The Proposed General Data Protection Regulation (GDPR)

BEERG / HR Policy Comments and Questions

May 8 2012

Key Features

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 US. It also applies to firms outside the EU who offer goods or services within the EU. It would become law across the EU two years after its adoption without the need for any national transposing legislation. The Regulation is targeted on 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 companies in relation to their employees.

2. There are two ways the EU can enact laws. The first is to adopt a Directive, which is an instruction to all 27 Member States to bring their domestic law into line with the text of the Directive. This gives individual Member States a good deal of discretion in how to frame their national laws meaning there can be variations from country to country. A Regulation is legally binding on all Member States without them needing to change their domestic laws. It is roughly equivalent to a US federal law which pre-empts State laws.

3. The proposed GDPR would create one data protection regime across Europe, which, in principle, is to be welcomed. However, the Regulation would allow individual Member States to introduce specific rules for employment-related data, thereby undercutting the benefit of having a single Regulation. (See below on this).

4. The Regulation contains language that would allow the European Commission to issue “delegated and implementing acts” to flesh out the Regulation on a continuing basis in almost all areas covered by the Regulation. Such additional “acts” do not appear to be subject to full parliamentary scrutiny at either European or national-levels. This is presumably aimed at ensuring the law keeps abreast of fast-moving developments in social media, but gives quite draconian powers to the European Commission to frame prescriptive laws without proper scrutiny of their potential effects.

5. The Regulation would result in significant additional burdens for business such as new requirements to respond to information requests, the need to keep ever more documents or the requirement to carry out impact assessments. Businesses could be overwhelmed with requests from employees who wanted to chase down every bit of information about themselves that might be in the system. Companies could spend more time “data mining” than engaging in value-added work.

6. Any personal data breach would have to be reported quickly by the employer, normally within 24 hours, to the Data Protection Supervisory Authority; and very soon after to the employee(s) “when likely to adversely affect the protection of the personal data or privacy” of the employee (whatever that might mean in practice). Reporting of data breaches should be limited to such breaches as material. Further, the 24 hours’ notice period should be extended to at least 7 days. Fines for such breaches could be up to 2% of a company’s worldwide turnover. Such a level of fines is completely disproportionate and should be reduced considerably.

7. Independent ‘data protection officers’ (DPO) with protection from dismissal would have to be employed or retained by every firm with more than 250 employees to police application of the rules. According to some current national laws a company with a DPO could be exempt from the need to notify the data supervisory authorities as regards data processing operations. It doesn’t make sense to extend the requirement to appoint a DPO EU-wide without keeping that exemption. Companies with a DPO should be exempt from having to clear issues with the data protection authorities but should be required to demonstrate compliance if audited.
8. A second set of questions in relation to DPOs present themselves. Who should be involved in the selection process of a DPO? What qualifications will they require? Will a company be required to only appoint one DPO or will it be necessary to have one per country (especially if countries can adopt their own employment-related data laws)? Will their advice and behaviour be consistent? Will they see themselves as an extension of the data protection authorities? To what extent does the protection against dismissal of DPOs go? For instance, if a DPO were found guilty of theft would he/she still be exempt from dismissal? While some of these questions are referred to in Article 35 of the proposed Regulation what the language in the Regulation might mean in practice is open to interpretation. Is it realistic to think that large, complex, multi-divisional enterprises would only need one DPO?

9. The US would not benefit from the unrestricted transfer of personal data from European operations to the US because State rules on data protection would never be seen as ‘adequate’, forcing continued reliance on ‘Safe Harbour’, Binding Corporate Rules or the EU’s ‘model clauses’. (See below).

**Personal Data**

10. It threatens new and more demanding rules about when and how employee consent to processing of any ‘personal data’ is to be obtained. ‘Personal data’ is very broadly defined – as ‘any information relating to a natural person who can be identified, directly or indirectly’. Would it make sense to sub-divide employees’ personal data into “private” personal data (bank account number, medical data) and “business” personal data (performance review results, salary data, training plans etc.) Employees should not be able to object to the processing of data that is required for the efficient running of business. In other words, “business essential data” should not require employee consent.

11. People would be granted the right to access any ‘personal data’ held – on files, in e-mails, on CCTV – without making any payment, however costly it might be for the employer to compile this. There is a complete failure to comprehend the sheer amount of data that is generated in workplaces every day and that now remains in computer systems – for example, e-mails and text messages. A right on the part of employees to demand access to all such data would be impossible to comply with as no one person in any company is responsible for such data, which can be dispersed across hundreds, if not thousands, of individual computers.

12. 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 exercises such right to be forgotten, on the grounds mentioned in Article 17. What sort of data can an employee demand be deleted so that he/she can be “forgotten”?

13. Article 33 requires data controllers when proposing to process data which “presents special risks to the rights and freedoms of data subjects” to seek the views of the data subjects “or their representatives” on the intended processing. This would appear to legally require companies to consult works councils/union in each of the 27 Member States before introducing or changing any human resources program that required data processing. What would “seek the views” mean in practice? Would it be consultation with a “view to reaching an agreement”? What would happen if there was no agreement? Article 73 appears to provide unions/works councils, and other organisations, with their own right to lodge a complaint with the supervisory authorities if a personal data breach has occurred. This is in addition to the right to lodge a complaint on behalf of a data subject.

**Employment Data**

14. Article 82 of the proposed Regulation allows EU Member States to adopt additional rules as regards employee data. This means that companies are faced with not only the new Regulation but also with 27 individual regimes in individual Member States. In other words, as regards employment-related data the Regulation will impose new EU-wide obligations on top of obligations imposed by individual Member States. The value of a Regulation – a unified EU-wide regime, is thereby negated.
15. Article 82 reads:

*Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*

16. We propose the deletion of Article 82. In its place we propose a “Model Employee Consent” document which would cover the issues referred to in Article 82, with the exception of such data as is “business essential (see 10 above). Companies that made use of such a model employee consent would not be required to seek consent from individual employees or their representatives in relation to the data covered by the consent document. The “model employee consent document” would automatically be read into the employment contracts of all existing employees (i.e., the Regulation would automatically amend their contracts to that effect). Data that fell outside the scope of the model employee consent would still require express employee consent. In other words, it would be possible to draw a line between “essential” and “non-essential” employment data with the latter being covered by the model employee consent document?

17. The Regulation needs to recognize that business is global, IT HR systems are global. It should allow employers to store and process HR data anywhere within the organization, but hold them liable not to misuse such data. Protect this data from misuse by holding the local legal entity responsible, and allowing the parent company to contractually commit itself on behalf of the local legal entity not to misuse the data. This is essentially what Binding Corporate Rules (BCR) should do in practice. Based on the fact that BCRs now have clear recognition (in the proposed Regulation) it should be made easier to draft such rules and have them approved by the data regulation authorities within much shorter timeframes. This should certainly be the case when companies have appointed DPOs.

18. Allow employers to share employee data with third party processors who need such data to accomplish work for the employer with appropriate confidentiality agreements in place. Most agreements with third party processors already use the EU model clauses.