Top Ten HR Things You Should Know About The European Union
Proposed General Data Protection Regulation (GDPR)

1. The EU Commission is proposing to introduce a mandatory Regulation that would apply to all personal data processed by firms within the EU and from the EU to other countries, including the U.S., while still allowing the EU member states to adopt stricter rules for HR data. The Regulation even aims to include companies totally outside the EU who simply offer goods and services within the EU or who monitor the behaviour of EU “data subjects.” e.g. customers – in effect imposing rules globally rather than just within the EU. An EU “Regulation” unlike a “Directive,” does not need to be implemented into national law by the individual EU member states but applies at an EU-level rather like a pre-emptive U.S. federal law creating, in principle, uniformity. Interestingly however, Article 82 of the Regulation then goes on to provide that the 27 member states may “within the limits of this Regulation” adopt specific laws regulating the processing of employee’s personal data in the employment context. This potentially removes any benefit of uniformity (in the employment arena) of using a regulation and could create an undesirable situation where there is a one EU-wide Regulation and also up to 27 member states with separate and different laws governing the processing of employment personal data.

2. The proposal is targeted at the explosion of data held electronically and particularly on social media, with little or no thought to its impact on the great mass of data routinely collected and held by employers on their employees. While U.S. social media businesses are currently the focus of criticism in Europe, the new regulation will equally apply to “regular” companies who have employees within the EU and who routinely “process” their workforce’s personal data by storing e-mails, keeping HR records, using Closed-circuit Television (CCTV), or just running payroll. Lobbying efforts at the European Commission level by social media businesses is intense while efforts from “regular” companies need to be stepped up.

3. The proposal threatens to create new and even more demanding rules about when and how employee consent to processing of any “personal data” is to be obtained. “Consent” would have to be explicit and separate, so it could no longer be simply dropped into an employment contract. More problematic is that Art. 7.4 provides that “consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.” In practice, employers, because of the imbalance of their position (and particularly so at the commencement of the employment relationship when entering into the legally required written contract), will need to look to the other five methods of attaining lawful authority to process employees personal data as listed in Article 6.

4. “Personal data” is very broadly defined – as “any information relating to a natural person who can be identified, directly or indirectly.” This is very wide ranging compared with much U.S. law in this area – one reason why the U.S. is excluded from the very short list of approved countries considered to have an adequate level of data protection law – and threatens, for example, to cover almost any CCTV use at any premises.

5. People would win the right to access any “personal data” held – on files, in e-mails, on CCTV – however costly it might be for the employer to compile this, without making any payment. Individuals continue to have the right of access to their personal data and the EC takes a hostile view of companies continuing to charge even a nominal sum for the provision of such data in future, as they can now. This right, already utilized now by employees and their lawyers on “fishing trips” looking for claims, would in the future become a potential weapon for tying up management time and racking up administrative costs, including during labor disputes.
A new “right to be forgotten” aimed at embarrassing entries on social media, could prove very troublesome in the workplace as it requires “data controllers” – businesses – to delete personal data when the employee withdraws consent, objects to the processing of the data, and once it is no longer needed. Another potential device for labor unions to exploit, this worthy attempt to close the door after the horse has bolted in the world of social media could prove very troublesome when applied to the employment relationship. Given the mass of data on employees, held in a range of places both physical and electronic, it is going to be almost impossible to track all such records in most businesses. It is also likely to create conflicts with record retention requirements in various national jurisdictions, e.g. for Internal Revenue Service purposes.

Independent “data protection officers” (DPOs) with protection from dismissal would have to be employed by every firm with more than 250 employees to police application of the rules. Enterprises with more than 250 staff will be required to appoint a DPO (as an employee or contractor) on the basis of his or her professional qualities, and in particular, expert knowledge of data protection law and practices. The DPO appointment is to be protected from dismissal, similar to the protection afforded works council members in many EU countries. The minimum duties (tasks) include not only providing the Company as a “data controller” with information and advice, but extensive monitoring obligations, ensuring documentation is maintained, and acting as the contact point for the national Supervisory Authority, on the DPO’s own initiative.

Any breach of the GDPR requirements would have to be reported quickly by the employer, normally within 24 hours, to the Data Protection Supervisory Authority; and soon after to the employee. A new and very rapid process is proposed. Companies will be required to notify the national Supervisory Authority of any personal data breach without undue delay, and, where feasible, not later than 24 hours after becoming aware of it. Any delay beyond 24 hours must be justified and explained in writing at the time of notification. The data controller must then, without undue delay after notification, communicate the personal data breach to the data subject with little opportunity to plan for the potential effect on the business and its reputation.

Fines for such breaches could be up to 2% of worldwide revenues. The GDPR provides various maximum fines of up to €250,000, €500,000 and €1,000,000 and, in the case of an enterprise, up to 0.5%, 1% and 2% of the enterprise’s worldwide revenue. Fines should be proportionate to the wrong at which the law aims to cure and not, as in this case, where 2% of global turnover could be disastrous for a business and its employees and also a pension fund scheme which may “mix up” members’ data.

The U.S. would not benefit from the unrestricted transfer of data from European operations to the U.S. because State rules on data protection would never be seen as “adequate,” forcing continued reliance on ‘Safe Harbor’, Binding Corporate Rules or the EU’s ‘model clauses’. Other than the EU and EEA countries (and Britain’s Channel Islands), only Switzerland, Argentina, Israel and, to some extent, Canada are currently approved by the EU Commission as having ‘adequate’ protections, allowing free transfer of employee and other business information to them. All others have been found to be inadequate. The more demanding GDPR proposals are unlikely to be matched by any U.S. State legislature or the U.S. Congress. The current US-EC Safe Harbor Program administered by the FTC, Binding Corporate Rules (BCR s) and EU Model Clauses will continue to be the only ways for making such transfers, with BCR’s now recognized by Article 43 of the GDPR.