

## 从招聘流程再造到数据出境安全评估 金融机构“备战”个人信息合规操作

本报记者 陈植

随着《数据安全法》、《个人信息保护法》等法规相继实施，越来越多金融机构发现自己的招聘流程正发生着新变化。

“每个人才招聘流程都需经历新的合规操作考验。”一家股份制银行 HR 人员告诉记者。以往，无论是官网/公众号直接招聘，还是第三方招聘平台或内推/猎头渠道，他们都可以随意使用海量应聘者个人信息或存储很长时间（用于人才库建设），但如今，上述做法不再被允许。

比如通过公司招聘官网或公众号收集应聘者个人信息时，银行需先征得每个应聘者的同意，才能收集与处理个人信息；且收集个人信息范围与处理目的需严格遵循最小必要原则；

再如通过第三方招聘平台收集应聘者个人信息时，银行不能再随意使用第三方平台共享的个人信息，而是严格遵守后者的招聘用户服务协议；

若通过猎头或内推渠道收集应聘者个人信息，银行还需先与猎头/内推人签订数据共享协议。

在他看来，这很大程度影响金融机构的人才招聘效率——在通过第三方招聘平台招募人才时，他们还需严格遵守后者的个人信息隐私保护协议，不得将个人信息使用范畴超过上述协议条款；若通过内推或猎头招募高端金融科技人才或专业人才，鉴于内推人与猎头未必与应聘者签订个人信息授权使用协议，他们不得不在必要时通过邮件等方式发送隐私政策，重新取得应聘者的告知同意。

“让我们更伤脑筋的是，有些应聘者需经过海外总部远程面试，由后者决定谁就任境内分支机构高层岗位，但这涉及个人信息出境的安全评估，令整个应聘流程变得漫长。”一位外商独资私募基金 HR 人士向记者直言。

### 招聘合规流程大变革

记者多方了解到，上述应聘环节的个人信息合规操作问题，不仅困扰着金融机构，其他各行各业公司对此也相当“茫然”。

近日，由大成律师事务所与 HR SaaS 服务平台 Moka 联合发布的《在华企业招聘数据合规白皮书》（下称《白皮书》）显示，在参与调研的各行业企业里，仅 15.91% 已深入了解企业数字化招聘领域的“个保法”合规操作相关政策，22.73% 正处于政策研究阶段，40.91% 仅限于初步了解，20.45% 则不了解相关政策。由此可见，当前各行业企业在人才招聘环节的“个保法”合规意识仍有待加强。

大成律所北京办公室高级合伙人邓志松告诉记者，在通过互联网等渠道开展人才招聘环节，企业在简历获取、简历筛选、笔试面试、人才归档等众多复杂的环节与场景均涉及大量应聘者个人信息的处理与收集，需要制定合理方案以应对《个人信息保护法》项下的合规要求，否则可能面临刑事、行政、民事等多重法律责任，甚至直接危及企业的生存。

记者了解到，相关刑事责任包括侵犯公民人格信息罪（最高刑期 7 年）、拒不履行信息网络安全管理义务罪（最高刑期 3 年）。相关罚款则包括按《个人信息保护法》，对某些个人信息违规处理行为向单位处以最高 5000 万元或上一年度营业额 5% 的罚款，向个人处以最高 100 万元罚款；按《数据安全法》，对某些个人信息违规处理行为，向单位处以最高 200 万元罚款，向个人处以 20 万元罚款等；其他行政处罚则包括责令暂停或终止提供服务，责令暂停相关业务或者停业整顿，吊销相关业务许可或吊销营业执照等。

上述股份制银行 HR 人员直言,目前他们已意识到要在人才招聘环节严格遵守《数据安全法》、《个人信息保护法》等法规,银行需对相关个人信息处理制定新的“合规”操作准则,包括开展数据分类分级,识别敏感数据;制定完善的数据安全管理制度规范;选择招聘敏感数据场景开展针对性的数据安全管控;对标相关法律法规进行风险评估,识别新的数据处理安全风险;统筹规划数据安全治理工作,制定安全工作实施路径等。

《白皮书》指出,目前逾 1/3 受访企业决定由 HR 部门牵头处理人才招聘相关的数据合规问题,其次是信息/数据部门(24.39%)和法务部门(21.95%),这意味着这三个部门都将面临较大的招聘流程合规再造与个人信息保护职责。

Moka 首席执行官李国兴告诉记者,这无形间也给 HR SaaS 服务商提出更大的考验。在《数据安全法》、《个人信息保护法》等法规发布后,Moka 针对相关法规要求,对相关数字化招聘管理系统进行调整,包括在应聘者个人信息收集、委托处理、存储等方面做好告知同意、遵循个人信息存储最小必要时间等;针对应聘者个人信息出境要求,则根据企业相关数据出境量,提供数据出境安全评估、个人信息保护认证(CCRC)、个人信息出境标准合同(SCC)操作等服务,力争协助金融等各行业企业做到应聘者数据获取合规、个人信息数据应用与存储合规、应聘者个人数据出境传输合规等。

在他看来,在招聘环节增强数据安全责任意识,完善个人信息数据安全管理体系,正成为企业夯实人才基础的必要措施。HR SaaS 服务商要做的,就是在贴合客户对个人信息合规处理要求的场景下,令相关 HR SaaS 产品做到“开箱即用”,不增加额外负担和培训成本,进而提供好用、易用、实用的数字化招聘个人信息数据合规解决方案。

记者多方了解到,为了简化应聘者个人信息收集使用流程,当前部分银行、私募基金、金融科技平台打算将个人招聘用途与建立人才库需求“合并”,向求职者征求个人信息授权使用许可。

邓志松向记者指出,此举未必合适。究其原因,一是两者涉及的个人信息使用目的明显不同,二是个人数据存储时间也明显不同,比如人才招聘需保留的个人信息通常不超过半年,但建立人才库则可能需保留个人数据数年时间。

“因此,若企业想将应聘者个人信息用于建立人才库,最合适的办法是另外与应聘者签订新的个人信息使用授权协议,明确个人信息用途是用于建立人才库。”他强调说。

#### 个人信息出境安全评估“新挑战”

上述外商独资私募基金 HR 人士向记者透露,此前他们计划在境内招募一位运营总监,但相关应聘者需通过海外总部远程面试,由后者确定最终人选。但这涉及个人信息出境安全评估。

“此前,我们也不知道如何合规操作。所幸《个人信息出境标准合同办法》及标准合同文本在 6 月 1 日正式实施,我们打算通过这种方式申报个人信息出境,等待相关部门通过安全评估后,尽早完成相关岗位的面试招聘工作。”她告诉记者。

在多位金融业内人士看来,相比人才招聘场景,个人信息出境安全评估的更大挑战,将出现在更多跨境金融服务场景。比如在私人银行领域,随着高净值客户热衷资产全球化配置、搭建财富传承架构或寻求海外高端医疗,银行机构需申报大量敏感个人信息出境,并交给海外资管机构或医疗机构以提供更具针对性的服务。但这涉及大量敏感个人信息出境,包括个人以往病史、个人财富信息、个人家庭成员个人信息等,银行都要先向相关部门进行申报,再由后者对出境的个人信息开展安全评估。

“此外,若私人银行要将通过安全评估的出境个人信息交给第三方金融机构或医疗机构,以便他们向境内高净值客户提供专业资产配置/诊疗服务时,还需先与境内高净值客户另外签订一份个人信息授权使用协议,以便相关个人信息使用合规,避免出现私人银行违规对外传送个人敏感信息的状况。”一位熟悉相关业务流程的外资银行合规部人士向记者指出。随着《数据安全法》、《个人信息保护法》相继实施,银行众多金融服务流程难免会变得更加繁琐,但基于个人信息使用合规要求,这都是必须做出的“牺牲”。

邓志松认为，若需要申报个人信息出境的人数较少，通过标准合同文本申请个人数据出境或许是一个合适方法，但需注意对某些敏感个人信息（比如以往病史、个人电子邮件地址等）做好去标识化处理；此外，标准合同文本方式还需企业境外总部尽早签订相关协议以遵守国内个人信息保护相关要求。