EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR)
WHAT IT MEANS FOR EMPLOYERS

by Arnaud Gouachon
Chief Legal & Compliance Officer
PeopleDoc

What is the E.U. General Data Protection Regulation (GDPR)?

The GDPR is a recent regulation published by the European Union as Regulation 2016/679 on 27 April 2016, designed to enhance data protection for EU residents and replacing the 1995 EU Directive (95/46/EC) as well as fragmented data privacy national laws from EU Member States.

There was a 2-year transition period and the **deadline for compliance is May 25, 2018**. From that date on, the new GDPR requirements and procedures will be directly applicable in all EU 28 Member States and in Iceland, Liechtenstein and Norway, which are part of the European Economic Area ("EEA").

The GDPR includes a wide range of data privacy and security requirements which will impact all employers with EU-based workforces. Relevant requirements for employers include in particular:

- Employees' personal data controlling, processing and sub-processing activities
- Employees' personal data transfers outside of the European Union
- Technical and organizational security measures around employees' personal data
- Employees' rights regarding consents, access to data, "right to be forgotten"

So... What's New?

Following are some of the major changes that will impact employers and HR departments:

- **A wider scope**: GDPR applies to all companies, whether established in Europe or not, as long as they have some EU-based employees.
- **More data caught**: Personal data is defined as «any information relating to an identified or identifiable natural person». The standard for "identifiable" person is set low.
- **Vendors caught too**: GDPR directly regulates data processors for the first time, i.e. vendors engaged by the employer to process employees' personal data on its behalf.
- **Breach Notifications**: wide requirement to notify data breaches to supervisory authorities (72 hours max) and affected employees.
- **More rights for employees**: transparency about type and purpose of data collection, right to access and rectify data, right to erase data ("right to be forgotten"), right to object,...
- **Data Protection Officer**: Certain types of employers must appoint a Data Protection Officer, which is a new requirement outside of Germany.

Who Does it Apply to?

The GDPR protects the personal data of EU residents, which includes anyone physically residing in the EU, even if they are not EU citizens. The GDPR is applicable to **all employers with employees located in the EU**.

The GDPR now extends obligations and potential liability to not just data controllers (i.e. employers) but also data processors (i.e. any third party vendors retained by the employer).

Why Complying?

The GDPR comes with significant penalties for non-compliance - **fines up to 20,000,000 EUR or 4% of total worldwide annual revenue** of the preceding year (whichever is higher). **Multinational group global revenues are at risk when fines are calculated, even if only a few group subsidiaries are caught by GDPR or were responsible for the infringement of its requirements**.

Employees (data subjects) will be able to take legal ation against --and claim damages from-- both employers (controllers) and their vendors (processors). These changes will take significant efforts and resources to develop and implement, therefore organizations should start the compliance process as soon as possible.

5 Questions to Get Started

To prepare for the new GDPR, an important first step will be to assess personal data risks and identify compliance gaps by responding to the following questions:

- How does the definition of "Personal Data" under GDPR apply to the employees' data collected as part of an employer's HR activities?
- Where is such personal data stored across the organization?
- Where is it transferred from and to (including third party vendors)?
- How is it secured throughout its lifecycle?
- What policies and procedures need to be revised or created to achieve compliance with the GDPR?

How to Comply?

Here are some of the actions that employers must take in order to start complying with the GDPR requirements and procedures:

- Map current data collection and use, perform a gap analysis of current compliance against GDPR and develop and implement a remediation plan, prioritizing high risk areas.
- Build a data breach management process to identify, escalate and manage data breaches effectively to enable prompt and compliant notification to authorities and affected employees. Process should be based on a cross-divisional approach involving at a minimum resources from IT, PR and Legal and HR departments.
- Regarding international data transfers, set up standard due diligence checklists and data processing agreements with customers and vendors incorporating EU model clauses or "Binding corporate rules", as appropriate.
- Implement detailed collection notices to employees using clear, plain and concise language.
- Review and update HR documents retention and destruction policies.
- Review and update procedures allowing employees to access their collected personal data.
- Develop, implement and test policies and procedures to ensure compliance with employees' rights within the time limits set by the GDPR.
- Start training staff regularly.
- Check if the company is required to appoint a data protection officer.
- Consider adding cyber and data breach protection exposure to existing insurance program.

PeopleDoc HR Compliance Assist

HR Compliance Assist helps PeopleDoc clients proactively and effectively manage compliance of their HR files and employees' data with foreign laws and regulations. Led by PeopleDoc's Chief Compliance Officer, the HR Compliance Assist team relies on a network of internal and external lawyers to provide clients with best practices and recommendations on topics such as HR document retention, employee data privacy, electronic signature and electronic archiving. HR Compliance Assist also provides local compliance monitoring and alert services in select countries where PeopleDoc's customers have employees. HR Compliance Assist is a service available to PeopleDoc customers.

PeopleDoc is on a mission to make the difficult job of HR easier. The PeopleDoc HR Service Delivery platform helps HR teams more easily answer employee requests on demand, automate employee processes, and manage compliance across multiple locations. PeopleDoc cloud solutions include case management, process automation and employee file management.

100% software as a service, PeopleDoc solutions integrate with existing HR systems, can be implemented in 8-12 weeks, and are designed for agile ongoing use by HR teams serving diverse workforces. More information is available at www.people-doc.com.

people doc | HR Compliance Assist

www.hrcomplianceassist.com - hrcomplianceassist@people-doc.com