2026-HG-E019
CZE/EHS/CPG

区域国别研究报告

上海市哲学社会科学规划办公室　　2026 年 8 月 4 日

捷克企业经营安全合规指南

上海外国语大学俄罗斯东欧中亚学院
上海全球治理与区域国别研究院

上海市企业走出去综合服务平台

《区域国别研究报告》是上海市哲学社会科学规划办公室依托上海市各高校和科研院所专业研究力量，紧扣服务企业走出去现实需要，专为“上海市企业走出去综合服务平台”打造的区域国别研究品牌。

《报告》基于学者“在地研究”田野调研、企业出海实务经验以及其他信息，聚焦国别/区域、产业/行业、在地合规运营三类场景，推出三类系列成果。其中，**“国别报告”系列**以对象国政治、经济、社会、文化等内容为研究对象，重点围绕宏观经济形势、营商环境、中资企业经营状况、机遇挑战等维度，解析对象国各领域的发展态势，为企业海外布局提供决策参考；**“行业报告”系列**针对重点产业跨境布局或企业走出去的行业赛道，深入研判对象国的重点行业发展格局；**“合规报告”系列**回应企业海外合规运营实务关切，系统梳理对象国重点领域的监管要点，为企业在地运营提供应对策略参考。

摘　要

近年来，欧盟对企业安全合规的要求已超出传统意义上的人身安全和生产安全，逐步扩展到出口管制、反洗钱、网络安全、供应链安全、关键基础设施保护以及企业内部合规等多个领域。中国企业在捷克经营时所面对的安全合规，是一个由欧盟安全治理规则、捷克本地执行制度和企业内部风险控制机制共同构成的综合体系。企业宜遵循欧盟和捷克本地两个层面的制裁措施相关规则、出口管制规则、网络及基础设施安全规则、数据保护规则和职业健康规则，根据企业实际情况因势利导，在捷克市场安全合规经营。

目　录

一、欧盟规则：综合性安全合规

（一）欧盟限制性措施

欧盟通过理事会条例、共同外交与安全政策以及相关实施条例，对受制裁国家、实体、个人、货物、技术、资金和服务进行限制。企业在捷克开展贸易、设备供应、工程承包、技术服务、金融结算和物流安排时，均需确认交易对象、最终用户、最终用途和货物流向是否涉及欧盟制裁或限制性措施。

（二）两用物项出口管制

欧盟两用物项出口管制规则直接影响中国企业在捷克从事设备、软件、技术和工程服务的合规安排。所谓两用物项，是指既可用于民事目的，也可用于军事目的，或有助于提升军事潜力的货物、软件和技术。对机械设备、自动化系统、传感器、无人机、工业软件、半导体、先进材料、网络安全产品和能源设备企业而言，必须在交易前判断产品是否属于两用物项。

（三）网络安全

欧盟网络安全合规正成为企业安全合规的新核心。网络与信息安全第 2 号指令（NIS2 指令）建立了覆盖多个关键行业的欧盟网络安全统一框架，要求成员国加强对关键重要服务提供者的网络安全监管。其影响不只局限于 ICT 企业，也可能覆盖能源、交通、金融、医疗等传统企业。对于在捷克从事工业控制系统、能源设备、数据平台、供应链管理、智能制造和远程运维的企业而言，网络安全不再只是 IT 部门事务，而是关系到市场准入、客户审查、合同履行的综合事务。

（四）欧盟跨境数据安全

欧盟通用数据保护条例是直接适用于成员国的个人数据保护基本规则。欧盟数据保护规则包括个人数据在欧盟内外流动时的保护机制，数据跨境传输可通过标准合同条款和约束性公司规则等工具实现。在捷中国企业如果处理员工信息、客户数据、供应商联系人信息、网站用户数据、摄像头监控数据或项目现场人员信息，都必须将其纳入安全合规体系。

（五）职业健康安全和现场安全

欧盟对职业健康安全也提出较高要求。对中国工程承包、制造、仓储物流和设备安装企业来说，职业健康安全、工作场所风险评估、员工培训、工伤事故报告、非法用工防范和内部举报机制，都是企业安全合规的重要组成部分。尤其在工程项目和生产现场，安全合规不仅影响员工权益，也直接影响项目工期、业主评价、保险责任和监管处罚。

二、捷克本地制度：落实欧盟规则

捷克作为欧盟成员国，在安全合规领域具有明显的“欧盟规则本地执行”的特征。欧盟制定统一或协调性规则，捷克则通过国内法律、主管机关和行政程序加以落实。中国企业在捷克经营时，既要理解欧盟规则，也要掌握捷克本地的相关规定。

（一）国际制裁执行

在捷克，国际制裁执行由捷克金融分析办公室（简称FAÚ），承担协调职责。捷克金融分析办公室负责协调联合国、欧盟以及捷克本国的国际制裁措施的实施。捷克国际制裁执行的主要国内法依据是2006年的第69号法令（Act No. 69/2006 Coll., on the Implementation of International Sanctions）。该制度不仅适用于金融机构，也会通过银行支付、合同交易、海关监管、保险、物流和商业尽调传导至普通企业。

在捷的中国企业不直接面对欧盟委员会，其实际交易受到捷克本地监管和市场主体的共同约束。银行会审查收付款方是否在制裁名单上，物流公司会关注货物目的地和

最终用户，保险机构可能拒绝承保制裁相关业务，欧洲客户也会在供应商准入中要求制裁合规声明。

企业应特别关注以下几类场景：一是与俄罗斯、白俄罗斯、伊朗、朝鲜、叙利亚等国家相关的直接或间接交易；二是货物虽发往捷克或欧盟其他国家，但可能被转售、转运或再出口至受限制目的地；三是客户、股东、最终受益所有人、实际控制人、物流方、银行或保险方与制裁名单存在关联；四是合同履行过程中因新增制裁导致付款、交付、售后服务或技术支持无法继续履行；五是欧洲业主要求承包商、供应商或分包商出具制裁合规、最终用户和最终用途声明。

（二）两用物项出口管制

捷克工业和贸易部负责两用物项和技术的授权程序。其下属国际管制制度部门负责商业中涉及两用物项和技术的许可事项。

许多中国企业在捷克设立公司后，可能将捷克作为欧洲区域销售、仓储、售后、技术服务或再出口平台。如果捷克公司向欧盟外客户提供设备、零部件、软件升级、远程维护或技术资料，就可能触发两用物项出口管制。需要

特别注意的是，出口管制不仅限于有形货物，技术资料、软件、图纸、源代码、远程调试、云端传输和工程技术服务，也可能构成受控技术转移。

对中国企业而言，在捷克经营中可能出现以下受控场景：从中国向捷克出口受控设备或零部件；从捷克向第三国再出口设备、软件或技术；在捷克向欧盟或非欧盟客户提供受控技术服务；通过云端、电子邮件、远程调试或技术平台转移受控软件、图纸、源代码、工艺参数或控制程序；为敏感最终用户提供维修、升级、培训、调试或售后服务；经由捷克项目向其他国家转供可能被用于军事或安全用途的设备。

企业安全合规报告中应特别强调，两用物项判断不能只看商品名称，而要看技术参数、最终用途、最终用户和目的地。例如，同样是传感器、阀门、控制系统、工业软件、加密设备、无人机部件或高性能材料，是否受管制往往取决于具体技术指标和使用场景。

（三）反洗钱和客户尽调

捷克反洗钱制度与欧盟反洗钱框架相衔接，由捷克金融分析办公室负责。企业会通过银行开户、跨境收付款、

并购交易、房地产租赁、审计、会计、律师服务和客户尽调间接受到反洗钱法的约束。捷克银行通常会核验企业受益所有人、资金来源、业务模式、主要客户和交易目的。如果企业存在多层控股、离岸平台、复杂资金路径、现金交易、高风险国家客户或不透明最终受益所有人，银行和专业机构可能要求补充大量材料。

对中国企业而言，反洗钱合规的重点在于：清晰说明集团股权结构和最终受益所有人；保存资金来源和交易背景文件；避免不明第三方代付、代收或绕道付款；审查客户和供应商的公司背景、制裁风险和受益所有人；对大额交易、异常付款路径和高风险地区交易建立内部审批；在并购、资产购买、项目合作和代理分销中开展基础尽调。

（四）网络安全

捷克网络安全主管机关是国家网络与信息安全局（NÚKIB）。捷克新《网络安全法》已于 2025 年 11 月 1 日生效，其内容基于原有网络安全法，并满足网络与信息安全第 2 号指令的最低要求，从而将网络与信息安全第 2 号指令所要求的变化转化为法律。

对中国企业而言，网络安全合规应重点关注三个层

面：一是企业是否属于受监管实体，尤其是能源、交通、制造、数字基础设施、云服务、数据中心、工业系统运维和关键供应链企业。二是企业是否作为供应商向受监管实体提供 ICT 产品、远程维护、工业控制系统、数据服务或网络安全设备。三是企业是否涉及中国与捷克之间的数据传输、远程管理、系统接入、源代码维护或供应链安全审查。

即使企业未被直接列为网络与信息安全第 2 号指令或捷克网络安全法下的关键实体，也可能因成为欧洲客户、关键基础设施运营商或大型工业企业的供应商，而被要求提供网络安全证明、访问控制方案、事件响应机制、供应商安全承诺和数据处理说明。

（五）关键基础设施

捷克在关键基础设施保护方面也逐步加强制度建设。2025 年，捷克通过关于关键基础设施实体韧性的法律，用以转化欧盟关键实体韧性指令。其重点是确保能源、水务、交通、航空、医疗、数字基础设施等关键服务在重大风险、事故、自然灾害、网络攻击或供应链冲击下保持连续运行。

中国企业如果进入能源、水务、交通、通信、数据中

心、医疗、公共服务和大型工业设施领域，即使不是直接运营关键基础设施，也可能作为设备供应商、工程承包商、系统集成商或运维服务商被纳入安全审查范围。这类项目通常要求企业提交更详细的供应商信息、人员背景、技术方案、远程接入安排、应急预案和保密承诺。

（六）数据保护

捷克个人数据保护制度由欧盟通用数据保护条例与捷克国内法共同构成。捷克个人数据保护办公室（Úřad pro ochranu osobních údajů，ÚOOÚ）是数据保护监管机关。捷克《个人数据处理法》（Act No. 110/2019 Coll）是对欧盟通用数据保护条例、执法指令和旅客姓名记录指令等欧盟新法律框架的实施，并重建了捷克数据保护监督机构。

在企业经营中，个人数据安全场景非常广泛，包括：员工护照、签证、工作许可、工资、社保、考勤和健康信息；客户和供应商联系人信息；厂区门禁、视频监控和访客登记；网站、电子营销和客户服务数据；人事招聘简历和面试记录；项目现场人员名单、安全培训记录和事故报告；跨境向中国总部传输员工或项目人员数据。

企业应特别关注跨境数据传输问题。若捷克公司将员

工、客户或项目人员个人数据传输给中国总部或非欧盟系统服务商，需按照欧盟通用数据保护条例的第三国传输规则进行评估，必要时采用标准合同条款、补充安全措施和数据传输影响评估。

（七）职业健康与劳动监察

捷克职业安全合规（BOZP）关注工作安全与健康保护，而劳动监察体系则通过国家劳动监察局和区域劳动监察机构执行。劳动监察通过 8 个区域劳动监察机构开展工作，重点关注劳动关系、工作条件、非法就业、职业安全与健康等事项。如果怀疑雇主违反劳动法规，自然人或法人可向区域劳动监察机构或国家劳动监察局提交投诉。

对工程、制造、设备安装、物流和仓储企业而言，职业安全合规应覆盖：入场安全培训；风险评估；个人防护用品；高处作业、动火作业、吊装、焊接、电气作业许可；机械设备安全；化学品和危险物管理；工伤报告和事故调查；工作时间和休息制度；分包商安全管理；应急疏散和急救制度；职业健康检查和岗位适任性评估。

在捷克开展工程项目时，企业不能简单沿用中国项目现场管理方式。捷克和欧洲业主通常更强调书面风险评

估、培训记录、作业许可、个人防护、事故报告、分包商责任和现场文件留存。如果缺少书面记录，即使企业实际采取了措施，也可能在检查或争议中处于不利地位。

（八）危机管理与应急制度

捷克国家危机管理体系由内政部、消防救援系统、地方政府和相关主管机关协作执行。捷克消防救援部门关于危机管理的说明指出，其人口保护和危机管理部门承担国家行政任务，协调人口保护、危机管理、危机和应急计划以及危机状态下经济措施等事项。内政部关于紧急状态的说明还指出，政府有权宣布紧急状态，期限通常不超过30日，延长需经众议院同意。

企业虽不是政府危机管理主体，但在捷经营时应建立自身业务连续性和应急处置机制。特别是工程项目、制造企业、仓储物流、能源设备和跨境供应链企业，应准备火灾、洪水、网络攻击、停电、供应链中断、员工事故、公共卫生事件、交通事故、重大设备故障、社区投诉和媒体舆情等场景的应急预案。

三、企业适用场景：不同的合规要求

（一）贸易型和供应链企业

对于从事机械设备、汽车零部件、电子电气、消费品、工业材料、化工品、仓储和批发零售的企业，安全合规重点在于制裁筛查、最终用户审查、物流路线审查和供应链文件留存。企业应确认客户及其最终受益所有人是否被列入欧盟、联合国或捷克制裁名单，货物是否可能转售至受限制国家或受制裁实体，付款路径是否经过高风险银行或中间商。

这类企业容易忽视间接出口风险。即企业表面上只是向捷克或欧盟客户销售产品，但如果客户后续将产品转售至受制裁国家，并且企业明知或应知风险仍继续交易，可能被视为参与规避制裁。对于电子元器件、机床、工业软件、传感器、无人机部件、精密轴承、化工材料和运输设备，尤其需要加强最终用途声明和客户尽调。

（二）工程承包和项目型企业

工程承包企业在捷克面临的安全合规最复杂，通常同时涉及职业健康安全、分包商管理、施工现场安全、设备

进口、外籍员工许可、业主 HSE 审查、制裁条款、合同保函和事故责任。项目型企业应重点建立现场安全管理制度，包括安全培训、进入现场许可、动火作业、高空作业、起重作业、电气作业、个人防护用品、事故报告和分包商安全责任。

此外，工程企业常需从中国或第三国进口设备，并由中方工程师在现场安装、调试或指导施工。如果设备或控制系统涉及受控技术，或者中方人员远程访问欧洲业主系统，就需要同时判断出口管制、网络安全和数据访问风险。对参与能源、水泥、钢铁、化工、交通、水务、数据中心等项目的企业，还应关注关键基础设施和业主供应商安全审查。

（三）制造业和工业投资企业

制造业企业的安全合规重点在生产安全、职业健康、机械设备安全、消防、化学品管理、网络安全、供应链稳定和内部举报机制。汽车零部件、机械设备、电池、新能源、电子电气、材料和化工企业尤其要关注危险作业、生产设备维护、员工培训、工伤事故处理和外包人员管理。

如果企业的生产系统高度数字化，涉及工业控制系

统、远程运维、企业资源规划系统、客户数据、生产数据和供应商平台，还应建立网络安全和数据安全制度。对服务欧洲大型客户的制造企业，客户通常会通过供应商准入审查要求企业证明其网络安全、业务连续性、反腐败、制裁合规和供应链韧性。

（四）并购型企业

通过并购进入捷克的企业，安全合规重点在并购前尽调和并购后整合。尽调阶段应重点审查目标公司是否存在制裁交易、出口管制违规、职业安全事故、未决劳动监察、重大工伤、网络安全漏洞、数据泄露、反洗钱问题、内部举报案件、环保事故和供应商黑名单风险。

并购完成后，中国母公司不能只关注财务报表和业务协同，还应建立与捷克本地制度相匹配的集团合规控制体系。尤其要尊重目标公司原有客户、员工和合规流程，避免因管理方式突变导致员工流失、客户担忧或监管关注。

（五）科技、数据和关键供应商企业

ICT、云服务、数据中心、网络安全、AI、工业软件、半导体、通信设备、卫星、无人机和远程运维企业，应重

点关注网络与信息安全第 2 号指令、捷克网络安全法、关键基础设施供应商审查、数据传输和远程访问安全。此类企业在捷克经营的核心风险，不仅是产品能否销售，还包括是否被客户、监管机构或公共采购程序视为高风险供应商。

如果企业为能源、交通、医疗、政府、金融、通信或大型工业客户提供系统、软件、设备或维护服务，应提前准备供应链安全说明、数据访问边界、远程维护制度、源代码和漏洞管理政策、网络事件响应机制以及客户审计材料。

四、安全合规重要事项提示

（一）查明最终受益人和最终用途

许多企业在制裁合规中只查询直接客户名称，但没有识别客户背后的实际控制人、最终受益所有人、中间贸易商和实际收货人。对于绕道贸易风险较高的货物，仅查直接买方远远不够，还应确认最终用户、最终用途、收货地点、运输路线和付款主体。

（二）并非军品才受管制

两用物项并不等于军品。工业设备、软件、芯片、传感器、无人机部件、加密产品、化学材料、激光设备、数控机床和测试设备，都可能具有两用属性。企业如果只按普通民用产品处理，可能忽视许可要求和技术转让限制。

（三）重视技术服务的出口管制

出口管制不仅针对实物货物。图纸、软件、源代码、技术手册、远程调试、云端访问、工程指导和售后技术服务，也可能构成受控技术转移。中国企业在捷克提供远程

运维和技术支持时，应特别关注技术传输方向和访问权限。

（四）备齐合规文件

捷克银行和欧洲客户可能要求企业提供股权结构、受益所有人、资金来源、制裁筛查、供应商声明和反洗钱材料。如果企业没有提前准备，可能导致开户延迟、付款受阻、合同签署推迟或客户准入失败。

（五）网络安全重在平时

网络与信息安全第 2 号指令背景下，网络安全已经成为企业治理问题，而不是单纯技术问题。企业需要管理层负责、资产识别、风险评估、供应商管理、访问控制、事件响应、备份恢复和员工培训。如果只在客户审计前临时补文件，难以满足欧洲大型客户或监管机构要求。

（六）安全要求不匹配

工程企业在捷克需要严格遵守工时、休息、劳动合同、职业安全、现场风险评估和分包商管理要求。未经培训上岗、缺少个人防护用品、工时记录不完整、危险作业审批不足、工伤事故报告不及时，都可能引发监管处罚和业主

索赔。

（七）重视分包商风险

在工程、物流和制造外包中，企业常认为分包商人员安全、非法用工或现场事故由分包商自行负责。但在欧洲业主和捷克监管体系下，总包、项目管理方或实际控制现场的一方，仍可能承担监督、协调和连带风险。因此，分包商安全准入、合同安全条款和现场安全培训必须纳入企业合规体系。

（八）建立内部举报机制

如果企业没有内部举报渠道，员工对工资、工时、安全、歧视、腐败、环保或合规问题的不满，可能直接转向监管机关、媒体、客户或法院。对于中资企业而言，内部举报机制不仅是法律合规要求，也是提前发现风险、降低声誉损害的重要工具。

五、建议

（一）进入捷克前：安全风险预评估

企业在进入捷克前，应先完成以下判断：第一，业务是否涉及受制裁国家、实体、个人或高风险地区；第二，产品、软件、技术和服务是否可能属于两用物项；第三，客户是否为能源、交通、医疗、通信、金融、政府、国防、数据中心或其他关键行业；第四，企业是否可能被纳入NIS2 或捷克网络安全法监管范围；第五，项目是否涉及关键基础设施或公共采购安全审查；第六，是否需要派驻中方员工或使用本地分包商；第七，是否存在高风险作业、生产安全、危险化学品或大型设备安装风险；第八，是否需要建立举报人保护和内部合规渠道。

（二）交易前：制裁和出口管制筛查

每一笔高风险交易前，企业应执行以下流程：识别直接客户、最终用户、实际收货人、付款方和中间商；筛查欧盟、联合国和捷克相关制裁名单；核实最终受益所有人和控制关系；判断货物、软件或技术是否属于两用物项；收集最终用户声明和最终用途声明；审查运输路线、交货

地点和转售风险；判断是否需要向捷克工业和贸易部申请出口许可；在合同中加入制裁、出口管制、不得转售、信息披露和终止条款；保存筛查记录、客户声明、合同和物流文件。

（三）项目启动前：现场安全和用工合规准备

工程、制造和设备安装企业在项目启动前，应完成：现场风险评估；安全管理计划；HSE 责任分工；分包商安全准入审查；员工安全培训；个人防护用品发放记录；高风险作业审批制度；工伤事故报告流程；外籍员工许可和工作范围核验；劳动合同和工时制度检查；消防和应急预案；保险安排和业主 HSE 要求对接。

（四）运营期间：网络安全和供应链安全管理

企业进入正常运营后，应建立持续安全管理制度：识别关键系统、数据和工业控制设备；建立访问权限管理和账号管理；对远程运维和跨境访问进行审批；建立备份、恢复和业务连续性计划；制定网络安全事件报告流程；对关键供应商进行安全审查；定期开展员工网络安全培训；保存安全日志和客户审计资料；与欧洲客户约定事件通报

和责任边界。

（五）风险事件发生后：响应和报告

一旦发生制裁命中、货物扣押、网络安全事件、严重工伤、举报事项、客户安全审计失败或监管调查，企业应立即采取以下措施：暂停相关交易或作业；保存证据和沟通记录；通知内部合规负责人和管理层；联系捷克本地律师、税务或安全顾问；按法律要求向主管机关报告；与客户、银行、保险公司和业主协调；采取补救措施；形成事件复盘报告；更新内部制度和培训内容。

六、安全合规所需材料

（一）制裁和出口管制文件

客户尽调表；供应商尽调表；最终用户声明；最终用途声明；制裁名单筛查记录；受益所有人识别文件；产品分类和 HS 编码；两用物项分类判断记录；出口许可证申请材料；合同中的制裁和出口管制条款；物流、清关和交付文件；异常交易审批记录。

（二）反洗钱和银行客户尽职调查文件

公司股权结构图；最终受益所有人说明；资金来源说明；主要客户和供应商说明；业务模式说明；董事和授权签字人资料；跨境付款合同；银行开户文件；重大交易背景说明；集团内部交易说明。

（三）网络安全文件

IT 资产清单；关键系统清单；网络安全风险评估；访问权限管理制度；远程运维审批记录；数据备份和恢复方案；网络事件响应预案；供应商安全审查表；客户安全审计材料；员工网络安全培训记录；日志留存和漏洞修复

记录。

（四）职业健康安全文件

工作场所风险评估；HSE 管理计划；安全培训记录；个人防护用品发放记录；特种作业资格文件；高风险作业审批单；设备检查和维护记录；消防和应急预案；工伤事故报告；分包商安全协议；现场安全检查记录；劳动监察应对资料。

结　语

当前，捷克营商安全合规的核心是：企业在捷克经营时，安全风险不再是单点风险，而是跨越交易、资金、技术、人员、数据、供应链和现场管理的复合风险。对于中国企业而言，最容易出问题的地方往往不是完全不知道某项制度，而是低估了不同制度之间的联动关系。例如，制裁合规会影响客户选择、合同履行、银行付款和物流；出口管制会影响设备、软件、技术资料和售后服务；网络安全会影响生产连续性、远程运维和客户信任；数据保护会影响员工管理和中国总部管控；职业安全会影响项目进度、劳动监察和企业声誉；分包商安全会影响总包责任和业主评价。

因此，中国企业在捷克经营应建立交易前筛查、合同中控制、执行中记录、事件后可追溯的安全合规体系。对于工程、制造、能源、ICT、设备供应、物流和并购型企业而言，安全合规不应作为辅助事项，而应纳入进入捷克市场前的商业决策、项目报价、合同谈判和组织管理之中。

只有将欧盟规则、捷克本地制度和企业内部流程有效衔接，才能真正降低境外经营中的法律、安全和声誉风险。

杨睿（上海外国语大学俄罗斯东欧中亚学院、上海全球治理与区域国别研究院）

联系地址：淮海中路 622 弄 7 号 308 室

联系电话：021-33165460

联系邮箱：zbzh@sh-popss.gov.cn