EMPLOYMENT
LAWYERS
ASSOCIATION

P.O. BOX 353
UXBRIDGE UB10 0UN
TELEPHONE/FAX 01895 256972
E-MAIL ela@elaweb.org.uk
WEBSITE www.elaweb.org.uk

Call for Evidence on EU Data Protection Proposals

Response from the Employment Lawyers Association

6 March 2012

CALL FOR EVIDENCE ON EU DATA PROTECTION PROPOSALS

RESPONSE FROM THE EMPLOYMENT LAWYERS ASSOCIATION

The Employment Lawyers Association ("ELA") is a non-political group of specialists in the field of employment law and includes those who represent both Applicants and Respondents in the Courts and Employment Tribunals. It is not, therefore, ELA's role to comment on the political merits or otherwise of proposed legislation, rather to make observations from a legal standpoint. ELA's Legislative & Policy Committee is made up of both Barristers and Solicitors who meet regularly for a number of purposes including to consider and respond to proposed new legislation.

A working party was set up by ELA's Legislative & Policy Committee under the chairmanship of Ellen Temperton of Lewis Silkin to respond to the Ministry of Justice's Call for Evidence on the current data protection legislative framework. Its comments are set out below. A full list of the members of the working party is annexed to the report.

GENERAL COMMENTS

Overall, ELA welcomes the current review and the Commission's desire to harmonise rules across the Member States of the EU. We have responded to the key aspects of the proposed Regulation which touch particularly of the employment relationship. It is not our goal to conduct a line by line critique of the draft legislation itself.

1. The unique nature of the employment relationship

As ELA noted when it responded to the MOJ's previous Call for Evidence on the Data Protection Legislative Framework, the employment relationship is unique in terms of the amount of personal data held by the employer about his employee and the volume of documentation created, especially by email. It is unlikely that a data controller in other contexts would have to address the same quantity of data as that which is created in the employment context and much of this is due to reliance on email in the workplace.

A single employee may receive and generate hundreds in a single day. Many of these may originate from outside the organisation but, even where they originate from within, an employer- or data controller in the current context- cannot easily control the content. Most organisations will have rules about the appropriate use and content of email traffic but in a given moment, replicated hundreds of times daily, they cannot really control content. Thus an employee may retort to a colleague by email that they had a bad weekend because they split up with their partner over another woman, or that they are late that morning because their child has a stomach upset. Both of these references could be capable of constituting special data within the scope of Article 9 (1) of the Regulation. The mere holding of the email on the employer's system, or its deletion, constitutes processing of the data within it. There is then potentially a breach of

the principles and the risk of a 2m fine.

2. Harmonising compliance

The Regulation will, if implemented in its current format, lead to a compliance culture which creates huge additional bureaucracy and compliance costs but where full compliance for employers is practically impossible.

While the aim to harmonise is a good one, some of the present inconsistency derives from factors such as the way that different legal systems operate, including the cultural, regulatory and social norms in a particular member state. Under the current regime the ICO has been able to adopt a pragmatic and sensible approach to compliance. Technical breaches are not pursued as might be appropriate in the examples given above concerning the contents of specific emails. The Regulation, however, adopts a prescriptive tone, allowing little room for flexibility, and then potentially imposes hefty fines.

An example might be that under Article 79, fines can be imposed for procedural or record keeping failures alone. There is no link between the failure and the consequences of failure. The article is formulated in mandatory tones- "shall" rather than "may".

There are then two risks that we can foresee. The first is that there is now significant risk that the approach to compliance becomes strict, technical, and not risk based, massively increasing the burdens on employers, but failing to achieve the impossible goal of full compliance.

The second is that a move towards over prescription may mean that business look for ways to avoid compliance and therefore the Regulation may fail to deliver the desired protection for employees.

Flexiblity and discretion in enforcement based on significant risks should be considered.

3. The use of data protection rights as levers in employment disputes

The employment relationship is probably also unique in the sense that data protection rights can be used as leverage for employment disputes where the real dispute is, in fact, about "pure" employment rights and not the infringement of rights concerning the protection of the employee's data.

The current regime which affords subject access rights to employees, for example, has created significant administrative burdens and costs of compliance for employers, a point which we developed in some detail in our response the earlier MOJ consultation. Here we noted that the impact assessments which had been produced seemed to completely disregard the costs of compliance for many employers.

Our concern is that what is proposed in the EU Regulation does nothing to address this

fundamental problem with the way that the data protection regime operates and in fact increases the number of rights which create additional forms of leverage in employment disputes.

Some of these rights in the employment context are almost impossible for an employer to comply with fully as we explain elsewhere in this response.

4. The solution proposed by the Regulation for employment

Article 82 of the draft Regulation offers potentially welcome protection for employment but it is noted that it does not go far enough. This is because Article 82 permits member states to adopt employment specific rules *"within the limits of"* the Regulation. To be effective the Regulation itself would need them to include the specific derogations or modifications which are to be permitted in the employment context otherwise it is difficult to see how this provision can operate to provide any exemptions or moderation of the impact of the Regulation at all.

5. The need for the rules to be clear and well drafted

As stated above ELA completely understands the rationale for a Regulation. It is in the interests of both employers and employees that there is consistency in the standards which apply.

We note however that the drafting of the proposed Regulation is not clear in material respects and too much is left to the powers of the Commission to add more detail by "delegated acts". This is unsatisfactory in that the legislation is a Regulation and not a Directive and businesses need to know what rules are to be applied to them in good time to adapt their processes before the rules are implemented and not afterwards when the lack of clarity has led to enforcement proceedings. As the Regulation will usher in hefty fines for non-compliance this is a pressing concern.

Should the Commission provide the requested clarification there is still a real risk that the drive to a completely harmonised approach will lead to a single strict regime in which there is little room for interpretation and discretion in enforcement.

By way of illustration, in the conditions for consent, Article 7 (4), what will constitute a "*significant imbalance* between the position of the data subject and the controller"? In terms of subject access requests Article 8 (4) provides for requests which are ***"manifestly excessive***"- or ***unreasonable***- to be refused. What constitutes a manifestly unreasonable request? Article 8 (4) goes on the state that the request may be manifestly excessive because of the request's repetitive character. The repetitive nature of the request is not generally the issue for employers, but the sheer volume of documentation and the data which it contains which has to be reviewed. It would be helpful therefore if more flesh could be added to a provision which is of such potential importance before reliance is made erroneously on such a provision and the reliance is deemed not to be lawful.

SPECIFIC COMMENTS

Article 3 and article 7 -the data subject's consent

ELA welcomes a single definition for all types of processing. We have significant reservations however, about the fact that consent does not provide a legal basis for processing where there is a significant imbalance between the data subject and data controller. Recital 34 makes it clear that there will be a significant imbalance in the context of the employment relationship.

First we do not accept that there this imbalance always exists. To regard it as given in the employment context is to reduce all employment relationships to traditional concepts of the little employee who has no bargaining power. This is not appropriate in a modern context. It may be that more senior employees or those whose skills are vital to the business have more negotiating power. Second, we do not agree that consent can never be valid in an employment context, even where there is an imbalance overall. There are occasions such as on recruitment, or on the negotiation of terms for promotion, or when the employer is asked to provide details so that the employer knows who to contact in an emergency, or where if the employee choses to take advantage of the employer's policy to enable employees to use their own technology in the workplace rather than the equipment supplied by the employer, where the employee may have a genuine choice. There may also be occasions where there is no alternative basis for processing but where having given full information to the employee about the nature and reasons for the processing the employee gives his consent. There is no clear reason why this consent should not form a valid basis for processing.

Article 5 – Principles of processing

ELA is concerned about Article 5 (f). The proposed requirement is that data should be processed under the responsibility and liability of the data controller who shall "***ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.***" (our emphasis added).

Please refer back to our comments at the beginning concerning the particular problems of email in the workplace. We would argue that if the data controller is required to demonstrate this for each processing operation (even deletion!) then it will be impossible for employers to comply. If this is not the intention and a generic approach is permissible then the Regulation should indicate this clearly.

Article 9 – Processing of Special Categories of Personal Data

"Religion of beliefs" The concept of sensitive personal data under the Directive covered religion or philosophical beliefs. What is meant by "beliefs" in the Regulation? Is a narrower meaning intended. Our case law in the discrimination context indicates that any coherent belief system is protected under the Equality Act such that a belief in climate change was a belief capable of protection.

Article 9(2)- this permits processing of special data in the field of employment "law" where that processing is "necessary" to carrying out the obligations and exercising the rights of the data controller. What is meant by "employment law" in this context? The drafting should simply refer employment rather than "employment law". Second, what is the standard of necessity which is to be applied in this context? Is it absolute or reasonable necessity?

Article 12 – Procedures and Mechanisms for Exercising the Rights of the Data Subject

The Regulation imposes a heavy compliance burden on data controllers and data processers.

The time limit for compliance (from 40- 30) is a concern, given the volume of data which needs to be collated and reviewed to ascertain whether it should be provided, and if so, what other individual's data is present and if so, how to protect that data. Typically data subject access requests take the form of a request for all the personal data which the employer holds and is not limited in duration. This covers the personal data which is held in emails over the course of employment including deleted and archived emails. Sometimes it is necessary to restore or reconstitute several employees' mailboxes in order to comply. This can take time. Then the employer has to trawl the thousands of documents produced for the employee's personal data, discounting that which is not their personal data, and ensuring that there is no inappropriate disclosure of the personal data of third parties. This is how DSAR requests become excessive. It is, infact, fairly rare for requests to fall within the limited circumstances where the period for compliance may be extended to 2 months. It is a great shame that there has been no consideration to addressing these concerns.

Under the proposed Regulation therefore, a new compliance industry will spring up whereby data controllers, however small, will have to establish procedures to enable them to provide the information required by Article 14 and for the exercise of the rights in articles 13, 15- 19.

These rights will be exercised to act as leverage in employment disputes (see our general comments above).

It is essential that the costs of compliance should be limited, whether by including rules which exempt emails – or certain types of emails such as those which have been archived or deleted- or where the employer does not need to comply where the costs of compliance takes him above a certain fee cap. We note that the data controller can charge a fee where the request is manifestly excessive but in fairly narrow circumstances. There is no guidance on what level of fee would be permissible. The fee would need to operate effectively in the different member states and thus it would be better if this was something which was set by the ICO, in the UK, rather than centrally.

We note that the employer has to provide information to the employee about his right to make a complaint to the supervisory authority and to seek a judicial remedy. This would seem to be overly prescriptive, particularly because the existence of the employment relationship means that the employee may have other channels to complain or resolve his grievance before he needs to take the matter up with an external body. This may for example occur through the grievance procedure or just through continued dialogue with the employee. It would seem to be preferable for the relevant authorities not to be swamped with complaints.

This is one example of a context in which the Commission and not the ICO (in the UK context) may, by "delegated acts", specify the criteria and conditions for manifestly excessive requests. Such clarification should be produced urgently.

Article 14 – Information to the Data Subject

Recognition should be given to the fact that there are other options available for the data subjects (employees) in those circumstances. Data subjects in this sense are different to consumers or members of the public, who have no direct link perhaps with the data controller and cannot approach them directly, through their manager or human resources.

The obligations under Article 14 are onerous and potentially unclear. If you read Article 14 alongside Article 5(f) then it will be necessary to provide all of this information in relation to each act of processing.

In this context, email communication again pose problems. As one example of the difficulties of compliance, if the information is contained in an email from an external source, how does the employer comply with paragraph 2, 3 and 4?

Overall we would query the usefulness to the data subject of this information. If implemented formulaic responses will need to be auto-generated. It is difficult to see in the employment context how this will protect the data subject or enhance his understanding of his rights.

Article 15 – Right of Access for the Data Subject

Are employers required to provide this information again, even where it has already been provided at the point of collection of the data?

Article 22 – Responsibility of the Data Controller

Action against employers who fail to have the mandatory paperwork should not automatically follow. There should be discretion for the ICO, in the case of the UK, to consider this using a risk based approach.

When does the verification requirement in Article 22 (3) require the data controller to engage an independent auditor? Clarification would be desirable as to when this would be considered to be proportionate.

How does this requirement work alongside the role of the data protection officer who must appointed under Article 32? Although the requirement to have a data protection officer is not mandatory for employers with less than 250 employees (unless they are in the public sector), is it going to be the case that employers of more than 250 employees will need to appoint an independent officer and separately have their compliance audited?

Under Article 22 (4) a clearer indication of the Commission's intentions should be provided as a matter of urgency.

Article 28 – Notification of a Personal Data Breach to the Supervisory Authority and to the individual (Article 29)

This should be notified no later than 24 hours after the personal data breach has been established, and again, there is provision for the Commission to lay down a standard format for such notification to the supervisory authority, and the procedures applicable to notification requirement. It will be helpful to know how and when these will be produced, and whether they are mandatory in their form.

A target of 24 hours would seem to be unrealistic. What if the breach occurs at weekend or comes to light then? The default position is that the data controller must then explain his non-compliance. This will add to the burdens which are placed on the ICO who will be swamped with notifications and full explanations for the delay irrespective of the nature and severity of the breach. ELA would advocate the proportionate approach presently followed by the ICO which is based on an assessment of the risk, and the nature and severity of the breach.

There is also no logical reason why the emphasis is on notifying the authority before the individual. Where the breach is serious, surely the rights of the data subject are better served if they are notified promptly so that they can act to protect themselves. It would also be important that any timescales enable the employer to assess what the risks are to their individual employees rather than being forced to notify them when this may cause unnecessary concern.

Article 35 Data Protection Officer

Article 35(5) sets out the professional qualities required of the data protection officer, which stipulates "expert knowledge". This however is not defined, but the data protection officer should have expert knowledge of data protection law and practices, and be able to fulfil the tasks referred to in Article 37. The necessary level of qualification is said to be determinable by the processing carried out. This is really unclear, and could expose companies and in particular, employers to a level of risk that is unnecessary.

Article 32(5) also provides that the data protection office shall be employed for a period of at least two years, and that "*during their term of office the data protection officer may only be dismissed from the post of the data protection officer if they no longer fulfil the conditions required for the performance of their duties.*" This is a potential problem in the employment context, as it places data protection officers in somewhat of a protected position as an employee. The employers may be unable to discipline or dismiss a data protection officer if this section takes precedence.

Article 36 – Position of the Data Protection Officer

This provides that they shall be independent and not receive any instructions from the data controller or processor although they "report" directly to management. This could be seen as contradictory, and should be clarified.

Article 44 – Derogation

The reference to "frequent, massive or structural" transfers is slightly unhelpful. It does not anticipate permitting the smaller and much more regular flows of personal data in the employment context, particularly between multinational groups of companies, and yet does not define what may be frequent, massive or structural. It would be helpful if this were clearer.

ELA WORKING PARTY

Ellen Temperton, Lewis Silkin LLP (Chair)

Andrea Ward, McGuire Woods London LLP