Insight

IN-DEPTH DISCUSSION

JANUARY 21, 2016

Ten Steps For U.S. Multinational Employers Towards Compliance With Europe's New Data Protection Framework – The General Data Protection Regulation

BY PHILIP L. GORDON

The European Union's (EU) new data protection framework, known as the General Data Protection Regulation (the "Regulation"), is, at bottom, a response to the astonishing evolution in online commerce.[1] As a result, only one of the Regulation's 91 articles specifically addresses the personal data of employees. This gap means U.S. multinational employers — especially those engaged in business-to-business ("B-to-B") commerce — must carefully parse the Regulation to figure out how it applies to their management of a global workforce. To assist in that effort, this Insight describes 10 practical steps that U.S. multinationals can take towards satisfying those provisions of the Regulation with the greatest impact on managing a global workforce.

Overall, the Regulation will not demand dramatic changes in the policies and procedures previously implemented to comply with the European Union Data Protection Directive (the "Directive"), the EU's pre-existing framework document for data protection that the Regulation expressly repeals and replaces. However, in order to comply with the Regulation, virtually all U.S. multinational employers likely will need to update at least some of their existing policies and procedures, and re-align some of their practices, for handling the personal data of employees of their EU subsidiaries.

While the compliance requirements have not changed significantly, the enforcement risk has increased dramatically. The Regulation empowers data protection regulators to impose administrative fines of 20 million Euro, or up to 4% of a corporate group's worldwide gross annual revenue, for most violations and up to 2% of that amount, or 10 million Euro, for less serious violations. Regulators also can ban data processing at the EU subsidiary and suspend data transfers to the parent corporation. Consequently, U.S. multinationals should take advantage of the two-year grace period to come into compliance. The grace period will commence at some point in early 2016 when the Regulation is published in the *Official Journal of the European Union*.

1 This article was first published in the International Association of Privacy Professionals' *Privacy Tracker* blog.

Ten Practical Steps For Compliance

1. Watch For New Member State Employment Laws To Implement The Regulation

As noted above, only one of the Regulation's 91 articles specifically addresses the personal data of prospective, current or former employees (collectively, "employee data"). Article 81 of the version published by EU authorities in December 2015 provides that EU Member States may enact laws specific to the processing of employee data to implement the Regulation. For multinational employers, this provision could defeat one of the principal putative benefits of the Regulation—to establish a single set of data protection rules applicable in all 28 EU Member States to eliminate complexity, ensure consistency and reduce administrative costs. In respect of employee data, the Regulation should therefore be read in conjunction with any applicable laws of relevant EU Member States that regulate the handling of employee data.

Even though the Regulation specifically addresses employee data in only one article, the Regulation applies broadly to the processing of all "personal data," which is defined to mean "any information related to an identified or identifiable natural person." Consequently, U.S. multinationals need to determine how to apply, in the employment context (together with the applicable local employee data protection laws), regulatory requirements designed to protect online consumers and numerous other categories of data subjects.

The Regulation's scope is broad in another way that impacts U.S. multinationals. The Regulation applies to all EU residents, regardless of citizenship. For U.S. multinationals, this means that expatriates working at an EU subsidiary are entitled to all of the Regulation's protections when their data is collected while they reside in the EU.

2. Identify Permissible Purposes For Processing Employee Data

In contrast to U.S. law, which allows employers to collect, use and disclose employee data for almost any purpose unless specifically prohibited by law, the Regulation—following prior law—establishes the exact opposite rule, *i.e.*, employers can lawfully "process" employee data only if the Regulation specifically permits the processing. The Regulation defines "processing" to cover any operation during the course of the information life cycle, from initial collection to final destruction, and includes cross-border data transfers.

Only a few of the permissible purposes for processing personal data identified in the Regulation may apply in the employment context. Identifying the permissible purpose for processing each category of employee data is a critical exercise. The Regulation authorizes the maximum administrative fines—as noted above, up to 4% of gross annual worldwide revenue for the corporate group—for the processing of personal data without a permissible purpose.

a. Consent Generally Will Not Be A Valid Ground For Processing In The Employment Context

While the Regulation permits processing of personal data with the consent of the data subject, the Regulation also provides that consent is not valid unless it is "freely given, specific, informed and unambiguous." Neither the preamble to the Regulation nor the Regulation itself specifically addresses whether an employee can freely give consent in the context of the employment relationship. However, EU regulators construed similar language in the Directive to mean that employees generally could not freely give consent to their employer's processing of their personal data due to the significant imbalance in power between employers and employees. Consequently, employers who consider relying on employee consent as a lawful ground for processing personal data should carefully assess whether consent would be freely given

or voluntary. Any threat of discipline, termination, or other significant detriment for refusing to consent likely would invalidate the employee's consent. In addition, employers should watch for new Member State laws and administrative guidance addressing this issue.

Employers who do identify circumstances where consent could be a lawful basis for processing must fulfill the Regulation's other requirements for valid consent. To be specific and informed, employees' consent should be preceded by a robust notice of data processing that meets the requirements described in Step 3, below. To be unambiguous, the consent must be manifested by an affirmative statement or action, i.e., "opt-in" consent; failure to object to a request for consent, also known as "opt-out" consent, will not suffice.

The Regulation imposes on the "data controller" the burden of proving the validity of consent, and any request for consent in a written document must be "clearly distinguishable" from the document's other text. The Regulation defines "data controller" as the natural person or legal entity that decides the "purposes and means of processing" personal data. This definition would include an employer. Consequently, employers who intend to rely on consent as a ground for processing should consider satisfying these requirements by having employees execute a clearly separate consent statement at the end of the notice of data processing described in Step 3, below, or if that notice does not address the specific processing that is the subject of the request for consent, by executing a standalone consent statement in some other form.

Employers should beware that employees have the right to withdraw consent at any time, and they must be informed of that right. This can be accomplished through the notice of data processing or other form used to obtain consent.

b. Processing Necessary To Perform An Employment Contact Is A Viable Ground But Likely Will Be Narrowly Construed

The Regulation permits processing if "necessary for the performance of a contract" with the data subject, *i.e.*, an employee. Given administrative interpretations of prior EU law, this ground likely will be construed to cover only processing with a close nexus to the employment contract, such as the payment of compensation and benefits or processing requests for sick leave or vacation. By contrast, this ground likely will not be broad enough to cover processing that is more ancillary to the employment relationship, such as for purposes of making travel arrangements or offering diversity awareness training. It is still uncertain whether and to what extent this ground would support any data processing by the parent corporation for the parent corporation's own (or joint) purposes, such as global succession planning, because the parent corporation does not have an employment contract with the employees of its EU subsidiaries. However, processing by the parent corporation to facilitate the subsidiary's administration of its employment contract with the employee, such as to make a human resources information system (HRIS) database available to the subsidiary-employer, likely would fall within the scope of this ground.

c. Processing To Comply With Legal Obligations Is Limited To Obligations Established By EU And Member State Law

The Regulation permits the processing of employee data to comply with legal obligations "to which the data controller is subject." Importantly for U.S. multinationals, this ground applies only to legal obligations imposed by EU or Member State law on the controller, *i.e.*, the subsidiary-employer. Consequently, U.S. legal requirements, such as the requirement to implement a litigation hold in civil litigation or to produce information in response to a subpoena issued by a U.S. court, would not provide a valid basis for processing the personal data of EU employees.

d. Processing For The "Legitimate Interests" Of The Employer Is Subject To An Employee's Right To Object

The Regulation permits processing that is necessary to achieve the "legitimate interests" of the employer. However, an employer cannot rely on this ground unless it (a) balances its legitimate interest against the employee's rights and determines that those rights are not overriding; and (b) notifies the employee, in writing, of the legitimate interest pursued and of the employee's right to object to the processing. If the employee objects, the employer must cease its processing in reliance on this ground unless the employer can demonstrate (a) "compelling legitimate grounds" for the processing that override the employee's interests, or (b) that the processing is necessary to establish, pursue or defend legal claims.

Applying the balancing test in the absence of further guidance will prove difficult. That said, an employer likely will be able to justify processing of employee data that is not particularly sensitive on the legitimate interest ground where there is a tight nexus to the employment relationship, such as processing an employee's contact details to arrange business travel or for diversity awareness training. By contrast, processing employee data with little or no tie to the employment relationship, such as to market the employer's own products or services to the employee, almost surely would not be justified on this ground.

3. Update Notices Of Data Processing

As with prior law, the Regulation requires that data controllers distribute a notice of data processing to each individual when personal data is first collected. As applied in the employment context, this means that employers will be required to provide a notice to job applicants concerning the processing of their data during the application process as well as a notice to new hires, typically during the onboarding process, explaining how their personal data will be processed during the employment relationship.

While this basic notification requirement is unchanged, the Regulation requires a far more robust notice. The notice must include the following information: (a) the identity and contact details of the employer; (b) the purposes for the processing and when the processing is based on legitimate interests, a description of those interests; (c) the categories of recipients of disclosures of personal data; (d) that the controller intends to transfer personal data to a third country and the legal basis for the transfer (described in Step 5, below); (e) the period for which the personal data will be stored or the criteria for determining the period; (f) how employees can exercise the rights of access, correction, erasure, and objection; (g) where processing is based on consent, the right to withdraw consent; (h) the right to file a complaint with a data protection authority ("DPA"); (i) whether the employee is obliged to provide the data by statute, contract, or for another reason, and the possible consequences of failing to provide the data; and (j) whether the personal data will be subject to automated processing and, if so, the logic and the consequences of the processing for the data subject.

It is not yet clear whether employers will be required to issue updated notices to employees who received a notice that was valid under prior law or whether a notice that meets all of the Regulations' requirements will need to be distributed only to employees who are hired after the Regulation goes into effect.

4. Ensure That Employees Can Exercise Their Rights Of Access, Correction, Erasure, And Objection

The Regulation places substantial emphasis on individuals' rights of access, correction, erasure, and objection as a means of achieving the new law's broader objective of protecting individuals' fundamental right of privacy. To that end, the Regulation requires that employers provide employees with a mechanism

to exercise these rights and to respond, in writing, to any request without undue delay and, at the latest, within one month. The response period may be extended for up to two additional months in light of the complexity and number of requests. Any denial of a request must include the reasons for the denial and the right to file a complaint with the DPA or to seek judicial relief. All responses to requests must be free of charge unless the request is manifestly excessive (generally because it is repetitious). If the employer has doubts regarding the identity of a person making a request, it may ask for verification of the person's identity.

While prior law provided a right of access and correction, the right of erasure (also known as the "right to be forgotten") is new. Employees generally have the right to require the employer to delete their personal data when, for example, (a) the data no longer is necessary for the purposes of which it was collected; (b) the employee has withdrawn consent to processing, and no other ground for processing is available; and (c) the employee objects to processing, and there is no compelling ground that overrides the employee's interests. However, employers are not required to erase any employee data that they are required to retain under EU or Member State law that is necessary to establish, pursue, or defend legal claims.

Employers should note that, subject to further administrative guidance, executing an employee's request "to be forgotten" could be technically challenging and administratively burdensome. In today's online environment, employee data rarely is confined to a personnel file maintained by the human resources (HR) department. Rather, to fully comply with an erasure request, employers could be required to search numerous internal systems — including the corporate intranet, internal social media platforms, document management systems, and corporate e-mail — and to communicate with the many service providers with which HR departments routinely contract.

5. Implement A Mechanism For Lawful Cross-Border Transfers Of Employee Data

The Regulation's overall scheme for cross-border data transfers is materially the same as that under the Directive. This scheme generally prohibits transfers of employee data outside the EU unless the EU subsidiary-employer ensures that the recipient, typically the parent corporation, but sometimes also other non-EU members of the corporate group, will ensure an adequate level of protection for the transferred data.

The employer-subsidiary satisfies this adequacy requirement if the European Commission (the "Commission") has determined that the receiving country ensures an adequate level of protection for the transferred data. The Commission's prior adequacy determinations under the Directive remain in effect. Hundreds of U.S. multinational employers relied on the Commission's determination that the U.S.-EU Safe Harbor Framework provided an adequate level of protection until the European Court of Justice invalidated that determination on October 6, 2015. If current negotiations between the U.S. Commerce Department and the Commission result in an adequacy determination for a replacement framework, the Regulation would permit EU subsidiaries to rely on that mechanism to transfer employee data to a U.S. parent corporation provided that (a) the parent corporation complies with the replacement framework; and (b) one of the lawful grounds for processing employee data described in Step 2, above, applies to the cross-border data transfer.

Until the Commission issues an adequacy determination regarding data transfers to the United States, U.S. multinationals generally will need to rely on one of the other mechanisms identified in the Regulation. These mechanisms include the standard contractual clauses ("SCCs") approved by the Commission under the Directive as well as binding corporate rules ("BCRs"). The SCCs are a form agreement between the data exporter (the EU subsidiary-employer) and the data importer (the U.S. parent corporation and any non-EU affiliate that receives EU personal data). BCRs are legally binding policies applicable to all members of a corporate group, whether located within or outside the EU, and are enforceable by employees as third-party

beneficiaries. To date, fewer than 75 U.S. companies have implemented BCRs as compared to more than 4,000 that certified to the Safe Harbor Framework.

The Regulation potentially makes BCRs more attractive by codifying a "one-stop shop" approach to regulatory oversight that provides a more streamlined and timelier approval process for BCRs. Under this process, the DPA for the employer's "main establishment" would be the employer's "sole interlocutor" or "lead" DPA with respect to the approval process, meaning that the employer would not be required to deal directly with any other DPA for purposes of obtaining approval of the BCRs. The employer's "main establishment" would be "the place of central administration in the [EU]" unless another establishment in the EU determines how data will be processed. The Regulation also establishes specific deadlines for review and approval of BCRs by other concerned DPAs and by the European Data Protection Board. The Board is composed of the head of the DPA for each of the 28 EU Member States and replaces the Article 29 Working Party, which was responsible for overseeing implementation of the Directive.

U.S. multinationals should note that the one-stop shop approach is just one way in which the Regulation streamlines the DPA's supervision of data processing. The Regulation also abolishes virtually all requirements to submit notifications to, and otherwise to consult with, DPAs regarding data processing.

6. Develop A Written Information Security Program And A Security Incident Response Plan In Light Of The Regulation's New Breach Notification Requirement

The Regulation requires employers to implement administrative and technical safeguards for employee data to reduce identified risks and to prevent a "personal data breach." The Regulation defines a breach to mean a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data." The Regulation does not specify safeguards that must be implemented, but it does identify the following steps and objectives as potentially appropriate: (a) pseudonymization and encryption; (b) the ability to ensure the confidentiality, integrity and availability of personal data; (c) disaster recovery capabilities; and (d) a process for regularly testing, assessing and evaluating the safeguards. Having a subsidiary-employer implement safeguards similar to those required by the HIPAA Security Rule or by Massachusetts' information security regulations likely will meet this standard.[2] In addition, regulators most likely will publish detailed security guidelines during the two-year grace period before the Regulation goes into effect.

When a personal data breach does occur, the Regulation requires prompt action. The employer must notify the DPA within 72 hours, and if that notification is delayed, explain the reason for the delay. Notification is not required if the breach "is unlikely to result in a risk for the rights and freedoms of individuals." The employer must document its breach response sufficiently to permit the DPA to verify compliance with the Regulation.

Employers must notify affected employees of a personal data breach "without undue delay," if the breach is "likely to result in a high risk to the rights and freedoms of individuals," or if ordered to do so by the DPA. As with U.S. breach notification laws, the Regulation establishes an "encryption safe harbor," meaning that the employer is not required to notify affected individuals if their personal data is subject to encryption that renders the information unreadable. Notification to individuals also is not required if (a) the employer took steps to ensure that the high risk to employees does not materialize, or (b) notification would involve

2 The HIPAA Security Rule establishes standards for safeguarding protected health information. See generally 45 C.F.R. pt. 164.302-164.318. Massachusetts' information security regulations establish standards for safeguarding sensitive personal information of Massachusetts residents, such as Social Security numbers, driver's license numbers and credit card numbers. See generally 20 CMR 17.00.

disproportionate effort, but in this case, the employer must provide notice by public communication, such as by posting notice on a web site or by publication in the media.

7. Vet Vendors That Will Receive Employee Data And Negotiate Vendor Agreements That Meet The Regulation's Requirements

The U.S. parent corporation typically will select certain vendors to provide employment-related services to the entire corporate group, such as stock option administrators, online performance evaluation platforms, and providers of HRIS data bases. Because the parent corporation effectively is contracting on behalf of its EU subsidiaries, it should comply with the Regulation's requirements when entering these arrangements if the service provider will process EU employee data.

To begin with, the parent corporation should vet the service provider's ability to comply with the Regulation. In particular, the parent corporation should take steps to assess whether the service provider has adequate technical and administrative safeguards in place and has the capability to fully satisfy employees' requests to exercise their rights with respect to their personal data stored at the service provider.

The Regulation also specifies a long list of matters that must be addressed in the service agreement. The service agreement must address, for example, (a) the subject matter and duration of the processing; (b) the nature and purpose of the processing; and (c) the types of personal data and categories of data subjects. The service agreement also must impose numerous obligations on the service provider, including, for example, that the service provider: (a) process personal data only subject to the employer's instructions, (b) require its employees to execute a confidentiality agreement; (c) implement required security measures; (d) assist the employer fulfill its obligations to respond to requests by employees to exercise their rights; and (e) cooperate with the employer in fulfilling its breach notification obligations.

8. Beware Of High-Risk Processing That Can Trigger Additional Compliance Requirements

The Regulation provides that the processing of "special categories of personal data," also known as "sensitive personal data," is prohibited unless an exception applies. Sensitive personal data includes race or ethnic origin, data concerning health or sex life and sexual orientation, trade-union membership, genetic data, biometric data, political opinions, and religious or philosophical beliefs. An employer can process sensitive personal data only in the following limited circumstances: (a) the employee gives explicit consent (except where the law does not permit the employee to consent); (b) processing is necessary for the employer to fulfill obligations and exercise specific rights established by EU or Member State law; or (c) processing is necessary to establish, pursue or defend against legal claims. In addition, a health care professional can process personal data concerning an employee's health when necessary for preventive or occupational medicine, to assess the working capacity of the employee, or to provide care.

Given the Regulation's emphasis on protecting sensitive personal data, regulators likely will narrowly construe these exceptions. Consequently, EU subsidiary-employers should scrutinize and restrict their collection of sensitive personal data. Likewise, U.S. parent corporations should carefully assess whether any of the exceptions would justify transferring any categories of sensitive personal data to the United States, and if so, whether the cross-border data transfer really is necessary.

The Regulation also establishes a special rule for the processing of criminal history information, albeit that category is not specifically identified as sensitive personal data. Under that special rule, an employer can process criminal history information — even with an applicant's or employee's consent — only if specifically authorized by EU or Member State law to perform a criminal history check. Consequently, the U.S. parent

corporation likely will not be able to lawfully apply policies broadly requiring criminal history checks of U.S. applicants and employees to applicants and employees located in the EU.

9. Maintain Required Records Of Data Processing

The Regulation requires that employers maintain detailed records concerning their data processing. These records must be provided to the DPA upon request.

The information to be recorded includes the following: (a) contact information for the employer; (b) the purposes of the processing ; (c) the categories of data subjects and of personal data processed; (d) the categories of recipients, including those in third countries; (e) the third countries to which personal data will be transferred and the instrument, e.g., SCCs or BCRs, used to provide an adequate level of protection; (f) where possible, the envisaged retention periods for different categories of employee data; and (g) a general description of the security measures for employee data.

10. Watch For Additional Guidance

Although the Regulation contains more detailed compliance requirements than the Directive, the Regulation's requirements are much less detailed than what U.S. multinationals are used to seeing in U.S. regulations. However, the Regulation confers on the European Data Protection Board the authority to issue guidance on topics such as breach notification and binding corporate rules. Further guidance on these and other topics almost surely will be forthcoming during the two-year grace period before compliance with the Regulation becomes mandatory.