May 2018

For U.S. Employers with E.U. Employees

How to be GDPR-ready if you have E.U. employees or Applicants for E.U. based roles

---

With less than 10 days to go before the E.U. General Data Protection Regulation (Regulation (E.U.) 2016/679) (GDPR) becomes law in the European Union, many U.S. companies with employees in the E.U. or in an E.U. subsidiary are still grappling with how the new regulations will impact them.

This is particularly so, in terms of applicants for job roles within the E.U.

Under GDPR, all employers or prospective employers will be required to provide job applicants with extensive information about how will process each candidate's personal data.

The new requirements are more detailed than under the current Data Protection Directive.

As such, many U.S. employers with E.U. employees will need to adopt the new directives in order to remain compliant.

A key component in GDPR compliance is a company 'GDPR-ready' Privacy Notice in which an employer communicates to employees / job applicants, the categories of personal data that will be processed, the purposes for which they will be processed, to whom and where they are disclosed and whether they will be transferred outside of the European Economic Area (EEA).

A GDPR-ready Privacy Notice gives employees and job applicants, the applicable legal basis for processing, be that legitimate interests, performance of an employment contract or a legal requirement.

WHAT SHOULD BE INCLUDED IN A GDPR-READY PRIVACY NOTICE

Employer's Identity: E.U. based employees and job applicants for E.U. based roles are entitled to know who makes the decision about how their data is used.

As an E.U. employer, you must ensure your Privacy Notice includes the full legal name and contact information of the entity that makes this decision.

U.S. companies that do not have legal entities in the E.U. but have E.U. based employees, need also to consider who actually makes this decision.

This is also true in the case where there is an E.U. based legal entity but where the actual decision making in relation to employee data is made by the management of the U.S. entity.

If you have appointed a Data Protection Officer, their details should also be included.

Employee Data: When considering the collection of data from E.U. based employees and job applicants for E.U. based roles, employers need to take full consideration of the definition of 'personal data' under GDPR.

For those who already understand the requirement under the now expiring E.U. data protection directive, the GDPR definition, while similar, has a number of important nuances.

In order to inform Individuals about the types or categories of personal data being collected, it is important for employers to consider the definition of personal data under the GDPR.

The definition has not changed fundamentally, however there are specific additions that require careful attention.

"Personal Data" means, any information relating to an identified or identifiable natural person.

An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that person.

The new additions to this definition are location data, online identifiers and genetic data.

How Personal Data is Collected: As an E.U. employer, you are required to set out the ways in which your organisation collects personal data.

In most instances, this will be self-evident. For example, for an E.U. based vacancy, this will typically be applicant's name, email address and CV.

However, it is important to also refer back to the definition of personal data to ensure that the application fields capture all the data collection methods.

Personal Data Collection: Employees and job applicants are 'data subjects' just like any other individuals from whom you collect data.

So, just like other data subjects, they too must be informed of the purposes for which you, as their employer are collecting their personal data and how you intend to use that data.

An employee's or prospective employee's data must not be processed for any purposes beyond those contained in your Privacy Notice.

In addition, they cannot be further processed in a manner that is incompatible with the primary purpose for which the data was initially collected.

As an employer you must also provide clear and comprehensive information about how you intend to use their personal data and why you need their data in order to satisfy the transparency principle under the GDPR.

However, simply being transparent about any dubious processing of that data will not make the processing of that data legitimate.

It is therefore essential that only the personal data that you require essentially is collected and processed for the purposes of evaluating candidates' suitability for the E.U. based role for which they are applying.

An Employer's Legal Basis for Processing: Your employees' personal data can only be processed where there is a lawful basis.

One such lawful basis is obtaining consent.

However, consent requirements imposed by the GDPR are more onerous than the previous data protection regime.

Consent must be freely-given, specific, informed and revocable.

GDPR also provides that, where there is an imbalance of power between the parties, consent will not be valid.

In the employer-employee context, consent alone will likely not be a lawful basis for processing personal data and employers will need to establish an alternative lawful basis.

One such alternative is processing for 'necessary for the purposes of legitimate interest'.

However, in using legitimate interest, employers must ensure that their interest(s) outweigh(s) the interests and rights of the employees whose data they are processing.

If, as an employer, you rely on legitimate interests, the purpose of the processing activity must be legitimate, necessary and proportionate.

Whether an employer's interests are legitimate will depend on the specific interest(s) of the business and its purposes for processing.

The recitals to the GDPR include a number of examples of cases in which an interest may be legitimate.

For example, companies within the same group may have a legitimate interest in transmitting personal data within the group for internal administrative purposes.

Other than legitimate interests, processing will also be lawful where it is necessary for the performance of an employment contract, or to comply with a legal obligation.

Sharing Employee Data: As an employer you must explain whether and when an employee's personal data may be disclosed to third parties and the purpose for such disclosures.

Ideally, this will include links to your privacy policies and those of your third parties.

You also will need to explain your practices regarding the sharing of employee data with other entities, such as recruitment partners, payroll providers or third parties such as reference or background checking bureaus.

Transferring Employee and Job Applicant Data Outside the EEA: An employer is prohibited from transferring personal data outside of the EEA, unless there is a valid adequacy mechanism legitimising that transfer.

It is extremely important to understand that the concept of "transfer" is wider than a direct transfer of personal data from, for example, a UK subsidiary to a U.S. parent.

It also includes data that is hosted in the U.S. by third party service providers.

If an employer intends to transfer data from the European Economic Area, the employer must inform its employees and job applicants of this likelihood, via your Privacy Notice and specify in that, the relevant mechanism under which the transfer will be made.

For example, E.U. model clauses, Privacy Shield certification, Binding Corporate Rules or other valid adequacy mechanisms.

Where such transfers occur, the employer must also have a valid legal basis for such transfers.

Employee Rights as Data Subjects: Fair processing under the GDPR requires that data subjects are given control over how their personal data is used.

It is therefore fundamental that your Privacy Notices communicate to your employees and job applicants, how and when they can exercise this control.

As an E.U. employer your must outline the choices that are available to your employees including, for example, how to indicate preferences in relation to whether their personal data is disclosed to third parties, and preferences

regarding the frequency, subject matter, and/or format of that communication.

Holding Employee Data: GDPR requires employers to be specific with regards to their data retention durations.

Rather than simply stating that personal data will be "kept for as long as necessary", an employer must specify the period for which the category of personal data will be stored or, where this is not possible, the criteria that will be used to determine the time period.

It is accepted that data retention periods may be different for every employer, depending on the purposes for which personal data is to be processed.

However, for all employers, accountability is key when it comes to setting data retention periods and employers must be able to justify their stated data retention periods.

Employee / Job Applicant Rights: The rights afforded to data subjects under GDPR are more numerous and more stringent than under the previous data protection regime.

A Privacy Notice must bring these to the attention of the employee / job applicant.

Under GDPR, employees and job applicants can:

- request access, deletion or correction of their personal data;
- request their personal data be transferred to another person; and
- complain to a supervisory authority

As an employer, details about how employees can exercise these rights must be communicated.

This could for example, be an email address to which a data request can be made.

This is referred to as a subject access request.

It is also advisable as an employer, to outline your internal complaints procedure so that complaints can be resolved without the need to involve a data supervisory authority, first-off.

Putting Your GDPR-ready Privacy Notice in Place

Due to the nature of a recruitment process, it would be not advisable to have a catch-all employee and job applicant within a single Privacy Notice.

Instead, employers should prepare Privacy Notices for each stage of the recruitment process.

For example, for unsuccessful job applicants, an employer will not need to hold the personal data for extended periods whilst for successful candidates and internal applicants, data will need to be held and processed for extended periods.

These differences should be reflected in the Privacy Notices made available to job applicants at each stage of the recruitment process.

Privacy Notices should be reviewed on a periodic basis and, where appropriate, updated and re-circulated.

GDPR does not require the Privacy Notice to be in a particular format.

Therefore, it is possible to provide electronic notices to employees, subject to any local employment law requirements mandating hard copies of, for example, work rules or employment policies.

However, if you opt to issue Privacy Notices electronically, you should still make it as accessible as possible. For example, the notice should be formatted in such a way that applicants can print and review it in hard copy and to retain it should they desire.

A key element of GDPR is accountability.

In the context of Privacy Notices, an employer must be able to demonstrate that they have correctly issued the notices under GDPR.

This means that an employer must be able to track its Privacy Notice process and issuance.

Also, the Privacy Notice should be easily intelligible to the employee and it should not presume an employee or applicant is versed in privacy or law.

The notice therefore they should be void of technical and legal jargon and convoluted syntax.

The text itself should be broken-up with simple header titles to identify each relevant section.

Where an employer operates in a region where English is not the first language, or where applications are being sourced from a pool whose first language may not be English, we advise making the notice available in a relevant other language, as well as English.

In the case where an employer collects and retains personal data, not sourced directly from the job applicant or employee, e.g. personal data obtained through a background check, the employer must provide the job applicant / employee with information about the source of that personal data.

THE COST OF NON-COMPLIANCE

GDPR confers a wide range of enforcement powers upon supervisory authorities.

If, as an employer in the E.U., you fail to present your Privacy Notices in an appropriate manner, or fail include required information, the organisation is exposed to potential enforcement action by supervisory authorities in the E.U., including;

- **Compliance Order.** Where a Privacy Notice is found to be non-compliant with GDPR, supervisory authorities can make an order for the employer to bring its notice up to compliance standard. The supervisory authority can also give specific directions and a time period in which compliance must be attained.

- **Financial penalties.** Supervisory authorities can issue fines for non-compliance at a level deemed “effective, proportionate and dissuasive”.

- Fines will be imposed instead of, or in addition to, other measures that may be ordered by supervisory authorities.

- The level of the fine imposed depends on the type of contravention. A non-compliant Privacy Notice can attract a fine of up to Euro 20,000,000 or 4% of global turnover, whichever is the higher. However, supervisory authorities have indicated that these much media-hyped, top-end fines will be rare and will be reserved for the most egregious offenders.

If you require further assistance or guidance on any of the above or on U.K. or E.U. related H.R. matters generally, please contact:

Peter Tuomey E.U. HR / People Director email: ptuomey@orsasaiwai.com

The leading E.U. expansion experts for U.S. companies entering the E.U.