Insight

IN-DEPTH DISCUSSION

SEPTEMBER 7, 2017

# Navigating Global Payroll Under the Impending EU General Data Protection Regulation

BY PHILIP L. GORDON AND KWABENA A. APPENTENG

The European Union's General Data Protection Regulation (GDPR), while designed primarily to update current law to address the digital economy, will impact every aspect of the employment relationship, including the processing of payroll for all employees located in the European Union (EU). In light of the new rules, which go into effect on May 25, 2018, U.S. multinationals with EU subsidiaries will need to scrutinize their current payroll practices at both the parent corporation and the subsidiary level and likely introduce new policies and procedures to address GDPR's heightened protections for personal data. After providing some brief context for these changes, this article will explain the steps that global payroll departments should consider taking to comply with GDPR's requirements.

## Background

Payroll processing in the United States involves a patchwork of privacy and information security laws focused primarily on preventing the misuse of social security numbers (SSNs). Different state laws address information security for SSNs, restrictions on certain uses and disclosures of SSNs, destruction of documents containing SSNs, and data breach notification when SSNs are compromised. There is no overarching federal law.

The EU follows a completely different approach to data protection. Under the current data protection framework, known as the European Union Data Protection Directive (the "Directive"), and under GDPR, which will replace the Directive, all individually identifiable information about a natural person or "personal data" falls within the scope of the law's protections. Consequently, payroll information that receives no legal protection in the United States, such as work location, hours worked, and holiday entitlement, is subject to tight regulation in the EU.

While all personal data is protected under the Directive and GDPR, GDPR is intended to remedy several of the Directive's shortcomings. For

example, GDPR introduces new obligations, such as mandatory data breach notification, and confers new rights on individuals, such as the right to data portability and the right to be forgotten. In addition, GDPR will generally apply uniformly in all EU member states, whereas the Directive permitted substantial variation in data protection requirements across the EU. Notably, GDPR will also substantially enhance the enforcement power of the national data protection authorities (DPAs), responsible for overseeing GDPR compliance, by authorizing monetary penalties of up to the higher of 20 million euro or 4% of gross annual revenue for the entire corporate group regardless of the size of the EU subsidiary responsible for the violation.

## Tightening of Payroll Data Processing Rules

The new rules tighten down the processing of payroll data in the following two ways:

### *1. Limitations on Collecting Personal Data for Payroll Processing*

Under GDPR, employers are required to carefully analyze whether they have a lawful basis for processing employees' personal data and to process only those categories of personal data falling within the scope of a legal justification. In the context of payroll processing, only two of the six recognized justifications likely would apply:

1. Processing necessary for the performance of a contract with the employee; and
2. Processing necessary to comply with a legal obligation under EU law or the law of the EU member state.

These justifications generally will cover basic categories of payroll data, such as work location, status (part-time or full-time), hourly rate and hours worked, salary, holiday entitlement, deductions for benefits, and absences. In fact, regulatory guidance published in late June 2017 noted that processing personal data to "pay the employee" falls within the first ground and processing personal data for "tax calculation" and "salary administration" often falls within the second ground.

However, the term "necessary" in each of these grounds for processing demands a tight nexus between the category of personal data to be processed and the purpose for the processing. Consequently, personal data not directly relevant to processing payroll, such as the reason for an employee's absence from work, generally should not be included in payroll systems or otherwise be accessible to payroll personnel.

GDPR establishes heightened protections for "special categories" of personal data, commonly referred to as "sensitive personal data." GDPR classifies the following categories of information, which might be relevant to payroll processing, as sensitive personal data:

- Trade union membership
- Religion
- Biometric data

Under GDPR, employers are generally prohibited from processing sensitive personal data. However, GDPR does permit processing "when necessary for the purposes of carrying out … the obligations of the [employer] … in the field of employment … law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law …." This exception would justify collecting and using trade-union membership in countries where employers are required by law to deduct union dues from payroll as well as religion in countries where employees are required to pay "church taxes."

The exception described above would not justify using biometric data to authenticate an employee's identity in a biometric time clock (which are becoming increasingly common in the United States) because such time clocks are not required by any Member State's law. While GDPR recognizes consent as a lawful basis for processing sensitive personal data, that consent must be "freely given." However, as reiterated in the

June 2017 guidance mentioned above, the DPAs have taken the position that employees' consent generally cannot be freely given because of the hierarchical nature of the employment relationship. As a result, U.S. multinational employers seeking to extend the use of biometric time clocks to the EU likely will confront legal challenges to doing so.

***2. Mandatory Notice to Employees Before Collecting Personal Data***

Under GDPR, EU subsidiaries must provide employees with a data processing notice "at the time when personal data are obtained," which generally will be during the onboarding process. The required notice must be more detailed than what was previously required under the Directive. As relevant to the processing of payroll data, GDPR requires the notice to include the following information:

- An identification of the categories of personal data collected
- A description of the intended purpose(s) for processing the personal data
- A description of the legal basis for processing the personal data
- The intended recipients of the personal data
- Whether the employer intends to transfer the personal data to a country outside the EU
- The period of time that the employer will store the personal data
- The employee's rights to request access to, correction or deletion of, personal data and the rights to data portability and to restrict processing of personal data
- The employee's right to lodge a complaint with the relevant DPA

## Enhanced Safeguards for Payroll Data

GDPR requires employers to enhance safeguards for employees' personal data, including payroll information, by mandating implementation of an information security program. That program should take into account an assessment of risks to personal data, the state of technology, cost, and the nature and scope of the data processing. GDPR does not specify steps employers must take. Instead, it generally requires physical, technical, and administrative safeguards to protect personal data, a disaster recovery plan, and regular assessments of the effectiveness of the information security program. As a result, to the extent that a U.S. multinational has not already extended its U.S.-based information security program to its EU subsidiaries, it should consider doing so now.

EU subsidiaries of U.S. multinationals commonly rely on local payroll processors. GDPR specifies a long list of mandatory contract provisions intended to ensure that its privacy and information security protections "flow with" the personal data. For example, vendor agreements must now (a) require the payroll processor to implement information safeguards; (b) specify the time frame of the processing; and (c) mandate return or destruction of payroll data on termination of the vendor relationship. In addition to amending existing agreements to address these requirements, EU subsidiaries should conduct due diligence to confirm that their payroll processors can live up to these new contractual obligations.

GDPR's new, mandatory breach notification requirements provide an impetus for implementing effective information security and vendor management programs. Under GDPR, employers must report a data breach to the appropriate DPA within 72 hours of discovery unless the security incident is unlikely to result in a risk of harm to individuals. Employers must notify affected employees if the breach is likely to result in a high risk of harm, or if ordered to do so by the DPA. Given the potential for certain payroll data, such as national identification numbers or SSNs, to be used for identity theft, breaches involving payroll data may trigger breach notification obligations. Consequently, U.S.-based payroll professionals should consider providing

training to their EU counterparts to ensure they understand their obligations in the event of a breach and have implemented a security incident response plan.

### Transferring Employees' Payroll Data to the U.S.

U.S. multinationals that perform payroll processing in the United States for their EU employees will need to comply with GDPR's data transfer rules. While GDPR introduces wholesale changes into other aspects of EU data protection law, the rules surrounding cross-border data transfers will not change substantially under GDPR, at least for the foreseeable future. Under current law and under GDPR, the personal data of EU employees can be transferred to the United States only if the U.S. parent corporation implements a data protection mechanism to ensure that the transferred data will receive a level of protection similar to that required by EU data protection law. U.S. multinationals most commonly satisfy this requirement either by certifying to the EU-U.S. Privacy Shield Framework or by entering into a data transfer agreement approved by the European Commission, known as the Standard Contractual Clauses, with their EU subsidiaries. A third, and less commonly used data transfer mechanism is known as binding corporate rules (BCRs). Because BCRs must be approved by relevant data protection authorities, they often can be costly and time consuming to implement. To date, fewer than 40 U.S. multinationals have obtained approval of BCRs.

### Employees' Rights

As noted in the discussion of data processing notices above, GDPR confers on employees the rights to access, correct, erase, restrict, or entirely stop the processing of their personal data and the right to data portability. These rights apply to payroll data. While applying the rights to access and correct will be relatively straightforward, application of the other rights will be more difficult given the complex rules surrounding those rights. Payroll professionals should, therefore, be prepared to involve legal counsel before responding to a request by an EU employee to exercise any of those rights with respect to his or her personal data.

### Now Is the Time for Review

With just under one year left before compliance with GDPR becomes mandatory, now is the time for U.S. multinational employers to review the application of GDPR to their payroll processes. As a result of that review, many U.S. multinationals likely will need to modify some of their payroll practices and implement new policies and procedures or supplement existing ones.

On September 28, 2017, Littler will conduct a complimentary webinar: Meeting The Next HR Data Protection Challenge: What Multinational Employers Must Do Before The EU's Upcoming General Data Protection Regulation (GDPR) Takes Effect. Click here for more information.

*This article was originally published by the Global Payroll Management Institute (GPMI) in Global Payroll Magazine. The GPMI, www.GPMInstitute.com, spearheads the APA's global initiatives to provide the world with a leading community of payroll leaders, managers, practitioners, researchers, and technology experts. Subscribers connect with each other through networking discussions, collaborative opportunities, and access to education and publications dedicated to global payroll strategies, knowledge, research, employment, and training. GPMI also publishes several global payroll texts and white papers as a benefit to subscribers. Get more information at www.GPMInstitute.com.*