A GDPR Update for Employers, Part III: Preparing Required Data Protection Impact Assessments

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 third article in a four-part series examining 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, which follows, addresses the criteria for conducting required data protection impact assessments of processing activities.

Article 35 of the GDPR provides that a data protection impact assessment (DPIA) must be performed for data processing that “is likely to result in a high risk to the rights and freedoms of natural persons.” DPIAs must contain (1) a description of the processing operation along with the purpose of the processing and, where applicable, the legitimate interest for the processing; (2) an assessment of the necessity and proportionality of the processing operation in relation to the purpose; (3) an assessment of the risks to the rights and freedoms of the data subjects; and (4) the measures to be taken to mitigate the risks. Article 35 of the GDPR also requires the supervisory authority of each EU country to submit a list of the kind of processing for which a DPIA must be performed (a so-called “blacklist”) to the European Data Protection Board (EDPB) for review and recommendations.

During 2018, the EDPB issued opinions regarding the draft lists submitted by each EU country. In its opinions, the EDPB attempted to harmonize the criteria for conducting DPIAs across all EU countries and provided recommendations regarding the need for a DPIA for several types of data processing. Specifically, the EDPB made the following findings and recommendations:

- **Criteria for DPIAs:** The EDPB recommended that each country make reference to and follow the Working Party Guidelines regarding DPIAs and to require DPIAs if any two of the following nine criteria were present: (1) evaluation or scoring (which would include employee performance evaluations and applicant evaluations); (2) automated decision making; (3) systematic monitoring; (4) sensitive data or data of a highly personal nature; (5) data processing on a large scale; (6) matching or combining data sets; (7) processing data of vulnerable subjects, which include children, the elderly, and employees; (8) innovative use or application of technological or organizational solutions, such as using fingerprints or facial recognition for physical access control; and (9) processing that “prevent[s] data subjects from exercising a right or using a service or a contract.”

- **Non-Exhaustive Nature of the Lists:** The EDPB stated that each country should indicate that its list is not to be considered exhaustive.

- **Employee Monitoring:** The EDPB stated that each country should indicate that a DPIA must be performed when an employer engages in systematic monitoring of employees. The EDPB stated that the Working Party’s June 8, 2017, Opinion on data processing at work remains valid in defining when systematic monitoring of employees occurs. The Working Party’s Opinion requires or recommends that a DPIA be performed for the monitoring of employee computer, email, and mobile device usage; monitoring employees for time and attendance; monitoring employees through video surveillance; monitoring employees for access control; and monitoring location and vehicle use data.

- **Biometric Data:** The EDPB stated that each country should indicate that a DPIA must be performed for the processing of biometric data for the purpose of uniquely identifying a natural person so long as at least one of the nine criteria is present.
• Genetic Data: Similarly, the EDPB stated that each country should indicate that a DPIA must be performed for the processing of genetic data so long as at least one of the nine criteria is present.

• Location Data: The EDPB also stated that each country should indicate that a DPIA must be performed for the processing of location data so long as at least one of the nine criteria is present.

• Migration of Data: The EDPB stated that each country should indicate that a DPIA should be performed when data is migrated from one system to another and at least one of the nine criteria is present.

Significantly, the EDPB stated that DPIAs should not be performed for cross-border data transfers or data processed by joint controllers (for example, HR data of EU employees processed by both an EU subsidiary and U.S. parent company) and instructed applicable countries to remove such processing from their lists.

Based on the EDPB opinions, employers must perform DPIAs for any monitoring of employees located in the EU. Also, because employees are considered to be vulnerable subjects, the processing of HR data will always meet at least one of the criteria that trigger the need to perform a DPIA. Thus, employers will be required to perform DPIAs for data processing involving biometric data, genetic data, location data, and the migration of data as well as data processing involving the one of the following criteria:

• Employee and job applicant evaluations

• Automatic decision making, such as the use of algorithms in online job applications that screen applicants without the need for human intervention

• Sensitive data such as racial and ethnic background, trade union membership, religious beliefs, and employee health data

• Innovative technology such as the use of fingerprints or facial recognition for access control

Part four of this series will address developments related to GDPR complaints and enforcement actions.
