Legal Update Article

Is Employee Consent under EU Data Protection Regulation Possible?

By Joseph J. Lazzarotti

February 27, 2018

Meet the Authors

Joseph J. Lazzarotti

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

Construction
Financial Services
Government Contractors
Healthcare
Higher Education
Hospitality
Insurance
Life Sciences
Manufacturing
Media
Privacy, Data and Cybersecurity
Real Estate
Retail
Technology
Transportation

U.S. organizations that control or process the personal data of European Union residents likely are subject to the EU's new data protection requirements, the General Data Protection Regulation (GDPR). The GDPR takes effect on May 25, 2018.

The GDPR, which supersedes the 1995 EU Data Protection Directive, imposes harsh penalties for noncompliance. Non-EU organizations that were not expressly required to comply with the 1995 standard may be covered by the GDPR. Now is the time for U.S. employers to determine whether they are covered by the GDPR (see our blog post, Does the GDPR Apply to Your US-based Company) and, if they are, begin preparing their HR data systems for compliance.

Bases for Processing Employee Data

An employer that needs to process EU employee data must have a lawful basis for doing so under the GDPR. One of the six lawful bases for processing an EU resident's personal data in Article 6 of the GDPR is *"the data subject has given consent to the processing of his or her personal data for one or more specific purposes."*

A common practice in the U.S. is to rely on blanket consent clauses in employment contracts or handbooks that permit employers to process employee personal data. U.S. employers often also rely on implied consent from employees. (For example, consent is implied when an employee uses a company-provided laptop and is told the employer monitors use and may search the laptop and the employee should have no expectation of the privacy in the laptop.) However, such practices may not be considered valid forms of consent for lawful processing of personal data under the GDPR.

Concerns Over Validity of Consent

The Data Protection Authorities (DPAs) of EU member states implement and enforce data protection law and offer guidance. They also have the authority to impose substantial fines.

In recent years, DPAs have stressed that the use of employee consent requires careful evaluation. They questioned the employee's ability to give valid consent because of his or her dependence on the employer. The inherent imbalance in the employment relationship calls "voluntary" consent into question.

Codifying the DPAs' position, the GDPR provides that consent must be *"freely given, specific, informed and unambiguous."* Moreover, the GDPR adds, consent is not *"freely given"* where a *"clear imbalance of power"* between the data controller (*i.e.,* employer) and the data subject (*i.e.,* employee) exists.

The EU Information Commissioner's Office in its GDPR Guidance (March 2017 draft) states that employee consent for use of personal data by an employer is likely

considered inappropriate under the GDPR:

> *if for any reason you cannot offer people a genuine choice over how you use their data, consent will not be the appropriate basis for processing. This may be the case if, for example: … you are in a position of power over the individual – for example, if you are a public authority or an employer processing employee data.*

The Article 29 Working Party, an advisory board comprised of a representative from the DPAs of each EU member state, the European Data Supervisor, and the European Commission, proposed guidelines on consent under the GDPR. The Working Party emphasizes the imbalance of power in the employment context:

> *Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.*

Organizations may need to reconsider, for example, whether standard video monitoring of employees in common work areas is permissible generally without the affirmative consent of employees. The Working Party also advises that the imbalance of power in the employment relationship makes voluntary consent questionable and, for most work-related data processing, the GDPR lawful basis relied upon "cannot and should not" be the employee's consent.

Where Consent May be Permitted

According to the Working Party, in limited circumstances, an employer may demonstrate that consent is freely given and is a lawful basis for data processing. "Employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent."

The Working Party offers the following example of consent freely given and is a lawful basis for data processing under the GDPR:

> *A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penali[z]ed in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.*

Avoid "Bundling" Consent

Article 7 of the GDPR warns against "bundling" consent with standard contract terms or conditions. The Working Party advises that Article 7 seeks to ensure the purpose of personal data processing is not disguised or bundled with the provision of a contract of a service for which these personal data are not necessary.

Another of the six lawful bases for processing an EU resident's personal data in Article 6 of the GDPR is when "processing is necessary for the performance of a contract." The Working Party advises against merging the consent and "necessary for the performance of a contract" lawful bases.

An example of a "necessary for the performance of a contract" basis for processing employee data that is not considered "bundled" with consent is the processing of salary and bank account information for payment of wages. It often can be difficult to determine whether the lawful basis of "necessary for the performance of a contract" is bundled with consent or stands on its own.

The Working Party encourages assessing the scope of the contract to determine whether there is bundling. "Necessary for the performance of a contract" should be strictly interpreted, the Working Party advises, and "[t]he processing must be necessary to fulfill the contract with each individual data subject." Further, there should be a "direct and objective link" between the data processing and the purpose of the contract. Otherwise, consent and acceptance of the term or conditions of a contract are assumed to be "bundled" together.

Consent and Preparing HR Data System

Following are steps employers can take to help assess and prepare for the GDPR:

1. Identify what HR data is processed.

- This includes establishing how long the employee data is processed, for what purpose, and the legal basis for processing such data. For example, social security data may be processed for tax purposes or employee payment data may be processed out of a contractual obligation.

2. Review and update employee contracts, handbook, policies, and procedures.

- Where employee consent was relied upon, identify an alternative legal basis under Article 6 of the GDPR (*e.g.,* a *"legitimate interest")* that does not result in potential harm to employee rights. Broad consent policies in employment agreements or handbooks are no longer acceptable. Privacy policies can still be referred to in an employment agreement or handbook without requiring an employee to consent to the policy.

3. Identify the limited circumstances where employee consent will be valid.

- An example of a fact-specific circumstance where employee consent will remain a valid basis for employee personal data processing is adding a voluntary benefit to an employee's compensation package. In such circumstances, include consent provisions in a separate document from the general employee agreement to ensure consent is not associated with the employee's acceptance of employment.
- Where consent is valid, an employee has the right to withdraw consent at any time. Procedures should be put in place to facilitate consent withdrawal while avoiding any major disruption to the organization.

4. HR Department participation in organization-wide preparation.

- Non-EU organizations that process the personal data of EU data subjects will have to consider new policies, processes, and practices that involve more than HR data, such as client/customer data.

Jackson Lewis attorneys are available to answer questions on how to prepare for the GDPR.

Focused on labor and employment law since 1958, Jackson Lewis P.C.'s 1000+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged, stable and diverse, and share our clients' goals to emphasize inclusivity and respect for the contribution of every employee. For more information, visit https://www.jacksonlewis.com.