Even though the General Data Protection Regulation ("GDPR") became effective on May 25, 2018, its application to U.S.-based employers continues to evolve and increase in complexity. For U.S. employers of European Union ("EU") residents, renewed concerns have arisen regarding the transfer and protection of such data, and with meeting GDPR compliance demands. This is particularly important with regard to remote working arrangements, COVID-19 contact tracing, and interaction with global HR data systems. In light of these developments, the following is a refresher concerning common questions U.S. employers may have regarding GDPR compliance (as it relates to their employment of EU residents), and highlights of new compliance considerations. As U.S. employers update their privacy and security policies, attention to GDPR compliance issues should be addressed, as applicable.

- **When is a U.S. company an “establishment” within the EU?**

  - The [European Data Protection Board ("EDPB") Guidelines](#) provide that the GDPR applies to the processing of personal data in two scenarios: (1) in connection with the activities of an establishment within the EU, and (2) in regard to activities targeted at individuals located within the EU related to either (a) the offering of goods or services, or (b) the monitoring of behavior.

  - For U.S. employers, note the example of a company based in New York with no offices in the EU that may still be considered an establishment within the EU if the company has an “effective and real exercise of activities through stable arrangements” within the EU. Indeed, if a New York-based company has a branch office in Paris, the branch office could be considered an establishment in the EU. Further, if HR data from the Paris branch office is processed from the New York office, the GDPR applies simply because the data it processes is of individuals located within the EU. Even the presence of one employee within the EU can be sufficient to create an establishment in the EU if the employee acts with a sufficient degree of stability.
• **Do I have employees who are protected by the GDPR?**

  o The GDPR applies to any person residing or located in an EU country. Accordingly, if a U.S.-based company is subject to the GDPR and sends one employee to work in Paris, that one employee’s personal data is protected by the GDPR. Conversely, if an EU citizen leaves the EU to work at a ski resort in Denver, that person is no longer protected by the GDPR. However, when that EU citizen returns to the EU, if he or she continues to interact with the U.S. employer for any HR or benefits-related issues, for example, then his or her personal data is protected by the GDPR.

  o The GDPR can also apply to companies with no establishment within the EU. In this context, the monitoring of employee behavior (e.g., when the activity includes the systematic and purposeful targeting of EU residents) is the activity most likely to subject the employer to the requirements of the GDPR.

  o The [EDPB Guidelines](#) provide examples of the activities encompassed by the term “monitoring,” including online tracking, closed-circuit television video surveillance, and location tracking activities.

• **Does my company process or control personal data as described by the GDPR?**

  o Companies are subject to the GDPR if they process or control data. Notably, data controllers are subject to more obligations than are data processors. Data controllers are people or businesses that determine the purposes for which and how personal data is processed. Data processors are people or businesses that process personal data on behalf of a data controller.

  o For example, an automobile manufacturer may collect an employee’s personal data in order to make a uniform for her. The company may outsource the process and have a second company make the uniform. In this scenario, the automobile manufacturer is the controller and the vendor is the data processor. A simpler example is a company storing data on a third party’s server. The company would be the controller in this scenario, and the third party would be the processor.

• **What kind of HR data processing activities are covered under the GDPR?**

  o The following examples of HR data processing activities are subject to the GDPR:

    ▪ HR data processing performed by an EU-based company or a subsidiary/affiliate of a U.S. company located in an EU country with at least one EU resident employee who regularly conducts business within the EU;
- HR data processing on behalf of the EU-based company or U.S. subsidiary/affiliate located in an EU country that is performed by a third-party service provider located in Oregon;
- HR data processing of data that originated in the EU, or is about EU residents, regardless of where the processing takes place;
- HR data processing performed by a New York company that contracts with a sales representative who exercises real and effective business activity in Italy;
- Data processing performed by a Texas company that monitors the emails, internet usage, and/or social media of employees of its German subsidiary;
- Data processing performed by a North Carolina company that monitors the location data of employees of its Danish subsidiary through GPS; and
- Data processing performed by an Ohio company that recruits job applicants from France if the recruitment process involves behavior monitoring (e.g., social media accounts) and takes such behavior into consideration when deciding whether to offer employment.

**What is considered sensitive personal data, and how should my company handle it?**

- “Personal data” is any information relating to an identified or identifiable natural person. A person can be identified from information such as name, ID number, location data, online identifier, or other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. This could include IP addresses, cookie strings, social media posts, online contacts, and mobile device IDs.

- The following personal data is considered sensitive and therefore subject to specific processing conditions:
  - personal data revealing racial or ethnic origin, political opinions, or religious or philosophical beliefs;
  - trade-union membership;
  - genetic data or biometric data processed solely to identify a human being;
  - health-related data; and
  - data concerning a person’s sexual activities or sexual orientation.

- Sensitive personal data should be separately stored in a secure location.
The processing of sensitive personal data is generally prohibited. However, certain exceptions may apply. In addition to needing a legal basis to process sensitive personal data, one of the exceptions enumerated in Article 9(2) must apply.

- **What if an employee is a resident of California (with protections under the California Consumer Privacy Act (“CCPA”)) and decides to move to an EU country for three years? Do both CCPA and GDPR protections apply?**

At the current time, the CCPA has limited application with regard to employee data, except for certain notice requirements. There is a draft ballot initiative in California to extend the exception beyond January 1, 2021, to the year 2023. Therefore, it is important to consider that if the employee is no longer a resident of California, his or her personal information will no longer be protected by the CCPA. Whether the CCPA will apply, however, depends on the nature of the move. If the move is considered “temporary” (e.g., less than 546 days under an employment-related contract), that person would still be covered by the CCPA. In addition, the GDPR protections would apply as long as the employee is located in the EU.

- **What if a U.S. employer uploads data to its HR system in the United States and transmits it to the EU—to a parent company or subsidiary—or the data travels in the cloud?**

  o U.S. employers that customarily send and receive HR data to an affiliated company in the EU could potentially be transferring or processing GDPR-protected HR data. Consequently, companies transferring such data should ensure that the transfers themselves comply with the GDPR. If the data entirely contains information regarding individuals residing in the United States, that data would not be subject to GDPR protection even if it is processed in the EU.

  o Previously, the EU-U.S. Privacy Shield provided companies in the United States and the EU a mechanism through which they could comply with the GDPR when transferring personal data from the EU and Switzerland to the United States. However, the Privacy Shield was struck down in July 2020 by the European Court of Justice after finding that U.S. national security laws do not protect EU citizens from government snooping. U.S. companies will now have to sign EU-drafted non-negotiable “standard contractual clauses,” which are currently used in other countries. For more information, see “ECJ Invalidated the EU-US Privacy Shield Framework.”

- **Does a U.S. employer need a Data Privacy Impact Assessment (“DIPA”) or update to other policies to address the GDPR in other privacy/security policies?**

  o If an employer will collect data that is subject to the GDPR, the employer should perform a DIPA and update any policies and procedures relating to processing activities.
o For example, the EDPB has stated that each EU member state should require employers to perform a DIPA when planning to engage in the systematic monitoring of employees.

o Employers first should review their employee and retiree rosters to determine whether any employees reside within the EU, thereby necessitating a more in-depth review.

o Employers should also review and revise as needed to comply with the GDPR:

- third-party provider services to identify where personal data is being shared,
- privacy notices,
- data security and breach notification processes, and
- privacy training.

- **Does a U.S. employer need to be concerned about the GDPR’s requirements if it obtains the employees’ consent to process their personal data?**

  o Generally, the GDPR requires that data subjects consent to the processing of their personal data for any specific purpose. In the United States, most companies obtain similar consents through blanket consent clauses in employment agreements or handbooks. However, obtaining employee consent is insufficient under the GDPR. The United Kingdom’s Information Commissioner’s Office issued interpretive guidance noting that consent is inappropriate in the employer-employee context, as consent cannot be “freely given” when a “clear imbalance of power” exists.

  o With this in mind, companies must identify a lawful basis in order to process the personal data of employees. Lawful bases include the performance of an employment agreement, compliance with legal obligations, and to further a legitimate interest of the employer. Note, however, that many U.S. employees are “at will” and do not have an employment agreement with their employer. The employment agreement basis would apply to collective bargaining contracts.

  o A company must prove it has a legitimate interest to process the personal data by documenting why the company’s right to the data outweighs the employee’s privacy rights. This involves performing a data protection impact assessment.

  o In addition, as a practical matter, because the blanket consent clauses typically found in employment agreements are inadequate under the GDPR, it is advisable to remove these clauses and instead reference the company’s legal basis for processing personal data.
• **What are the U.S. employer’s service agreement requirements with a third party that processes data on its behalf?**

  o If the U.S. employer will collect and process data related to EU residents, the employer (the data controller) must have a written contract in place outlining each parties’ obligations under the GDPR.

  o These agreements should include a Data Protection Agreement (“DPA”) that outlines how the data will be processed and stored. As an exhibit to that DPA, a Business Associate Agreement may also be needed if the processing is being done on behalf of the group health plan and the data being processed includes protected health information. When using a cloud service provider, the DPA may also address that the data center being utilized is located in the EU.

  o Model GDPR contract clauses and binding corporate rules are also available under the EU guidance that can be included in the agreement.

• **How can a U.S. employer ensure that it properly secures this data under GDPR requirements, including erasure of this info?**

  o **SECURITY**

    ▪ The GDPR requires the implementation of appropriate technical and organizational measures. This includes risk analyses, security policies, and physical and technical measures. Where appropriate, measures such as pseudonymization and encryption should be employed. If data is stored on an IT system, access to that system should be limited and the security settings of the system should be regularly updated.

    ▪ Employers should maintain employee data only for as long as necessary, which is typically until all legal obligations are fulfilled after the employment relationship ends.

  o **ERASURE**

    ▪ First, companies must notify any other company to which the employee’s data was disclosed.

    ▪ Erasing personal data includes erasing such information from backup systems. If complete erasure is impossible, the personal data contained in the backup system must be rendered “beyond use.” Employers must commit to permanent erasure of the data if and when it becomes possible.

    ▪ Complying with a request for erasure must be done without undue delay, and at least within one month of receipt of the request.
Under the GDPR, EU member states are entitled to enact additional and more restrictive laws in regard to the processing of personal data in the employment context. These derogations allow member states some discretion as to how select provisions apply and specifically allows them to introduce broad derogations concerning national security, the prevention of crime, and the enforcement of civil claims, where such derogations respect the essence of the individual’s right to data protection and are a necessary and proportionate measure.

- **Are there safe harbors for employers in certain industries (e.g., financial institutions)?**

  The Privacy Shield and its predecessor, the Safe Harbor, have both been deemed invalidated, thus the major safe harbors have been removed. The GDPR does provide some specific exemptions that must be examined on a case-by-case basis and are not automatically applied.

- **Are there special breach notification procedures?**

  The breach notification rules can be found in Articles 33 and 34. In the event of a breach, it is necessary to report the breach to the President of the Personal Data Protection Office within 72 hours of the breach being identified. This report should provide a description of the nature of the violation and any potential consequences. Depending upon the circumstances, notifying the data subjects whose data has been breached may also be necessary.

- **What are potential penalties for noncompliance?**

  Penalties for noncompliance with the GDPR are significant, but vary depending on the severity and the intent of the violation or a history of noncompliance by the company. However, even the less severe violations could result in a fine of up to 10 million Euros or 2 percent of the company’s worldwide annual revenue from the preceding year, whichever amount is higher. More severe violations could result in up to twice the penalty amount of less severe violations.

**What U.S. Employers Should Do Now**

U.S. employers should consider the following, especially in light of COVID-19 contact tracing and remote work:

- Recognizing that remote work generally increases a company’s data security vulnerabilities, make sure that your company, if it has not done so already, adopts procedures for the protection of personal data in the context of remote work and update the DIPAs to reflect such changes.

- Understand that training may be necessary to ensure that employees are aware of the company’s minimum security requirements for any devices and networks they use. Warn employees about the increased vulnerabilities resulting from remote work, and ensure that they are “on alert” for any potential phishing attacks sent via email.
Review and update the company’s cybersecurity policy. The NIST cybersecurity framework provides a set of best practices.

Ensure that sensitive information, including personal data, is encrypted and that access to personal data is limited to those whom need it. Using a corporate VPN further limits access to personal data.

Review and update service agreements to make sure that GDPR requirements are addressed and protective language is incorporated. This process may have already begun. As noted above, the EU-U.S. Privacy Shield previously provided companies in the United States and EU a mechanism through which they could comply with GDPR when transferring personal data from the EU and Switzerland to the United States. However, the Privacy Shield was struck down in July 2020 by the European Court of Justice after finding that U.S. national security laws do not protect EU citizens from government snooping. U.S. companies will now have to sign EU-drafted non-negotiable “standard contractual clauses,” which are currently used in other countries.

Ensure that any new technologies (such as for contact tracing) that might impact employees’ privacy undergo an evaluation for access and authorization prior to storing live employee data. Thus, if contact tracing occurs during non-working hours, or if mobile apps are used, it is important to make sure that you are not collecting data that is not intended to be collected. For more information regarding COVID-19 and cybersecurity risks, see “Security Implications: Privacy & Security Considerations for Managing Compliance Risk amid COVID-19, Part 4.”

****

For more information about this Advisory, please contact:

Matthew H. Berger
Washington, DC
202-861-1829
mberger@ebglaw.com

Michelle Capezza
New York
212-351-4774
mcapezza@ebglaw.com

Audrey Davis
Washington, DC
202-861-1830
adavis@ebglaw.com

This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

About Epstein Becker Green
Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in locations throughout the United States and supporting domestic and multinational clients, the firm’s attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.

© 2020 Epstein Becker & Green, P.C.