GDPR下涉欧企业的员工个人数据合规管理*

王　倩　顾雪莹

摘　　要： 欧盟的《通用数据保护条例》(GDPR)号称是“史上最严个人数据保护立法”，该条例适用于劳动关系。我国有众多涉欧企业，在生产经营和用工管理中经常要进行员工数据处理活动，从而面临着GDPR的合规挑战。在合规管理中，涉欧企业首先要确保处理员工个人数据具备合法性基础，然后要履行与员工的知情权、删除权、可携带权等权利相对应的义务，还应该遵守保障数据处理过程安全性、全面记载处理活动、事前风险评估等合规要求，在做好员工个人数据的本地化管理的同时也要确保数据跨境传输时流动的合法性。

关 键 词： GDPR；　员工个人数据保护；　涉欧企业；　数据合规

作者简介： 同济大学　法学院　副教授　上海　200092
同济大学　法学院　硕士研究生　上海　200092

中图分类号： D95
文献标识码： A
文 章 编 号： 1005－4871(2021)02－0117－15

* 本文受国家社会科学基金一般项目“数字化时代劳动者的个人信息保护研究”(编号：20BFX190)资助。

数字经济时代移动互联网、大数据、云计算、人工智能等科技的发展，使数据的产生和处理呈现爆炸式增长，给个人数据保护带来了巨大的挑战。2018年5月25日《通用数据保护条例》(General Data Protection Regulation，以下简称“GDPR”)在欧盟成员国内正式生效实施，该条例可谓是史上最为严格的个人数据保护规范，违反者可能面临最高2000万欧元或上年度全球总营业额4%金额的罚款。据2020年10月的报道，由于H&M公司过去几年中一直大范围地收集员工请病假、就医以及病情诊断等详细信息，还有管理人员在与员工的非正式聊天中挖掘其家庭问题或宗教信仰等个人数据作为员工考评或任用决定的参考，德国汉堡数据保护局开出了高达3530万欧元的罚单。①

GDPR适用于劳动关系中的个人数据保护，其第88条明确规定，成员国可以通过法律或通过集体协议制定特定规则，以确保在雇佣语境下处理雇员个人数据时保护其权利和自由，这在如下情形中尤其适用：为了招聘、履行劳动合同，履行法律或集体合同规定的义务；对工作的管理、计划和组织；工作场所的平等与多样性；工作中的健康和安全；对员工和顾客财产的保护；为了行使和履行与雇佣相关的权利和义务；为了终止雇佣关系。德国《联邦数据保护法》第26条正是基于此授权对员工的个人数据保护做了针对性安排。我国有众多在欧盟境内设立了业务机构或雇佣了欧盟境内员工的企业，生产经营和用工管理中不可避免地要进行员工的个人数据处理。虽然目前我国还没有出现涉欧企业因为违反GDPR而受罚的案例，但是仍然应该提前了解相关情况、做好相应预防措施，尤其在我国个人信息保护的意识比较淡漠的背景下，涉欧企业更容易“触雷”。那么，应该采取什么措施才能达到GDPR的合规要求，如何平衡企业的经营管理需求与员工的个人数据保护？了解GDPR对个人数据保护的设计理念与制度框架，探究其在劳动关系中适用的特殊问题，是涉欧企业在用工中实现GDPR合规管理所必须关注的问题。

一、受到GDPR管辖的涉欧企业

根据GDPR第4条的定义，“个人数据”是指一个被识别或可识别的自然人(数据主体)的任何信息，而可识别是指通过姓名、身份证号码、位置数据、在线身份识别码这类标识，或通过自然人的一个或多个身体、生理、遗传、心理、经济、文化或社会身份等要素，能够直接或间接地识别该自然人。“处理”是指针对个人

① EDPB, Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre, https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_de, 访问日期：2020-12-12.

数据或其集合的任何一个或一系列操作，如收集、记录、组织、建构、存储、修改、检索、咨询、使用、披露、传播或以其他方式利用、排列或组合、限制、删除或销毁，无论该操作是否采用自动化方式。“数据控制者”是能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、代理机构或其他组织，而“数据处理者”是指为数据控制者处理个人数据的个人或组织。劳动关系中的数据主体是员工，而涉欧企业一般是以数据控制者的身份出现，少数情况也可能是数据处理者。[①] GDPR极大地扩张了其域外管辖范围[②]，具体到员工的个人数据保护，我国涉欧企业可能在两种情形下受到GDPR管辖。

（一）欧盟境内存在业务机构的企业

根据GDPR第3条第1款，该条例适用于数据控制者或处理者在欧盟境内存在业务机构活动的背景下所实施的个人数据处理行为，无论该处理行为是否发生在欧盟境内。要理解这一复杂的表述，关键注意以下三点。

第一，重要的是在欧盟境内存在业务机构，而非住所。GDPR在序言（22）条中将业务机构又称为“营业场所”，而营业指通过稳定的安排有效且真实地开展经营活动，而该安排的法律形式并非判断其是否可以称为营业场所的决定性因素。[③] 即只要企业在欧盟境内设有机构并营业，无论机构是否具有分公司或子公司的地位，即使是以办事处、派遣机构等形式存在，企业也应当受到管辖。

第二，条例的适用与数据主体是否拥有欧盟公民身份、是否长期居住在欧盟境内无关，与个人数据处理活动是否发生在欧盟境内也无关。[④] 比如我国涉欧企业将中国国籍的员工外派到欧盟境内的办事处工作，即使对员工的个人数据处理发生在中国总部，也受到GDPR的管辖。

第三，条例的适用限于“在业务机构活动的背景下”所实施的个人数据处理行为，包括“该欧盟境内的业务机构自己进行的个人数据处理活动”和“为该欧盟境内的业务机构进行的个人数据处理活动”。也就是说，我国涉欧企业并不会因为在欧盟境内设有业务机构而将企业全部的个人数据处理活动置于GDPR的管

① 但GDPR对于数据控制者和处理者几乎是同等对待的，数据主体可以直接起诉或投诉处理者来寻求救济，原则上控制者和处理者需对数据主体的损害承担连带责任。所以，一方面涉欧企业作为数据控制者在选择薪酬外包服务商等处理者时应该审慎，另一方面即使涉欧企业只是数据处理者，也同样面临着较高的GDPR合规要求。

② 俞胜杰、林燕萍：《通用数据保护条例域外效力的规制逻辑、实践反思与立法启示》，载《重庆社会科学》，2020年第6期，第62－79页，这里第63页。

③ Wolfgang Däubler/Peter Wedde/Thilo Weichert/Imke Sommer-Wolfgang Däubler, Kommentar zum EU-Datenschutz-Grundverordnung und BDSG neu, 2. Aufl. 2020, DS-GVO Art. 3 Rn. 10ff.

④ Boris Paal/Daniel Pauly-Stefan Ernst, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl. 2018, DS-GVO Art. 3 Rn. 4.