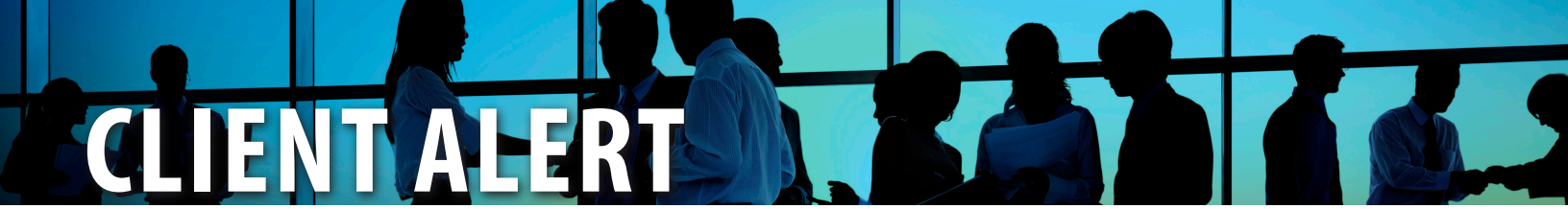


DATA PRIVACY AND CYBERSECURITY

THE GDPR COVERS EMPLOYEE/HR DATA AND IT'S TRICKY, TRICKY (TRICKY) TRICKY: WHAT HR NEEDS TO KNOW

by Sara H. Jodka

The European Union (EU) General Data Protection Regulation (GDPR) comes into effect on May 25, 2018, so in less than 60 days. While many companies have been working to ensure compliance with respect to their customer and vendor data, one extremely tricky area that must not be overlooked is the GDPR's application to employee/HR information.

While many US companies may think the GDPR does not apply to them because they do not have a location in the EU, the GDPR applies to US or multinational companies that have any employees in the EU. The GDPR specifically applies to the processing of "*personal data or data subjects… who are in the EU*". There is no requirement that the employee reside or be a citizen of the EU, just that the employee be in the EU.

So, what is "employee data" or "HR data"? Quite simply, it is an employee's application file, personal file, payroll information, leave/medical file, and all the information employers have about their employee whether it be to hire/fire, pay, provide benefits, enroll in 401k and similar programs, etc. In other words, anything that employer collects that contains an employee's personal information.

Personal information is broad under the GDPR and includes any information relating to an identified or identifiable person who can be identified by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

As for "processing", that term is also broad and includes collecting, storing, recording, gathering, organizing, altering, retrieving, using, disclosing, or otherwise making available and employee's personal data. Basically, if you collect an employee's personal data you are a processor.

There are number of GDPR compliance concerning HR data as opposed to compliance obligations for customer or vendor data, *i.e.*, business to customer (B2C) or business to business (B2B) data that make GDPR/HR compliance extremely challenging and tricky for employers. Here are a few.

Consent v. Legitimate Interest

One of the fundamental principles of the GDPR is that a data subject, *i.e.*, an employee must consent to the processing of personal information. Consent requires that the data subject be fully informed of the nature and scope of the processing, including understanding fully how the information will be processed, used, and transferred to other entities.

While a lot of guidance has been published as to how businesses can obtain consent from customers and vendors, guidance has also been issued that has indicated that it is basically impossible for employees to give voluntary consent to their employer to allow the employer to gather, process, and/or transfer their HR data because of the unequal negotiation power between employers and employees.

Without consent, there are only a number of other ways an employer can process data, and those are identified in the GDPR as "legitimate basis", which include, in relevant part: (1) to perform an employment contract; (2) to comply with legal obligations; and (3) to further a legitimate interest of the employer.

One issue with the employment contract allowance is that very few employees have "employment contracts" as most employees are "at-will" and most policies, including the eligibility to medical and other benefits is a matter of policy. This allowance, however, would apply to contracts, including collective bargaining contracts, which provide terms for employee pay, leave, discipline, and any terms outlined expressly in the contract.

The "legal obligation" allowance is also fairly narrow as the legal obligation must be based on an EU law, not a US law.

Most employers will have to rely on the "legitimate interest" allowance, but to do so, employer must first do some ramp up work. To use the legitimate interest allowance, employers must perform a privacy impact assessment balancing their legitimate interest against the employees' privacy interests. The hard part, this must be documented to demonstrate that the employer's legitimate interest does outweigh the employees' rights.

The next step that employers cannot overlook is that, even if the employer has a basis to process employee data, the employer must then provide notice to the employee that spells out exactly what data the employer is going to collect and what the employer is going to do with it.

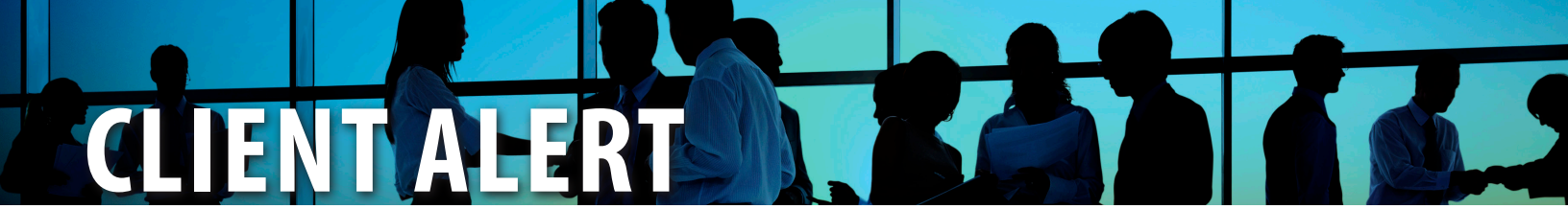
Requirements for Sensitive HR Data

Under the GDPR there is "personal data" (discussed above) and there are special categories of data, *i.e.* sensitive data. Sensitive data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing of sensitive data is strictly prohibited unless 1 of 10 exceptions are met, including: with express consent; as necessary for the purposes of carrying out employment obligations, including compliance with a collective bargaining agreement; and to protect the vital interest of the data subject.

Data Protection Impact Assessment (DPIA)

The GDPR requires businesses perform a DPIA when data processing



is likely to result in a high risk to the rights of data subject. Recent guidance on this issue provides that a DPIA should be performed when any **two** of the following exist:

1. use of automated decision-making with legal or significant effect;
2. evaluation of scoring of data subjects, including evaluating work performance;
3. systematic monitoring;
4. processing of sensitive data (which employers will have);
5. processing data on a large scale;
6. processing data of vulnerable data subjects (which includes employees);
7. transferring data outside the EU;
8. engaging in an innovative use or application of technological solutions; or
9. engaging in processing that prevents a data subject from exercising a right.

Given that employers will almost definitely meet two of these, employers will have to perform a DPIA.

Notice of Rights

Under the GDPR, data subject are afforded a number of rights regarding their personal data, including the right to erasure, the right of portability, the right of recertification, the right to restrict processing, the right to object, etc. While many of these rights are limited in the employment context, many require employers act to ensure data subject rights are protected. As such, employers must ensure they have put measures in place to notify employees of these rights, to afford employees these rights; and that allow them to continue to monitor the exercise of these rights for future compliance.

Designation of a Data Protection Officer (DPA)

The GDPR provides that a company must designate a DPA if its core activities involve regular and systematic monitoring of data subject on a large scale or involve the processing of sensitive data on a large scale. The issue for HR data processing is that it typically involves large amounts of sensitive data and monitoring of employees. As such, a company that might otherwise not have to designate a DPO for processing of consumer or vendor data, may be required to for processing HR data.

Compliance with Country-Specific Data Protection Requirements

The GDPR allows EU countries to enact additional requirements for processing HR data through national laws and collective agreements, and these laws can be stricter than the GDPR. France has laws that prohibit personal information from being transferred outside France. Germany passed a law with additional or stricter HR data processing requirements. In addition, many union collective bargaining agreements and works council agreements that cover employees cover additional or stricture requirements for processing employee data.

This also extends to following specific country labor laws that regulate how and when employee information can be processed and how long specific types of HR data can be retained.

Enforcement

Business are more likely to face enforcement issues concerning employee HR data because employees and/or their trade unions and work councils are more likely to initiate claims exercising employee rights under the GPDR, collective agreements, national data privacy laws, and works council agreements.

Increased Financial Exposure

The GDPR has two levels for fines for GDPR violations depending on the nature of the violation. Unfortunately for employers, the majority of processing HR data triggers risk exposure in the higher fine category which allows fines of 20 million euros or 4 percent of the company's worldwide revenue, whichever is greater.

Don't Miss Steps:

1. Ensure HR it is part of the GDPR compliance discussion. GDPR compliance is a team effort and HR should play a critical component of that role.

2. Determine what personal and/or sensitive information on employees you have and determine what you are using it for and where that information is located/stored.

3. Conduct a DPIA.

4. Determine if you need to designate a DPO.

5. Determine what legitimate basis you have to process information, and if it is because of the employer's "legitimate interest" ensure you have documented the balancing of the employer's legitimate interest against the employees' data privacy rights.

6. Notify employees of the nature and scope of processing and gain consent to the extent any personal data is being processed for any reason other than one based on a legitimate basis (even though consent may be challenged as the GDPR enforcers will likely prefer you ask permission rather than ask forgiveness).

7. Ensure employees are informed of data subject rights regarding their information and ensure internal policies and procedures are in place to allow employees to exercise these rights and to monitor compliance going forward.

8. Review specific EU country laws and collective agreements to ensure that stricter laws for processing HR data are being followed, including data destruction laws.

9. Ensure policies and mechanisms are put in place to ensure future compliance as the GDPR is not a one-and-done deal. Employers must continue to stay in compliance as new employees entire the workforce, as employees leave the workforce, and as new data containing protected information are produced, collected, stored, transferred, etc.

While this certainly does not cover everything employer needs to know about HR data and the GDPR, it is a good starting point and can assist you in structuring a more in-depth conversation with data privacy counsel.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of data privacy and cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.