Reinhart

# New European Data Privacy Law Impacts U.S. Employers' Handling of Human Resources Data

The European Union recently expanded protections for EU data, with far reaching implications for companies even outside of the EU. Its new law, the General Data Protection Regulation ("GDPR"), went into effect on Friday, May 25, 2018. Earlier this year, Reinhart's Data Privacy and Security group published an overview of the law and its requirements.

Employers in the U.S. should assess whether their HR data systems (e.g., payroll, benefits, directories, or recruitment) collect, process, or store data that is protected by the GDPR. If the data is protected, the GDPR places new requirements on employers that are far more stringent than those required in the U.S. For example, U.S. employers will not generally be able to rely on employee consent to justify collecting, processing, or monitoring GDPR-protected data. Non-compliance with the GDPR's requirements carries harsh financial penalties.

The GDPR protects individually-identifying data (referred to as personal data) about an EU "data subject." Any information that connects to an individual is covered (e.g., name, e-mail address, IP address, and social media posts). Although "data subject" will often mean someone who lives in the EU, it could also describe someone who travels in the EU and creates data while she is there (as we all do, regardless of our location, by using computers, personal devices, or the internet).

Employers that have an active and ongoing practice of sending and receiving HR data to an affiliated company in the EU (for instance, a parent-subsidiary or franchise relationship) are those most likely transferring or processing GDPR-protected HR data. Companies that transfer GDPR-protected HR data to the U.S. also need to assess whether the transfers themselves comply with the GDPR.

Still, other U.S.-based employers should assess their risks. Hiring from the EU or sending employees to the EU for work could trigger the GDPR's requirements. For instance, employers may be required to protect any e-mails and other documents containing personal information (e.g., credit card receipts) transmitted to and from employees who are based or traveling in Europe.

If U.S. employers collect, process, or store EU data within their HR data systems, they should align their systems with the GDPR's stringent requirements. Employers, for example, should revise their employee privacy and monitoring

**POSTED:**

Jun 1, 2018

**RELATED PRACTICES:**

Corporate Law
https://www.reinhartlaw.com/practices/corporate-law

Labor and Employment
https://www.reinhartlaw.com/practices/labor-and-employment

**RELATED SERVICES:**

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

Employment Litigation
https://www.reinhartlaw.com/services/employment-litigation

Labor Relations
https://www.reinhartlaw.com/services/labor-relations

FMLA Leave and Disability Management
https://www.reinhartlaw.com/services/fmla-leave-and-disability-management

Cafeteria Plans and Fringe Benefits
https://www.reinhartlaw.com/services/cafeteria-plans-and-fringe-benefits

Software, Technology and Licensing
https://www.reinhartlaw.com/services/software-technology-and-licensing

policies, electronic communications policies, and similar policies to account for circumstances in which the GDPR applies.

If you have questions about how your HR data systems or policies are impacted by the GDPR, please contact a member of Reinhart's Data Privacy and Security group or your Reinhart attorney.

**RELATED PEOPLE:**

Michael J. Gentry
https://www.reinhartlaw.com/people/michael-j-gentry