Reinhart

Employers Caught Off-Guard by the GDPR Should Prepare for a New Wave of Similar US State Laws

Many employers in Wisconsin and around the United States were surprised to recently learn that the European Union's new data privacy law, the General Data Protection Regulation (GDPR), may apply to them. Despite being based in the US, an employer's HR data systems (e.g., payroll, benefits, directories, or recruitment) might collect, process, store, or transfer data tied to EU-based employees (either its own employees or those of an affiliated company). If so, the GDPR, requires impacted employers to notify those EU-based employees about how and why it uses their data, grant them access to the data and to provide greater data protections than are generally required by US law.

While US-based employers evaluate how best to comply with the GDPR, California legislators have passed a bill that moves US law in the same direction. On June 28, 2018 Governor Jerry Brown signed that bill – the California Consumer Privacy Act (CCPA) – into law. The CCPA will require covered companies that receive personal information (broadly defined) about California residents to provide greater protections to that personal information, and to offer those California residents more liberties with respect their personal information. For instance, like the GDPR, the CCPA will provide California residents with the right to request disclosure, deletion, and portability of their personal information, and will require companies to disclose the reasons why they collect and store that personal information. For employers covered by the CCPA, this means assessing HR data systems and potentially revamping them if they interact with employee data protected by the CCPA (i.e., personal information about California-based employees).

Critically, when the CCPA goes into effect in January 2020, it will apply to more than just California-based companies. Instead, any company must comply if it receives personal information about California residents and meets any one of the following thresholds:

- Has annual revenues of at least U.S. $25 million.
- Obtains personal information from at least 50,000 California residents, households, or devices.
- Receives more than 50% of its revenue from selling personal information about California residents.

POSTED:

Sep 5, 2018

RELATED PRACTICES:

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

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

Employee Benefits
https://www.reinhartlaw.com/practices/employee-benefits

RELATED SERVICES:

Corporate and Governmental Benefit Plans
https://www.reinhartlaw.com/services/corporate-and-governmental-benefit-plans

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

Wage and Hour
https://www.reinhartlaw.com/services/wage-and-hour

FMLA Leave and Disability Management
https://www.reinhartlaw.com/servic

Reinhart

Employers in Wisconsin and from other states around the US with California-based employees should evaluate whether they will need to comply with the CCPA. Even companies that are comfortably below the $25 million global revenue threshold may need to comply if their websites (even inadvertently) collect IP addresses from or use cookies to collect browsing information on 50,000 or more California residents or devices. If applicable, employers must abide by the CCPA's requirements in handling all of their California-based employees' personal information.

California is not the only state to hold employers and other companies to heightened data privacy and security standards. Colorado recently expanded the requirements for handling Colorado resident personally identifiable information. As a result, employers with Colorado-based employees are, as of September 1st, required to implement "reasonable security procedures" to protect their Colorado-based employees' personally identifiable information, and to require their third party vendors to do the same. Colorado's law also expands data breach notification requirements in the event that Colorado resident personally identifiable information is compromised.

Without a doubt, the CCPA and Colorado's data security law will require compliance from more Wisconsin companies than does the GDPR. Employers with employees in Colorado should immediately review and update their HR data security protocols. Employers with California-based employees should similarly evaluate their HR data systems to avoid being caught off-guard when the CCPA goes into effect.

If you or your company has compliance questions about the CCPA or about Colorado's data privacy law, please contact Michael Gentry or a member of Reinhart's Data Privacy and Cybersecurity Group.

es/fmla-leave-and-disability-management

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

Employee Benefits Plans in Mergers and Acquisitions
https://www.reinhartlaw.com/services/employee-benefits-plans-in-mergers-and-acquisitions

Trade Secret and Nondisclosure Counseling
https://www.reinhartlaw.com/services/trade-secret-and-nondisclosure-counseling

RELATED PEOPLE:

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