Published on *The National Law Review* https://natlawreview.com

A GDPR Update for Employers, Part II: Aligning HR Practices to Comply with National Legislation Implementing the GDPR

Article By:

Grant D. Petersen

Simon J. McMenemy

Danielle Vanderzanden

Stephen A. Riga

Cécile Martin

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 second article in a four-part series examining national legislation, opinions, and guidelines that have been enacted or issued clarifying the GDPR's requirements. The series also covers data protection impact assessments, claims alleging violations of the GDPR, enforcement actions, and fines that have been issued. Part one *focused on threshold issues of GDPR coverage. This article addresses requirements enacted by individual EU countries that impose additional obligations related to the processing of HR data.*

Although the GDPR was intended to provide a uniform set of data protection requirements across the EU, the GDPR contains several provisions, known as "opening clauses," that expressly permit individual EU countries to implement additional and/or stricter requirements for certain types of data that employers typically process. For example, Article 9 of the GDPR provides that EU Member States may introduce further conditions and limitations on the processing of genetic data, biometric data, and health data. Article 10 of the GDPR provides that data concerning criminal convictions and offenses may be processed only if authorized by EU or EU country law. Finally, Article 88 permits EU countries to provide, either by law or by collective agreements, more specific rules regarding the processing of personal data in the employment context.

Several EU Member States have taken advantage of these opening clauses and have enacted

legislation providing stricter or additional requirements for processing HR data:

Bulgaria

An employer may process HR data without an employee's or job applicant's consent if the collection and processing of the data is for employment relations; is required by the Labor Code, Health Act, or Social Insurance Code; or where the legitimate interest of the employer prevails over the interests and rights of employees, such as in the case of video surveillance for security purposes.

Croatia

- Employers may process employee biometric data to monitor employment performance (e.g., working hours) and for access control on company premises if there is a legal basis for such monitoring or the employee gives express consent and the biometric data processing serves as an alternative to other means for such monitoring.
- Employers may use closed-circuit television (CCTV) surveillance cameras in the workplace provided that applicable health and safety regulations are followed; employees receive adequate notice of the CCTV use; and the CCTV does not monitor changing rooms, relaxation and resting areas, or bathrooms.

Cyprus

- Employers will commit a criminal offense if they process the criminal history data of employees or job applicants without having an Article 30 record of processing activities, if they fail to update the record of processing, or if they fail to provide a record of processing to authorities upon request or otherwise provide an inaccurate or incomplete record of processing to the authorities.
- Employers will commit a criminal offense if they fail to conduct a required data protection impact assessment.

Denmark

All organizations, including employers, must encrypt emails that contain sensitive personal data. "Sensitive personal data" under the GDPR includes data concerning a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric data ideology, union membership, sexual orientation, beliefs, or health, sex life, or sexual orientation.

France

- Private-sector employers are prohibited from processing criminal history data as such data may be processed solely by public entities or in connection with legal proceedings.
- Employers may process biometric data if such processing is strictly necessary to control access to the workplace and devices and applications used by employees, agents, trainees, or service providers.

Germany

- Employers may process HR data including special categories of personal data on the basis of

collective agreements or Works Council agreements, but such agreements must meet the requirements of the GDPR.
- An employer must appoint a data privacy officer if it employs 10 or more people whose duties include the processing of personal data.
- An employer may process data based on employee consent where such consent is in writing and the employee receives a “legal or economic benefit” or the interests of the employer and employee are aligned.

Examples of a “legal or economic benefit” to an employee include an employer’s implementation of an occupational health management or support program or an employer’s permitting private use of company IT systems. Examples of aligned interests include situations in which employers and employees work together to add employees’ names and birthdays to a company birthday list or use photographs of employees for a website. When determining whether consent is voluntary, the timing of the consent must be considered. For example, prior to the conclusion of an employment contract, employees are subject to greater pressure to consent and, therefore, such consent may not be voluntary.

- Employers may process sensitive data without employee consent in order to manage the employment relationship or to exercise rights or fulfill duties under employment law or social services law so long as the employee’s privacy rights do not override the company’s interest in processing such data.
- An employer may engage in employee monitoring only when the company can document reasons to believe the employee is engaged in criminal conduct or has or is committing a serious breach of duty.
- The definition of “employee” includes temporary or agency employees.

Greece

Employers may process criminal history data when absolutely necessary for, among other purposes, determining eligibility for employment, processing data in the employment context, and establishing, exercising, or defending legal claims.

Ireland

- Employers may process health data for an occupational pension, a retirement annuity contract, or any other pension arrangement.
- Employers are prohibited from requiring individuals to make data access requests or to supply information from a subject access request in the employment context.

Luxembourg

Employers may ask prospective employees to provide an extract of their criminal record in the recruitment process. The data can only be used for recruitment or human resources purposes and cannot be kept for longer than one month.

The Netherlands

Employers may process criminal history data if the individual provides explicit consent or the processing of such data is necessary for litigation purposes.

Poland

- Employers may not engage in “blind recruitment” in which the identity of an employer is not disclosed at the beginning of the recruitment process.
- Employers may not process the criminal histories of job applicants, even with applicant consent.
- Employers may not contact the prior employers of job applicants without the applicants’ consent.
- Employers may not confirm the authenticity of job applicants’ university degrees.
- Employers may not retain the data of unsuccessful job applicants for future employment consideration unless the job applicants consent.
- Employers may not process job applicants’ social media data.
- Employers may not use biometrics for the purpose of recording working time.
- Employers may not use photographs of employees without their consent.
- Employers may transfer HR data within an organizational group for internal administrative purposes including the centralization of HR and payroll processes.
- Employers may use CCTV monitoring for security purposes to protect employee safety, company property, or confidential information. Employers cannot use video monitoring to monitor restrooms, changing rooms, company lunchrooms and smoking areas, or areas made available for trade union activities unless the employees recorded are made unrecognizable. CCTV recordings may be kept no longer than three months unless needed for judicial proceedings. Notice must be provided to employees no later than one day before the launch of the CCTV monitoring and may be done by appropriate signage or sound notices indicating which area or areas will be monitored. If there is a collective agreement, notice of CCTV monitoring may be provided in the collective agreement.
- Employers may engage in email monitoring and other non-video monitoring of employees for the purposes of tracking working time and ensuring proper use of work tools and equipment.
- Employers must provide prior notice to employees regarding any type of monitoring.
- Employers are not required to obtain employee consent to introduce monitoring in the workplace and an employee may be terminated for refusing to be monitored so long as the monitoring complies with applicable data protection laws.
- Monitoring that was implemented prior to May 25, 2018, must be compliant with the Polish Labor Code.

Slovakia

An employer may process sensitive data when necessary for the purposes of carrying out and exercising the obligations and specific rights of the employer or employee in the areas of labor law, social law insurance, social protection, or public health insurance.

Spain

- Employers may rely on the legal basis of legitimate interest to process employee data.
- Employers cannot rely on employee consent to process sensitive data. An employer must notify employees of any video surveillance by placing a sign regarding the surveillance in a visible location. Video surveillance data must be deleted within one month unless needed to prove the commission of acts against individuals, property, or facilities.
- Employers may access corporate electronic devices used by employees pursuant to clear rules drafted with the participation of the workers’ representatives. However, employees have

the right to disconnect from company networks outside of working hours in accordance with predefined policies.
- Employers cannot process criminal record data unless specifically permitted by a sector law.
- Employers may use CCTV or video surveillance to monitor employees as long as the monitoring complies with Spanish labor laws and employees are informed about the video surveillance. Video surveillance footage can be stored for a maximum of one month unless a longer retention period is required for an ongoing investigation.
- Employers may implement whistleblower reporting systems that permit both anonymous and non-anonymous reporting from employees. Employers must notify employees about the existence of whistleblowing systems and must restrict access to the data contained in the whistleblowing systems to persons who carry out internal control and compliance functions, or persons designated to handle complaints. Employers can maintain logs of employee complaints and whistleblowing, so long as the employees are informed of the logs' existence. Personal data in these systems must be stored only for as long as necessary and no longer than three months, except if the purpose of the storage is to demonstrate compliance with the crime prevention model by the legal entity.

Sweden

Employers may process social security numbers without employee consent when the processing is necessary for security or authentication purposes.

United Kingdom

- An employer may process sensitive data such as data concerning ethnic and national origin, religious and philosophical beliefs, health, and sexual orientation where such processing is (1) necessary to enter into or perform an employment contract; (2) necessary for "exercising or performing any right or obligation which is conferred or imposed by an enactment or rule of law" on the employer in connection with employment; or (3) necessary for the purpose of identifying, reviewing, or promoting equal opportunities or treatment in the workplace. Further, an employer must have an appropriate policy in place that explains the employer's procedures for securing compliance with the principles of the GDPR in connection with the processing of HR personal data and that explains the employer's policies regarding the retention and erasure of personal data processed, setting forth how long such personal data is likely to be retained.
- Employers are not required to provide employees or job applicants access to confidential references provided for employment purposes.
- Employers may process criminal history data only if one of the following conditions is met: "the data subject has given consent to the processing"; "the processing is necessary to protect the vital interests of an individual"; the processing is performed by a not-for-profit entity; the "personal data is already in the public domain"; "the processing is necessary for the purpose of, or in connection with, any legal proceedings" or is necessary for obtaining legal advice or establishing, exercising, or defending legal rights; "the processing is of personal data about a conviction or caution" for an indecency offense involving children; the processing is "necessary for reasons of substantial public interest"; or the processing is necessary for insurance purposes.

The Article 30 record of processing that requires an appropriate policy document must include the following information: the condition relied upon, the extent to which the processing is lawful under the GDPR, and, where applicable, the reasons for not complying with the policy.

Part three of this series will address the obligation under the GDPR to conduct data protection impact assessments of processing activities that are "likely to result in a high risk to the rights and freedoms" of individuals.

National Law Review, Volume IX, Number 114