A GDPR Update for Employers, Part IV: Implementing Lessons Learned From GDPR Complaints and Enforcement Actions

May 20, 2019

Much has happened since the European Union (EU) General Data Protection Regulation (GDPR) went into effect on May 25, 2018. Many EU countries have enacted national legislation to implement and expand the requirements of the GDPR, while other developments have directly affected employers and created new obligations regarding the collection and processing of human resources (HR) data.

This is the final article in a four-part series that has examined the national legislation, opinions, and guidelines that have been enacted or issued clarifying the GDPR’s requirements. Part one addressed threshold issues of GDPR coverage. Part two focused on additional data protection requirements imposed by individual EU Member States implementing the GDPR. Part three analyzed the criteria for conducting required data protection impact assessments of processing activities.

The fourth and final part of the series addresses GDPR enforcement efforts and steps employers may want to take with respect to their collection and processing of HR data.

The European Data Protection Board (EDPB) and EU supervisory authorities have reported that they have received a large number of complaints during the first six months following the effective date of the GDPR. For example, the EDPB reported that it had received more than 42,000 complaints since May 25, 2018. The French Supervisory Authority (CNIL) reported a 20 percent increase in complaints filed during the first six months the GDPR was effective compared to the same period in 2017. Similarly, the Irish Supervisory Authority reported a 50 percent increase in data breach reports and a 65 percent increase in data protection complaints over the same period. The Irish Data Protection Commissioner also stated that several investigations of multi-jurisdictional complaints against large companies are being completed and that she expects major GDPR fines to be issued in 2019.

Additionally, supervisory authorities in the following countries issued the first fines for GDPR violations:

Portugal: In June 2018, after conducting an inspection of a hospital based on a newspaper article that outlined potential violations of the GDPR by the hospital, the Portuguese Supervisory Authority issued a €400,000 fine against the hospital for three GDPR violations. First, the hospital had violated the GDPR’s data minimization requirement by permitting several staff members to have access to patient data for which they did not need access in order to perform their jobs. Second, the hospital failed to implement and document appropriate data access and data security procedures. Third, the hospital failed to implement technical and organizational
measures generally to ensure a level of security adequate to the risk, including a process to regularly test, assess, and evaluate the technical and organizational measures to ensure the security of the processing.

Austria: In October 2018, the Austrian Supervisory Authority issued a €4,800 fine against a small company that had installed a closed-circuit television (CCTV) surveillance camera in front of its facility that not only recorded individuals entering the facility but also recorded individuals who passed by on the public sidewalk. The Austrian Supervisory Authority found that the recording of the individuals on the public sidewalk violated the GDPR because the company did not have a legitimate interest in recording individuals in public spaces and the company did not provide proper notification of the surveillance through appropriate signage. The Austrian Supervisory Authority determined the amount of the fine based upon the company’s financial resources, thereby demonstrating the Supervisory Authority’s willingness to enforce the GDPR and impose fines against companies of any size.

Germany: In November 2018, the State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (LfDI) imposed a €20,000 fine against a social media company for data security violations in connection with a data breach. The company reported that over 800,000 email addresses and passwords of users had been hacked. Alerted to the unauthorized disclosure of personal data, the company timely reported the incident to the LfDI and informed the affected users about the breach.

The LfDI’s investigation of the data breach revealed that the company had stored user passwords in an unencrypted format. Therefore, the LfDI found that the company had violated Article 32(1)(a) of the GDPR, which requires data controllers to implement data security measures, including the pseudonymization and encryption of personal data, as appropriate.

The €20,000 fine imposed by the LfDI was well below the GDPR’s maximum allowable fine for the infringement (€10 million or up to 2 percent of an organization’s worldwide annual revenue from the prior financial year, whichever is higher). The LfDI indicated that it had credited the company for timely contacting the LfDI, notifying affected users, cooperating with the investigation, and investing approximately €100,000 to make improvements in its data security measures.

Further, several supervisory authorities have announced or engaged in aggressive enforcement activities. For example, in June 2018, the Supervisory Authority for the German State of Lower Saxony sent comprehensive questionnaires to several mid-size and large businesses requesting the companies submit their Article 30 records of processing, privacy notices, data protection impact assessments, data processor agreements, and data breach notification procedures to the Supervisory Authority for review.

In November 2018, the Supervisory Authority of the State of Bavaria announced that it was intensifying its compliance monitoring of major companies to determine compliance with GDPR data security requirements with a focus on preventing data breaches and compliance with Article 30 record of processing requirements.

France: In July 2018, the CNIL announced that it would conduct 300 predawn raids on businesses, either on-site or online, to enforce the GDPR.
In January 2019, the CNIL issued a €50,000,000 fine against a major U.S. technology company for violating the transparency and consent requirements under the GDPR. Specifically, the CNIL found that users did not have easy access to relevant information on the company’s website because the information was spread over several documents that were accessible only in multi-stage processes. In addition, the information provided was not always clear and understandable and, therefore, users could not understand the extent of the data processing operations carried out by the service. Thus, user consent had not been specifically and unambiguously obtained.

The Netherlands: Also in July 2018, the Dutch Supervisory Authority reported that it had begun ex officio investigations of 30 random companies to determine their compliance with Article 30 of the GDPR, which requires organizations to maintain detailed records of processing activities.

GDPR enforcement activities have not been confined to EU supervisory authorities. In August 2018, a shareholder of a major U.S. media company filed a class action lawsuit against the company alleging that the company had made misleading statements regarding its preparedness for the GDPR and the impact that the GDPR would have on its business, thereby violating U.S. securities law.

Based on these enforcement activities, it is apparent that EU supervisory authorities are focusing on compliance with the internal technical and accountability requirements of the GDPR. Thus, employers should consider taking the following steps:

1. Preparing or reviewing the organization’s Article 30 record of processing for HR data to make sure it is complete and updated
2. Preparing, reviewing, and updating policies and procedures regarding data security measures, including data access controls, and data breach notification procedures
3. Preparing or reviewing the use of data processors and ensuring data processor agreements are in place.