

企业人力资源数字化转型中的数据安全治理框架

陈世秋

贵州航天计量测试技术研究所 贵州 贵阳 550009

【摘要】：在数字化浪潮推动下，企业人力资源管理正加速向智能化、数据化转型，人力资源数据的价值释放成为核心竞争力。然而，数据涵盖员工身份、薪酬、健康等大量敏感信息，在采集、存储、传输、使用全流程面临泄露、滥用、篡改等多重风险。本文主要就企业人力资源数字化转型中的数据安全治理框架进行分析，为企业平衡数据价值释放与安全风险防范提供理论支撑与实践路径，助力 HR 数字化转型合规、有序、高效推进。

【关键词】：人力资源；数字化转型；数据安全治理

DOI:10.12417/2705-0998.26.12.049

引言

数字经济的蓬勃发展，推动企业进入全面数字化转型阶段，云计算、大数据、人工智能等技术正深刻改变着企业的运营逻辑。人力资源管理作为企业核心职能之一，其数字化转型进程直接影响企业管理效能，但实践中仍面临诸多阻碍。在此背景下，构建科学、完善的数据安全治理框架，成为企业人力资源数字化转型的前提与保障。

1 数据安全治理的核心意义

1.1 保障员工隐私权益

人力资源数据包含大量敏感个人信息，这些信息的安全直接关系到员工的合法权益。个人信息处理者需采取必要措施保障个人信息安全，防止信息泄露、篡改、丢失，否则将面临高额罚款。数据安全治理通过明确数据使用边界与存储期限，从源头防范隐私侵权风险，确保人力资源数字化转型在法律框架内有序推进，避免合规风险。

1.2 防范经营风险

人力资源数据不仅是员工个人信息的集合，更是企业战略决策的重要支撑。人才画像、绩效分析、晋升轨迹等数据反映企业人才梯队建设现状与核心竞争力，薪酬结构、招聘渠道转化率等数据涉及企业经营策略与商业机密。一旦发生数据泄露，可能被竞争对手利用，导致核心人才流失、商业策略泄露，引发经营风险。数据安全治理通过构建全方位防护体系，防范内部滥用与外部攻击，保障 HR 数据的完整性、保密性与可用性，守护企业战略资产安全，为经营决策提供可靠的数据支撑。

1.3 支撑数字化转型深化

数据安全是数字化转型的基础前提，缺乏安全保障的数字化应用难以持续推进。若员工因隐私担忧对数字化工具产生抵触，或企业因安全风险频繁出现数据泄露事件，将严重阻碍人力资源数字化转型进程。数据安全治理能够消除员工对数据安全的顾虑，通过规范数据管理流程、提升数据质量，确保数据在安全可控的前提下实现共享与分析，充分释放数据价值，支撑人才效能优化、招聘效率提升、薪酬体系优化等战略目标实

现，推动人力资源数字化转型向纵深发展。

1.4 提升企业品牌形象

在人才竞争日益激烈的市场环境中，企业对员工隐私的保护力度与数据安全水平，已成为人才选择雇主的重要考量因素。完善的数据安全治理体系能够体现企业对员工权益的尊重与重视，提升企业雇主品牌形象，增强人才吸引力与留存率。同时，透明、规范的数据安全管理流程能够让员工感受到组织的责任感与专业性，减少因数据安全问题引发的信任危机，增强组织凝聚力，为企业可持续发展奠定人文基础。

2 企业人力资源数字化转型中的数据安全治理框架

企业人力资源数字化转型中数据安全治理框架主要围绕数据治理技术展开，以管理制度规范和数据安全标准体系贯穿整体治理过程，同时，以现有网络安全管理平台作为数据安全治理的支撑基础。

2.1 数据治理技术

数据治理技术是数据安全治理的主要内容，其中，数据资产安全是数据治理的主要内容；网络安全为数据资产安全提供了基本的稳定安全的网络环境；身份安全为数据资产安全提供了基本的访问控制和身份认证；基础保障是数据资产安全保障的基本条件；全生命周期是数据产生到销毁的基本过程。

2.1.1 网络安全

网络安全指传统网络安全防御措施，搭建在人力资源网络系统中保障其安全稳定运行。主要包括防火墙、入侵检测系统、入侵防御系统、Web 应用防火墙、堡垒机、漏洞扫描系统等。

2.1.2 身份安全

身份安全基于网络安全措施实现，以保障数据的可控性为目标，主要包括 2 种能力。（1）身份管理能力：包括用户身份发现、身份管理、黑名单、用户画像、用户行为分析、动态指纹等技术。（2）身份认证能力：包括多因子认证、一次性密码认证、短信认证、指纹认证、认证证书发放、安全终端等技术。

2.1.3 数据资产安全

数据资产安全是数据安全治理技术的核心部分，基于数据分类分级实现包括数据访问安全、数据存储安全和数据流动安全等部分。（1）数据访问安全。数据访问安全是以保护数据资产安全为核心的访问控制技术。技术手段主要包括数据库防水坝、数据库防火墙、动态脱敏和数据库审计等。数据访问与外界产生行为交互，是最易遭受外部攻击的部分，要保障数据访问这一行为的安全性，就要收敛数据暴露面，通过访问控制限定用户对数据资产的访问。（2）数据存储安全。数据库是数据资产的存储载体，在系统日常运行过程中，多数系统的外部访问行为并非大量产生的实时行为，因此需要通过数据加密和数据防勒索重构新数据存储边界，构建完整的数据存储安全保护防线。数据存储安全所涉及的技术主要包括透明加密和防勒索。其中，透明加密可以在保障业务系统透明访问的前提下，实现数据加密存储，主要是指根据用户权限返回明文或密文数据，从而有效保障数据安全和数据使用效率平衡；数据防勒索可以实现主动识别和发现未知风险，提供主机防护、端口防护、文档保护，阻断非法入侵，有效抵御勒索病毒、挖矿病毒等常见病毒。（3）数据流动安全。数据的流动主要包括数据的传输、加工、使用、提供等涉及到数据复制、产生数据副本的过程。一般数据流动是从高安全区域到低安全区域的，由于数据副本可能脱离原安全策略控制，所以需要在数据流动的源头上设置流动边界，从而保障数据流动的目的地受到系统数据安全整体控制。数据流动安全涉及到的技术包括通过静态脱敏、水印溯源、API 检测与访问控制、数据防泄漏等。数据流动安全的要素为：数据是可知的，可流动的，只有流动的数据才能更好地促进数据价值释放；数据流动必须经过授权，严禁任何未授权的数据流动；数据是通过特定的管道或路径单向流动的；数据流动的目的地是可知的，被允许的；流动后的数据使用和再流动是受到限制的；流动的每个环节是全链路可见的，是可追溯的。（4）数据分类分级。数据分类分级是指人力资源系统现行的数据分类分级保护制度，通过对数据敏感性、重要性和潜在风险对数据进行等级划分，规定了数据访问权限、数据存储域划分和数据流向，是实现数据资产安全技术的基本原则。

2.1.4 基础保障

基础保障是应对数据安全事件的重要支撑。现有人力资源数据运行的综合性安全管理平台可以提供基本的整体网络系统的安全保障；通过异地容灾、数据备份保障系统等手段，可确保系统安全稳定运行，降低因意外情况导致数据丢失或系统瘫痪的风险。此外，对备份数据的合理运用还可以进一步释放数据资产的价值。

2.1.5 全生命周期

数据全生命周期管理包括数据收集、数据存储、数据传输、数据处理、数据交换及数据销毁等流程。人力资源网络数据安全治理是基于数据全生命周期进行的全面、完整的治理和保障。

2.2 管理制度规范

数据安全管理制度规范是保障数据安全治理举措行之有效的必要前提，为提升数据安全防御能力、建立健全数据安全保障制度，国铁集团从数据安全事件处置、数据安全应急预案、数据出境管理等方面规定了相应的管理规范制度。

2.3 数据安全标准体系

我国针对新时代数据安全保护的新形势，发布了包括数据分类分级保护、数据安全风险评估、数据监测预警和个人信息保护等一系列数据安全标准体系。这些数据安全标准体系为人力资源数据安全治理提供了理论依据和基本方法。

2.4 平台支撑

以现有各网络安全平台为基石，充分发挥整合现有网络安全保障平台的数据安全防护能力，在数据服务平台、大数据和人工智能平台、数据全流程监管平台、态势感知平台等基础上进一步提升数据安全治理的有效性。

3 企业人力资源数字化转型数据安全治理路径分析

3.1 构建全流程规范体系

制度建设是数据安全治理的根基，需立足人力资源数字化转型场景特性，形成覆盖数据生命周期的规则框架。一是在数据采集环节，明确“合法、正当、必要”原则，例如员工人脸信息仅用于身份核验且需单独授权，学习记录采集需同步告知用途及保存期限，从源头守住合规底线。二是在存储环节，推行分类分级管理制度，采用加密存储并定期异地备份，通过差异化管理提升资源配置效率。三是在使用与流转环节，需细化权限管理规则，按照“最小权限”原则设置访问层级：人力资源部门可查看全员培训数据用于分析，业务部门仅能调取本部门员工的相关记录，普通员工仅可查阅个人学习档案。同时建立动态修订机制，每年度结合法律法规更新、业务模式调整等情况，组织跨部门评审并优化制度条款，确保规则始终与发展需求同频共振，为数据安全治理提供持续有效的制度指引。

3.2 形成协同联动机制

管理效能的发挥需要打破部门壁垒，企业应构建全链条协同的治理格局。一是企业可建立“数据安全治理委员会”，由企业分管领导牵头，人力资源、信息技术、法务、业务部门代表共同参与，每月召开联席会审议安全风险、协调资源投入，例如在上线新培训平台前，委员会需联合审核数据安全方案，避免出现“重功能轻安全”的情况。二是企业在日常管理中要

明确各部门职责,例如人力资源部门负责培训业务与安全要求的衔接,信息技术部门承担技术防护实施,法务部门提供合规咨询等,避免出现职责不清导致的工作推诿现象,形成人人有责、人人负责的良好局面。

3.3 加强技术创新

技术创新是数据安全治理的核心支撑,企业需构建“主动防御+智能预警”的技术体系。在基础防护层面,可采用国密算法对静态数据加密存储,传输过程中启用SSL/TLS协议确保链路安全,防止数据在存储和流转中被非法获取。在访问控制环节,可引入“多因素认证”技术,员工登录培训平台时,除账号密码外,还需通过手机验证码或人脸核验,重要数据的导出操作需经部门负责人审批并留下数字签名。在智能化升级方面,可引入数据安全态势感知平台,通过机器学习分析历史访问数据,构建正常行为模型。当出现“非工作时间批量下载数据”等异常行为时,系统自动发出预警并触发临时冻结,技术人员可在5分钟内响应处置。针对新兴场景需求,企业可探索隐私计算技术的应用。同时,企业应定期开展技术适配性评估,确保防护手段能应对新型攻击方式,让技术防护始终跑在风险前面。

3.4 提升全员素养能力

人员素养水平直接影响治理成效,需实施分层培养策略。

一是针对管理层,企业可开展“数据安全与企业战略”专题培训,通过案例讲解,帮助其理解安全投入对人才培养的长期价值。二是对执行层员工,企业可用漫画、短视频等形式讲解日常操作规范,通过在线测试检验学习效果,确保规范入脑入心。三是技术与风控团队需强化专业能力,企业内部可定期组织攻防演练,模拟“数据泄露应急处置”“系统被入侵后的恢复流程”等场景,提升实战能力;同时,鼓励企业技术人员积极参与行业技术论坛,跟踪数据脱敏、零信任架构等前沿技术的发展动态。此外,企业可建立正向激励机制,如可设立“数据安全金点子”奖项,对提出有效改进建议的员工给予表彰,将安全表现纳入绩效考核,让每个岗位的员工都成为数据安全的守护者。

4 结语

人力资源数据作为企业战略资产与员工隐私权益的核心载体,其安全与否直接关系到企业的合规经营、品牌形象与可持续发展。有效的数据安全治理不仅能够防范安全风险、保障合规经营,更能为人力资源数据价值释放扫清障碍,支撑人才效能优化、智能决策落地。未来,随着人力资源数字化工具的持续迭代、法律法规的不断完善,企业需坚持动态适配原则,持续优化治理框架,强化技术创新与文化建设,最终实现数据价值与安全风险的动态平衡,为企业高质量发展注入持久动力。

参考文献:

- [1] 王丹.信息化背景下高校人力资源数据分析问题及改善措施[J].人才资源开发,2022,(22):32-34.
- [2] 李健男.大数据时代下的人力资源管理[J].上海商业,2022,(03):153-155.
- [3] 李霞.人工智能对企业人力资源管理的影响研究[J].企业改革与管理,2022,(03):67-69.
- [4] 任仁.浅析大数据技术下的公共资源交易信息安全风险[J].电子元器件与信息技术,2021,5(08):133-134.