EU DATA PROTECTION PROPOSALS - IMPLICATIONS FOR EMPLOYMENT

Background

1. The proposed Data Protection Regulation (DPR) will apply to all processing of personal data across the EU. The rationale for a regulation is that it will be a "one stop shop" applying consistently throughout the EU without the need for domestic implementation. So a business operating in the EU will be required to comply with the same rules in the UK, Spain and Estonia.

   The EU Commission's Impact Assessment estimates that the proposals will lead to a *reduction* in administrative burdens for business across the EU of €2.3 billion per annum, mainly resulting from savings in the harmonisation of rules. It estimates that the cost of demonstrating compliance is £160 per organisation based on four hours of clerical work and that this will be repeated every three years giving an annual cost of £53 per organisation.

   Given the administrative and regulatory burden described below, we find these figures, to say the least, surprising. But, in the context of employment the Commission's approach breaks down. Article 82 deals with processing in that context permitting member states to adopt specific domestic rules for all aspects of employment (including recruitment, performance of the contract, management, planning and organisation of work, health and safety and termination). See our remarks on Article 82 at paras 13 and 14 below.

   Since virtually every business processing personal data will have employees, this is likely to undermine the "one-stop" strategy underpinning use of a regulation. It also raises serious questions about the Commission's costings. Employers with over 250 employees will need to appoint a data protection officer, an independent and relatively senior position. In the UK, costs for someone operating independently and at a senior level might be between £75k and £100k per year. In Germany (which already has data protection officers) it is common to employ a consultant on a daily rate. Fees might typically be between €800 and €1200 per day. According to UNCTAD, there were over 47,000 trans-national corporations operating in the EU in 2010. Even if only a modest proportion had over 250 employees, one can see that the costs would be very considerable. And appointing a data protection officer is only one element of the regulatory regime.

   In formulating the DPR, the Commission has not taken take proper account of its implications for employment. The DPR would impose very significant new burdens on employers across the EU. When questioned about this at a meeting of the European Data Protection and Privacy Conference on 4 December 2012, the European Parliament Rapporteur for the DPR was frank,; he recognised that the omission of employment was a weakness but explained that there was no agreed view from the Commission or the members states on what a single employee data framework would contain.

Processing of personal data in relation to employment

2. The nature and quantity of the data processed in an employment context is different from that processed in almost all other contexts. In most modern workplaces, an employee turning up at work would typically "generate" the following personal data:

CCTV record of entry to a building, a log of pass entries to the building, use of and exit from a lift, log on information for a computer, information on use of telephone, data on website use, email traffic and content data.....followed by data connected with whatever work that individual happens to do. It would be very unusual for a controller in another context to hold even a fraction of the data generated by employment.

Although banks, credit card companies and utilities will have personal data on customers, it is generally structured and channelled into systems operated by those companies. Although there may be some unstructured data (notes of meetings with a bank manager for example) relatively little will be held. Most data held will be accessible via complex databases. Most of these organisations (at least in the UK) do not offer normal email access to their customers. If electronic communication is available at all it is achieved through structured forms.

3. In contrast much data held by employers with staff who use computers in their work will be in the form of unstructured emails and documents. Although an employer will have responsibility for such data, it will not have detailed (and perhaps only minimal) knowledge of the content. So, although one would assume that most of the content was business-related, it will certainly include data about employees and those they communicate with which is not business-related (e.g. "I can't come to the meeting because my daughter has mumps" or "Met X last night, we had a few drinks, one thing led to another"). Data such as this is not only sensitive personal data (so subject to higher regulatory standards) but outside any real control of the employer. Even if it could stop its staff making such comments, it could not stop third parties sending emails to the same effect.

Approach of the proposed DPR

4. From the perspective of employment, key features of the proposed DPR include the following:

Data protection principles and conditions for processing

(a) A stricter and more detailed approach to compliance with data protection principles.

(b) Stricter conditions for consent as a justification for processing (see Article 7).

(i) Consent will generally not be available "where there is a significant imbalance" in the position of data controller and data subject (such as employment).

(ii) Consent given may be withdrawn at any time.

Information and the development of policies, procedures and impact assessments

(c) A requirement to give a data subject detailed information on personal data collected (Article 14) including the purposes of the processing, if processing is based on the "legitimate interests" of the data controller (which is common in an employment context) an explanation of those interests, the period for which personal data will be stored and who will receive the personal data.

(d) A requirement to develop transparent and easily accessible policies on processing of personal data and data subjects rights. (Article 11)

(e) A requirement to develop procedures for compliance with data subject access requests (DSAR) and an obligation to give reasons for not taking action based on a request (Article 12).

(f) Employer (data controller) must adopt policies and implement measures to ensure and be able to demonstrate compliance. Measures must include keeping documentation of **all** processing operations (see art 28).

(g) Having created a policy and implemented measures to demonstrate compliance, the controller must then implement mechanisms to verify that the policy and measures are effective. If proportionate, independent auditors must be used.

(h) A requirement to carry out a formal impact assessment where certain information is held (in particular on heath, race and ethnic origin) coupled with an obligation to consult ("to seek views of data subjects or their representatives") (Article 33).

Right to be forgotten

(i) A right to be forgotten (to have personal data relating to them erased). This would apply to emails (Article 17).

Appointment of data protection officer

(j) If there are 250 or more employees, a requirement to designate a data protection officer who even if employed by the controller is to have formal independence with protection against termination (Article 35).

Commission and regulatory regime

(k) Much is left unsaid - the Commission has extremely wide powers to make delegated rules supplementing the DPR.

(l) The regulator will have enhanced regulatory powers including, in particular, power to impose fines up to 2% of annual worldwide turnover.

(m) The regulator operating within the UK will not necessarily by the Information Commissioner. The relevant supervisory authority will be that applying to the "main establishment". This is where the business determines purposes and conditions for processing. So, if a company's main office is in France or Spain the relevant regulator for UK activity will be the French or Spanish regulator.

Implications for employment

5. It will be clear from the summary set out above that, particularly in the employment context, the DPR will impose significant new burdens and costs, not least engagement of a Data Protection Officer. We set out below some particular concerns.

The focus on the detail of process rather than on risks to privacy and "stuff that matters" is more likely to lead to "red tape" than effective protection of data and individual privacy.

Unstructured auto-processed data and DSARs

6. The approach of the DPR is not appropriate to unstructured auto-processed data such as emails. A distinction should be drawn between personal data over which a controller has real control and that over which it can have no substantive control.

   Employment relationships generate vast quantities of data, much of it personal. Special rules are needed for employment data and, in particular, unstructured data such as emails. Data subjects' rights in relation to such data should be modified.

7. Where there are disputes between an employer and an employee or a trade union, the law on data protection is often deployed, in particular by making DSARs. The aim may be to give an employee leverage in a dispute in circumstances where there is no genuine concern about use of personal data or privacy. Data protection is simply a proxy for, or extension of, the true dispute. Proper compliance is generally impossible because of the volume of data processed. The request may be made merely to put the employer to expense.

   Such requests may involve reviewing many thousands of emails to identify relevant data, to ensure that references to personal data of others is redacted and to avoid providing privileged documents. Compliance can take days or weeks and involve a considerable staff resources and costs. In addition, in seeking to comply with DSAR a controller has to trawl historic emails for personal data with a risk to the privacy rights of everyone other than the person making the subject access request.

   The power in Article 12(4) to refuse "manifestly excessive requests" is of marginal use in this context. Although there is nothing manifestly excessive about asking about the information being processed, looking for that information, even over a period as short as a few days, is likely to be exceedingly time-consuming.

Data protection principles (Article 5) and employment

8. Although it is unusual for an employer to engage in practices which infringe privacy rights, strict compliance with data protection principles is extremely difficult. In our experience most employers fail to comply strictly. Against the background of a strict enforcement regime and a regime which may be enforced by overseas regulators, this potentially creates significant problems for employers.

9. The requirement (Article 5(f) that a data controller must ensure *and* be able to demonstrate compliance for "each processing operation" is too strict, It assumes that a data controller has more control over data than it can have in practice in the context of unstructured data.

Provision of information to the data subject

10. The rules on provision of information to the data subject (Article 14) are onerous in an employment context, particularly taking account of the obligation to demonstrate compliance (Article 5(f)). Although compliance would provide a lot of information, it is questionable to what extent that would be useful to an employee. Where use of data may prejudice privacy rights (or impinge on them) in a significant way that should be highlighted. That is what matters - not, in itself, how long an email will be stored.

To the extent that the rules relate to unstructured auto-processed data, they can only be complied with at a level of generality that is unhelpful to anyone. As a result, the proposals set up a requirement for "red-tape" but do not deliver effective data protection.

Data protection officer

11. Appointing a data protection officer and providing training will be costly. Many businesses will need to hire someone externally.

    In addition where there is a dispute a DPO, the quasi-independent status of a DPO is likely to be used by an aggrieved employee to provide leverage and as an adjunct to exercise of data subject rights. This will become a particularly acute problem if data subject rights are not limited in the context of unstructured auto-processed data.

Special rules for employees?

12. Although the Commission has not taken account of employment when drafting the main provisions of the DPR, Article 82 permits member states to adopt employment-specific rules – as long as they are "within the limits of" the DPR. This power is too narrow. It permits stricter rules than the DPR requires but does not permit different rules or more relaxed rules to take account of the specific nature of the employment relationship.

    For example, the rules on DSARs ought to be modified in an employment context in relation to unstructured auto-processed data such as emails. But, because the powers in Article 82 must be exercised "within the Regulation", a members state could not do that (and of course it is preferable that any such modification be determined at an EU level).

13. However, Article 82 creates a more fundamental problem. Assuming member states introduce domestic rules on employment, there will be some 28 different regimes applying to data protection in that context. A key strategic aim of the DPR (and the rationale for using a regulation rather than a directive) is to have one-stop shop with one data protection law applying throughout the EU. This exception undermines that aim and means that, at least in the field of employment, multi-national organisations will have the costs of ensuring compliance with a range of different regimes. Although there is an argument that this is similar to the current position, business will have the costs of increased and more specific compliance and of employing data protection officers underpinned by much higher fines.[1]

Enforcement regime

14. The DPR has more specific and expanded duties backed up by the potential for very significant fines. In the UK, we currently have what many see as a proportionate and pragmatic enforcement regime. Although not complying strictly, most data controllers put emphasis on key risks to privacy (e.g. data security); the Information Commissioner as regulator takes a risk-based focus to enforcement. He shows little interest in pursuing technical breaches and puts resources and effort into "what matters". The DPR aims to

---

[1] At the European Data Protection and Privacy Conference on 4 December 2012, Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner said "Businesses need to realise that with handling personal data comes responsibility. And part of that responsibility is to follow the law. And if they can partake in profits, they are also liable for lack of compliance with the law. That is why the new Regulation will have a larger fines regime that will ensure compliance."

have a single set of rules and a common approach to enforcement. There is a risk that this will lead to a "highest common denominator" approach to regulation under which there is a creep across the EU towards strict and literal compliance. This is bad for business and should be avoided.

Conclusion

15. On a European level issues associated with employment are not being given the level of consideration that they deserve. Communication with the Ministry of Justice and the Information Commissioner suggest little specific engagement with employment issues. The UK Government is trying to negotiate a more business-friendly DPR. Every business with anything more than the most basic personal data employs staff; the Government should engage more actively with the application of the DPR in an employment context.

Steven Lorber
Lewis Silkin LLP

20 December 2012

steven.lorber@lewissilkin.com

T: +44 20 7074 8078