Insight

IN-DEPTH DISCUSSION

SEPTEMBER 13, 2017

The Next HR Data Protection Challenge: What U.S. Multinational Employers Must Do To Prepare for the European Union's Impending General Data Protection Regulation

BY PHILIP L. GORDON

With summer holidays over and only eight months remaining in the two-year enforcement grace period, U.S. multinational employers and their European Union (EU) subsidiaries have little time to spare before starting to address compliance with the EU's General Data Protection Regulation (GDPR or the "Regulation"), the EU's new data protection framework. By May 25, 2018, the corporate group will need to implement new policies, procedures, and practices to address the GDPR's many new requirements for handling EU employees' personal data.

Because the GDPR was drafted with the primary intention of protecting consumers who participate in the "digital economy," determining how the GDPR's new requirements apply to HR data can be challenging. To assist in that effort, this Insight describes 10 practical steps that U.S. multinationals can take to address the Regulation's provisions with the greatest impact on managing a global workforce.

While the late May 2018 deadline may translate into a "back-burner issue" for many, delay is not a real option. Several of the steps towards compliance will require months to complete. Moreover, developments since the Snowden leaks in June 2013 have left EU employees far more demanding about data protection. Employees' complaints to EU data protection regulators of alleged non-compliance could snowball into a significant administrative enforcement action. The GDPR empowers data protection regulators to levy administrative fines of up to 4% *of a corporate group's worldwide gross annual revenue* for most violations. In addition, because EU regulators are authorized to bar data processing at the EU subsidiary and to suspend data transfers to the parent corporation, noncompliance could ultimately result in severe disruption of EU operations.

Ten Practical Steps To Implement The GDPR

1. Determine Who Will "Own" The GDPR Implementation Process

Given the large number and wide range of steps required to implement the GDPR, U.S. multinational employers likely will need to build a team to execute a project plan. That team typically will include at least five groups: (a) HR professionals responsible for global workforce management and their in-house legal counsel; (b) information technology (IT) employees, especially those responsible for information systems used to manage HR data; (c) HR professionals with regional or local responsibilities for EU-based employees; (d) payroll personnel; and (e) personnel on the procurement team responsible for vendor contracting. For many U.S. multinationals, the U.S. parent corporation often will need to lead the implementation effort because EU subsidiaries will not have the HR and in-house legal support to undertake the implementation effort. This is particularly likely to be true for those organizations engaged exclusively in business-to-business (B-to-B) commerce.

For many organizations, this team approach likely will be preferable to appointing a data protection officer (DPO), *i.e.*, an executive or third-party contractor specifically designated to oversee GDPR implementation and on-going compliance. Contrary to popular perception, the GDPR does not mandate the appointment of a DPO. Instead, the Regulation requires organizations to appoint a DPO only in limited circumstances. Guidance issued by EU regulators confirms that these limited circumstances do not include the routine handling of HR data.[1] The regulators also take the position that organizations that voluntarily appoint a DPO must comply with all of the Regulation's requirements regarding DPOs.[2] These requirements could be onerous, especially for smaller EU subsidiaries. They include, for example, minimum (and high) levels of knowledge and expertise, on-going training, independent authority, direct reporting to senior management, and substantial protections against adverse employment action.[3] However, the regulators also have clarified that none of these requirements apply to a person to which an employer voluntarily assigns GDPR-related responsibilities, as long as the organization does not refer to that person in any compliance documentation as the "data protection officer."[4]

U.S. multinational employers should be aware that while individual EU countries have no authority to vary most provisions of the GDPR, EU countries are authorized to supplement the circumstances requiring organizations to appoint a DPO. Germany, for example, recently did so in legislation implementing the GDPR.

2. Identify All Systems Used To Process EU Employees' Personal Data

U.S. multinationals increasingly rely on cloud-based human resources information systems (HRIS) to manage their workforce globally. Because of the wide scope and volume of HR data maintained in these databases, employers typically should focus their compliance efforts on the HRIS. Nonetheless, employers should not neglect other systems where they collect and maintain the personal data of EU applicants and employees. Given the GDPR defines "personal data" broadly to include any individually identifiable information about a natural person or from which a natural person could be identified,[5] the relevant systems likely will be numerous and far-reaching. They may include, for example, learning management systems, digital timekeeping systems, and online surveillance systems.

---

1 Article 29 Working Party, "Guidance on Data Protection Officers ('DPOs')", 16/EN WP 243 (Dec. 13, 2016), at 7.

2 *Id.* at 5 [hereinafter "DPO Guidance"].

3 *See generally* GDPR, Arts. 37-39

4 DPO Guidance at 5-6.

5 *See* GDPR, Art. 4(1).

3. Determine The Permissible Purposes For Processing Employee Data

In contrast to U.S. law, which allows employers to use 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 definition of "process" is broad. The Regulation defines "processing" to cover any operation during the course of the information life cycle, from initial collection to final destruction.[6] If it engaged in any of these activities without a permissible purpose, an EU employer would violate the GDPR.

Only three of the permissible purposes for processing personal data identified in the Regulation are likely to apply in the employment context. First, the Regulation permits processing if "necessary for the performance of a contract" with the data subject, *i.e.*, an employee.[7] Under prior law, EU regulators construed the term "necessary" narrowly, and they likely will continue to do so under the GDPR. Consequently, this ground may be interpreted to cover only processing with a tight nexus to the employment contract, such as the payment of compensation and benefits or processing requests for sick leave or vacation.

Second, the GDPR permits the processing of employee data to comply with "a legal obligation to which the data controller [*i.e.*, the employer] is subject."[8] This ground will justify a wide range of HR data processing required to comply with local employment and labor laws, such as mandatory fitness-for-duty exams, processing trade union membership to deduct union dues from payroll where legally required, and reporting compensation information to tax and social security authorities.[9] Importantly for U.S. multinationals, the "legal obligation" must be imposed on the EU employer by local law. This ground, therefore, would not permit the U.S. parent corporation to process EU employees' personal data to comply with legal obligations emanating from U.S. law, such as responding to a subpoena issued in civil litigation in the U.S.[10]

Third, the Regulation permits processing that is necessary to achieve the "legitimate interests" of the employer or a third party, such as the parent corporation. However, an entity 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.[11] Applying this balancing test, an employer likely would be able to justify processing of employee data that is not particularly sensitive where there is a tight nexus to the employment relationship, such as the EU employer's using business contact details to arrange business travel or the parent corporation's reviewing performance appraisals for global succession planning.

While the GDPR recognizes consent as a permissible ground for processing personal data in most circumstances, EU regulators have emphasized that EU employers generally cannot rely on employees' consent because such consent cannot be "freely given" as required by the GDPR.[12] In the words of the regulators: "Employees are almost never in a position to freely give . . . consent given the dependency that results from the employer/employee relationship. . . . [E]mployees can only give free consent . . . when no consequences at all are connected to acceptance or rejection of an offer."[13]

---

6 *See* GDPR, Art. 4(2).

7 GDPR, Art. 6(1)(b).

8 GDPR, Art. 6(1)(d).

9 For a detailed discussion of GDPR's impact on payroll administration, *see* Philip L. Gordon and Kwabena A. Appenteng, "Navigating Global Payroll under the Impending EU General Data Protection Regulation," Littler Insight (Sept. 7, 2017)..

10 GDPR, Art. 6(3).

11 GDPR, Art. 6(1)(f).

12 GDP, Art. 6(1)(a).

13 Article 29 Working Party, "Opinion 2/2017 on Data Processing at Work," 17/EN WP 249 (June 8, 2017), at 23.

4. Apply The Principles Of Privacy By Design And Privacy By Default

The GDPR embraces the principles of privacy by design and privacy by default.[14] These principles mean that privacy should be built into the design of information systems and that default settings should favor more privacy rather than less.[15]

Applying these general principles to an HRIS database and other HR information systems can be challenging, especially because employers often are relying on "software-as-a-service" (SaaS) solutions and have limited or no control over the software's design. However, many of these solutions contain some features that permit employers to implement the principles of privacy by design and by default. For example, data entry fields for an HRIS database or for an online employment application, designed primarily for the broad data collection permitted under U.S. law, could be locked when data is entered about EU employees or job applicants to prevent the entry of data that the EU employer does not have a permissible purpose to collect. As another example, the database may permit the creation of detailed access lists that not only restrict access by employee category but also by data type within a category of employees.

The GDPR implementation team can best implement privacy by design and privacy by default by first obtaining a comprehensive understanding of the functionality of the HR systems that they, or a vendor, will be implementing. They can then look for ways to use the technology to implement the principles. Importantly, the Regulation recognizes that implementation of these principles may take into account "the state of the art, the cost of implementation, and the nature, scope and context of the processing" as well as the likelihood and severity of the risk to individuals' data protection rights.[16] In other words, U.S. multinational employers and their EU subsidiaries should have a reasonable amount of flexibility when applying the principles.

5. Update Data Processing Notices

As with prior law, The GDPR requires that data controllers distribute to individuals, when personal data is first collected from them, a notice of data processing that describes how the personal data will be handled. For EU employers, this means providing 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.

The Regulation substantially expands on the basic notice requirements under prior law, such as the categories of data collected, the purposes for the collection, recipients of the data, a description of data protection rights, and whether the data will be transferred outside the EU.[17] For example, EU employers that rely on the "legitimate interests" ground for processing (described in Step 3, above) must now describe those legitimate interests. As another example, data processing notices must now include information about the period for which employee data will be retained. This requirement highlights the importance of developing data retention schedules for each EU subsidiary that align with local employment and labor laws. EU regulators have not yet opined whether employers will be required to issue to current employees updated notices that address all GDPR requirements if the employer previously provided those employees with a notice that complied with prior law.

6. Ensure Employees Can Exercise Their Data Protection Rights

The GDPR confers on individuals the same rights to access, correct, and object to the processing of, their personal data that existed under prior law and adds two new rights: the right of data portability and the

14 *See generally* GDPR, Art. 25.

15 *See* GDPR Art. 25(1).

16 GDPR, Art. 25(2).

17 *See generally* GDPR, Art. 13.

right to be forgotten. The application of these new rights to HR data likely will be narrow. For example, the right of data portability, which provides data subjects with the right to move digital data from one entity to another, applies only to personal data provided by the employee and does not apply to personal data that the employer is required by law to collect.[18] Consequently, the right would not apply, for example, to performance appraisals prepared by supervisors.

Application of the "right to be forgotten" to HR data likely will be similarly narrow. For example, while this right allows employees to request deletion of files that no longer are necessary for the purposes for which they were collected, employers are not required to delete any employee data necessary to establish, pursue or defend legal claims, or that the employer is required by local law to retain. These exceptions likely will provide a valid basis for rejecting erasure requests until the relevant statutes of limitations or legal retention period expires.

Unfortunately, the limited scope of these two new rights will not relieve EU employers of the need to maintain policies and procedures for responding to requests exercising these rights. The procedures will need to address the timing for responses; when the deadline can be extended; the circumstances where requests can be denied; and the amount of the fees, if any, the employer can charge to recover the cost of responding.[19] Developing standardized forms and tracking logs can greatly facilitate implementation of these requirements and tracking of compliance with them.

7. Develop A Written Information Security Program And A Security Incident Response Plan

The GDPR introduces mandatory security breach notification to all EU countries and requires administrative and technical safeguards for personal data to reduce identified risks and to prevent data breaches. The Regulation, however, does not prescribe specific measures that organizations must take; instead, it establishes only general mandates, such as requirements to ensure the confidentiality, integrity and availability of personal data and to implement disaster recovery capabilities.[20]

Many U.S. multinational employers have responded to mandatory breach notification and information security requirements under a variety of state and federal laws by implementing a comprehensive written information security program that applies to all corporate data, including HR data globally. The policies composing this information security program should be extended to the personal data maintained by EU subsidiaries. To adequately modify corporate policies to local conditions, corporate IT staff or external consultants may need to assess risks specific to the EU subsidiaries.

The GDPR establishes a standard for breach notification similar to that of many U.S. breach notification laws, but requires notification far more quickly.[21] An organization that experiences a data breach generally must notify the relevant data protection authority (DPA) *within 72 hours* of discovering the breach unless it "is unlikely to result in a risk" of harm.[22] Notification to individuals is required if and when ordered by the DPA or, "without undue delay," if the breach is "likely to result in a high risk" of harm to affected individuals.

Given the newness of breach notification to most EU countries[23] and the expedited timeline for notification to the DPA, U.S. multinational employers should ensure that their EU subsidiaries have developed a security incident response plan and have trained all employees on the plan's key elements. The incident response plan should designate a security incident response team of local employees, and where necessary, supplemented

18 *See* GDPR, Art. 20

19 *See generally* GDPR Art. 12.

20 *See generally* GDPR, Arts. 32-34.

21 GDPR, Art. 4(12).

22 GDPR, Art. 33(1).

23 A few countries, such as Austria, Germany and the Netherlands, have previously enacted mandatory breach notification laws.

by U.S. resources, with responsibility for HR data. This team should be responsible for investigating, mitigating, and remediating the breach and for communicating about the breach with the DPA, employees, and where necessary, law enforcement.

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

U.S. multinational employers and their EU subsidiaries commonly share the personal data of EU employees with a wide range of service providers. For example, even smaller EU subsidiaries often use local payroll companies to administer payroll for local staff. At the same time, U.S. parent corporations increasingly retain a wide range of cloud-based service providers to collect and manage HR data globally. These vendors may include HRIS database providers, online performance appraisal platforms, and expense reimbursement solutions.

The GDPR requires vetting of service providers before they are retained to confirm the provider's ability to comply with the Regulation. The Regulation also specifies a long list of matters that must be addressed in service agreements. The list includes, for example, a detailed description of the data processing to be undertaken by the service provider and requirements the service provider (a) process personal data only subject to the employer's instructions; (b) implement required security measures; and (c) assist the employer in fulfilling its obligations to respond to requests by employees to exercise their data rights.

While the list of mandatory provisions is extensive, it is not complete. For example, if the vendor is located outside the EU, the vendor agreement must ensure that the vendor will provide an "adequate level of protection" for the transferred personal data (see Step 9, below). In addition, because of the significant enforcement and litigation risks associated with data breaches, the vendor agreements should address at least the specifics of breach reporting by the vendor, responsibility for notification to the DPA and affected employees, and indemnification for claims by employees arising from the data breach.

9. 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 prior law. This scheme generally prohibits transfers of HR 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 or a service provider — will ensure an adequate level of protection for the transferred personal data.

The EU 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 has issued such a determination for the EU-U.S. Privacy Shield Framework, which went into effect on August 1, 2016. Thus, EU subsidiaries can transfer their employees' personal data directly to U.S.-based members of the corporate group and to U.S.-based service providers that have certified to the U.S. Department of Commerce that they will handle transferred personal data in accordance with the Privacy Shield's requirements.[24]

U.S. multinationals and service providers not certified to the Privacy Shield generally will need to rely on one of the other data transfer mechanisms identified in the Regulation. These mechanisms include the standard contractual clauses (SCCs), approved by the Commission, 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, any non-EU affiliate that receives EU personal data and any non-EU service providers). BCRs are legally binding policies applicable to all members of a corporate group, whether located

24 For more information about transfers of EU employees' personal data to the U.S. pursuant to the Privacy Shield, *see* Philip L. Gordon, "The Privacy Shield: What U.S. Multinational Employers Need To Know To Enjoy The Benefits Of The Newest EU-U.S. Data Transfer Mechanism," Littler Insight (July 13, 2016).

within or outside the EU, and are enforceable by employees as third-party beneficiaries. To date, fewer than 100 U.S. companies have implemented BCRs as compared to almost 2,500 that have certified to the Privacy Shield Framework.

U.S. multinationals should note that both Privacy Shield and SCCs currently are subject to some uncertainty. Both mechanisms are the subject of litigation in the EU, meaning the Commission's adequacy determination for each mechanism could ultimately be reversed by the EU's highest court, the European Court of Justice. In addition, U.S. and EU officials will meet later this month (September 2017) for the first annual review of the Privacy Shield. This review is particularly significant because (a) the Commission's initial adequacy determination was based on prior law, not the GDPR; (b) the Privacy Shield has been subject to heavy criticism by EU regulators, members of the EU Parliament, and EU privacy advocates; and (c) this will be the first review since the change in U.S. administrations.

10. Periodically Review GDPR Implementation And Maintain Required Records Of Data Processing

U.S. multinationals' and their EU subsidiaries' handling of HR data is continuously in flux, so GDPR implementation needs to be just as dynamic. When information systems are modified, or new information systems are brought online, the change likely will trigger a wide variety of compliance tasks. By way of illustration, the modified or new system should be scrutinized with privacy by design and privacy by default in mind. The EU employer should confirm that it has a permissible purpose for all new categories of data that will be collected and for all new uses and disclosure of that data. Data processing notices may need to be revised or drafted. Information security policies may need to be modified. Vendor agreements may need to be amended or entered for the first time.

In light of the evolving nature of HR data processing, the implementation team should oversee the organization's data protection efforts on an on-going basis after initial implementation. The team could conduct annual reviews of the overall implementation program. These periodic reviews could be supplemented by reviews before existing systems are materially modified and before new systems are implemented.

This on-going compliance effort should assist the U.S. multinational in maintaining on-going compliance with the GDPR's mandatory record-keeping requirements. The Regulation requires that employers maintain detailed records of their data processing. The information to be recorded includes: (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. These records must be provided to the DPA upon request.

Conclusion

Implementing a GDPR compliance program for HR data, "operationalizing" the program, and maintaining on-going compliance will require a multi-disciplinary team, typically led by corporate headquarters. The program likely will impact all of the organization's policies, procedures, and processes involving the handling of EU employees' personal data. Some of the steps required to achieve compliance, such as amending vendor agreements, could take several months to complete. Given the breadth of the undertaking and the lead time needed to compete it before the May 25, 2018 enforcement deadline, the time to get started is now.

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 first published in the IAPP's Privacy Tracker blog.