PUBLICATION

Employers Get Ready: GDPR Implications in the Employment Law Arena

March 06, 2018

If you manage employees or regularly practice or advise in the area of employment law, you know one of the primary rules in the playbook: document, document, document. In the employment-law world, we regularly rely on data housed on the employer's system, such as email communications, to bolster investigations or to refute allegations during the course of litigation. But what if you could be subjected to substantial monetary penalties for improperly collecting your employees' data or for failing to adequately inform employees of the purpose for which the data will be collected? If you're wondering how this situation could arise, you should consider the European Union's General Data Protection Regulation (GDPR).

The Basics

The GDPR will be enforced starting May 25 of this year. It will apply to all companies processing the personal data of data subjects in the EU, regardless of the company's location, if it offers goods or services to data subjects in the EU or monitors the behavior of data subjects in the EU. A data subject is generally defined as a natural person whose personal data is processed by a controller or processor. Notably, the EU defines personal data as any information related to a natural person that can be used to directly or indirectly identify the person, which can include a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. The penalty for breaching the GDPR is a fine of up to four percent of annual global turnover or €20 Million (whichever is greater). This is the maximum fine, but it can be imposed for noncompliance with the conditions for employees' consent to processing their personal data.

The rules governing consent are rigorous. Valid consent requires that it be (1) freely given, (2) specific, (3) informed, and (4) an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. These elements have been strictly construed in the EU.

For example, for consent to be freely given, there must be a real and genuine choice. The Article 29 Working Party, which will be the European Data Protection Board as of the effective date of the GDPR, has issued guidelines on consent under the GDPR. Those guidelines provide that "consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment." In the employment context, the imbalance of power between employers and employees creates particular challenges to obtaining freely given consent. In fact, the consent guidance indicates that consent from employees is only likely to be freely given in exceptional circumstances. Therefore, the vast majority of processing of employee data will likely need to be carried out based on lawful grounds other than consent.

There are a variety of lawful grounds for processing personal data that are set forth in the GDPR. For instance, the GDPR provides that it is lawful to process personal data when doing so is necessary:

- for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- for compliance with a legal obligation to which the controller is subject; and
- in order to protect the vital interests of the data subject or of another natural person.

Consent is not required in the presence of other lawful bases for processing.

Implications in the Employment Law Context

In American jurisprudence, employees generally do not have a reasonable expectation of privacy in data stored in their employers' systems. But, if you are operating in the EU, the GDPR will apply to your processing of personal data for employees in the EU. So, if you have employees in EU countries, you should, at a minimum, identify what employee data you have, where it resides, how you use and disclose it, and what your lawful basis is for processing the data. You may also need to reevaluate your company policy regarding collection of employee information and employer access to that information. For example, you may need to revisit your handbook if you have a computer policy that states that employees should not use company devices or email for personal matters and that employee email use may be monitored. Also note that the GDPR will apply to any service providers (i.e., data processors) you utilize for processing employee data. Employers who rely on other companies to collect and/or process data relating to EU-based employees would be well-advised to review and update contractual relationships to ensure the service providers are able to perform the services in accordance with the GDPR.