保护法》（以下简称《个保法》）与《欧盟通用数据保护条例》，对敏感数据的法律属性作出了明确规定，并对其处理设定了比一般个人信息更高的合规门槛。

从立法定义上看，中欧对“敏感数据”的界定均采取了“列举+开放”结合的方式。《个保法》第28条指出，敏感个人信息是指“泄露或者非法使用可能导致自然人尊严受损或者人身、财产安全受到危害的个人信息”，并列举了生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等具体类别。同时，该条规定“法律、行政法规规定的其他个人信息”也可被认定为敏感信息，保留了立法灵活性。相比之下，欧盟《通用数据保护条例》第9条则将敏感数据称为“特殊类别的个人数据”，主要包括种族、政治观点、宗教信仰、工会成员资格、健康、性取向以及生物特征等信息。两者在列举内容上有一定重合，但欧盟更强调“与歧视相关”的个人身份特征，而中国立法则更注重“可用于身份识别与经济损害”的信息维度。

处理敏感数据的合法性条件在中欧也表现出较强的制度要求。《个保法》第29条规定，处理敏感个人信息需有“特定目的和充分必要性”，并需取得“个人的单独同意”，其中“单独同意”在实践中通常要求通过更明确的书面或点击确认形式实现。该法还强调了处理前应告知信息的内容应更加详尽，包括处理目的、

方式、范围、保存期限及退出机制等 [1]。与此类似，欧盟第9条也规定敏感数据原则上禁止处理，除非满足若干例外情形，例如获得“明确同意”、履行雇佣法律义务、保护重大利益或用于公共卫生等。相比而言，欧盟的豁免事由设置更为复杂，给予数据控制者一定弹性空间，但也要求其承担更强的合规责任，如建立记录制度、进行数据保护影响评估等 [2]。

在安全保障义务方面，中欧均对敏感数据设置了更严格的要求。《个保法》第51条提出，处理敏感信息的个人信息处理者应采取“必要措施”确保其安全，并制定“专门的处理规则”；同时还应定期组织合规审查与风险评估。在具体实施上，如配备加密存储、访问权限控制、员工合规培训等均属常见措施。而欧盟法律则通过引入“技术与组织措施”这一概念，要求数据控制者根据敏感性程度设计风险响应机制，并在数据泄露后72小时内向监管机构报告，确保对高风险数据处理活动形成事前控制与事后响应机制的闭环。

值得注意的是，敏感数据在出境场景下面临的监管强度也明显高于一般个人信息，成为制度设计中最具保守性的部分之一。在中国的法律体系中，敏感数据通常被视为可能影响公共利益或国家安全的潜在要素，因此即使满足个人同意和合法处理前提，仍需额外通过数据出境安全评估、标准合同报备或专业认证机制方可传输。这一机制反映出中国强调数据本地化与“实质性控制”的立场 [3]，敏感数据因其风险等级更高，适用更为谨慎的评估标准。而欧盟则基于“适当性认定”或“标准合同条款”方式进行传输管理，并未对敏感数据出境设置独立流程，但实际上在处理风险评估与合同义务方面仍赋予其特殊审查义务。总体而言，中欧在原则路径上虽有所不同，但均体现出敏感数据的合规要求高于一般信息的共识。

2. 中国敏感数据出境规则的制度逻辑与实践困境

为应对日益复杂的数据跨境流动风险，近年来中国围绕个人信息特别是敏感数据的出境行为，逐步建立起一套相对完整的法律规范体系。其中，《中华人民共和国个人信息保护法》《数据出境安全评估办法》以及《个人信息出境标准合同办法》等规范性文件构成了当前敏感数据跨境合规的主要依据。这些制度在一定程度上回应了个人信息安全保障的现实需求，但在实施过程中也显现出评估路径不清晰、责任边界模糊等问题，给企业带来了较大的合规不确定性，也使中外数据制度之间的协调更具挑战。

《个人信息保护法》第38条确立了我国数据出境的基本规则。该条规定，个人信息处理者因业务需要向境外提供个人信息的，应满足至少一项前置条件，包括：通过国家网信部门组织的安全评估；与境外接收方签署标准合同并履行备案程序；通过第三方机构的数据保护认证。同时，第40条进一步指出，关键信息基础设施运营者以及处理达到一定数量个人信息的处理者，必须将其收集和产生的个人信息存储在境内，除非经国家网信部门评估同意。这些规定确立了我国数据出境的“许可式”监管模式，特别是对敏感个人信息的处理设置了更高的合规门槛。根据《数据出境安全评估办法》第4条，处理敏感信息且达到一定数量（如超过一万人份）即属于需提交安全评估的范畴。由此可见，敏感数据在我国跨境传输中始终处于重点审查位置。

目前实践中较为常用的三种数据出境路径，分别是：行政安全评估、标准合同签署以及认证机制。第一种路径即由国家网信办组织的“行政评估”，适用于处理敏感信息规模较大、涉及关键信息基础设施或向境外集中提供数据的情况。该机制由企业提交风险自评报告、合同草案等材料，国家网信办对数据类型、传输路径、安全保障等要素进行审查。第二种路径为标准合同制度，适用于规模较小的处理者，企业需使用网信办发布的合同模板与境外接收方签署，并在签署后10个工作日内向所在地网信部门备案。第三种路径则是通过认证机构完成“个人信息保护认证”，由专业机构依据国家标准审核企业数据管理体系，并形成认证意见 [4]。在法律设计层面，这三种路径试图为不同体量、不同业务模式的企业提供差异化选择，构建出境合规的“多轨机制”。

然而，在实际操作过程中，企业往往难以判断自身应当选择何种路径，甚至面临三种路径之间互相重叠、适用标准不清的问题。例如，何种情形应归入“向境外提供敏感信息超过一定数量”的范围，各地对评估触发门槛的理解不完全一致；标准合同虽然为中小企业提供了合规路径，但其备案要求、条款适用与境外法律之间存在较大差异，难以直接满足欧盟等地区监管要求；认证机制尚处于探索阶段，目前市场认可度与操作规范性仍不稳定。此外，企业在具体操作中还面临对“个人信息接收方履行保护义务”的判断困难 [5]，合同中如何明确双方责任分配、数据权利救济路径以及违规后果处理，均缺乏统一标准，增加了合规风险。

这些困境在一定程度上反映了我国敏感数据出境规则在制度逻辑上的深层特点。总体而言，我国当前立法更强调对数据流动的“国家层面控制”[6]，以防范跨境传输对数据安全、公共利益及国家安全构成潜在影响。制度设计以“数据主权”理念为核心 [7]，优先考虑数据本地存储、出口前审批和行政监管介入。这种保护逻辑在立法初期阶段有其合理性，但在全球数据流动趋于常态化、企业面临多法域监管压力的情况下，也带来了制度兼容性的问题。特别是对于希望开展国际业务的企业而言，如何同时满足我国与其他法域对数据跨境的不同要求，成为迫切需要解决的问题。

3. 欧盟《通用数据保护条例》中的敏感数据出境规制机制

欧盟自2018年正式施行《通用数据保护条例》以来，确立了较为系统、细致的数据保护制度体系。在全球范围内，该条例以高标准的个人信息保护、严格的执法机制以及域外适用条款，对各国数据立法产生了深远影响。尤其在跨境传输与敏感数据处理方面，条例中构建了完整的法律逻辑链条，不仅对企业提出了更高的合规义务，也在制度设计中体现出程序化、可证明的监管思路。

从适用范围来看，《通用数据保护条例》不仅适用于在欧盟境内设立机构的数据处理者，也适用于向欧盟境内个人提供商品或服务、或监控其行为的非欧盟组织。这一“域外适用”条款使其对全球范围内涉及欧盟用户数据的企业均构成约束 [8]。这种超越属地的立法方式，被普遍视为对数据主权概念的扩展，体现了欧盟将个人数据保护作为基本权利的法理基础 [9]。该条例设立的六项基本原则——合法性、公平性与透明性；目的限制；数据最小化；准确性；存储限制；完整性与保密性——贯穿于整个数据生命周期，对数据控制者提出全程可追溯的合规要求。

在敏感数据处理方面，《通用数据保护条例》第9条明确规定，属于“特殊类别的个人数据”的信息原则上不得处理，除非满足法定例外情形。这些信息主要包括种族、政治立场、宗教信仰、工会成员、健康状况、性生活及性取向等。在处理此类数据时，数据控制者必须获得数据主体的“明确同意”[10]，且需说明处理目的、范围和潜在风险。此外，还可以基于履行雇佣法律义务、保护数据主体或他人的重大利益、出于公共卫生目的或科学研究等理由进行处理，但这些例外情形通常伴随着更高的法律解释门槛与技术保障要求。例如，在公共卫生场景下，需经成员国立法授权；在科研使用中，需确保数据匿名化或采取相应保护措施 [11]。相比之下，《通用数据保护条例》对“敏感数据”的保护强度明显高于一般个人信息处理，强调其合法性基础的具体性与限定性。

就跨境传输机制而言，《通用数据保护条例》建立了以“适当性”为核心的三层管理路径。首先，若欧盟委员会认定某一第三国或国际组织具备“充分程度的数据保护水平”，则可以发布“适当性决定”，该国的数据接收方即可在无额外法律障碍的情况下接收来自欧盟的数据。目前，日本、韩国、新西兰等国家已获得此认定。其次，若无适当性决定，则可通过签署“标准合同条款”作为保障措施，由数据控制者与接收方明确各自义务与违约责任 [12]。标准合同条款需采用欧盟官方模板，并纳入充分的安全保障与权利救济机制。第三种方式为大型企业集团内部常采用的“具有约束力的公司规则”，适用于在多个国家设有子公司的跨国集团，通过集团内部政策构建统一的合规体系，并经成员国数据保护机构批准后实施。

上述机制体现出欧盟在数据跨境治理方面“合规条件前置+结构程序强化”的制度特征。无论采用何种路径，数据控制者均需履行“可证明合规”的义务，即不仅需实现合规结果，更应在组织流程、员工管理、技术措施等方面证明其具备持续履行义务的能力。例如，在使用标准合同条款的情形下，企业需对接收方的本地法律环境进行“额外评估”，如发现其存在国家强制访问风险，还需补充技术加密或法律补救措施。这一制度安排反映出《通用数据保护条例》“动态合规”的思路，即要求数据控制者根据业务变化与外部环境更新其保护措施，确保合规义务在数据流动全过程中始终有效。

4. 中欧敏感数据出境规则的差异比较与衔接障碍

对于敏感数据的出境管理而言，中国与欧盟分别建立了相对完整的法律框架，但由于其制度基础、治理理念与技术路径的不同，企业在实践中往往面临“规则不一致”甚至“相互冲突”的双重压力。以下将从几个关键制度维度出发，对中欧敏感数据出境规制中的核心差异进行分析，并初步探讨制度衔接的障碍与应对挑战。

在对“敏感数据”本身的分类标准上，中欧两者均采用列举结合开放性条款的方式，但具体内容与认定机制存在差异。在中国，《个人信息保护法》第28条规定了敏感个人信息的基本范围，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户和行踪轨迹等，并由法律、行政法规进一步补充。但这些类别的认定主要依赖法律部门与行政机关的解释，缺乏细化的公开分类标准或动态调整机制，企业在实操中往往难以判断某一类信息是否构成“敏感信息”。相较而言，欧盟《通用数据保护条例》第9条将“特殊类别的个人数据”限定为可能引发歧视风险的个人身份信息，并将是否属于敏感数据的判断权部分交由数据控制者结合上下文自行评估。这种机制虽然提高了企业的判断责任，但也在某种程度上提升了制度的适应弹性。

在处理敏感数据的合法性基础上，中欧制度展现出不同的价值重心。中国强调“评估优先”，即在进行敏感数据出境前应完成风险评估、合同备案或获得行政许可，处理行为需具备明确的“必要性”与“最小化”原则支撑，突出国家对数据流向的整体性掌控。行政机关（如网信办）在制度中居于核心位置，对数据出境安排具有最终判断权。而欧盟体系则更加强调“个人意愿”与“组织自律”，将合法性基础主要限定为取得明确同意，或基于法定事由处理。尽管其也要求数据控制者履行一系列证明义务，但行政机关并不直接介

入单项处理行为的许可。这种制度差异反映出中国以国家数据主权为主导的监管模式与欧盟以基本权利保护为核心的治理理念之间的深层分歧。

在合同机制设计方面，中欧亦存在明显不同。中国《个人信息出境标准合同办法》提供了统一合同模板，强调企业与境外接收方必须采用该标准合同，并向所在地网信办备案，其法律效力来自行政机关的制度授权。虽然标准化程度较高，但合同内容较为固定，调整空间有限 [13]；同时，由于需备案审查，企业在签署前后的时间安排与操作路径受到较强监管约束。而欧盟所使用的标准合同条款则更多作为企业合规证明的一种手段，其不需事前审批，可直接由双方签署并实施，后续仅需在监管要求下展示其内容与执行情况。欧盟标准条款允许一定程度的合同补充与技术保障协商，使其更具灵活性与适应性。由于两者在格式、义务分配、执行机制与法律效力来源上存在本质差异，企业在中欧之间难以实现合同文本的“兼容使用”，常需针对不同地区重复拟定与执行合规文件。

在监管机构定位方面，中国目前仍以中央集中监管为主，由国家网信办统筹数据跨境审查与标准制定，地方网信部门配合执行；而欧盟则采取多元化监管体系，各成员国数据保护机构依据条例开展本地监管，同时通过“欧洲数据保护委员会”进行制度协调。这种机制使欧盟监管更加地方化与可谈判，但也可能在跨国案件中带来管辖权重叠或执行不一致的风险。中国的集中模式虽然统一性较强，但在具体业务多样化与行业实践差异较大时，缺乏精细化弹性回应机制，尤其在新兴行业（如云计算）中的监管匹配能力仍需进一步提升 [14]。

基于上述制度差异，在法理层面，中欧之间的数据出境规则也可能产生“规则冲突”问题 [15]。在涉外法律适用上，若同时存在中国的安全评估义务与欧盟对数据控制者的独立责任要求，企业将难以选择优先执行哪一套标准。此外，合同的有效性、数据主体权利行使路径以及合规证明材料的可接受性 [16]，也因监管机构判断标准不同而面临“互不承认”的法律后果。进一步地，跨境数据案件中可能同时触发中国与欧盟的执法程序，涉及法律适用、争议解决与行政协查义务的法律冲突，反映出数据领域“跨法域合规”的复杂性。

企业在这种双重监管环境下面临的实务难题不仅在于成本增加，更在于制度适用的不确定性。以标准合同为例，由于中国合同需备案而欧盟合同侧重自证合规，企业常需分别起草两套文本；部分敏感数据类型在中国被视为高风险对象，而在欧盟并不构成“特殊类别”，导致判断依据难以统一；在欧盟处理的数据需回传中国时，可能因未满足出境安全评估条件而受限，进一步影响数据服务链条的完整性。对于多国运营的平台型企业而言，这类制度冲突可能构成业务扩展与数据部署的重要合规障碍。

5. 对制度衔接路径的初步探讨与可能方向

当数据跨境流动愈发常态化，中欧之间围绕敏感数据出境规制所形成的制度差异，已逐渐显现出合规协调的实际压力。由于双方立法理念、监管机制与技术路径存在显著不同，在短期内实现制度统一或直接互认可能面临较大难度。然而，若能从部分制度工具和实践经验中寻找共识基础，探索可行的衔接方式，仍有望在维持各自制度独立性的基础上，缓解合规冲突、提升制度兼容性。

一个较为可参考的路径是适当性认定机制的构建或互认。欧盟现行的跨境数据传输体系中，适当性决定是其首要合规路径，即由欧盟委员会判断第三国是否具备“实质等同”的数据保护水平，并据此授权数据自由流动。该机制虽然标准设定较高，评估过程复杂，但从程序设计上为不同法域之间建立合规互认提供了明确框架。若未来中欧双方能在敏感数据出境层面开展阶段性评估，并尝试建立分领域、分行业的“有限互认机制”，或许能在保持各自制度特色的前提下，找到一定的技术接口。例如，在医疗健康、金融科技等对数据保护标准要求较高但跨境需求强烈的领域，可探索以指导性标准或协议方式形成部分标准协调基础。

除适当性机制外，标准合同互认亦可能成为实现制度对接的重要方向。目前，中国与欧盟均采用标准合同作为敏感数据出境的重要合规工具，但二者在条款内容、执行模式、法律效力来源等方面存在较大差异。中国标准合同强调行政备案与格式统一，欧盟标准合同则更侧重于合同义务履行与自主评估。尽管如此，二者在核心内容方面均涉及数据接收方义务、数据主体权利保障、违约责任设定等基础要素。在此基础上，若能推动中欧监管机构围绕标准合同条款建立对照表机制、参考指南，或者就部分条款内容达成共识文本，企业在进行敏感数据跨境处理时将具备更明确的合同协调依据，亦有助于降低重复评估成本与合规不确定性。

在中欧制度间衔接尚未实现直接对话的背景下，行业层面的指导规则也可能作为过渡性工具发挥作用。例如，在跨境支付、电子商务、健康平台等典型敏感数据场景中，行业组织可在中欧监管框架允许的范围内，发布合规操作指引或模板条款，帮助企业理解并对照不同制度要求，形成基本的“最低共识线”。这类机制虽不具法律强制效力，但可作为企业内部风险防控的重要参考来源，亦有利于在多边谈判中为制度协调提供实践样本。

与此同时，企业自身在应对双边监管时，也可从合规体系内部结构优化入手，探索更具弹性的双重合规模型。一方面，企业可建立跨法域的敏感数据识别机制，将中国与欧盟对敏感数据的定义、处理原则与出境

要求在系统中并行设置，并设立风险等级评估参数，以实现差异化应对；另一方面，对于具有跨境组织架构的大型平台类企业，亦可考虑借鉴欧盟“具有约束力的公司规则”路径，建立集团内部的数据治理政策体系，明确成员单位在不同法域下的处理责任、审查机制与合规记录义务，并在可能范围内通过境外监管机构的形式审查。虽然这一机制在中国法律框架中尚无对应制度，但其所体现出的“结构内控制”与“组织自证合规”理念，值得企业在当前政策背景下予以关注与探索。

从更长期的发展角度来看，中欧在数据制度衔接方面的路径选择，或将受到双边数字贸易合作机制的推动影响。例如，“中欧全面投资协定”草案中曾包含数据保护议题，中欧之间亦在数字经济领域保持多层次政策对话 [17]。未来，若能以数字贸易为切入点，推动建立制度层面的协调平台，有望为敏感数据出境这一技术性较强、法律风险较高的领域提供更正式的沟通与协商渠道。尤其是在敏感数据认定标准、评估责任分配与纠纷解决机制等关键议题上，双边协商机制的建立有助于降低制度摩擦，提升企业在中欧运营的可预期性。

当然，当前我国在数据出境规制方面仍处于制度不断完善与规则逐步落地的阶段，许多配套制度仍在不断试点与修订中。未来在全球数据治理体系日益演进的趋势下，我国如何在坚持数据安全与国家利益的基础上，提升制度弹性与外部协调能力，将直接关系到我国数字产业的国际竞争力与跨境业务的合规成本。对于敏感数据这一法律与技术高度交织的领域而言，在坚持自主立法的同时，通过机制性探索与国际协作逐步推进规则对接，或许是当前最为可行的制度衔接路径之一。

6. 结语

在全球数据要素跨境流动日益频繁的背景下，敏感数据的出境管理已成为多国数据治理体系中的关键议题。中欧两地分别构建了以《个人信息保护法》和《通用数据保护条例》为核心的数据保护制度，并在敏感数据定义、处理规则与跨境传输路径方面形成了一定体系。然而，由于双方在立法理念、监管方式和制度技术路径上存在差异，企业在面向中欧双重监管时常面临合规选择困难、制度衔接障碍以及执行路径不一致等现实问题。

本文尝试从敏感数据出境规则出发，梳理中欧在分类标准、合法性基础、标准合同机制和监管体系等方面的主要差异，并结合现有制度逻辑对企业实际操作中可能遇到的合规障碍进行了初步观察。在此基础上，提出了若干可讨论的衔接路径，如适当性认定互认、标准合同内容协调、行业指导规范制定及企业内部合规结构优化等，期望为中欧数据制度的协调提供一些思路。

需要说明的是，当前中欧关于敏感数据出境的法律制度仍处于不断演进之中，相关政策文件、实践规则及执法尺度均可能随着技术发展与监管重点调整而发生变化。本文在资料理解和理论分析上均存在局限，主要立足于文本整理与初步比较，不构成全面或定量的研究结论。

未来若要进一步深入探讨中欧数据制度的互动机制，还需结合更多具体的企业实践案例、数据跨境争议处理经验及多边数字治理规则的演进趋势，开展更具实证基础的研究。对于数字时代下的数据法治建设而言，在强化本国制度完备性的同时，如何实现跨法域规则的衔接与协同，或将成为全球范围内面临的共同课题。

参考文献

[1] 胡锐. 告知同意规则的完善: 我国个人信息保护法的实践与反思 [J]. Dispute Settlement. 2025 Apr 30; 11: 213.

[2] LABADIE C, LEGNER C. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR [J]. Journal of Information Technology. 2023 Mar; 38(1): 16-44.

[3] 王睿, 宋兴鸽. 数字贸易背景下数据本地化法律问题研究 [J]. 北方经贸, 2023, (10): 93-96.

[4] 龚雪. DEPA个人信息保护规则研究 [D]. 西南政法大学, 2023.

[5] 卜学民. 个人数据跨境传输限制法律问题研究 [D]. 对外经济贸易大学, 2022.

[6] 陈思琦. 我国跨境数据流动法律规制问题研究 [D]. 中国人民公安大学, 2024.

[7] 杨晓娇, 陈明劼, 吴文博, 等. 我国数据主权的立法保护对策分析 [J]. 数字通信世界, 2023, (11): 9-10.

[8] KUNER C. Protecting EU data outside EU borders under the GDPR [J]. Common Market Law Review. 2023 Feb 1; 60(1).

[9] 沈易航, 陈娜. 数字经济背景下个人数据权保护研究 [J]. 科技创业月刊. 2025 Mar 25, 38(3): 150-6.

[10] DOVE ES, CHEN J. What does it mean for a data subject to make their personal data 'manifestly public’? An analysis of GDPR Article 9 (2)(e) [J]. International Data Privacy Law. 2021 Apr 1, 11(2): 107-24.

[11] 李奕扉, 王协舟. 突发公共卫生事件中欧美个人信息保护法律政策的经验及启示 [J]. 情报资料工作, 2022, 43(3): 104-112.

[12] 冯春阳. 数据跨境流动标准合同条款的路径分析 [J]. 中国国际私法与比较法年刊, 2022, 30(1): 307-323.

[13] 梅傲, 谢冰姿. 全球数据监管竞争下我国个人信息出境标准合同研究 [J]. 国际贸易, 2024, (6): 15-23.

[14] 肖夏. 云服务数据保护法律适用规则研究 [J]. 中国国际私法与比较法年刊, 2019, 25(2): 102-120.

[15] 谢贤保, 郭明军, 邱尔丽. 中欧数据跨境流动合作:共同关切, 现实挑战与实践路径 [J]. 中国经贸导刊, 2025, (1): 89-92.

[16] 张冰. 欧盟个人数据跨境流动的规则研究与借鉴 [D]. 华东政法大学, 2020.

[17] ZENG L, ZENG L. Significance of China-EU Investment Agreements in the Construction of China-EU Comprehensive Strategic Partnership [J]. Contemporary International Law and China’s Peaceful Development. 2021: 599-615.