Dispute Settlement 争议解决, 2024, 10(6), 99-105
Published Online June 2024 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2024.106310

Hans汉斯

反外国制裁法背景下企业数据合规研究

葛子文，李　昱

西南民族大学法学院，四川 成都

收稿日期：2024年5月11日；录用日期：2024年5月27日；发布日期：2024年6月30日

摘　要

随着欧美国家泛化制裁，将经济制裁作为战争的替代手段打击别国经济，直接承受打击的就是被制裁国的涉外企业。而随着全球化的推进和数据的跨境流动，我国企业因数据问题被制裁的风险大大提高，企业数据合规领域面临着前所未有的合规挑战。我国应该从国家和企业两个角度出发，加强我国阻断法体系建设，不断完善我国企业数据合规体系，才能更好地把握机遇，确保企业在全球化发展中牢固立足，从而维护我国经济安全。

关键词

数据合规，反外国制裁法，阻断体系，企业合规

Study of Corporate Data Compliance in the Context of Anti-Foreign Sanctions Laws

Ziwen Ge, Yu Li

Law School of Southwest Minzu University, Chengdu Sichuan

Received: May 11th, 2024; accepted: May 27th, 2024; published: Jun. 30th, 2024

Abstract

With the generalization of sanctions in European and American countries, economic sanctions are used as an alternative means of war to attack the economies of other countries, and the foreign enterprises in the sanctioned countries are directly under the blow. With the advancement of globalization and the cross-border flow of data, the risk of Chinese enterprises being sanctioned due to data problems is greatly increased, and the field of enterprise data compliance is faced with unprecedented compliance challenges. China should start from the perspective of the country and

文章引用: 葛子文, 李昱. 反外国制裁法背景下企业数据合规研究[J]. 争议解决, 2024, 10(6): 99-105.
DOI: 10.12677/ds.2024.106310

enterprises, strengthen the construction of the blocking system, and constantly improve the data compliance system of Chinese enterprises, so as to better grasp the opportunity, ensure that enterprises in the development of globalization, so as to safeguard China's economic security.

Keywords

Data Compliance, Anti-Foreign Sanctions Law, Blocking System, Corporate Compliance

1. 引言

目前，以美国为首的西方国家为实现政治目的，打击别国经济，将制裁手段延伸到了经济领域。2023年8月3日，新美国安全中心发布报告——《制裁数据：2022年回顾》[1]，报告指出，2022年被美国列入“特别指定国民和被封锁人员”(SDN)名单的个人和实体数量激增，共2275个，其中1698个与俄乌战争有关。与俄罗斯无关的577人被美国财政部加入SDN名单，这一数字与去年同期相当。此外，2022年还有519个实体被加入了实体名单，被禁止接受美国原产技术和商品，其中大部分是俄罗斯(72%)和中国(13%)，这反映了美国将制裁作为实现外交政策工具的持续性趋势。

在当下泛化制裁的背景下，企业涉及的数据越多、越敏感，被制裁的风险也越高。自中国加入世贸组织以来，全球化进程得到了进一步的加速，中国企业也以更快的速度走向海外。从数据上看，2002年中国非金融类对外直接投资流量仅为27亿美元，而到了2022年，这一数字已经飙升至1168.5亿美元[2]，其储存的数据也是海量的，极易挑起外国政府敏感的神经。当下，很多国家意识到了数据安全问题的严重性，并采取了一系列的措施来加强数据安全的保护。如美国为加强企业数据管理，在TID业务上进一步加强了外国投资者在美国的投资安全审查力度，提升了外国投资者在涉及美国关键技术、关键基础设施和敏感个人数据领域的投资壁垒，已形成中国企业境外投资面临的新壁垒[3]。国家要防止企业未经授权地访问、泄露和滥用各种数据，企业需要对产生的数据进行合规管理。所以在规范数据使用上，特别是规范企业在国际间的贸易和合作中产生的各种数据，国家和企业的许多想法不谋而合，也更加凸显了数据合规的重要性，因为这些数据不仅涉及个人和组织，同时也涉及国家的重要信息。

随着中国的崛起，外国庞大的制裁网络必然会对我国“走出去”，甚至国内的企业产生重要影响。尤其是在数据合规方面，企业稍有不慎就可能陷入他国设置的制裁陷阱。因此，做好企业涉外数据合规体系是企业在跨国经营中避免踏入制裁陷阱的关键，以确保企业在跨国经营过程中能够遵循各国的法律法规，避免不必要的法律风险。企业要高度重视数据合规，加强内部管理和风险防范，建立健全监控机制，并善于利用专业团队，从而为企业的国际化发展奠定坚实的基础。在当前国际环境下，企业唯有做好数据合规，才能在激烈的国际竞争中立于不败之地。

2. 企业的数据合规困境出现

企业在运行过程中常涉及多个领域，包括国家安全、个人隐私、行业规范，著作权保护等等，这恰恰也是外国制裁关注的领域。同时，企业可能会涉及的制裁行为也不相同，常见的情形有违反数据保护法规、进行跨境数据传输、数据泄露和安全漏洞、未经授权使用数据、合规审计和监督不合作等行为。而且不同的国家和地区的规定也不同，这就给企业数据合规造成了企业在欧盟和美国的合规困境如下所示。

2.1. 不断对外的制裁

2.1.1. 欧盟对外制裁措施

自 19 世纪以来，各国开始寻求一种崭新的、现代化的多边合作机制。到 21 世纪多边主义的发展和国际秩序中的权利均衡与大国主导的外交政策准则开始紧密联系[4]。欧盟开始致力于推动一种“有效的多边主义”并将倡导“有效的多边主义”置于自己安全战略的核心位置。欧盟的共同外交与安全政策(CFSP)于 1993 年签订的《马斯特里赫特条约》(Maastricht Treaty)中正式被提出。之后又被各项文件所加强形成一种安全战略，这种战略具有广泛的安全概念，外交、人道主义援助、发展合作、气候行动、人权、经济支持和贸易政策都是欧盟全球安全与和平工具箱的一部分[5]。具有外交和经济性质的制裁措施应运而生，被欧盟用作促进共同外交与安全政策目标实现的新工具[6]。欧委会副主席兼贸易委员东布罗夫斯基斯表示，“欧盟对外资开放不是无条件的，如果我们想实现开放的战略自主，就必须在欧盟范围内开展高效的投资审查合作[7]。”这一举措旨在配合欧盟对外国企业加强审查的措施，以“反经济胁迫”为名，实施对外经济制裁。目前，欧盟实施的四十多个制裁中，仅有 19 个获得联合国授权[8]，大多数属于欧盟在必要时，自主决定实施制裁措施[9]。

2.1.2. 美国对外制裁措施

制裁需要有法律的载体，也需要法律将制裁的手臂延伸至域外。美国发布的与制裁相关的法律法规已经形成一个体系庞大、涉及范围广、惩罚力度大的经贸制裁体系。典型的例子就是，美国正在不断加强制裁和管辖权的法律制定工作，其中包括《对敌贸易法》(Trading with the Enemy Act)、《国际紧急经济权力法》(International Emergency Economic Powers Act)、《通过制裁反击美国对手法》(Countering America’s Adversaries Through Sanctions Act)、《反海外腐败法》(Foreign Corrupt Practices Act)以及《赫尔姆斯-伯顿法》(Helms-Burton Act)等。另外，美国的《美国爱国者法》(USA PATRIOT Act)和《国防授权法》(National Defense Authorization Act)等其他法律也涵盖了对外制裁的条款。不仅如此，总统的行政命令中也涉及到了发起制裁[10]。且由于制裁规则大多直接出自总统之手，且针对特定的实体和特定的情况量身定制，很多规则是“随时随地”根据被制裁主体的现实情况即时决定和发布的，因此规则的变动性、灵活度不言而喻[11]。通常这些规则会在《联邦公报》(Federal Register)正式发布后生效，前后所用时间往往不超过 30 天。

2.2. 不断扩张的管辖权

美国正在不断加强对于长臂管辖权的法律制定工作。这一目标是通过颁布多部法律来实现的，其中包括《对敌贸易法》(Trading with the Enemy Act)、《国际紧急经济权力法》(International Emergency Economic Powers Act)、《通过制裁反击美国对手法》(Countering America’s Adversaries Through Sanctions Act)、《反海外腐败法》(Foreign Corrupt Practices Act)以及《赫尔姆斯-伯顿法》(Helms-Burton Act)等。另外，美国的《美国爱国者法》(USA PATRIOT Act)和《国防授权法》(National Defense Authorization Act)等其他法律也涵盖了长臂管辖权的条款，总统的行政命令中也涉及到了长臂管辖权[12]。这些立法举措的主要目的是防止企业通过设立分公司或者子公司的方式来规避美国的管辖或制裁等，典型的例子有中兴事件和华为事件。

虽然欧盟声称不会对非欧盟个人或实体产生义务，制裁并不适用于域外，但实际上制裁预计会通过对名单所列人员施加压力而在第三国产生影响。根据《数据法案》第 1(3)条，其适用范围包括：(1) 位于欧盟境内外的，① 欧盟市场内的互联产品(connected product)制造商和相关服务提供商(含虚拟助理、软件等，不含短信、邮件、社交媒体等电子通信服务)，② 向欧盟境内的数据接收者提供数据的数据持有者；及③ 向欧盟境内客户提供相关服务的数据处理服务提供商；(2) 欧盟境内的数据接收者；(3) 欧洲共同数据空间的参与者和使用智能合约的应用程序的供应商。可见欧盟即使是部门法也有域外效力。换

句话说就是即使是第三国的企业，如果它们的业务全部或至少部分在欧盟境内进行的，欧盟就可以进行制裁。因此勿论是在欧洲的跨国企业，还是与欧洲有业务往来的国内企业，都有可能遭到欧盟制裁。

3. 合规困境成因分析

3.1. 我国阻断法体系不完善

制裁法与阻断法，两者在维护国家主权、保护国家安全和国民经济方面发挥着不可或缺的作用。它们相辅相成，一方面通过扩大国内法的域外效力，强化国家在国际舞台上的话语权；另一方面，则通过阻止别国法律的域外适用，维护本国的合法权益。这两大法律工具已成为各国对外交往和斗争中的“国之重器”，成为“法律工具箱”中不可或缺的组成部分。

然而，当前我国的阻断法体系仍处在不断完善的过程中。现有的《反外国制裁法》《阻断条例》《不可靠实体清单规定》等法律或文件虽然为我们提供了一定的法律框架，但其中许多内容仍显得较为笼统，缺乏具体的操作性。这导致在实际操作中，往往会出现架构不清晰、政策性因素过强等问题。以《反外国制裁法》为例，该法规定了我国企业在遭受外国制裁时有寻求救济的权利。然而，如何具体操作、如何有效地行使这一权利，却并未给出明确的指引。这种模糊性不仅增加了企业的合规成本，也可能导致企业在面临制裁时无法及时、有效地维护自己的合法权益。此外，为了监控外国法律域外适用的不利影响，《阻断办法》规定了企业的报告义务。然而，企业在履行了报告义务后，行政单位应如何处理这些报告，却并未给出明确的规范文件和处理流程。这导致企业在做出合规选择时常常感到无所适从，不知道该如何应对可能出现的问题。

3.2. 企业数据合规能力弱

在当今数字化快速发展的时代，企业数据合规能力成为了衡量企业健康发展的重要指标之一。然而，现实情况却不尽如人意，许多企业的数据合规能力仍然显得相对薄弱。这一问题不仅影响着企业的正常运营，更可能带来严重的法律风险和声誉损失。首先，须要明确什么是企业数据合规能力。简单来说，它指的是企业在处理、使用和保护数据时，能够遵守相关法律法规、行业标准和道德规范的能力。这包括但不限于对个人隐私的保护、对数据安全的维护以及对企业商业机密的保密等方面。

然而，尽管数据合规的重要性已经得到了广泛认可，但许多企业在实际操作中却往往存在诸多不足。一方面，一些企业可能缺乏对数据合规的足够重视，认为这只是形式主义，没有实质性意义。这种心态导致他们在数据处理过程中往往忽视合规要求，甚至违法违规操作。

另一方面，一些企业虽然意识到了数据合规的重要性，但由于缺乏专业的人才和有效的技术手段，导致他们在合规方面力不从心。例如，一些企业可能缺乏专业的数据合规团队，无法对数据进行有效的管理和保护；或者一些企业可能缺乏先进的数据安全技术，无法有效防范数据泄露和黑客攻击等风险。

此外，还有一些企业可能受到行业特点、企业文化等因素的影响，导致数据合规能力难以提升。例如，一些行业可能对数据合规的要求相对较低，使得企业在这方面缺乏足够的压力和动力；或者一些企业可能过于注重业务发展和利润追求，而忽视了数据合规对企业长远发展的重要性。

4. 中国企业数据合规困境的应对策略

4.1. 国家层面

4.1.1. 完善中国制裁与阻断法体系

制裁法与阻断法作为维护国家主权和安全的重要工具，其完善和发展对于我国在国际舞台上的地位和影响力具有重要意义。我们应继续努力，不断完善我国的阻断法体系，为企业和行政机关提供更为明

确、具体的法律指引，为我国的对外开放和国际合作提供更加坚实的法律保障。

4.1.2. 完善我国相关立法，扩大我国法律域外适用

目前世界各国已经加快了制裁法和阻断法的立法进程。以欧盟为例，在扩展国内法域外效力方面，欧盟的《数据法案》就具有一定的域外适用效力。在阻断外国法域外适用方面，欧盟颁布了《抵制第三国立法域外适用效果及行动条例》(以下简称《欧盟阻断条例》)，并于 2018 年修订，同时还将美国的制裁法规都列入了禁令范围[13]。除欧盟外，英国、墨西哥、加拿大、南非等国家都出台了类似的阻断法规，给本国企业以法律保护。

我国阻断法和数据法领域将规制的范围延伸到域外的法规很少，只在部分部门法的条文中存在，且处于初期发展阶段，只在少部分领域存在。在数据领域，我国数据安全法规定了在“中华人民共和国境外开展数据处理活动损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。”《个人信息保护法》也规定：“在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：(一) 以向境内自然人提供产品或者服务为目的；(二) 分析、评估境内自然人的行为；(三) 法律、行政法规规定的其他情形。”下一步应当继续扩大我国法律域外管辖的范围，在国内构建完善的阻断法体系，使各部门法有效衔接，形成完善的流程和机制，阻断外国法的不当域外适用。在保护我国司法主权的同时，给予我国企业以更好地保护，进而保护我国的数据主权和数据安全。

4.1.3. 对企业数据合规进行指导

在对企业进行合规指导方面，我国已经出台了《中央企业合规管理办法》、《企业境外经营合规管理指引》和《合规管理体系指南》等指导性文件。但纵观这些指导性文件几乎都是通用的合规管理规范，换句话说就是并没有具体针对某个行业的合规标准。当前我国已有部分地区出台了适用地方的合规标准，如广州市出台了《广州市跨境电商行业合规指引(试行)》，再如上海出台了《上海市化妆品行业广告宣传合规指引》，同时也针对敏感数据出台了《上海市网络点餐服务消费者个人信息保护合规指引》等文件。这些地区性的合规标准，无疑为当地的企业提供了更为明确和具体的合规管理方向。在当前全球经济一体化和数字化快速发展的背景下，企业合规已成为企业稳健运营和持续发展的重要保障。为了进一步提升企业合规水平，国家应当积极借鉴地方的成功经验，出台更多跨地区、针对特定行业或数据的企业合规指引。不仅有助于统一全国范围内的合规标准。同时也可以针对特定行业或数据的企业合规指引能够更好地满足行业的特殊需求，从而在数字化时代帮助企业降低因数据问题被外国制裁的风险。

4.2. 企业层面

4.2.1. 关注制裁领域动向

随着国际政治、经济形势的变化，国家可能会调整其制裁政策，以适应新的国际环境，因此制裁法规具有一定的变化性。企业在制定合规政策时，必须充分考虑国家的政策导向。这不仅包括东道国的法律，也包括母国的法律。企业需要对这些法律和法规进行深入研究和理解，灵活调整合规策略以适应国家政策的变化，以确保其经营行为符合法律要求，避免因违反法律而遭受制裁或损失。

4.2.2. 完善自身数据合规体系

中国企业，尤其是涉及数据管理和运营相关的行业、电商行业和境外上市的企业研究境外数据合规风险应对势在必行，中国企业可运用的境外数据安全风险防控工具主要有如下方面：

首先，建立数据安全的技术保障。数据加密技术是保障数据安全的重要手段之一。通过对数据进行加密处理，可以确保数据在传输和存储过程中不被非法获取和篡改。常见的数据加密技术包括对称加密、

非对称加密和公钥加密等。这些技术各有优缺点，需要根据具体的应用场景进行选择。其次，数据备份和恢复技术也是保障数据安全的重要措施。在数据遭受攻击或意外丢失时，及时的数据备份和恢复可以避免数据损失和业务中断。同时，为了保证备份数据的安全性，还需要采用加密和身份验证等技术手段。除此之外，访问控制技术也是保障数据安全的关键手段之一。通过对数据的访问进行严格控制，可以防止未经授权的用户或程序对数据的非法访问和篡改。常见的访问控制技术包括身份认证、权限管理和访问审计等。此外，网络安全技术也是保障数据安全的重要环节。网络安全技术可以保护数据在传输过程中的安全，防止数据被截获和篡改。常见的网络安全技术包括防火墙、入侵检测和 VPN 等。

其次，构建健全的数据合规管理体系。在当今数字化时代，数据已成为企业运营和决策的核心要素。然而，随着数据的不断积累和使用，数据合规风险也逐渐凸显。为了确保企业在利用数据的同时遵守相关法律法规，构建自己的数据合规管理体系显得尤为重要。构建数据合规管理体系首先需要明确企业的数据治理目标。企业应根据自身业务特点和法律法规要求，制定合理的数据治理策略，明确数据的使用范围、存储方式、共享和传输规则等。同时，企业还应建立数据分类分级制度，对不同级别的数据实施不同的保护措施，确保敏感数据的安全性和合规性。其次，企业需要设立专门的数据合规管理部门或岗位，负责数据合规管理体系的建设和维护。该部门或岗位应具备专业的数据合规知识和经验，能够及时发现和解决数据合规风险。同时，企业还应加强员工的数据合规培训，提高全员的数据合规意识和能力。此外，企业还应建立数据合规审计机制，定期对数据合规管理体系进行检查和评估。通过审计，企业可以及时发现数据合规管理体系中的问题和漏洞，并采取相应的措施进行改进和完善。

在实际操作中，企业可以参考国内外先进的数据合规管理体系和标准，如欧盟的 GDPR、我国的《网络安全法》各种区域经济合作组织的数据流动要求等，结合自身实际情况进行构建。同时，企业还可以借助专业的数据合规管理工具和技术手段，如数据脱敏、数据加密等，提高数据合规管理体系的效率和可靠性。总之，建立自己的数据合规管理体系是企业防止贸易制裁，完善数据合规的重要方式。

4.2.3. 取得信息安全管理体系标准认证

在当前数字化时代，信息安全已经成为企业持续发展的重要基石。一个完善的信息安全管理体系不仅能保护企业的核心数据和商业秘密，还能提升客户信任度，为企业的稳健运营提供坚实保障。信息安全管理体系标准认证，如 ISO 27001 等，是一种国际性的认证体系，旨在评估企业在信息安全方面的管理水平。通过这一认证，企业能够向外界展示自己在信息安全方面的专业能力和严谨态度，从而赢得客户和合作伙伴的信任。获得这一认证，企业首先需要建立一套完善的信息安全管理体系。这包括明确信息安全政策、设立专门的信息安全团队、制定详细的信息安全流程等。此外，企业还需要进行全面的风险评估，识别潜在的安全隐患，并采取相应的预防措施。在信息安全管理体系的建设过程中，企业可以借助专业的信息安全咨询机构或顾问的帮助，以确保体系的有效性和合规性。同时，企业还需要定期进行内部审核和外部审核，以检查体系是否得到有效执行，并及时调整和完善。获得信息安全管理体系标准认证后，企业不仅能提升自身的信息安全防护能力，还能在国际市场上展现其竞争实力。同时，这也将有助于企业在与客户和合作伙伴的合作中，更加顺利地沟通和交流。

4.2.4. 合同与供应链管理

企业不仅要确保自身的数据合规，还要确保与供应商和合作伙伴之间的合同管理和上下游服务等也符合相关法规，避免制裁风险。在全球化的背景下，企业经常需要与不同国家和地区的供应商和合作伙伴进行业务往来。这些业务往来往往涉及到数据的交换和共享。因此，在签订合同时，企业应当明确双方的数据合规责任。这包括确保数据的跨境流动符合各国的数据保护法规，以及要求供应商和合作伙伴遵守相应的数据合规标准。通过明确的合同条款，企业可以确保自身在数据使用和保护方面不会违反法

规，同时也能促使供应商和合作伙伴遵守相关要求。同时，为了确保数据在整个供应链中的合规性，企业需要对上下游公司进行定期的审查。这些审查包括评估公司的数据保护措施、数据处理流程以及员工的数据安全意识等。通过审查，企业可以及时发现并纠正可能存在的数据合规问题，从而避免在制裁中受到牵连。此外，企业还应建立与供应商和合作伙伴的沟通机制，确保在数据合规方面保持密切合作。当数据保护法规发生变化时，企业应及时将最新的合规要求传递给供应链中的各个环节，确保整个供应链的数据处理都符合最新的法规要求。

5. 结语

在当前全球化背景下，国际斗争中泛化制裁、加强制裁政治属性的趋势越来越明显。企业面临着日益严格的国际制裁法律法规，这不仅为数据合规带来了更高的风险，同时也挑战着企业的合规能力。数据合规早已成为企业发展中一个不可或缺的环节，特别是在背景下，数据合规已经成为保障企业利益和稳健发展的核心要素。从欧盟到美国，企业所面临的数据合规困境正变得日益严峻。企业不仅要积极回应国际制裁法规的变化和趋势，还要及时调整自身数据合规策略和管理模式。在如期落实欧盟和美国的数据保护本地化要求之际，企业需要建立健全的数据管理和风险防控措施，以应对潜在的制裁和法规风险，同时，更加重视国家层面和企业层面的合规措施。在国家层面，完善并落实国家制裁与阻断法体系，扩大相关法规的适用范围至国际领域，提升我国政策法律系统的全面性和有效性。同时，对企业提供更加全面深入的数据合规指导，以确保法规合规和权益保障。而企业层面，需要敏锐关注制裁领域动向，完善自身的数据合规体系，建立和完善数据安全的技术保障和管理系统，并且积极取得相应标准的认证，以提升自身的合规能力。只有如此，企业才能更好地规避合规风险，更好地适应和应对国际制裁法规的挑战，确保企业的合法合规发展道路。

基金项目

本文由中央高校基本科研业务费资助，“《反外国制裁法》背景下企业合规问题研究”(2023SYJSCX140)。

参考文献

[1] (2024) Sanctions by the Numbers: 2022 Year in Review.

[2] 黄河, 刘彦彤. 地缘政治风险及其对中国企业海外利益的影响[J]. 太平洋学报, 2023, 31(7): 45-58. https://doi.org/10.14015/j.cnki.1004-8049.2023.7.004

[3] 张小凤. 中国企业走出去合规风险防控指南[M]. 北京: 法律出版社, 2023: 4.

[4] [英]卡罗琳·布沙尔, [英]约翰·彼得森, [意]娜萨莉·拓茨. 欧盟与 21 世纪的多边主义[M]. 薄燕, 等, 译. 上海:上海人民出版社, 2013: 51-67.

[5] (2024) A Stronger EU on Security and Defence. https://www.eeas.europa.eu/eeas/stronger-eu-security-and-defence_en

[6] (2024) How and When the EU Adopts Sanctions. https://www.consilium.europa.eu/en/policies/sanctions/

[7] European Commission (2024) EU Foreign Investment Screening Mechanism Becomes Fully Operational. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867

[8] (2024) EU Sanctions Tracker. https://data.europa.eu/apps/eusanctionstracker/

[9] (2024) EU Sanctions Map. https://www.sanctionsmap.eu/#/main

[10] 徐以升, 马鑫. 美国金融制裁的法律、执行、手段与特征[J]. 国际经济评论, 2015(1): 131-153+8.

[11] 孟刚. 制裁和反洗钱合规风险应对[M]. 北京:中国金融出版社, 2021: 7.

[12] (2024) The U.S. Willful Practice of Long-Arm Jurisdiction and Its Perils. http://ao.china-embassy.gov.cn/por/zfgx/202302/t20230216_11026165.htm

[13] (2024) Council Regulation (EC) No 2271/96 of 22 November 1996 Protecting against the Effects of the Extra-Territorial Application of Legislation Adopted by a Third Country, and Actions Based Thereon or Resulting Therefrom. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996R2271