GDPR Assessment Report for Human Resources Data

Littler
Employment & Labor Law Solutions Worldwide®

GDPR Assessment Report for Human Resources Data:

This report discusses the potential obligations of your organization and its subsidiaries (collectively, "Organization") to comply with the European Union's General Data Protection Regulation (GDPR) with respect to human resources (HR) data. The GDPR will come into effect in the European Economic Area (EEA) on May 25, 2018. The risks of non-compliance with the GDPR will likely far exceed the risks of failing to comply with current European Union (EU) data protection law. The maximum fine under the GDPR has increased to 4% of global annual revenue for the entire corporate group, and EU regulators plan to increase enforcement.

We recommend that organizations subject to GDPR requirements start the compliance process as soon as possible. Many of the obligations imposed by the GDPR involve substantial changes to business operations and related administrative burdens. The steps to achieve compliance may take months to complete.

This report provides a basic overview of your Organization's likely compliance obligations under the GDPR with respect to HR data. The overview is based on your responses to the three questions below. For a comprehensive assessment, please contact Littler's GDPR Compliance Team.

PLEASE REVIEW THE TERMS OF USE BELOW.

Question 1

Does your Organization collect personal data from workers located in the EEA?

Personal data *means information that relates to an identified or identifiable natural person. For example, an individual's name, job title, business contact information, or employee identification number is personal data.*

Worker: *For purposes of this GDPR Assessment, "worker" refers to any individual who is located in the EEA and performs services for your Organization, for example: applicants; employees; independent contractors; interns; temporary workers; and volunteers.*

European Economic Area *includes Iceland, Liechtenstein, and Norway and the countries of the EU: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. The United Kingdom is expected to continue to be a member of the EEA into 2019. Switzerland is not a member of the EEA.*

If you answered "no" to Question 1

Your Organization may not have compliance obligations under the GDPR for human resources data. This analysis can be highly fact-dependent, however.

Please contact Littler's GDPR Compliance Team to confirm. In addition, please note that your Organization may be required to comply with the GDPR for other types of personal data, such as consumers' personal data.

If you answered "yes" to Question 1

Your Organization is required to comply with the GDPR with regard to HR data. Compliance includes, but is not limited to, the following:

1. **Ensure permissible purposes for processing:** Ensure that your Organization processes EEA workers' personal data only for a permissible purpose under the GDPR. Potential permissible purposes include the performance of the employment contract, a requirement under applicable employment or labor law, the legitimate interests of the employer or a third party, and the consent of the worker. Please note, however, that EU regulators generally take the position that, due to the imbalance of power in the employment relationship, employees cannot provide valid consent. Therefore, the employer may be able to rely on the consent of workers who are not employees, e.g., applicants, but should avoid relying on the consent of employees.
2. **Provide notice(s) of data processing:** When your Organization collects personal data from an EEA worker, your Organization is required to provide a notice of data processing to the worker. As a general matter, notices of data processing describe how your Organization processes EEA workers' personal data and must include, among other points, the following:
   - The purposes and legal basis for which your Organization will process the personal data;
   - The recipients of the personal data, if any;
   - Whether your Organization intends to transfer the personal data to a country outside of the EEA and the legal basis for the transfer;
   - The retention period for storing the personal data; and
   - The EEA worker's data rights.

   If your Organization has previously provided notices of data processing to comply with current EU data protection law, these notices likely must be updated to comply with the GDPR.
3. **Allow EEA workers to exercise their data rights:** Your Organization must allow EEA workers to exercise their rights to access, correct, object to or restrict the processing of, or delete their personal data processed by your Organization and to request that your Organization transfer their data to a third party (referred to as "data portability").
4. **Vet service providers and amend service provider agreements:** Your Organization should vet service providers that process the personal data of EEA workers and execute an agreement that contains all provisions required by the GDPR with each vendor.
5. **Implement privacy by design and by default:** Your Organization should implement technical and organizational measures to ensure that, by default, your Organization only processes and discloses the minimum necessary personal data to accomplish the permissible purposes for processing. In addition, your Organization should build safeguards into the design of its technical and organizational systems to reduce the risk of an unauthorized use or disclosure of personal data.

6. **Implement data security safeguards and a security incident response plan:** The GDPR requires the implementation of administrative and technical safeguards for EEA workers' personal data to reduce identified risks and to prevent a personal data breach. The GDPR does not specify safeguards that must be implemented, but it does identify a few steps and objectives as potentially appropriate, such as:
   - Encryption and pseudonymization;
   - The ability to ensure the confidentiality, integrity, and availability of personal data; and
   - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

   Your Organization also should consider developing a security incident response plan to be prepared to respond to a personal data breach.

EU regulators will likely issue additional guidance on complying with the GDPR as the May 25, 2018 deadline approaches. Littler will publish additional resources on our GDPR Resources page and you can contact Littler's GDPR Compliance Team with questions.

Question 2

Is any personal data of workers located in the EEA transferred to the United States or to another country located outside of the EEA?

Transfer *means to send personal data to a country outside the EEA or to permit access from outside the EEA to personal data located within the EEA. For example, personal data is transferred from the EEA to the United States if a German employee's salary information is stored in a database in Germany and HR employees of your Organization who are located in the United States remotely access that data.*

If you answered "no" to Question 2:

The GDPR likely does not require your Organization to comply with its cross-border data transfer requirements.

If you answered "yes" to Question 2:

Your Organization must comply with the cross-border data transfer requirements of the GDPR.

The GDPR's overall scheme for cross-border data transfers is materially the same as that under prior law. However, enforcement is likely to be stricter under the GDPR than under the current regime.

The GDPR prohibits the transfer of personal data to a country outside of the European Economic Area unless the European Commission has determined that the country "ensures an adequate level of protection" for personal data. The European Commission has not determined that the United States "ensures an adequate level of protection." As a result, personal data may only be transferred to the United States using one of the three data transfer mechanisms approved by the European Commission – model contracts; the EU-U.S. Privacy Shield Framework; and binding corporate rules – or under a derogation.

Model contracts: The model contracts or "Standard Contractual Clauses" are standard contracts approved by the European Commission. To rely on the model contracts for a

cross-border data transfer, the U.S. organization importing the personal data from the EEA must sign a model contract with the organization in the EEA that will export the personal data. Although most of the language in the model contracts cannot be modified, the parties must complete a form appendix to the model contracts that describes the data transfer in substantial detail, including the categories of data to be transferred and the purposes for which the transferred data will be processed. Employers should note that when a U.S. multinational has a large number of subsidiaries in the EEA, managing these agreements and the amendments to them can be administratively burdensome.

EU-U.S. Privacy Shield: The EU-U.S. Privacy Shield Framework (the "Privacy Shield") was designed by the U.S. Department of Commerce and the European Commission to facilitate transfers of personal data from the EU to the United States. In order to rely on the Privacy Shield for transfers to the United States, organizations must self-certify to, and fully comply with, the Privacy Shield Principles. These Principles include Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitation, Access, and Recourse/ Enforcement and Liability. Compliance includes publicly posting a privacy policy that embodies the Privacy Shield Principles. However, a privacy policy that applies only to human resources personal data need not be made publicly available as long as it is available for viewing by affected workers. In addition, organizations that have certified to the Privacy Shield must conduct an annual self-assessment to verify compliance with the Privacy Shield Principles.

Binding corporate rules: Binding corporate rules ("BCRs") involve the development and implementation of a uniform set of rules that are binding on all members of the corporate group, regardless of location, and that provide the level of protection for personal data required by the GDPR. The organization's BCRs must be approved by EU regulatory authorities before the organization can rely on the BCRs for transferring personal data out of the EEA. This review and approval process can require substantial resources to navigate and considerable time to complete.

Derogations: The GDPR sets out several exceptions, referred to in the GDPR as "derogations," to the general rule that personal data cannot be transferred to a third country unless that country "ensures an adequate level of protection" for personal data. The two derogations most likely to apply in the HR context are:

- transfers with the unambiguous consent of the worker; and
- "the transfer is necessary for the performance of a contract between the data subject and the controller," i.e., the EEA-based worker.

However, few employers will be able to rely entirely on these derogations to transfer HR personal data out of the EEA.

<u>Consent:</u>

EU data protection regulators strongly disfavor reliance on an employee's consent for data processing. According to these regulators, because of the hierarchical nature of the employment relationship, employees cannot freely give consent as a matter of law.

However, employers can potentially rely on consent from non-employees, for example, from applicants. Please note that the non-employee worker's consent must be "unambiguous."

To reduce the risk that consent of a non-employee worker might be deemed ambiguous, employers should provide the worker with robust notice and a means for the worker to affirmatively express consent.

Performance of a contract:

Although many EEA subsidiaries of U.S. multinationals require employees to execute an employment agreement, EEA subsidiaries cannot necessarily rely on the "performance-of-contract" derogation to legitimize cross-border data transfers. EU data protection authorities construe the derogations narrowly. In the case of the "performance-of-contract" derogation, the regulators likely would scrutinize whether the transfer to the parent corporation is "necessary" for the performance of the contract between the EEA resident and the EEA employer-subsidiary. This is because such transfers of personal data are often for purposes that are in the interest of the parent corporation, such as succession planning, but have limited, if any, significance for the contractual relationship between the EEA employee and the EEA employer-subsidiary.

Notice:

Regardless of the data transfer mechanism or derogation on which your Organization relies for transferring personal data out of the EEA, your Organization should provide clear notice to the worker of the planned cross-border transfer at the time of collecting the personal data. This point is also discussed in the response to Question 1 above, in section 2 on notices of data processing.

Question 3

Have the employees at any of your Organization's locations in the EEA organized a works council?

Works council *means a group of employees elected by co-workers and authorized to represent the entire workforce regarding certain matters, such as the processing of employee personal data.*

If you answered "no" to Question 3:

Your Organization does not have an obligation to confer with an EEA works council regarding personal data processing.

If you answered "yes" to Question 3:

Your Organization may be required to confer with the works council(s) at your Organization's EEA locations. Some countries in the EEA require that employers consult with works councils on the employer's processing of employees' personal data.

The level of required consultation varies widely. For example, in Hungary, the employer must simply request the works council's opinion 15 days prior to making a decision to change how the employer will process employee personal data. The Hungarian works council need not approve the change, however.

In contrast, in the Netherlands, the employer must submit a written request for approval to the works council, including details on the new data processing policy and the consequences to employees. The employer also must meet with the works council for at least one consultation session to answer any questions and cannot proceed with the new policy on processing personal data until the works council approves.

TERMS OF USE

NO ATTTORNEY-CLIENT RELATIONSHIP: The Littler GDPR Assessment tool, including the online questions, guidance, and annotations (the "LGDPRA"), and this GDPR assessment report generated by the LGDPRA (the "User Report") have been prepared by Littler Mendelson, P.C. for general informational purposes only. Your use of the LGDPRA does not constitute a request for legal advice, and no attorney-client relationship is formed by your use of the LGDPRA or the User Report. An attorney-client relationship will only be formed after Littler Mendelson, P.C. has conducted a conflicts check and we have executed an engagement letter with you. The responses you provide during your use of the LGDPRA and the User Report are not protected by the attorney-client privilege or any other legal protection that might prevent its disclosure. The LGDPRA is not advertising or a solicitation. You should not rely upon the LGDPRA or the User Report alone for any purpose without seeking legal advice from licensed attorneys in the relevant state or states. The User Report is only intended to highlight the possible implications of the European Union General Data Protection Regulation on your business. You should not use the User Report until after you have formed an attorney-client relationship with an attorney with the skills necessary to help you apply the law to your unique circumstances.

COMPLIANCE WITH LAWS: Through your use of the LGDPRA, you agreed to use the LGDPRA and the User Report in compliance with all applicable laws, and you agreed to indemnify and hold Littler Mendelson, P.C. harmless from and against any and all claims, damages, losses, or obligations arising from your failure to comply.

PRIVACY: The LGDPRA and the User Report have been prepared by Littler Mendelson, P.C. for your general informational purposes. Do not use the LGDPRA or respond to the questions unless you have the authority from your company to share the information you provide. We disclaim any and all liability in connection with the collection, use, or disclosure of the information furnished by you or otherwise collected by this tool. Please note that we cannot guarantee the security of any information transmitted to us over the Internet. Please also refer to the Privacy Policies that generally governs the use of the LGDPRA and www.littler.com site.

DISCLAIMER OF LIABILITY: THE LGDPRA AND THE USER REPORT ARE PROVIDED "AS IS." WE MAKE NO REPRESENTATIONS OR WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. YOU ASSUME COMPLETE RESPONSIBILITY AND RISK FOR USE OF THE LGDPRA AND THE USER REPORT. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. Littler Mendelson, P.C. expressly disclaims all liability, loss, or risk incurred as a direct or indirect consequence of the use of the LGDPRA or the User Report. By using the LGDPRA or the User Report, you waive any rights or claims you may have against Littler Mendelson, P.C. in connection therewith. Employment law is a dynamic field, often with varying results from state to state. You should contact your attorney to obtain advice with respect to any particular issue or problem. The LGDPRA and the User Report are not a do-it-yourself guide to resolving legal issues. Nonetheless, we trust you will find the information useful in understanding the issues raised and their legal context. The materials available at this site are not a substitute for experienced legal counsel and do not provide legal advice or attempt to address

the numerous factual issues that inevitably arise in any legal analysis. Littler Mendelson, P.C. at its sole discretion may choose to change the terms, conditions, and operation of the LGDPRA and the User Report at any time. Littler Mendelson, P.C., in its sole discretion, reserves the right to refuse to provide you access to the LGDPRA and the User Report. You agree that Littler Mendelson, P.C. shall not be liable to you for loss or damages that may result from our refusal to provide access to the LGDPRA or the User Report.

IRS CIRCULAR 230 COMPLIANCE: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax information contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of: (i) avoiding penalties under the Internal Revenue Code, or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein. You should seek advice based on your particular circumstances from a tax advisor.