On May 25, 2018, a short 12 months from now, employers must be in full compliance with the General Data Protection Regulation (GDPR) for EU human resources data. The GDPR requirements regarding notice, data breach notification, consent, and an individual's access to data are significantly broader and stricter than the requirements under current national data protection laws and the EU Data Protection Directive. Additionally, the penalties for noncompliance with the GDPR are severe. Employers that violate the GDPR face fines of 20 million Euros or 4 percent of the company's worldwide revenue, whichever is greater.

GDPR Compliance for HR Data Is Complex

Compliance with the GDPR for HR data will present greater challenges than the compliance requirements for customer data. For example, the GDPR expressly provides that individual EU Member States may enact laws specific to the processing of employee data to implement the GDPR. Germany and Austria have already passed legislation that provides for specific requirements regarding employee data or specifies that the processing of employee data will be governed by national employment laws in addition to the GDPR. Thus, to comply with the GDPR, employers must analyze and follow the data protection and employment requirements of each EU Member State in which they have employees.

Some other areas where GDPR compliance will differ for HR data include the following:

1. While businesses typically rely on a customer's consent to collect and process the customer's information, employers generally will not be able rely upon an employee's consent to process the employee's data because such consent will not be deemed voluntary or freely given because of the unequal bargaining positions between employers and employees. Thus, employers must rely on other grounds to legally process employee data.

2. Unlike customer data which typically is collected and processed through business websites, employee data is collected and stored on multiple sources such as human resources information systems (HRIS), corporate intranet and email systems, social media platforms, mobile devices, and third-party payroll and benefits service providers' systems. Thus, mapping employee data and providing employees access to their data will be more complex.

3. The GDPR restricts the processing of criminal history information to only those situations specifically authorized by EU or Member State laws. Thus, employers must tailor their criminal background check procedures to comply with individual Member State laws.

4. The GDPR creates new rights for data subjects regarding the portability of their data. Employers will need to provide a mechanism to permit terminated employees to...
transfer their data to new employers.

Next Steps

Because GDPR compliance for human resources data will be different from and more complex than compliance for commercial data, companies’ human resources departments and internal employment counsel should take the lead regarding their organizations’ compliance efforts. Further, while the GDPR effective date of May 25, 2018, seems to be a long way off, employers need to begin compliance efforts now to complete all compliance requirements by the effective date and avoid severe penalties.

On June 22, 2017, Ogletree Deakins Data Privacy Practice Group members Grant D. Petersen (Shareholder, Tampa) and Simon J. McMenemy (Managing Partner, London) will present a one-hour webinar, “The Countdown Begins: Complying With the EU General Data Protection Regulation.” For more information and to register, please click here.