Beisen北森 | HANKUN

中企出海
人力资源管理
数据合规白皮书
（2024版）

目录 CONTENTS

PART

01

趋势引领未来：
中企出海的新挑战与新机遇

探索未知，拥抱未来：全球化浪潮下的中企出海局势

随着全球百年未有大变局的加速演进，时代的风口之下，越来越多的企业以前所未有的决心扬帆出海，在全球探索新的机遇。回顾过去一年，在中国技术革新、能源转型和产业升级的新趋势下，一批批出海的先行者以创新的生命力，开拓出一片全球化的广阔天地。

据商务部、外汇局统计，2024 年 1~8 月，我国全行业对外直接投资 7894.5 亿元人民币，同比增长 12.5%。其中，非金融类直接投资累计 6692.4 亿元人民币，增长 14.3%。

2024 年上半年，上市公司实现海外业务收入 3.83 万亿元，同比增长 12.84%，增长率提升 9.93 个百分点。电气、电子及通讯、木材、家具、科学研究和技术服务业等行业海外业务收入份额较高，达 25% 以上。这些均显示出中国企业出海取得了显著成效。

这一次中国企业走向国际市场，也表现出了时代的特点。首先，这些企业在选择海外市场时更加注重市场潜力和行业发展趋势，不再仅仅局限于传统的贸易伙伴。其次，他们在进入新市场时，更加注重本土化策略及产业链的构建，以更好地适应当地文化和市场需求。此外，中国企业在本次全球化过程中，更加注重品牌建设和知识产权保护，努力提升自身在国际市场上的竞争力和影响力。最后，他们表现出了更强的灵活性和应变能力以应对国际贸易环境变化。

跨越国界的人力资源数据合规挑战：中企出海的新课题

当下的中企出海不仅是全球化，更要尊重各地本土化。然而一些企业往往容易陷入误区，带着固有的认知去海外经营。这种思维方式导致他们在海外运营常常会面临一些棘手的问题。

而在这其中，人力资源数据合规挑战已成为出海企业不可回避的关键命题。它不仅关乎企业的法律风险防控，更是企业稳健前行、赢得国际市场竞争力的核心要素。以下是出海企业会高频遇到的一些数据合规挑战：

法规遵循的挑战：

随着欧盟的《通用数据保护条例》（GDPR）、中国《个人信息保护法》及《数据安全法》等相关法律法规的出台，出海企业在数据处理方面需遵循更为严格的法律要求，涉及数据的收集、存储、使用、共享和销毁等各个环节。同时，不同市场间的合规差异也增加了企业的适应难度，如欧盟、美国、新加坡等地均有各自的数据保护法规，出海企业需要在全球范围内确保合规。

人力资源管理的数据合规挑战：

在招聘、入职、绩效管理等环节，企业需收集大量员工个人信息，这些信息的处理必须合法合规，尤其是敏感信息如生物识别、医疗健康等，一旦泄露将对个人权益产生重大影响。此外，内部数据管理流程也是关键，员工数据保护意识不足、系统漏洞、恶意攻击等都可能导致数据泄露。

技术发展的挑战：

随着云计算、大数据、人工智能等技术的快速发展，使得企业在处理人力资源数据时面临更多的技术难题。如何在合规的前提下高效应用新技术，以及不断更新和迭代的数据隐私保护技术，如加密、访问控制、匿名化处理等，都给企业带来了额外的技术挑战和成本投入。

出海启航：解锁中国企业人力资源数据合规密码

即便当前中企出海的热潮正以前所未有的势头席卷全球，众多企业在涉足陌生的海外市场时，面对纷繁复杂的政策体系与法律环境，依然会感到困惑与迷茫。

尤其在如何妥善处理各类合规问题上，这些企业往往缺乏足够的经验与策略，导致在国际化进程中步履维艰。更令人担忧的是，一些企业将合规管理简化为在本地部署一套软件，认为这样就能轻松满足所有合规要求。这种简单的做法，显然未能触及合规管理的本质与核心，更无法真正解决企业在出海过程中可能遭遇的各种合规挑战，反而将公司置于更大的合规风险中。

为了帮助中国企业更好地应对这一困境，我们策划并发布这份白皮书。这份白皮书旨在为中国企业提供指导与帮助，使其能够迅速识别并有效应对在出海过程中可能遇到的合规挑战。通过深入了解海外市场的政策与法律环境，企业将能够更快地适应新的市场环境，在全球化发展的道路上稳健前行。

PART

02

出海企业人力资源管理数据合规场景及挑战

出海企业人力资源管理数据合规场景及挑战

欧盟《通用数据保护条例》(General Data Protection Regulation，“GDPR”) 于 2018 年 5 月生效，其后，巴西、中国、泰国、越南等多国均加快了本国数据安全方面法律的立法节奏，中国企业当下的出海浪潮恰好在这样的背景下出现。这就对出海企业的人力资源管理提出了一个挑战：在全球化人力资源管理的同时，能够符合不同国家的个人数据安全法规和政策。

人力资源管理，管理的对象是人，而与人相关的个人信息及其他信息（统称“数据”）是人力资源管理过程中必然涉及的要素，例如招聘时收取应聘者简历，即是数据“收集”；向员工支付工资时，产生对员工银行账户信息的“使用”；发生劳动纠纷向仲裁机构或法院递交的证据材料，构成对员工相关信息的“向第三方提供”。企业进行人力资源管理的动作，无不交织着数据处理动作，因此除需遵守劳动用工相关法规外，还需遵守数据合规的相关法规。

中国企业出海成为跨国型集团公司后，增加了集团总部与分子公司之间，为了实现管理目的而不可避免的数据流动场景，例如海外招聘场景下，在总部参与人事聘用决策时，海外分子公司需将相应应聘者数据提供给位于中国的总部进行处理；集团对员工薪酬统一管控场景下，位于中国之外的分子公司自行招聘、管理的员工信息也需提供给中国总部进行薪酬管理；跨国公司通常使用一套人力资源管理软件，该软件的服务器可能在总部或者分子公司所在的国家 / 地区，则整个集团的人力资源管理数据均存在跨境传输及存储的问题。

实际上，除了人力资源管理软件外，出海企业办公中使用电子邮件、即时通讯 IM、公司通讯录等工具也有可能带来个人信息的跨境传递，同样构成个人数据跨法域流动问题。以上数据跨法域流动，使得出海企业除了遵守目的地国家 / 地区数据合规相关法规外，还需考虑遵守数据入境国家 / 地区数据合规相关法规。

因此，出海企业把人力资源管理动作拆解并抽象为对应的数据处理行为，有助于更好的识别本企业人力资源管理场景下具体产生了哪些数据处理行为，涉及哪些数据，从而明确企业应该匹配哪些数据合规动作。目前越来越多的中国出海企业选择扩大目的地国家 / 地区本土化团队规模来代替大量人员外派，因此，本白皮书重点以“员工当地化”的出海模式为模型，讨论出海企业在人力资源管理中将面临的数据合规问题。

以下列举部分人力资源管理场景中的数据处理行为，以便于基于场景理解数据合规面临的问题和挑战：

(1) 人员招聘过程中，涉及个人信息收集使用、存储删除、跨境传输等数据合规问题

人员招聘过程中企业收取应聘者简历是人力资源管理场景中，收集个人信息的主要入口；企业自行对应聘者进行背景调查时，从公开渠道或应聘者自行提供的渠道获取的应聘者简历以外的个人信息，也是企业收集应聘者数据的又一入口，依法收集是后续数据合规处理的源头。人员招聘过程中面试官阅读应聘者简历、面试时与应聘者讨论其简历等，是招聘场景下对数据使用的主要方式。企业需关注不同国家 / 地区对何为依法收集使用的限定。

如招聘失败，企业涉及是否可继续留存、使用应聘者简历，或需要何时删除应聘者简历问题。

如企业用于存储应聘者简历等个人信息的服务器位于应聘者所在国家 / 地区之外，或集团中 A 公司评估该应聘者更适合 B 公司招聘的岗位因而将应聘者简历推荐给位于与 A 公司不在同一个国家 / 地区的 B 公司时，或集团中 A 公司通过邮件形式将应聘者简历发送给总部评估时，都会导致应聘者个人信息跨境流动，则应满足数据跨境传输的合规要求。

（2）用工管理过程中，涉及个人信息收集使用、跨境传输等数据合规问题

招聘成功后，企业可依法向员工进一步收集除简历信息之外的个人信息，用于人力资源管理所必需的目的，以中国法为例，如用于签署劳动合同的身份证信息、用于支付工资的银行账户信息、用于为员工缴纳社保的社保账户信息等；企业对员工进行假勤管理过程中，可收集员工的打卡信息，员工请休病假、婚假等假期时，企业可向员工收集医院病假证明、结婚证明等必要的证明材料信息；企业对员工进行绩效、薪酬管理过程中，可收集员工的绩效信息及薪酬、社保、个税等信息；

企业用于存储员工个人信息的服务器或为企业提供人力资源服务的供应商的服务器位于员工所在国家 / 地区之外这样大的管理框架下，或企业集团总部统一向各分子公司员工配发期权等激励这样具体的管理场景下，均会产生员工个人信息跨境存储或流动，应满足数据跨境传输的合规要求。

（3）员工离职后，涉及个人信息使用、存储删除等数据合规问题

员工离职后，企业需依员工所在国家 / 地区法律规定，及时删除员工数据，或依法继续保存员工部分数据，并仅限于法律规定的范围内使用，如以中国法为例，企业与离职员工签署了竞业限制协议时，在该协议履行期限内，企业可不删除履行该协议所必需的信息，但也仅可为履行该协议而使用，不得转作他用，例如向该离职员工发送广告信息等。

（4）员工作为个人信息主体的权利响应合规问题

员工在发现企业违法收集、使用其个人信息，或企业应当依法删除其个人信息而没有删除等情形时，有权向企业提出停止、拒绝相应行为或删除其个人信息等要求，企业需依法予以及时响应。

（5）人力资源管理各阶段均涉及数据安全保障合规问题

企业在员工入、转、调、离整个人力资源管理场景下，均需采取必要的组织、制度、技术措施，保障应聘者及员工的个人信息安全。例如：任命数据隐私官或数据保护官，建立相关流程、以及对员工的权利做出响应，开展个人数据保护影响评估、报告数据泄漏等。

可见，中国企业出海，在人力资源管理数据合规方面，应重点了解目的地国家 / 地区在个人信息收集使用、存储删除、数据跨境、个人权利响应、安全保障义务等方面的法律法规，以防范可能产生的管理风险，建立一套支持企业多国家、跨区域运营的人力资源管理数据合规体系，提升企业的运营效率，为企业向其他国家或地区拓展业务提供良好的底层基础和支撑。

PART

03

人力资源管理数据合规的五大关键

个人信息收集、使用的合规处理

个人信息及敏感个人信息的定义

不同法域对个人信息的定义相近，多数都强调个人信息的可识别性特征，即能识别特定个人的信息是个人信息，很多国家在可识别性特征之外，又对个人信息进行了部分列举。

不同法域对敏感个人信息的定义不同，但多数法域的敏感个人信息（在部分法域称为“特殊种类的个人数据”等，以下统称敏感个人信息）包括为揭示种族或民族出身、政治观点、宗教或哲学信仰以及工会成员的个人数据，以及以唯一识别自然人为目的的基因数据、生物特征数据，自然人的健康、性生活或性取向数据等。下表为部分国家对个人信息和敏感个人信息的界定：

国家 / 地区		敏感个人信息
东南亚	泰国	没有明确提出“敏感个人数据”的概念，但是对部分特殊数据的处理进行了限制，包括种族、民族、宗教信仰、政治观念、性行为、犯罪记录、健康数据、残疾状况、所属贸易联盟、基因数据、生物识别数据或者任何以泰国数据保护监管机构认定方式影响信息主体的数据
	马来西亚	包括有关信息主体的身体或精神健康状况、政治观点、宗教信仰或其他类似信仰、犯罪记录相关信息，或主管部门确定的任何其他个人数据
	新加坡	未单独定义敏感个人数据，但以列举方式规定了需加强保护水平的个人数据类型，包括新加坡国民身份证号码（NRIC）及其他身份证件号码、财务性质个人数据、保险信息、个人不良行为的历史记录、敏感医疗健康信息、未成年人个人数据
欧盟	欧盟	包括显示种族或民族背景、政治观念、宗教或哲学信仰或工会成员的个人数据、基因数据、为了特定识别自然人的生物性识别数据、以及和自然人健康、个人性生活或性取向相关的数据
中东	阿联酋	包括任何直接或间接揭示自然人的家庭、种族出身、政治或哲学观点、宗教信仰、犯罪记录、生物特征数据，或与该人的健康、身体、心理、精神、遗传或性状况有关的任何数据，包括与其健康状况相关的医疗服务信息
	沙特	除欧盟涉及的敏感个人数据外，还包括揭示个人“部落起源”的数据、表明某人可能是非婚生或被收养的数据

非洲	肯尼亚	包括种族、健康状况、宗教信仰、财产状况、婚姻状况、家庭详情、性取向等数据
中亚	哈萨克斯坦	未明确定义敏感个人信息，但定义了“生物特征数据”指表征个人信息主体生理和生物特征的数据，并根据可访问性将个人数据分为公开个人数据和受限访问的个人数据
北美	美国	• SSN(社保号)、驾驶执照、州身份证或护照号码 • 消费者的登录账户、金融账户、借记卡或信用卡号码，并结合任何必要的安全或访问代码、密码或允许访问的凭证 • 精确的地理定位 • 种族或民族出身，宗教或哲学信仰，或工会会员资格 • 消费者邮件、电子邮件和短信 • 发送给公司之外其他人的信息沟通 (如邮件、短信) 的具体内容 • 基因数据 • 为识别个人的目的处理的生物识别信息 • 有关消费者健康的个人数据 • 有关消费者的性生活或性取向的个人数据
南美	巴西	包括健康状况、种族或民族起源、宗教信仰等数据

(表一)

人力资源管理中个人信息收集、使用的基本原则

大多数国家或地区的法律要求仅当满足特定法律规定的条件时才可以收集和使用个人信息，这些条件通常以获得个人信息主体的同意为主，同时规定了不需要获得同意即可收集、使用个人信息的例外情形，常见的例外包括为订立或履行合同所必需、法律授权或为履行法定义务所必需、收集和处理已公开的个人信息、为追求合法利益所必需等。

对于敏感个人信息的收集和使用，除需要满足法律针对个人信息所规定的条件外，部分法域规定了更为严格的处理条件，通常体现为更严格的同意条件、限缩不需要获得同意即可收集及使用的例外情形、需要履行额外的合法义务等。

在人力资源管理场景下，招聘过程中收集的应聘者简历通常为一般个人信息，而招聘成功后，用工管理过程中，难以避免会收集到员工敏感个人信息，因此需要分别考虑其合规路径。以下为部分国家 / 地区关于收集、使用应聘者、员工个人信息合规路径的对比：

国家 / 地区		收集使用应聘者个人信息合规路径	收集使用员工个人信息合规路径
东南亚	泰国	仅能通过获得应聘者同意的方式收集、使用其个人信息	• 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括履行劳动保护、社会保障和社会保护相关义务所必需的数据；履行劳动合同、保密协议、竞业限制协议等必需的数据；实现雇主的合法利益所必需的数据） • 收集员工其他个人信息需取得员工明示同意（可以书面或电子签名的方式）
	马来西亚	仅能通过获得应聘者同意的方式收集、使用其个人信息	• 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括依据就业相关法规及履行劳动合同所必需的数据） • 收集员工其他个人信息需取得员工同意（需要在确保告知内容完整情形下做出同意，且形式可记录，员工可随时撤回其同意）
	新加坡	建议通过获得应聘者同意的方式收集、使用其个人信息	• 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括员工的住址、身份证件号码、出生日期、性别、开始雇佣日期、结束雇佣日期、工作时长、休假记录、薪水记录信息、为管理或结束雇佣关系的信息） • 收集员工其他个人信息需取得员工同意 • 除法律规定的收集、处理情形外，企业在收集新加坡国民身份证号码 (NRIC) 及其他身份证件号码时必须遵守严格的必要性限制，仅在必须“以高保真度准确确定或验证个人身份”时才能收集、处理身份证号码信息
欧盟	欧盟	建议通过获得应聘者同意的方式收集、使用其个人信息（在 GDPR 规定的几项合规路径中，招聘场景采用获得应聘者同意的路径更加可行）	• 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括履行雇佣合同所必需的数据；企业为履行人力资源管理过程中法定义务所必需的数据；企业为维护自身合法利益所必须的数据） • 在慎重证明员工不同意也不会给其造成任何不利后果的前提下，可通过取得员工同意的方式收集员工个人信息

中东	阿联酋	通过获得应聘者同意的方式收集、使用其个人信息（同意应当以清晰、简洁的语言以及易于获取的方式作出，应聘者可以随时撤回同意）	● 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括评估员工工作能力所必需的数据；为履行就业、社会保障或社会保护相关法律项下的义务或行使有关权利所必需的数据；履行劳动合同、保密协议、竞业限制协议等必需的数据） ● 收集员工其他个人信息需取得员工同意
	沙特	○ 一般通过获得应聘者同意的方式收集、使用其个人信息 ○ 极特殊情况下如依法收集应聘者年龄以履行避免雇佣童工义务时可不取得应聘者同意	● 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括履行劳动合同、保密协议、竞业限制协议等必需的数据、履行用人单位法定义务所必需的数据） ● 收集员工其他个人信息需取得员工同意，如为敏感个人数据则需员工明示同意
非洲	肯尼亚	○ 需通过获得应聘者同意的方式收集、使用其个人信息 ○ 除非企业意向与应聘者签订雇佣合同，否则即使应聘者同意，也不得要求应聘者提供有关部门或机构出具的无犯罪证明或合规证明	● 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括员工的姓名、年龄、性别、职业、入职日期、国籍和学历水平信息；企业履行法律义务必须的数据、履行劳动合同、保密协议、竞业限制协议等必需的数据） ● 收集、使用敏感个人数据应充分向员工告知敏感个人数据处理、跨境传输（如有）的情况并取得同意，并开展数据保护影响评估
中亚	哈萨克斯坦	仅能通过获得应聘者同意的方式收集、使用其个人信息	● 无需取得员工同意可直接收集、使用为员工设立养老金账户的信息 ● 收集员工其他个人信息需取得员工同意
北美	美国	一般应当通过隐私政策等方式告知应聘者企业收集、使用其个人信息情况	一般应当通过隐私政策等方式告知员工企业收集、使用其个人信息情况，如涉及敏感个人信息，对隐私政策告知内容有特别要求
南美	巴西	○ 除非存在其他符合法律规定的例外情形，一般通过获得应聘者同意的方式收集、使用其个人信息 ○ 即使获得了应聘者同意，也不得为建立雇佣关系而要求应聘者提供与绝育或怀孕状态相关的证明、声明、检查报告等	● 在满足最小必要原则的前提下，无需取得员工同意即可直接收集、使用人力资源管理中所必需的个人信息（包括姓名、出生日期、地址、教育程度、国籍、工资、休假等信息） ● 收集员工其他个人信息需取得员工同意 ● 即使获得了员工同意，也不得为建立或延续雇佣关系而要求员工提供与绝育或怀孕状态相关的证明、声明、检查报告等

（表二）

从上表可以看出，多数法域下，对于收集、使用应聘者个人信息通常以取得应聘者的同意为合规路径；而对于收集、使用员工个人信息，在大多数法域内可依据人力资源管理所必需对员工信息进行处理，或取得员工同意收集使用个人信息两个主要的合规路径，因此建议出海企业：

- 对于应聘者，可通过取得其同意的方式收集使用其个人信息；
- 对于员工，可依据“人力资源管理所必需”的原则直接收集使用其个人信息，收集使用超过“人力资源管理所必需”范围外的个人信息，需取得员工同意。

在确定收集、使用的合规路径基础之上，如何确保企业已真实、有效地落实了合规动作，如何有效的“取得同意”、如何判断哪些信息是“人力资源管理所必需”的信息，是人力资源管理场景下的重难点之一。

人力资源管理中个人信息收集、使用的合规处理

对于依赖同意作为合规路径的情形，合规动作应重点考量“取得同意”的有效性。在收集使用应聘者个人信息及收集使用员工非人力资源管理场景必需的个人信息时，落实“取得同意”通常可采取要求应聘者或员工签署知情同意书的方式进行。由于有些法域对“有效同意”设置了具体要求，例如告知充分、自由自愿给予、针对特定目的、明确且具体、不得捆绑、不得欺骗胁迫、可便捷撤回等，因此知情同意书需设置相应的内容以满足该国充分、具体等告知要求；以员工自主线下书面签署、电子签署、线上勾选同意等方式进行签署，以满足该国自愿、明确等同意要求。

建议跨国集团企业按照全面详述收集应聘者或员工何种个人信息、收集使用的目的、方式、保存期限、是否会提供给第三方、是否涉及数据出境（如涉及，其可能的接收方）等内容，并由应聘者或员工线下签署或电子签署，以适配全球多地关于“取得同意”的合规路径要求。

对于依赖其它非同意作为合规路径的情形，合规动作应重点考量是否遵循了最小必要原则，是否为人力资源管理中所必需的信息。从表二所列国家收集使用员工个人信息合规路径的内容中可以看出，不同法域下人力资源管理中可能涉及处理的信息大致有以下几类：

人力资源管理中必需的信息	信息举例	参考国家	收集使用合规路径
订立及履行人力资源管理中劳动者作为一方当事人的合同所必需的信息	如为签署、履行劳动合同等人力资源管理所需的合同的信息	泰国、马来西亚、欧盟、阿联酋、沙特、肯尼亚、中国	在对应国家无需取得员工同意，可直接收集使用（但需注意的是，部分法域在使用合法利益这一合法性基础时，需在使用前开展平衡测试）
履行雇主法定义务所必需的信息	如中国法下为履行代扣个税、代缴社保等法定义务所必需的信息	泰国、马来西亚、欧盟、阿联酋、沙特、肯尼亚、中国	
为维护雇主合法利益所必需的信息	如雇主出于安全原因安装门禁记录员工进出工作场所的信息	泰国、欧盟	

非人力资源管理中必需的信息	信息举例	参考国家	收集使用合规路径
除上述人力资源管理中必需的信息外的所有信息	如中国法下收集员工全部家庭成员个人信息即非必需信息	中国	需取得员工同意

（表三）

上表从框架上界定了何为人力资源管理中必需的信息，但在实操中，并未有哪个国家的法律从字段级规定究竟何为人力资源管理中必需的信息。

因此，需要结合该国劳动用工相关法律的规定及人力资源管理场景，对“必需的信息”做限缩解释。一个判断标准为，如不收集员工的某项信息，依法或依据劳动合同必须进行的某项管理动作是否即无法进行，如回答为是，则该信息为必需的信息，如回答为否，则该信息非必需的信息。

例如在招聘场景下，收集应聘者的银行账号通常是非必需的，如收集则违反最小必要原则，即使经过应聘者同意也不应收集；而对于在职员工，为履行为其发放薪资的法定及劳动合同约定的义务而收集其银行账号则为必需的，不经员工同意也可以收集，此种场景下，通常收集一名员工一个银行账号即可实现发放薪资的目的，企业如想收集员工多个银行账号，同样违反了最小必要原则，即使经过员工同意也不应收集。

又如企业以订立或履行劳动合同所必需为基础处理员工个人信息，则应当确保处理个人信息的目的、方式、范围均为履行劳动合同所必需，不存在超出必要范围处理的情况。企业基于发放薪资等目的处理员工的薪酬信息通常为履行劳动合同所必需，而企业在办公区域内拍摄宣传视频将部分员工摄录入画面中，此行为则可能已超出为履行劳动合同所必需的范围，需要考虑通过取得员工同意的合规路径来实现。

跨境传输个人信息的合规处理

以 GDPR 为代表，大多数法域均规定了跨境传输个人信息的合规路径，通常约束数据控制者仅能将个人信息传输至与本法域提供同等保护水平的国家，并在此基础上规定相应的例外情形。针对如何衡量“提供同等保护水平”，各法域的标准不尽相同。其中，以GDPR为例，“提供同等保护水平”包括经过充分性认定的国家(“白名单”)、提供“适当的保障措施”。“适当的保障措施”则包括如下：

（1）基于公共机构之间具有约束力和可执行力的协议进行跨境转移；
（2）制定有约束力的公司规则（BCRs）且该 BCRs 获得了数据保护机关的批准；
（3）数据出口方与数据进口方签署了标准合同条款（SCCs）；
（4）基于经批准的行为守则（code of conduct）进行转移；
（5）基于经批准的认证机制进行转移。

类似地，其他法域在考量是否“提供同等保护水平”时，也多采取白名单机制、签订数据跨境传输合同等。特别地，东盟仿照 GDPR 标准合同条款的形式发布了东盟合同条款（MCCs）供数据控制者跨境转移个人信息时自愿采用。

基于上述，企业在人力资源管理场景下需跨境传输个人信息时，需首先建立个人信息跨境传输的合规路径，避免违规传输的情形。以下为部分国家 / 地区跨境传输应聘者、员工个人信息及敏感个人信息合规路径对比：

国家 / 地区		本地存储要求	跨境传输合规路径	参考实践
东南亚	泰国	没有明确的数据本地化要求	泰国的数据跨境传输机制： • 向具有充分数据保护水平的白名单国家传输：建立了该机制但尚未公布国家名单 • 具有约束力的公司规则 (“BCR”)：关联公司间可制订集团的 BCR 并经泰国数据保护监管机构批准后进行传输 • 适当保障措施：包括签署标准合同条款 (“SCC”)、依据认证及国家间条约或协议进行跨境传输 • 例外情形：存在以下例外情形时，亦可进行跨境传输，主要包括：法律要求转移；已取得信息主体有效同意，在转移到不具备充分保护水平的国家时确保个人信息主体充分知情；为履行信息主体作为一方当事人的合同所必需；为防止或消除对个人生命健康的危险；为实现重大公共利益传输	实践中出海泰国的企业通常选择签订标准合同条款的方式，将其个人信息传输、存储至泰国境外。如签署标准合同条款较为困难的，企业亦可选择取得应聘者或员工充分知情同意，以进行跨境传输

	马来西亚	没有明确的数据本地化要求	马来西亚《PDPA 修正案》（尚未生效）删去了原则上不允许跨境传输的限定，一定程度上放宽了对跨境传输的监管要求： • 开展跨境传输影响评估前提下，可向提供同等保护水平的国家和地区传输 • 通过制订具有约束力的公司规则（“BCR”）；签订标准合同条款（“SCC”）；认证进行传输 • 例外情形：存在以下例外情形时，亦可进行跨境传输，包括信息主体同意，同意以书面通知为前提，且形式可被留存记录；履行信息主体作为一方的合同所必要；为保护信息主体重大利益所必需等	实践中出海马来西亚的企业通常选择签订标准合同条款的方式，将其个人信息传输、存储至马来西亚境外。如签署标准合同条款较为困难的，企业亦可选择取得应聘者或员工充分知情同意，以进行跨境传输
	新加坡	没有明确的数据本地化要求	新加坡原则上禁止个人数据跨境传输，但满足下列条件之一可以跨境传输： • 接收方受到同等保护水平法律管辖 • 签订数据跨境传输协议要求接收方履行同等保护义务 • 集团内制定有约束力的公司规则（“BCR”） • 取得特定数据保护认证等 • 特定情形下可认为组织已满足适当保护要求，包括取得个人的同意或视为同意，及基于个人合法利益或国家利益所需，且已采取合理措施避免接收方用于其它目的	实践中出海新加坡的企业通常选择签订数据跨境传输协议的方式，将其个人信息传输、存储至新加坡境外。如签署数据跨境传输协议较为困难的，企业亦可选择取得应聘者或员工的同意或视为同意，以进行跨境传输
欧盟	欧盟	如未满足数据跨境传输要求，则需进行本地化存储	欧盟仅在以下情形下可以跨境传输： • 满足具有同等数据保护水平，即白名单国家机制，中国不在其列 • 提供适当的保障措施：例如获得数据保护或安全认证、签订标准合同条款（“SCC”）、制定有约束力的公司规则（“BCR”）等 • 其他情形：获得个人信息主体同意或满足履行合同所必需等合法性基础后可进行	实践中出海欧盟的企业通常会选择签订标准合同条款的方式，将其个人信息传输、存储至境外。如签署标准合同条款较为困难的，企业亦可选择取得应聘者或员工充分知情同意，以进行跨境传输
中东	阿联酋	经阿联酋央行许可的支付系统运营商需要将个人或企业	阿联酋的数据跨境传输机制： • 数据控制者与数据接收方之间签订合同	实践中出海阿联酋的企业通常会选择签订数据跨境传输协议的方

		客户数据（包括客户身份和交易记录）进行本地化存储和维护；提供医疗健康服务的机构一般情况下需要将医疗健康数据进行本地化存储	• 已获得信息主体关于跨境传输的明示同意 • 数据传输对于履行义务，以及面向司法机关建立、行使或辩护权利是必需的 • 数据传输对于信息主体作为合同一方所必需的 • 数据传输对于执行与国际司法合作相关的程序是必需的 • 数据传输对于保护公共利益是必需的	式，将其个人信息传输、存储至阿联酋境外。如签署数据跨境传输协议较为困难的，出海企业亦可选择取得应聘者或员工的充分知情同意，以进行跨境传输
	沙特	税务数据、人力资源记录，划分为第3级别和第4级别的消费者数据、未满18周岁的未成年人数据需进行本地化存储	沙特相关法律规定跨境传输首先限于特定目的，包括为履行与信息主体的合同所必需，以及为个人信息主体提供服务或福利等。在满足目的合法性要求的基础上，沙特企业可依据如下路径跨境传输个人数据： • 为履行与信息主体的合同所必需等法定豁免情形 • 签订标准合同条款（“SCC”） • 制订有约束力的共同规则（“BCR”） • 认证 • 以上跨境传输或是持续或大规模跨境传输敏感个人数据，均应当开展风险评估	实践中出海沙特的企业通常选择与境外数据接收方签订标准合同条款的方式，将应聘者或员工个人信息传输、存储至沙特境外
非洲	**肯尼亚**	没有明确的数据本地化要求	肯尼亚明确规定了合法跨境传输个人数据的情形： • 接收方采取了适当的数据保障措施（需向肯尼亚数据主管部门提交有关证明材料） • 接收方所在地已获得肯尼亚数据主管部门作出的充分性决定 • 转移具有必要性，具有必要性的情形包括但不限于履行合同所必需、涉及公共利益、保护信息主体利益但难以获得信息主体同意、数据控制者存在压倒性的正当利益等 • 已告知信息主体有关风险并取得信息主体同意 • 如向肯尼亚境外传输敏感个人数据，必须取得信息主体的同意且确保实施了适当的保障措施	实践中出海肯尼亚的企业通常会选择取得应聘者或员工同意，将其个人信息传输、存储至肯尼亚境外。如果较难取得其有效同意，企业需向肯尼亚数据主管部门提交有关证明材料并获认可，以实现合规出境

中亚	哈萨克斯坦	必须将个人数据存储在位于哈萨克斯坦境内的数据库中（即使存在跨境传输业务，仍需在哈萨克斯坦境内进行一份数据存储）	哈萨克斯坦目前人力资源场景下取得个人同意为主要可行的出境方式： • 建立了被认定为保护个人数据的国家可自由流动的机制，但尚未公布国家名单 • 如不满足上一条件，则只有在确保未落入哈萨克斯坦法律限制跨境传输的特殊情形，同时符合以下情形之一时可进行数据跨境传输：（i）个人信息主体明确同意；（ii）符合哈萨克斯坦批准的国际条约规定情形；（iii）在哈萨克斯坦法律规定的情况下，为保护哈萨克斯坦的宪法制度、公共秩序、个人和公民的权利和自由以及公共卫生和道德；（iv）涉及保护个人和公民的宪法权利，而无法取得当事人或者其法定代表人的同意的	实践中在确保未落入哈萨克斯坦法律的限制跨境传输的情形时，出海哈萨克斯坦的企业通常选择取得应聘者或员工同意，将其个人信息传输、存储至哈萨克斯坦境外
北美	美国	没有明确的数据本地化要求，但对于特定行业（例如国家安全、反外国政府调查 / 封锁、税务或财务记录、雇佣、出口管制）有数据本地化的要求	美国尚无生效的关于数据跨境传输的限制	原则上美国企业可直接将应聘者或员工个人信息传输、存储至美国境外。但企业需要关注政府针对跨境传输至中国的一系列行政令，避免落入受限制的情形
南美	巴西	对于政府数据、银行云服务数据等有数据本地化存储要求	巴西可依据如下路径跨境传输个人数据： • 建立了被认定为具有充分的数据保护水平的国家可自由流动的机制，但尚未公布国家名单 • 数据控制者采取相关保护措施：包括跨境传输相关的具体合同条款、标准合同条款、具有约束力的公司规则、以及认证和行为准则 • 获得巴西国家数据保护局批准 • 信息主体已被告知跨境传输活动情况，并给出了明确的单独同意	实践中出海巴西的企业通常会选择签订数据跨境传输协议的方式，将其个人信息传输、存储至巴西境外。如签署数据跨境传输协议较为困难的，企业亦可选择取得应聘者或员工的充分知情同意，以进行跨境传输

欧亚	俄罗斯	必须将个人数据进行本地化存储	俄罗斯数据可以通过如下方式出境： ● 在与俄罗斯达到同等保护水平的白名单国家之间数据可自由流动，但需要先通知俄罗斯通信监督管理部门。中国在俄罗斯白名单中 ● 数据传输至非俄罗斯白名单国家，需要俄罗斯通信监督管理部门审批通过且要取得自然人的书面同意	实践中出海俄罗斯的企业通常会在俄罗斯部署服务器存储在其境内收集处理的个人信息，并在有充分必要性时，再将数据依法传输出境

注：标准合同条款 SCC(Standard Contractual Clauses) 指一国数据保护监管机构制订并颁布的、相应场景下必须签署的数据跨境传输合同；数据跨境传输协议指由个人信息控制者和境外接收方间签署的，约定个人信息跨境传输的目的、方式、安全措施、各自权利、义务等事项的协议。

（表四）

可见，多数法域对人力资源管理数据没有强制进行本地化存储要求；多数法域都建立了“白名单”、签署 SCC、制订 BCR、取得个人同意等数据跨境传输机制，企业可视自身情况选择合适的机制将应聘者或员工的个人信息传输至境外：

（1）由中国总部与出海国家的子公司（如泰国子公司）之间签署“跨境传输标准合同 SCC”或其他数据跨境传输协议的方式；

（2）取得员工 / 应聘者充分知情同意的方式；

（3）集团内部制订有约束力的公司规则 BCR 的方式。因为包括欧盟在内的很多国家 / 地区都规定了 BCR 需经该国家 / 地区相关机构批准后方可适用，所以此种方式在实践中较少使用；

（4）如果集团总部所在国家和出海所在国家之间有“白名单”,可以通过“白名单”机制进行数据跨境传输，因为现在公布了本国数据出境白名单的国家尚不多，所以此种方式在实践中较少使用。

特别提示：俄罗斯

俄罗斯法律明确规定了依据劳动相关法律收集处理的个人信息不豁免数据出境的相关规定，也即：

（1）数据必须进行俄罗斯本地存储；

（2）数据可以出境，但都需要经过俄罗斯通信监管部门：

- 白名单国家，需要先通知俄罗斯通信监管部门；
- 非白名单国家，需要俄罗斯通信监管部门审批且要取得自然人的书面同意。

因此建议出海俄罗斯的企业，应首先将在俄罗斯境内收集的数据存储在俄罗斯境内，并在通知俄罗斯通信监管部门的前提下将数据传输至中国总部或向中国总部开放相应的访问权限。

个人信息存储、删除的合规处理

各法域个人信息保护法律法规均设置了个人信息处理的合法性与必要性原则，基于该原则，员工 / 应聘者个人信息的存储时间应限于实现处理个人信息的目的所需的时间，反言之，处理目的实现后即没有继续存储相关个人信息的必要性，需进行删除。

具体到招聘场景下的应聘者个人信息而言，从合法性原则角度来看，个别国家允许企业在应聘结束后继续保存未成功的应聘者的个人信息一段时间，例如德国和爱尔兰，通常允许企业在招聘结束后保留未成功应聘者的数据 6 个月，以便处理可能发生的就业歧视等申诉；爱沙尼亚法律规定，应聘者相关索赔的诉讼时效期限为 12 个月，因此企业将应聘者数据保留 12 个月后删除符合 GDPR 存储限制原则。出海至此类国家时，企业依据相关规定存储相应的时间后删除应聘者个人信息即可。

然而，多数国家并未就应聘者信息可存储时间做出明确规定，此时需要适用必要性原则进行判断，即该应聘者应聘失败且该岗位已招募到合适的员工，或直至与招聘流程相关的诉讼时效截止，即可认为处理该应聘者个人信息的目的已实现，已无继续存储该应聘者个人信息的必要，需及时删除。

具体到用工管理场景下员工个人信息而言，很多国家均在劳动相关法律法规中设置了相关文件 / 记录的法定存储期限，企业应注意梳理各法域的强制规定，在规定期限内留存相关数据，并在期限届满时及时删除。例如：

新加坡	新加坡《雇佣法》规定及人力资源部说明，企业应当通过纸质或电子方式留存员工的雇佣记录及薪水记录信息，针对在职员工应当留存近两年的记录，针对离职员工应当保留其离职前两年的记录，并且在员工离职后保存一年
印尼	目前印尼并未在劳动雇佣相关的法律内明确规定雇佣记录的维护要求，但根据《公司文件法》，员工招聘、雇佣记录可能被归类为“其他文件”，其保留期限由雇主根据其实用性或价值确定，根据文件性质保留期限要求可达 10 年
德国	《德国商法典》规定，企业的商业记录、财务报表等文件应保留 10 年；《德国税法》规定企业的账目和记录等数据应保留 10 年；如上述企业账目中包含员工薪资信息，此类员工个人数据也应一并保存 10 年
爱尔兰	爱尔兰相关法律对部分员工数据的存储期限做出了规定，如与员工的产假或不可抗力假期的日期和时间记录应保存八年，税务记录应保存六年，与工资信息相关的记录应保存三年，工作时间记录应保存三年等
肯尼亚	肯尼亚《就业法》规定企业应当在雇佣关系终止后的 5 年内留存雇员劳动合同等材料
南非	南非《就业基本条件法》规定雇主应当准确留存员工姓名与职位、工作时间、薪酬、未满十八岁员工的出生日期等记录至少三年
匈牙利	匈牙利《社会保障养老金福利法》规定，企业必须在员工达到退休年龄后的 5 年内保留所有包含有关员工就业年限以及员工所获工资或收入信息的文件，包括雇佣合同、纳税申报表和收入证明等；此外，其《劳动法》规定可在诉讼时效内即雇佣关系终止后 3 年内存储员工个人数据

（表五）

对于没有相关法律对员工个人信息存储期限做出规定的国家，或虽有法律规定，但仍有部分员工个人信息的存储期限没做出规定的，仍需适用必要性原则进行判断，在员工在职期间，一般可存储其个人信息；当员工离职年限已超过当地法律规定的相关诉讼时效期限时，一般认为处理该员工个人信息的目的已实现，已无继续存储其个人信息的必要，需及时删除。

因此，建议出海企业，无论是**对应聘者个人信息**还是**对员工个人信息**，均可遵循以下原则进行存储或删除处理：

（1）对所在国法律明确规定了存储期限的个人信息，依据规定的期限存储，到期后删除；

（2）对所在国法律没有规定存储期限的个人信息，按照必要性原则，在实现相应处理目的，继续存储该员工个人信息已无必要时，即删除其个人信息；

（3）对于离职人员，如企业有充分的必要性，需要在法律规定的期限之外继续存储其个人信息，可告知继续存储个人信息的期限、目的、信息类型等事项，并取得该离职人员的同意。

个人信息主体权利响应的合规处理

各法域个人信息保护法律法规均设置了较近似的个人信息主体权利，同时也就部分权利规定了宽严不等的响应时间，例如：撤回同意、要求删除、反对权、更正权等。

其中特别需要注意，在招聘场景中，应聘者应聘岗位失败后，如向企业提出删除其个人信息的要求时，企业需及时予以响应，并在该国家 / 地区个人信息保护法律法规规定的时间内完成数据删除。以下为部分国家 / 地区个人信息主体权利响应规则对比：

国家 / 地区		个人信息主体权利响应规则
东南亚	泰国	• 个人信息主体享有知情、同意和撤回同意、访问、更正、删除、限制数据处理、数据携带、反对数据处理、投诉、提起诉讼、索赔损害以及自卫的权利 • 针对访问权请求的行使，规定了收到请求后至多 30 天的响应期限
	马来西亚	• 个人信息主体享有知情权、访问权、更正权、撤回同意权、反对权、反对为直接营销活动进行处理的权利 • 针对访问、更正、反对处理要求权利的行使，收到请求后至多 21 天的响应期限
	新加坡	• 个人信息主体享有知情权、访问权、更正权、撤回同意的权利、可携带权等 • 其中访问权、更正权的响应期限限制在 30 天内
欧盟	欧盟	个人信息主体享有知情权、访问权、更正权、删除权、限制处理权、数据可携权、反对处理权等
中东	阿联酋	个人信息主体享有知情、访问、复制、数据携带、更正、删除、限制处理、停止处理、不受自动化决策约束以及向监管机关投诉的权利
	沙特	• 个人信息主体享有知情、访问、更正、删除、撤回同意、数据携带、投诉举报等权利 • 控制者一般应当在 30 日内响应权利请求
非洲	肯尼亚	• 个人信息主体享有知情、访问、更正、删除、反对数据处理、数据携带、不受自动化决策约束、投诉等权利 • 数据控制者应当在 30 日内响应信息主体的携带权请求
中亚	哈萨克斯坦	个人信息主体享有知情权、访问权、更正补充权、删除权、反对 / 退出的权利、撤销同意权、申请赔偿权

北美	美国	• 个人信息主体享有删除权、更正权、知情权、选择不出售或共享个人信息等权利 • 企业应向个人信息主体提供两种或以上的指定方式以供其提出行使知情权、删除权或更正权的要求，指定方式至少包括提供免费的电话热线 • 企业应在收到可经验证的个人信息主体要求起的 45 日内（最多延长至 90 天）进行权利响应 • 企业应保存个人信息主体提出的权利请求以及企业如何回应请求的记录至少 24 个月，且应实施并维护合理的安全程序和实践来维护这些记录
南美	巴西	• 个人信息主体享有知情、访问、更正、删除、反对、撤回同意、数据携带权等数据权利 • 数据控制者应当在 15 日内响应信息主体的查阅权请求

出海企业应建立个人信息主体权利响应机制，包括：

（1）使用具备权利响应功能特性的人力资源管理软件，如查询、更正、删除、撤回同意等功能；

（2）如企业未使用具备相应功能的人力资源管理软件，则应建立相应的权利响应机制，如公布权利响应邮箱、成立专门的部门或指定专人及时响应。

个人信息安全保障的合规处理

为保障企业持有的个人信息免遭未经授权或意外的查阅、处理、删除、丢失或使用，各法域均对如何保障个人信息安全提出了较为相近的要求，主要包括采取适当的技术和管理措施保护数据安全、告知个人信息主体处理情况、记录数据处理、规定情形下任命数据保护官、规定情形下开展个人数据保护影响评估、报告数据泄漏等。

以上要求分别涉及组织建设、技术措施、评估、报告等多角度的义务，因此，建议出海企业：

（1）集团内自上而下设置个人信息安全保护组织或人员，专门负责相关工作；

（2）集团内制订个人信息保护管理制度和流程，如主体权利保障制度、数据记录使用制度、数据泄露报告制度等，使得个人信息保护各项工作均在制度规制下有序开展；

（3）采取适当的技术措施 ，如 IT 安全管理措施、传输安全技术措施、使用具备隐私合规能力的人力资源管理软件等，保障信息安全；

（4）根据所在国法律规定，落实指定场景下数据保护影响评估、任命数据保护官等合规动作。

PART

04

人力资源数字化
如何做到全球数据合规

人力资源数字化
如何做到全球数据合规

随着中企出海热情持续高涨，中企出海的广度、力度和深度以及竞争力都在不断加强。在出海进程方面，中企出海已经从单纯的营销出海、产品出海、更进一步发展为品牌出海和研发出海。大量中国企业在海外设立公司及建立生产基地，全面推进涵盖生产、销售与研发的全球化业务布局。由于中企出海阶段不同，海外人员布局不同，海外人力资源管理面临的挑战不同，对人力资源数字化的要求也有所不同。如：

贸易伙伴型

以国内人员海外外派为主，少量属地化市场人员，主要负责开拓贸易伙伴，获取原材料及商品价差利益。人力资源管理以国内为主，重点关注外派人员的管理。

产品出海型

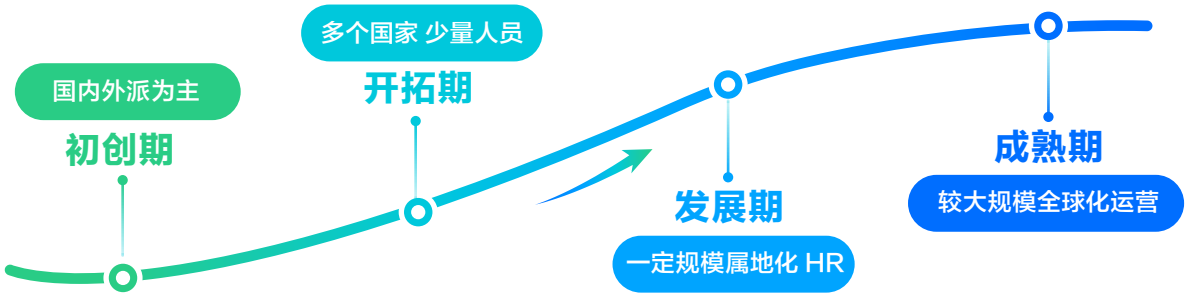
市场开拓阶段海外人员呈现“多个国家，少量人员”特点，国内生产的产品在海外市场开拓和营销，以获得更大的市场和品牌知名度。由于出海国家众多，海外人员分散，人力资源管理仍以国内为主，员工属地化招聘或 EOR 名义顾主方式为辅。

海外运营型

在海外设立公司及建立生产基地，整合当地优势资源，利用属地自然资源和廉价劳动力，为本地市场提供生产和服务能力，降低成本。这个阶段管理人员以国内外派为主，生产人员属地化招聘或采用三方劳务人员，人力资源管理以国内为主导，结合属地化政策进行管理。

全球运营型

开始设立海外国家区域性总部，整合全球资源和供应链，统筹研发、生产、供应链和市场营销。综合提供全球产品研发和属地化市场的开拓与服务。海外机构人员体量成一定规模，国内以管控为主，属地化独立业务运营，国内总部进行全球化数据分析。



贸易伙伴型

以国内人员外派为主，少量属地化市场人员，主要负责开拓贸易伙伴目的是获取原材料及商品价差利益

产品出海型

国内生产的产品在海外市场开拓和营销，目的是获得更大的市场和品牌知名度。市场开拓阶段呈现多个国家少量人员特点

海外运营型

成立区域公司或属地建厂，整合当地优势资源，利用属地自然资源和廉价劳动力，为本地市场提供生产和服务能力。目的是整合属地资源提供本地化服务，降低成本

全球运营型

全球一盘棋，整合全球资源和供应链，统筹研发、生产、供应链和市场营销。全球化企业多数为此类型，有海外国家区域性总部，综合提供全球产品研发和属地化市场的开拓与服务

管理模式	管理模式	管理模式	管理模式
国内统一系统管理	国内管理 +EOR(名益雇主) 或 GPO(新酬外包) 或 .IC(独立雇主) 服务组合过渡阶段	区域有属地化 HR 团队，国内进行整体管控	属地化 HR 团队，全球资源配置和管理

我们看到，作为中企出海无论业务发展处于哪个阶段，中国总部对海外机构人力资源都有管理或管控的诉求。不同于 CRM、ERP 等可以区域化的业务系统，人力资源数字化要遵循**“全球一张表”**的架构逻辑，这个设计与人力资源的业务特点有关。在全球化人力资源业务场景中，集团总部与分子公司之间存在大量人事业务流程，以及管理或管控场景。

例如：员工海外外派流程、员工跨机构海外调动流程、员工海外出差流程；集团总部对海外公司的编制情况、薪酬总额、人工成本等管控；从战略到目标的绩效分解，集团总部目标分解到各分子公司；总部和海外联络所必须的公司通讯录等，这都要求企业需要构建统一的全球人力资源数字化平台，在保证合规基础上，实现“全球一张表”，以满足全球人员调配、业务流程高效审批、合理的编制与成本控制、全球人力数据分析等需要。

我们反向观察，以欧美全球化知名跨国集团为例，已经出海全球几十年，这些跨国集团均遵循了全球一张表的人力资源数字化原则，他们的总部及子公司仍然要使用全球人力资源系统，并遵循全球的人力资源管理框架和流程，在全球标准化策略基础上，结合出海国家情况进行本土化经营。

因此，全球化人力资源管理数据合规的重点应该是：人力资源“全球一张表”的前提下，实现各个出海国家的数据合规，保护员工的权益。

人力资源数字化平台合规场景分析

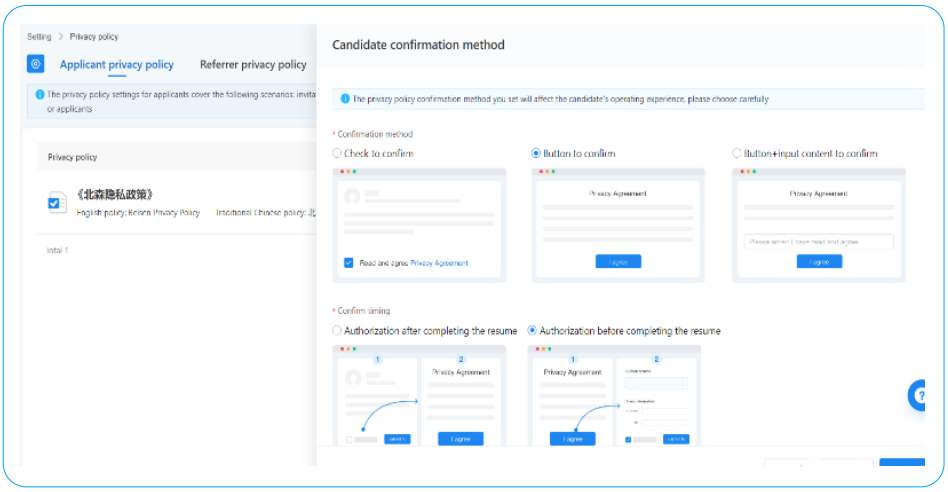
招聘环节中的应聘者数据合规要素

场景一：如何实现招聘场景中的充分同意、自愿原则？

出海企业在招聘环节需要遵守目标市场的数据保护法规 ，企业在招聘环节收集和留存应聘者个人信息应该怎么做？如何让应聘者充分的自愿同意，获取应聘者授权同意的方式有哪些？

在招聘环节中，如企业招聘官网、公众号等渠道通过招聘职位发布，应聘者线上投递方式直接收集应聘者个人信息，因此在信息收集环节需要让应聘者了解企业要收集哪些信息、收集的目的、使用方式、数据存储以及数据跨境传输情况，保护措施等关键内容。招聘环节直接收集应聘者信息，企业一般通过定义“隐私协议”或“隐私政策”的方式，清晰、完整的向应聘者告知，应聘者通过阅读勾选后，主动投递简历的方式证明其已给予同意，企业则以此依据协议内容开展后续的招聘活动。

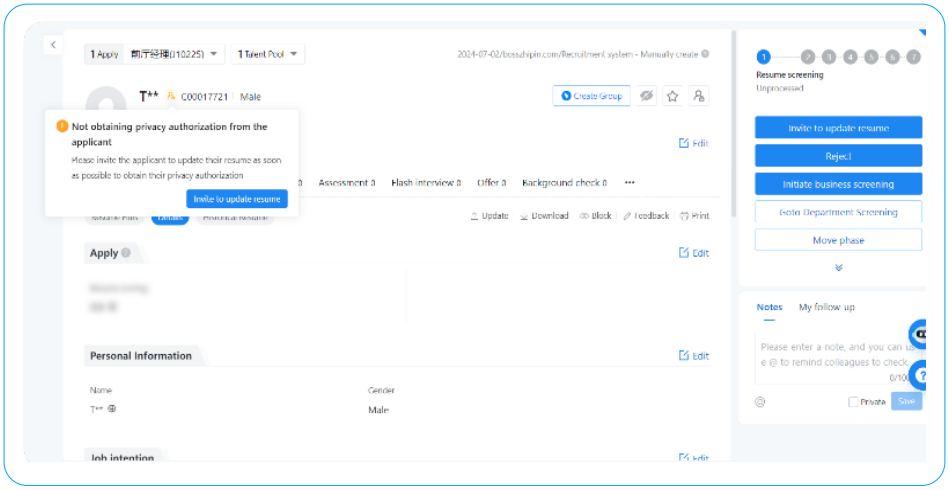
同时，为满足部分国家和地区法律法规中要求的“充分告知、充分理解获取授权的基准原则”，需提供多种版本，如大陆地区中文协议版本，港澳台地区繁体协议版本，海外英文协议，泰语版本等。另外，针对特殊场景需要提供多种应聘者隐私协议确认方式，企业可以根据合规要求程度进行选择，包括勾选确认、按钮确认、按钮 + 输入内容确认等。并要为企业提供隐私协议自定义能力，及同意记录留痕能力。



场景二：如何按照“最小化原则”实现最短时间留存个人信息？

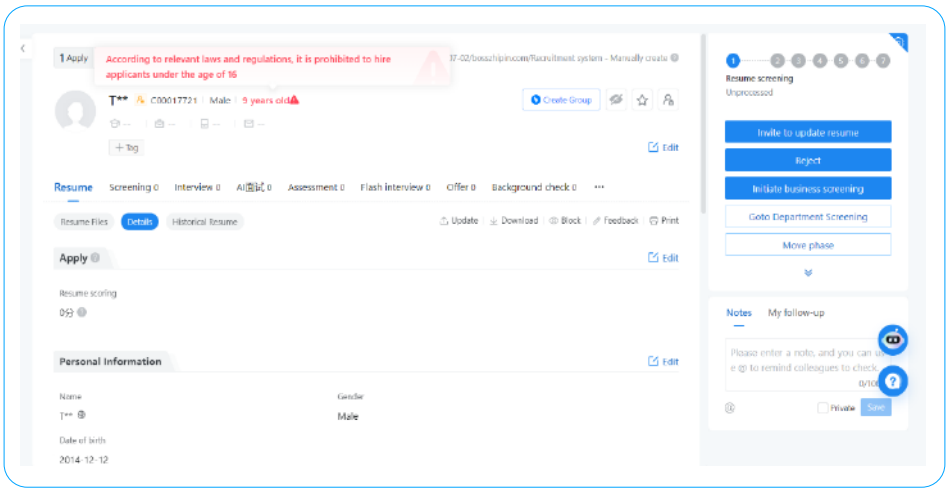
按法律规定，企业需要按照最小化原则收集和使用与目的相关的必要数据，并在实现招聘的最短时间留存个人信息，超出隐私协议说明的个人信息保留最长期限后，需重新获取应聘者授权，若应聘者没有继续给予授权但企业仍然存储简历信息，将不符合个人信息保护的相关法律规定。

在海外招聘过程中，企业要更加强化数据合规意识，招聘环节仅收集应聘者与职位相关的信息，如姓名、联系方式、简历信息、面试信息、考试信息、Offer 信息，不收集应聘者敏感个人信息。对于未授权 / 授权超期的应聘者，将自动提醒 HR 及时获取授权。并定期删除未授权 / 授权超期的应聘者信息，以确保符合合规要求。



未成年人用工风险提醒

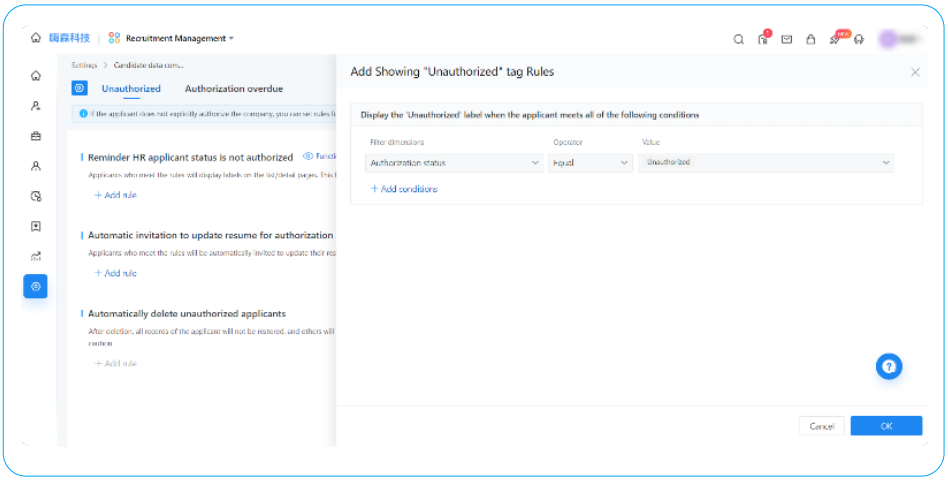
在多个国家法律当中，都有明确针对未成年人个人信息保护及用工要求的规定。原则上，企业应禁止招聘 16 周岁以下应聘者，针对 16 周岁 ~18 周岁的应聘者存在用工风险，需谨慎考虑。对于大量招聘的职位，如餐饮行业服务人员，销售岗位、生产岗位等，就需要系统帮助进行有效验证，如对 18 岁以下的应聘者进行及时提醒，防止企业使用年龄不合规的应聘者导致出现合规风险。



场景四：应聘者信息的存储与删除

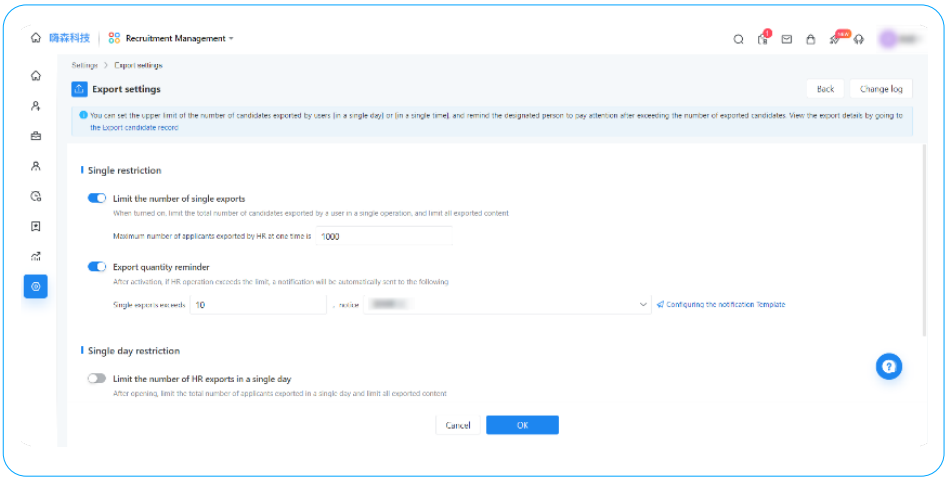
原则上，当企业招聘流程结束，对于未录用应聘者的信息即应删除处理。对于一些国家为了预防劳动争议或为应聘者提供未来工作机会，基于应聘者自愿同意的前提下可以保留一段时间，但有最长期限限制。因此，对于未录用应聘者或授权存储期限到期的应聘者，如果企业要继续使用或留存其个人信息，均需再次获得应聘者的有效授权，否则应对个人信息进行删除处理。

对于很多企业有建立出海招聘人才库的管理需求，但这并非招聘所必须的场景，需要通过“进入人才库授权”的方式，在充分告知应聘者后获得应聘者的单独授权同意。



场景五：容易忽视的高风险行为 – 数据导出

很多企业对于系统功能和数据权限的控制都很关注，但往往忽略了对于数据导出这个高风险行为的监管和控制。拥有数据导出权限的人员也在不断变化，这就可能导致简历等个人信息导出失控，这不仅会造成人才信息外流，还会加大数据合规风险。系统首先需要对数据导出行为进行监控，完整记录导出操作的人、时间、来源、具体内容。同时应该支持设置导出阈值，限制每次 / 每日导出的数量，拦截高风险导出行为并自动提醒企业管理员。



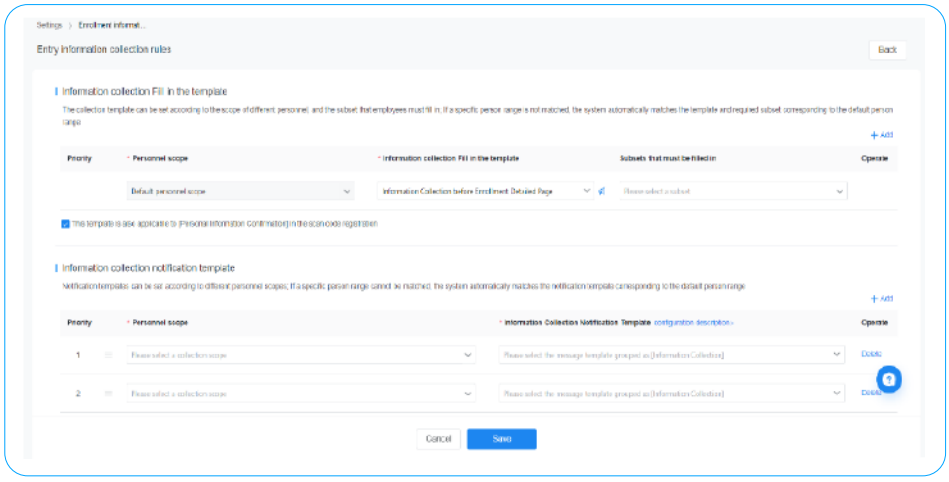
员工管理过程中的数据合规要素

出海企业在员工管理过程中，会涉及员工很多方面的信息收集和使用。因很多国家都有关于员工隐私信息处理的要求，也使大量中国出海企业对于海外员工的信息管理范围产生困惑。对于人力资源管理场景，很多国家都明确了收集使用条件，这些条件通常以获得个人信息主体的同意为主，同时规定不需要获得同意即可收集、使用个人信息的例外情形，常见的例外包括为订立或履行合同所必需、企业与员工签订劳动合同或协议、企业为了履行合同义务需要进行员工必要信息的采集。

场景一：员工信息采集授权，不同国家采用单独的采集模板

出海企业在海外进行员工信息采集时，需要遵守目的地国家的合规要求，这些要求因国家和地区的不同而有所差异。企业需要制定完善的隐私协议，有明确的使用目的限制，内容要涵盖数据的收集、存储、使用、共享、删除等各个环节，以符合个人信息保护法律法规要求，取得相应的处理合法性基础。涉及需员工给予同意的处理场景，鉴于企业与员工之间的权力的不平衡性，为了确保告知充分、自由自愿授权，企业需注意取得员工同意的方式，不得胁迫员工给予同意，同时需告知员工便捷的撤回同意的方式。

系统需要能够根据出海目的地国家对于隐私合规要求的差异，设定不同的信息采集范围，以满足合规要求。因此不同国家可以定义差异化的采集模板，确保信息采集范围的合规。如法国、德国、意大利等欧盟国家可以定义一套采集模板范围；泰国、新加坡、越南可以再单独定义不同的采集模板范围。



场景二：员工敏感信息单独授权、单独管理

企业在进行员工管理过程中，需要对部分敏感信息进行采集。例如 ：企业与员工签署劳动合同所需要的身份证信息、为员工支付工资收集的员工的银行账户信息、为员工缴纳社保的社保账户信息；以及企业对员工进行假勤管理过程中，员工请休病假、婚假等假期时，企业向员工收集医院病假证明、结婚证明等必要的证明材料信息; 还包括企业对员工进行绩效、薪酬管理过程中，需要收集员工的绩效信息及薪酬、社保、个税等信息等等; 这些虽然属于员工敏感信息，但企业因履行合同义务和必要的管理仍需要进行采集。

企业应确保收集和处理个人敏感数据符合“最小必要原则”，同时要对敏感信息进行权限控制，以便有效的保护员工隐私数据。因此，在进行员工信息采集过程中，对于敏感信息需要可单独控制和授权，对于没有权限的用户应限制查看和使用。

场景三：海外打卡位置信息和外勤照片信息的合规处理

中企出海考勤管理场景中，大量企业涉及多国少人状态，不是每个办公地点都有打卡设备，企业如何有效的进行海外人员考勤管理? 系统除了要支持硬件考勤设备打卡外，还要能支持 WIFI 或 GPS 等多种打卡方式，并能够自动匹配属地的时区，判断出勤情况。打卡控制：通过有效打卡范围限制，采用技术手段判断员工打卡是否在有效范围，同时不采集详细签到地址。因个人定位信息（如经纬度）和打卡照片等属于个人敏感信息，针对系统控制境外员工外勤打卡，如是否采集经纬度、外勤照片等信息，默认为“否”，如果选择“是”将提示告知隐私合规风险；对于外勤人员个人定位和照片信息，不建议企业进行采集。

员工离职后的数据合规处理

场景一：离职后员工信息保留期、删除处理

中企出海在处理离职员工的信息保留和删除时，需要严格遵守当地法律法规的要求。在员工离职后，企业应首先查询当地法律法规是否对离职员工的档案设定了强制性的存储期限，除此之外，特殊行业如金融、医疗等也会有额外的记录保留要求，需要特别注意。在具有强制性档案留存期限的前提下，企业应注意将相关数据进行归档或冻结处理，并在相关期限届满时及时开展删除或及时进行删除操作。

企业应建立离职员工信息存储档案，详细记录员工保留期内的信息，对于保留存储到期的信息，要能够自动提醒系统管理员，系统管理员可在授权情况下对离职员工信息进行删除。系统日志也需要进行完整记录，以备后续的相关核查。

员工作为信息主体的权利响应合规

员工作为个人信息主体，有权在发现企业违法收集、使用其个人信息时，或企业应当依法删除其个人信息而没有删除等情形时，向企业提出停止、拒绝相应行为或删除其个人信息等要求，企业需依法予以及时响应。

信息主体权利		需要做什么
知情权	信息主体有权被告知其个人数据将被如何收集、处理和存储。	在隐私协议授权，入职信息采集，特殊业务操作前进行用户确认。
访问权	信息主体有权访问和获取其个人数据的副本。	允许员工进行个人信息的查询和个人信息导出，以及敏感信息保护等。
纠正权	信息主体有权要求更正不准确的个人数据。	为员工提供个人信息自查询和修改的功能或路径。
删除权 被遗忘权	在特定情况下，信息主体有权要求删除其个人数据。	如员工进行个人数据删除申请，企业要按规定时间响应。
反对权	信息主体有权在特定情况下反对处理其个人数据。	提供员工撤回授权或拒绝授权的功能或路径。
数据 可携带权	信息主体有权将其个人数据从一个数据处理者转移到另一个数据处理者。	允许员工导出个人信息，并且系统提供信息变更日志及导出的功能或路径。
限制 处理权	信息主体在特定情况下有权要求限制对其个人数据的处理。	允许员工提出异议，并在异议期间内停止相关个人数据的处理活动。

因此，在员工发起主体权利要求时，需要人力资源数字化平台具备相应的功能和特性，帮助企业依法及时的做出响应。例如：单独确认授权、敏感信息隐藏保护、数据删除，员工撤回授权，数据的去标识化等。

全球人力资源数字化建设合规误区

误区一：海外员工数据不允许跨境传输

无论是欧盟的《通用数据保护条例》(GDPR),还是中国的《个人信息保护法》,均旨在加强对个人信息的保护，并没有禁止数据出境。

所以，大多数国家都有明确的数据出境的合法路径或允许跨境传输的豁免情况，如签署标准合同条款（SCCs）、制定有约束力的公司规则（BCRs）、特定情况下的豁免规则等，因企业在人力资源场景属于订立或履行数据主体要求的，或为数据主体利益的合同所必要，企业是可以通过选择合适的路径将应聘者或员工的个人信息传输至境外。

在日常管理中，通过通讯录查看员工的联络方式、通过邮件审批员工的请假、以及查看员工的绩效、薪酬，都是个人数据跨境传输，杜绝总部和海外公司的信息交互并不现实。所以，在海外应聘者 / 员工的个人信息管理上，合规才是我们的工作方向，而非禁止跨境传输。

误区二：数据本地化存储就是全球合规

很多企业为了规避出海合规风险，认为在出海国家当地选择一套人力资源管理系统，在本地部署服务器、本地数据存储就完全保证了数据合规。

但如果境外信息系统向境内总部管理者开放，使得境内管理者可以在中国境内对存储于境外的数据进行访问、下载或者使用，同样属于“数据出境”的场景，因此，数据出境不只是存储出境，也包括访问出境、使用出境，这是实践中经常被一些企业所忽略的误区。

其次，在出海国家当地安装一套人力资源管理系统，不仅未解决数据出境的合规问题，也未解决个人信息收集、使用、权利响应的合规问题。跨境传输合规只是数据合规的一个方面，还有更多其它的合规事项同样需要满足。

无论软件采取何种部署方式,我们都需要详细检查HR系统在数据合规的各个方面,是否做了必要的功能设计。

误区三：新加坡数据中心就能满足全球合规

在新加坡设立数据中心，并不能够满足全球的数据合规，原因如下：

- 对于非新加坡数据中心所在国家 / 法域的用户来说，数据中心在新加坡或中国，在跨境传输上并无太大差异，场景上都是把数据传输到用户所在国境外的数据中心；在合规动作上也都需要通过签署标准合规条款 SCC 等方式来满足数据跨境合规要求。
- 对于中企出海客户而言，大本营仍然在国内，即使在新加坡设立海外数据中心，中国总部访问存储在新加坡的员工数据、企业内部使用 IM 通讯软件沟通或查询全球员工通讯录信息等，仍然属于向中国跨境传输数据，该国的子公司仍需要与中国总部之间签署标准合同条款来满足合规要求。

对于全球范围内的出海企业而言，不同国家和地区对于数据保护的规定各不相同，即使新加坡的个人数据保护法在某些方面与欧盟的 GDPR 相似，但并不完全相同，与其他国家个人信息保护法规更是有着很多差异，因此，新加坡数据中心无法自动满足各法域法律的要求。此外，除了跨境传输，还有大量的其它数据合规事项，与数据中心的所在地无关，与流程以及 HR 系统的功能特性有关。 所以，仅依靠新加坡数据中心仍无法完全满足全球范围内的合规要求。

实践中出海企业通常选择通过签订标准合同条款 SCC、取得员工或应聘者同意等方式，将其个人信息传输、存储至境外。所以无论新加坡数据中心、还是中国数据中心，我们均需要完成相关的合规动作。

PART

05

关于本白皮书

关于本白皮书

近年来新全球化的演进，在北森服务的客户里已经有近 30% 的企业踏上了出海之旅。在启航初期，这些企业面临了诸多难以预料的不确定性挑战，错误的决策不仅导致后续频繁修正，还大幅消耗了企业的精力与资源，使得 HR 们常常陷入焦虑。

鉴于此背景，并结合广大客户的宝贵反馈和建议，北森决定编纂一本白皮书，旨在清晰阐述人力资源管理数据合规的精髓。我们携手国内在出海数据合规领域位居前列的汉坤律师事务所，共同深入访谈了众多具有代表性的客户、资深行业专家以及外资企业代表等，并组织了一系列业内研讨会，全面总结并提炼企业在全球化过程中的通用处理原则及实践。最终完成了本白皮书的编制。

《中企出海人力资源管理数据合规白皮书》的适用对象为在国际市场上运营的中国企业及其相关部门和合作伙伴，如企业高层管理者、人力资源部门、法务部门、IT 部门以及外部合作伙伴。通过阅读和使用此数据合规白皮书，这些企业和部门可以更好地了解和遵守各国在人力资源数据保护方面的法律法规，降低法律风险，提升企业的国际竞争力。

在此，我们衷心感谢那些为白皮书倾注心血的研究者、访谈对象及作者团队，包括汉坤律师事务所合伙人段志超律师、北森法务专家谢莉、北森隐私保护专家郭鹏程以及北森解决方案专家陈颖等。他们的专业贡献，为白皮书的成功问世奠定了坚实基础。鉴于各国政策环境的持续演变，为确保信息的时效性与准确性，我们决定将此白皮书作为一项长期项目，每年更新一版，以动态适应中企出海的新需求，助力您的企业在全球化征途中，合规先行，稳健致远！

PART

06

附 录

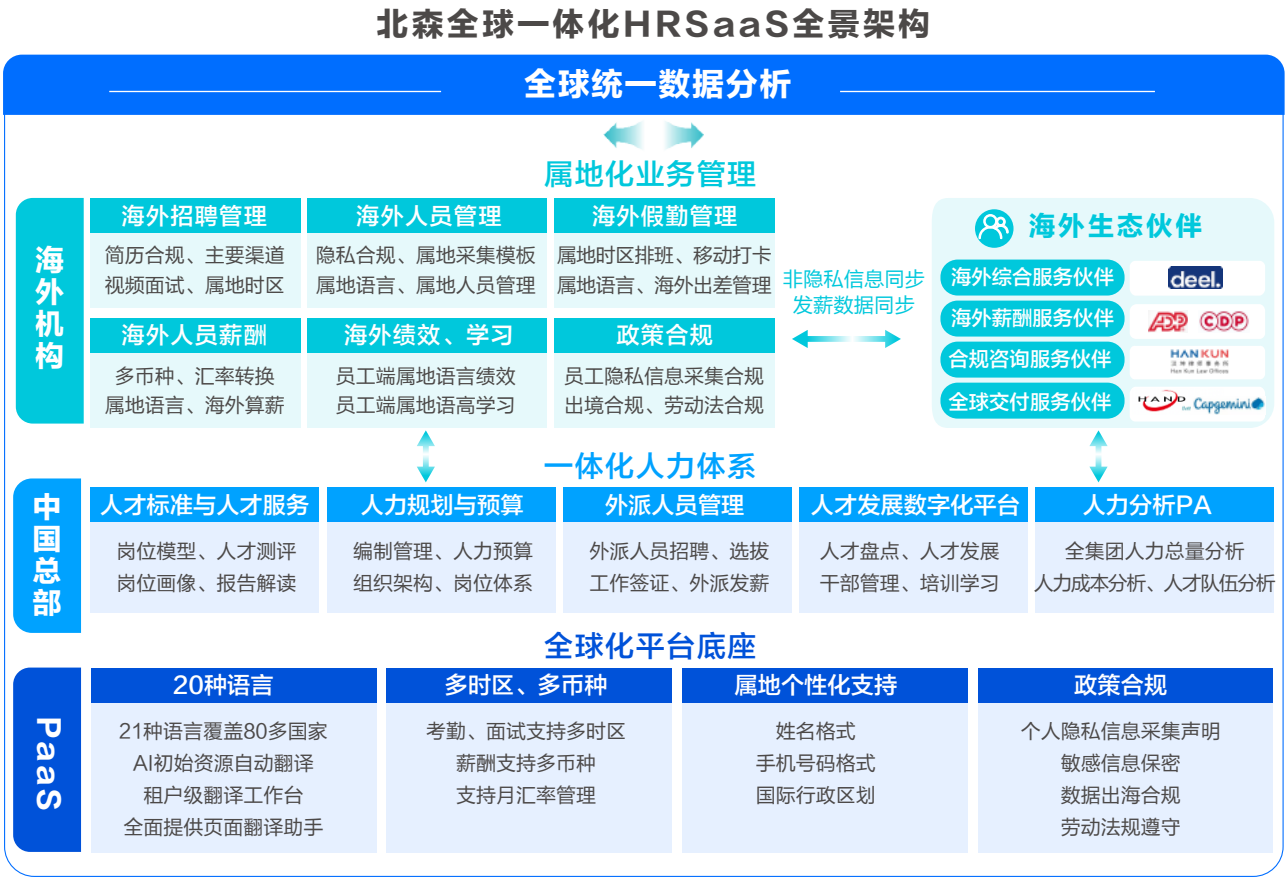
附录一

关于北森

北森成立于 2002 年，是中国领先的人力资源科技公司。通过一体化 HR SaaS 及人才管理平台——iTalentX，北森为中国企业提供人力资源管理全场景的产品和技术，包括 HR 软件、人才管理技术及咨询的端到端整体解决方案。帮助企业实现覆盖员工招募、入职、管理到离职的全生命周期的数字化管理，提升人力资源管理效率及人才管理能力、帮助员工快速成长，实现智慧决策。自 2016 年起，北森已连续 8 年位列中国 HCM SaaS 整体市场排名第一 [数据来源：IDC]，也是国内 HCM SaaS 领域唯一的上市公司。

顺应出海潮流并响应客户需求，北森依托强大的 PaaS 平台，已部署 26 种语言支持、多时区管理功能、30 多种货币结算选项以及严格的隐私与出海数据合规体系，确保企业 HR 管理在全球范围内既高效运作又严格合规；结合 PaaS 平台的国际化特性，北森的全球一体化 HR SaaS 解决方案全面覆盖了海外员工的招聘、人事管理、考勤、薪酬计算、目标绩效管理以及学习培训等全数字化场景。此外，基于出海企业的统一人力资源规划和体系，帮助企业打造全球人力一张表，全局分析全球组织效能和人事数据，满足企业出海人力资源政策合规、数据实时与流程闭环。

通过市场洞察、需求分析及持续的技术迭代，**北森已构建起全面的全球化服务能力与解决方案体系：**



北森全球一体化 HR SaaS 解决方案，已经为 300 多家客户提供了覆盖香港、台湾、泰国、越南、马来西亚、新加坡、印尼、印度、德国、英国、美国等 20 多个国家和地区的服务。

在实施和服务支持上，北森组建了海外云交付中心，组建了一支有流利英语沟通能力的专业交付顾问构成的团队。此外，北森与多家具备全球信息化交付能力的合作伙伴紧密协作，从合规角度出发，有效规避雇佣风险，确保实现属地化交付，保障项目平稳落地。同时，北森的 PaaS 平台国际化能力也在持续迭代升级，不仅全面适配国际化需求，还提供了国际化产品 OpenAPI 的应用集成能力，与更多出海生态服务集成伙伴携手，共同推进产品级系统集成的迭代规划，为中国企业的全球化发展注入强劲动力。

在**数据合规支持上**，北森高度重视用户数据安全和隐私合规，建立了隐私信息管理体系（PIMS）和云隐私管理体系，并且获得了 ISO27701 和 ISO27018 认证，这代表北森在隐私保护领域达到国际标准；北森的产品支持《隐私政策》细粒度定制，可以满足不同地区法规要求；在隐私合规技术措施上，北森从信息收集、传输、存储、使用、分享到销毁全程保护数据安全。如，采用 TLS1.2 以上加密协议传输数据，NoSQL 分布式存储加密敏感信息，实现精细权限控制和脱敏展示，提供生态伙伴服务时的隐私政策展示；北森产品支持账号注销和数据删除功能，合同到期后按需销毁数据，确保数据主体权利。

总的来说，**北森将隐私保护原则全面落实于产品功能，贯穿全生命周期。**

扫描二维码添加北小森，
获取更多专业的出海解决方案!

附录二

关于汉坤

汉坤律师事务所（“汉坤”或“我们”）是中国领先的综合性律师事务所，专注于国内、国际间复杂的商业交易和争议的解决，是中国律师行业的领军律所之一。在具体业务领域里，汉坤尤其以私募股权、兼并和收购、境内外证券发行与上市、投资基金 / 资产管理、反垄断 / 竞争法、银行金融、飞机融资、外商直接投资、公司合规、数据保护、私人财富管理、知识产权、破产与重组、争议解决等板块的法律服务著称，连年被国际权威法律媒体评为亚太区顶级中国律所。汉坤拥有 800 余名专业人员，分布在北京、上海、深圳、香港、海口、武汉、新加坡和纽约市。汉坤的律师拥有优秀的学历背景，具有长期服务境内外客户和参与复杂跨境交易及争议解决的丰富经验。

汉坤的数据保护业务团队由十余名专业人士组成，团队成员均毕业于国内外著名大学法学院。熟稔不同法域的数据相关法律法规，我们致力于协助不同行业和地区的领先公司解决其在数据领域的复杂数据合规问题。作为合规领域的专业律师，我们向客户提供直面问题和可落地的解决方案，而非仅限于提出问题。汉坤亦是数据合规领域新型法律服务的践行者。在诸如网络安全审查以及海外上市业务数据合规审核的新兴业务类型上，我们擅于整合不同领域的专业知识，在相关法规高速发展和不断变化的当下向客户提供满足其需求的创新解决方案。

我们在互联网、酒店出行、自动驾驶、新兴基础设施、金融科技、医疗教育等多行业网络安全及数据合规领域拥有丰富的项目经验，能够在个人信息保护、数据安全合规、网络安全合规方面为域内外企业提供全方位的法律服务，主要服务类型包括但不限于：

- 中国、欧盟、东南亚、中东、美加等主要国家和地区的数据合规尽职调查、差距分析及问题整改；
- 数据相关制度、协议的起草与修订；
- 数据本地化及跨境传输的解决方案；
- 协助处理境内外上市、投融资、并购交易中的数据合规问题；
- 协助配合及响应境内外监管机构、法院的数据调取；
- 协助开展数据相关的培训，追踪、评述数据领域最新立法动态及新闻热点。

汉坤数据保护团队近年来获得的代表荣誉包括但不限于：

- TMT：数据保护及隐私领先中国律师事务所（Chambers, 2023–2024）
- 第一梯队数据保护中国律所（The Legal 500 Asia Pacific, 2021–2024）
- 全球数据法领域百强律师事务所（Global Data Review, 2023–2024）
- 隐私及数据保护卓越律师事务所（China Business Law Journal, 2021–2024）
- 第一梯队网络安全与数据合规中国律所（Legalband, 2022–2024）

汉坤数据保护团队有丰富的出海企业数据合规法律服务经验，覆盖欧盟、东南亚、日韩、中东、美加等法域。汉坤数据保护团队具有广泛的境外律所网络，能够与境外合作律所深度合作，共同为客户提供全球化、全流程的人力资源数据合规法律服务，出海人力资源合规法律服务具体事项与流程可参考如下方案：

01. 事实调研与差距分析

- 通过问卷、访谈等方式，了解公司的海外人力资源数据处理情况、数据管理现状及规划
- 基于事实调研结果识别风险场景，调研目标法域有关法律法规，进行合规差距分析，出具主要合规风险清单与初步整改建议
- 针对自动化决策、员工监控、敏感个人信息处理等高风险活动，分析可行性并出具合规分析报告，在必要时协助公司开展数据保护影响评估

02. 数据跨境合规

- 基于事实调研结果识别人力资源相关数据跨境传输场景，基于目标法域数据保护法律要求，出县数据跨境合规方案
- 协助公司开展目标法域数据跨境合规方案落地工作，包括适用的数据出境影响评估、备案、申报等程序

03. 外部合规整改

- 为出海企业定制面向候选人及员工的隐私政策、告知同意函，满足目标法域数据保护法律要求

04. 内部合规体系搭建

- 结合公司实际业务需求，起草或完善出海人力资源管理配套内部制度，协助公司建立专门目标法域的人力资源数据合规细化制度与流程

扫描联系汉坤数据保护团队，
获取更多专业的出海人力资源数据合规法律服务方案!

附录三 重点国家/地区的数据合规要求概述

本白皮书汇总了来自七大经济体共 20 个国家及地区的数据合规法律框架，为中企思考、筹划业务出海提供支持。考虑到中国企业进入一个具体国家或地区时，需要了解具体的数据合规要求。基于此，我们将进一步整理 20 个国别的数据合规要求，以便于企业查询和参考。本次特选**新加坡、欧盟、阿联酋、南非、哈萨克斯坦**及**美国**这六大代表性国家和地区发布。

如果您想获取上述内容，或寻求出海数据合规的专业咨询，敬请联系北森与汉坤。

未来，我们将不断优化并更新更多国家及地区的数据合规框架供出海的中国企业参考，敬请持续关注北森与汉坤，以把握最新的出海数据合规动态与信息。

1. 东南亚

越南 | 泰国 | 马来西亚 | **新加坡** | 菲律宾 | 印度尼西亚

2. 欧盟

欧盟 | 德国 | 爱尔兰 | 匈牙利

3. 中东

阿联酋 | 沙特

4. 非洲

肯尼亚 | **南非**

5. 中亚

哈萨克斯坦 | 乌兹别克斯坦

6. 北美

美国 | 加拿大

7. 南美

巴西 | 墨西哥

Beisen北森 | HANKUN