Ministry of JUSTICE

CALL FOR EVIDENCE ON THE CURRENT DATA PROTECTION LEGISLATIVE FRAMEWORK

RESPONSE FROM THE EMPLOYMENT LAWYERS ASSOCIATION

We would welcome responses to the following questions set out in this consultation paper. Please email your completed form to: informationrights@justice.gsi.gov.uk or fax to: 020 3334 2245. Thank you.

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.

ELA wanted to respond to the Call for Evidence because, in its view, both the Call for Evidence and the Impact Assessment which accompanied it, do not seem to have considered the workplace and the set of issues which employers face when processing their employees' personal data. 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. Although it could be argued that the vast majority of data processed at work is not personal in that it is not sufficiently biographical in nature an employer still has to consider when and where employee data might be obtained and held. The section of the Impact Assessment which deals with Data Subject Access Requests seems entirely to miss the point so far as the cost of compliance and the administrative burden (for employers who comply with such requests).

GENERAL

Q1. What are your views on the current Data Protection Act and the European Directive upon which it is based? Do you think they provide sufficient protection in the processing of personal data? Do you have evidence to support your views?

1.1 The generally held view of the committee was that the data protection regime had contributed to a significant shift in the landscape so far as employers were concerned in that it had considerably raised awareness of rights and obligations. For the vast majority of the organisations that we advise as employment lawyers this raised level of awareness means that compliance is essential rather than an optional extra. However achieving compliance can be problematic in some key areas for employers. These include complying with the Data Subject Access Requests (DSARs), international transfers, and the preconditions to processing sensitive personal data.

1.2 The committee agreed that advances in technology do present challenges in adapting the existing regime to specific acts of processing. In the workplace this is most marked in the context of DSARs where the prevalence of email, texts, and other new forms of communication contribute to the creation of thousands and sometimes hundreds of thousands of documents and records. This reliance on these ever evolving forms of communication may have been unforeseen in 1998. The committee believes that wholesale reform of the regime for DSARs is necessary from both the employee and employer's perspective and we comment on how below.

1.3 Another example of how protection for employee personal data might be enhanced is that there is a growing tendency for employers to consult social networking sites in relation to recruitment decisions. In many cases employees do not have any expectation that their profiles will be viewed for this purpose. The principles based approach of the current regime is flexible enough to adapt to regulate this activity. But greater clarity and guidance in relation in particular to the ICO's approach to the protection of employee personal data in this context would be welcome.

1.4 Another area where reform would be desirable to clarify rights and obligations in the workplace is the growth of the practice of cloud computing. More generally, the sheer number of international transfers of data in a multinational employer and the cumbersome systems which are aimed at regulating those transfers is an area where reform would be welcome at an international level. See our responses to Questions 38 and 39 below.

DEFINITIONS

Q2. What are your views of the definition of "personal data", as set out in the Directive and the DPA?

The definition of personal data contained in section 1 (1) DPA is adequate. The problem is how it has been interpreted by the courts *Durant v FSA [2003] EWCA civ 1746* to cure practical problems presented by the exercise of DSAR under section 7 and 8, DPA, and the ICO's attempt to reinterpret that decision in its technical guidance, "Determining What is Personal Data"**.** These interpretations have the effect of undermining the definition in the DPA. It would be better to reform the right of access and set clear parameters around that in the employment context than seeking to tamper with the statutory definition.

Q3. What evidence can you provide to suggest that this definition should be made broader or narrower?

See above.

Q4. What are your experiences in determining whether particular information falls within this definition?

See above. While it may be argued that much of the data processed in the context of an employment relationship is not biographical in nature the issue is that the employer has to consider where he might obtain and retain personal data belonging to his employees and so the limitation on the definition introduced by Durant and its subsequent interpretation in the ICO's guidance (referred to above) does not relieve the employer's administrative burden or create clarity for employees.

Q5. What evidence can you provide about whether biometric personal data should be included within the definition of "sensitive personal data"?

Q6. If as a data controller you process biometric data, do you process it in line with Schedule 3 of the DPA which imposes an additional set of conditions?

Q7. Are there any other types of personal data that should be included? If so, please provide your reasons why they should be classed as "sensitive personal data"?

Care should be taken not to confuse the need for particular security measures which should be in place for a particular act of processing data and the preconditions

required to process that data in the first place. An example would be the suggestion that financial data should be regarded as sensitive personal data. If information such as bank account details were to be added to the definition of sensitive personal data because of the potential harm that could be caused to the employee as a result of the data falling into the wrong hands, or being misused, then this would mean that an employer needed to comply with the narrower preconditions to processing every time he paid the employee's salary.

Q8. Do you have any evidence to suggest that the definitions of "data controller" and "data processor" as set out in the DPA and the Directive have led to confusion or misunderstandings over responsibilities?

No particular evidence but greater clarity as to responsibility would be desirable for new activities such as "cloud computing", and outsourcing and insourcing, and the consultation of information available on the internet but which an employee may not have expected his employer to consult e.g. Facebook profiles.

Q9. Do you have any evidence to suggest that the separation of roles has assisted in establishing responsibilities amongst parties handling personal data?

Comments:

Q10. Is there evidence that an alternative approach to these roles and responsibilities would be beneficial?

Comments:

Q11. Do you have evidence that demonstrates that these definitions are helpful?

Comments:

DATA SUBJECTS' RIGHTS

Q12. Can you provide evidence to suggest that organisations are or are not complying with their subject access request obligations?

The committee considers that DSARs are the most significant issue arising under the DPA for ELA's members, in particular for those who act for employers but also in that employees seeking to exercise their rights often feel dissatisfied with the results. In the committee's view, the Call for Evidence and related Impact Assessment do not properly assess how DSARs operate in practice in the context of the employment relationship.

It is recognised that employers act as data controllers with respect to the personal

data of job applicants, employees, former employees and other data subjects and, to this extent, the DSAR regime will of necessity apply to the employment relationship. In straightforward cases, DSARs provide a helpful framework to enable the individual to establish what personal data is being processed by the employer organisation and, as appropriate, to take steps to ensure that the data is being processed in accordance with the DPA's principles relating to relevance, accuracy and proportionality etc. This is consistent with the purpose of DSAR as drawn down from the European Directive.

It is the experience of the committee, however, that the vast majority of the DSARs submitted by data subjects in connection with the employment relationship form part of a broader dispute between the parties. These disputes range from workplace grievances raised by the employee or disciplinary action being taken by the employer to threatened or actual litigation before the Employment Tribunals or civil courts. The consequences of this include:

- The DSAR may encompass (deliberately or otherwise) documents relating to the dispute between the parties. In the context of threatened or actual litigation, this may mean that the employer is obliged to disclose these documents (to the extent they contain the individual's personal data) significantly in advance of the timetable for the disclosure of relevant documents established by the Employment Tribunal or court. This often results in the duplication of the effort to locate, review and disclose relevant documents.
- It is noted that individuals can avail themselves of a number of other mechanisms to obtain the advance disclosure of documents or information in connection with litigation, for example the pre-action disclosure protocols before the civil courts and the option of submitting a statutory questionnaire for the purposes of assessing if/how to pursue a discrimination claim before the Employment Tribunal.
- The time and cost implications for the employer to respond to the DSAR are usually significant (see response to Questions 13 and 14 below). This represents a tactical advantage for the individual (whether inadvertently or otherwise) and, in the context of the broader dispute, this may encourage the employer to seek to resolve the dispute through a settlement.

The committee considers that both employers and individuals have been left confused by the comments of the Court of Appeal in *Durant –v- FSA* [2003] EWCA

Civ 1746 and the comments of the ICO in its Data Protection Technical Guidance on Subject Access Requests and Legal Proceedings. On one hand, it is recognised that the right to submit a DSAR is a freestanding right under the DPA which remains unaffected by any broader dispute between the data subject and data controller in question. On the other hand, both the Court of Appeal and the ICO appear to criticise the use of DSARs to fuel litigation and indicate that enforcement action in these cases may not be appropriate. As a consequence, the response of employers who receive DSARs in the context of a broader dispute with the individual varies significantly, from full compliance to declining to respond.

Adding to the confusion, the committee had anecdotal evidence that, in practice, the ICO's approach to taking action in response to complaints in this area lacks consistency. A similar issue arises in relation to the limited applications which are made before the civil courts under section 7(9) DPA on the basis that this falls to the exercise of discretion on the part of the judge hearing the application.

The committee considers that data subjects and data controllers would benefit from further clarification and/or guidance on the use of DSARs in the employment context, with particular focus on the circumstances where the parties are engaged in a broader dispute. Better still it would be preferable to enact specific provisions aimed at the employment context.

Q.13 Do businesses have any evidence to suggest that this obligation is too burdensome?

Please see comments above in relation to DSARs submitted in the context of employment disputes.

The Call for Evidence and related Impact Assessment do not take account of the large volumes of data which employers may process and retain in the course of the employment relationship. The result is that responding to a DSAR is often a very burdensome exercise for employers in terms of time and cost. The time estimates for dealing with DSARs referred to on page 7 of the Impact Assessment (e.g. 10 to 75 minutes to process general subject access requests) bear no semblance to the time taken by employers to deal with these requests in practice.

A key factor in this is the increase in the use of e-mails in the workplace for the conduct of day to day business and other purposes over the course of the last 15 years. The volume of e-mails processed by some employers' IT systems on a daily basis cannot be overstated. In many cases, employers will wish to retain the ability

to retrieve specific e-mails which have been sent or received (or even deleted) for a number of years either for regulatory purposes (for example, the specific requirements for companies in the financial services sector) or in order to maintain an accurate record of the exchanges. Given the sheer volume of data to be stored, the sytems used for archiving and retriveal purposes are often cumbersome and costly to search.

The developments in the definition of personal data further to the Court of Appeal's decision in *Durant* and the ICO's Data Protection Technical Guidance Determining What is Personal Data has assisted employers to understand their obligations when determining whether to disclose copies of e-mails sent, received or copied to the data subject in response to a DSAR. However, these developments have not led to any significant reduction in the time taken to deal with DSARs as the majority of this time is taken in the conduct of searches for potentially relevant e-mails and manually reviewing the content of these e-mails to establish whether they contain the personal data of the data subject. This exercise can easily run to the review of thousands, if not tens of thousands of e-mails, even if the net result is that only a small portion of these actually contain the personal data of the individual in question.

These problems are exacerbated in relation to e-mails which are stored on an archive system or which have been deleted by remain capable of retrieval. In these cases, it will often be necessary to go through a costly and time consuming process to restore the data before it can searched for e-mails potentially containing the individual's personal data.

The use of key words to search electronic documents can sometimes assist with the task of locating relevant documents containing the individual's personal data. However, the volume of e-mails often results in a large volume of "false positive" results so the task remains burdensome.

Employers faced with broad subject access requests often seek refuge in the provisions of section 7(3) DPA and request additional information from the data subject with a view to narrowing the request in terms of date ranges, topics, key words or particular IT users. However, the parameters on when it may be reasonable for an employer to take this approach are far from clear, and these requests from an employer can sometimes result in an impasse between the parties and a complaint to the ICO requesting action.

The committee considers that further clarification and/or guidance is needed in

relation to an employer's obligations to conduct IT searches in response to a DSAR, particularly e-mails, to ensure that this task is proportionate to the circumstances.

Better still it would be preferable to enact specific provisions which codify proportionality or which provide for a regime specific to the employment context.

Q.14 Approximately how much does it cost your organisation to comply with these requests?

The committee did not have access to comprehensive or verifiable evidence in relation to the costs for organisations to comply with their obligations in response to a DSAR. Anecdotally, those acting for employers reported that these costs can be very significant indeed (examples were given where the cost ranged from £3,000 to over £25,000), particularly in those cases where the individual has/had been employed over an extended period and where the DSAR was cast in broad terms. The costs are incurred in a number of different ways:

- direct management and personnel costs for searching for and reviewing relevant documents;
- external costs for taking legal advice on responding to the DSAR and, in particular, on technical issues such as the definition of personal data, the application of the exemption for legally privileged material and dealing with the personal data of third parties; and
- external costs for instructing specialist IT consultants to assist with the retrieval of archived or deleted data and/or to assist with the search for relevant items (for example, by removing duplicate items).

Q15. Have you experienced a particularly high number of vexatious or repetitive requests? If so, how have you dealt with this?

Employers have reported high numbers of vexatious or repetitive requests, almost exclusively in the context of a broader dispute between the parties (see response to question 12 above). Again anecdotally it was the committee's view that employees exercise their subject access rights almost exclusively in the context of a dispute with their employer rather than otherwise.

Q16. What evidence is there that technology has assisted in complying with subject access requests within the time limit?

Technological advancements appear to be of limited assistance to aid employers to respond to DSARs either quickly or efficiently.

One issue is that these advancements have not kept up with the rapid increase in the volume of e-mail usage over the last 15 years (see response to Question 13 above), and there are few cost-effective technological tools available to assist employers to search for relevant documents in response to a DSAR.

A further, but no less significant, issue is that technology often cannot assist with the qualitative task of reviewing individual e-mails or other documents to assess if they contain the individual's personal data.

The ICO's guidance Determining What is Personal Data contains an eight question process to be followed in tricky cases but is quite a cumbersome process to follow. Similarly, technology cannot assist with the application of the exemptions (such as that relating to legal privilege) or dealing with third party data contained in the documents. These are often the most time consuming and costly aspects of responding to a DSAR.

An open question for employers is the extent to which the ICO expects them to invest specifically in technology which enables subject access rights to be fully exercised.

Q17. Has this reduced the number of employees required and/or time taken to deal with this area of work?

See response to Question 16 above.

Q18. Is there evidence to suggest that the practice of charging fees for subject access requests should be abolished?

No. We believe that the use of the £10 charging fee is both proportionate and necessary to ensure that frivolous requests are discouraged. Indeed, as set out in our answers below, we believe that further consideration should be given to increasing fees in certain circumstances.

Q19. Do you have evidence that the £10 fee should be raised or lowered? If so, at what level should this be set?

As noted above, the current regime is sometimes used by employees (or former employees) and their legal advisors in situations where the employee is planning or has commenced litigation.

In this situation, the nature of requests made by such individuals may sometimes be unfocused and the amount of data requested is often very large and involves detailed searches of IT and other electronic mediums (especially email).

As such the cost of arranging for the physical retrieval of such information can in some circumstances be high. Depending on the IT system used by the employer and whether others who are within the ambit of the request have already left its business, the administrative burden (and hence cost) to employers of organising such disclosure can be high.

Of more concern is that, in circumstances where proceedings are underway or expected, the employer will often have to have a specialist legal review undertaken to check the nature of the documents (in light of the litigation risk) and whether any exceptions under the DPA apply. Again, the cost to employers of undertaking this process can be high.

As noted above, this constitutes a form of pre action disclosure of information but it does not attract the legal costs involved in an employee formally going through the court process. In effect, it can be used by employees as a way in which to obtain information as part of litigation at a subsidised rate than would be the case via ordinary court proceedings.

A straightforward increase in fees per se would probably not deal with this issue – since the rate at which the fee would have to be increased to discourage an employee contemplating litigation against their former employer would be so high as to make the fee penal in nature.

Q20. Do you have evidence to support the case for a "sliding scale" approach to subject access request fees?

A slightly more nuanced option would be to introduce a basic fee at or around the £10 level – in respect of which an employee could receive basic information (such as paper HR file and payroll information).

Further charges – perhaps set up on a sliding scale – would then apply to more onerous requests – with the amount of fees increasing according to the volume of material requested or produced. A mechanism would need to be included under which the fee could be agreed with the employee before the work commenced.

Q21. Is there evidence to suggest that the rights set out in Part Two of the DPA are used extensively, or under-used?

It is not clear whether these rights need to be increased from our perspective.

Q22. Is there evidence to suggest that these rights need to be strengthened?

Comments

OBLIGATIONS OF DATA CONTROLLERS

Q23. Is there any evidence to support a requirement to notify all or some data breaches to data subjects?

Comments:

Q24. What would the additional costs involved be?

Comments

Q25. Is there any evidence to suggest that data controllers are routinely notifying data subjects where there has been a breach of security?

It is rare in the employment context that there are security breaches involving the personal data of employees or other staff, which are sufficiently serious to justify a notification to the ICO under the current guidance.

The Committee suspect from their experience that, in the employment context, there are a large number of minor breaches of the data protection requirements by data controllers. Whilst data controllers (at least significant organisations) typically take their data protection responsibilities very seriously, there are almost inevitably many minor, inconsequential, breaches which arise either from inadequate systems, or inadequate application of those procedures by an organisation's employees (which can never be entirely policed). Examples include:

- Not informing unsuccessful applicants that their details will be kept on file.
- Allowing a manager to see too much of an employee's personnel file when reviewing it for legitimate purposes.
- Reviewing personnel information when undertaking an IT investigation into suspected misconduct.

Consequently, a requirement on data controllers who are employers to report all breaches would require a large number of reports to be made, either to employees, or to the ICO, and in our view would unnecessarily create burdensome bureaucracy and an additional level of cost. Reporting a breach to an employee will, by its very nature, give rise to a potential legal claim by the employee under the current legislation. Many breaches will not have financial consequences and so are unlikely to lead to actual litigation. However, such a disclosure requirement may lead to an increase on the burden on an organisation as a result of any consequential litigation

connected to such breaches.

Currently in the ICO's guidance on notification to the ICO the overriding consideration for the ICO is the potential for harm to the employee. In our view this is the correct approach and he same test should apply in relation to the notification of breaches to the employee with the employer retaining broad discretion to determine whether such harm exists or is perceived to exist.

An employer should have sufficient auditing processes in place, and training, to ensure that it identified those breaches which should be notified.

If a notification is introduced in respect of a specified category of breaches, the key issue for employers will be to have clarity as to which breaches should be reported. The greater the uncertainty, the greater the cost and burden to employers since they are more likely to have to obtain specialist advice (often legal advice).

Q26. Do you have evidence to suggest that other forms of processing should also be exempt from notification to the ICO?

Comments:

Q27. Do these current exemptions to notification strike the right balance between reducing burdens and transparent processing?

Comments:

POWERS AND PENALTIES OF THE INFORMATION COMMISSIONER

Q28. What evidence do you have to suggest the Information Commissioner's powers are adequate to enable him to carry out his duties?

Given that the Information Commissioner's power to impose monetary penalties of up to £500,000 only came into force on 6 April 2010, and that no such penalties have to date been imposed under this power, we have no direct evidence to suggest that the Information Commissioner's powers in this regard are inadequate to enable him to carry out his duties. Although the Information Commissioner has issued guidance on his power to fine, until such time as the power is exercised and there is a body of "precedent", it is very difficult to assess the adequacy of the power.

We understand from the ICO that the ICO's approach continues to be collaborative and that inadvertent or even careless breaches will not result in fines. This is at odds with the Guidance which suggests that a failure to conduct a risk assessment or to have regard to the risks is one of the factors that may lead to the imposition of a fine. This should be clarified.

We note that the Financial Services Authority ("FSA") has the power to levy unlimited fines on organisations regulated by it for data protection breaches and has in fact fined organisations such as Zurich Insurance £2,270,000 for data security breaches. At exactly the same time as this fine by the FSA, the Information Commissioner found both DSG Retail, the owner of PC World, and Yorkshire Building Society in breach of the Data Protection Act 1998. In neither case did the Information Commissioner impose a fine. All of this enforcement activity postdates the coming into force of the ICO's power to impose a fine.

Care should be taken to avoid the creation of a two-tier sanction regime, in which the Information Commissioner's lesser power to fine is overshadowed by the FSA's greater one, and is by comparison viewed as inadequate and/or an acceptable cost of doing business. We also note that the FSA recently issued a new penalties policy, effective from 6 March 2010, as a result of which enforcement fines could triple in size as fines will be linked more closely to income and be based on: (i) up to 20% of a firm's revenue from the product or business area linked to the breach over the relevant period; (ii) up to 40% of an individual's salary and benefits (including bonuses) from their job relating to the breach in non-market abuse cases; and (iii) a minimum starting point of £100,000 for individuals in serious market abuse cases.

Regarding the Information Commissioner's other powers (to conduct assessments, to serve information and enforcement notices and "stop now" orders, to prosecute and to conduct audits), we would welcome greater consistency of approach, as the guidance/advice regarding the use of these powers given to data controllers who are concerned about their level of compliance can seem to depend on the individual handling the particular query at the ICO.

We are not aware of any use by the Information Commissioner of the new power to conduct compulsory audits on public sector bodies and so cannot comment on its adequacy.

Q29. What, if any, further powers do you think the Information Commissioner should have to improve compliance?

See above. Care should be taken to avoid the creation of a two tier system where the amount of the penalty in relation to employee data depends on the sector in which the employer operates.

Q.30 Have you had any experience to suggest that the Information Commissioner could have used additional powers to deal with a particular case?

THE PRINCIPLES-BASED APPROACH

Q31. Do you have evidence to suggest the current principles-based approach is the right one?

In the committee‘s view, the principles-based approach is a good one, but there is room for improvement. The principles as drafted, are considered 'loose' enough to adapt to advances in technology and also allow data controllers some flexibility in the way they manage data. In the committee’s view, this flexibility should be maintained.

The structure of the DPA should be reviewed however, in particular, the circuitous drafting of the principles which can make them cumbersome and difficult to follow for data controllers. The data protection principles are the key features of the DPA but they are hidden at the back within Schedule 1, Part 1, DPA and require further interpretation in Part II requiring data controllers to plough through several layers of the legislation to arrive at a true construction of it.

Helpful interpretation is available to understand the second, fourth, sixth, seventh principles and eighth principles but not, inconsistently, the third or fifth.

Necessity is not defined in the Act and while this is generally interpreted as meaning reasonably rather than absolutely necessary clarification of what standard should be applied would be desirable.

Q32. Do you have evidence to suggest that the consent condition is not adequate?

It is notable that 'consent' is not defined in the DPA. In the committee’s view it would be helpful to include a definition of consent.

Consent is the common condition for fair and lawful processing of personal data, sensitive personal data and the transfer of such data to countries outside the EEA. In the employment context however, because of the generally held view that consent in this specific context may not be reliable (see Article 29 Working Party (2093/05/EN WP 114) and the ICO Employment Practices Code) employers often look for other ways to justify their processing rather than relying on employee consent. In that regard it could be said not to be available in practice. There are other alternative conditions for the processing of personal date, which employers may rely on, such as "legitimate interests", or "the performance of a contract" . In the vast majority of circumstances the employer can rely on the legitimate interests precondition instead

of consent.

There are however much more limited and narrow grounds for justifying the processing of sensitive personal data and no legitimate interests precondition available to employers. In the context of sensitive personal data the need to justify processing on these very narrow grounds can be problematic. For example, emails, or CCTV images may contain sensitive personal data. The mechanism of processing data is blind to the content of the processing and the content is to some extent out of the employer's control. Should employers then ensure that they meet the preconditions for sensitive personal data with regard to the use of email in the workplace or the installation of cameras at the entrance to the employer's premises? In practice this would be unworkable.

If the view that consent is unreliable in the employment context is to prevail in respect of any revised version of the Directive or DPA then there is an urgent need to consider the scope of the other preconditions to processing sensitive personal data, where possible to expand them, or at the very least, to clarify them. For example, there should be a general right to process health related data for employment purposes. Another approach would be to provide a legitimate interests precondition for the processing of sensitive personal data.

Another alternative is to soften the approach to the reliability of the consent of the employed data subject so that where employers do take the approach of relying on it they are safe to do so provided the parameters are clear. In the committee's view consent should be genuine, fully informed and the means of obtaining consent should be appropriate to the circumstances (see question 34 below).

Q33. Should the definition of consent be limited to that in the EU Data Protection Directive i.e. freely given specific and informed?

Yes.

Q34. How do you, as a data controller, approach consent?

Employers are well advised to place any request for consent in a different document because of the concern over its reliability. There is also the concern that even if they accept and understand the nature of the data processing at the time of signing a contract, over time, data processing changes and (consciously or not) employers may not renew their contracts. In addition employees should be allowed to revoke or withhold their consent.

One approach would therefore be to explain the conditions in which employers can regard the consent as reliable because it is contained in a full separate policy. If full information is given this should ensure that it is fully informed consent. In addition if consent is contained in a separate policy or notice then it can be sought again when changes are made to that policy to bring it up to date.

In this workplace context therefore the fair processing notice should take the form of a full data protection policy which is given to employees along with all the other employer's policies and which is available in an employment handbook and on the employer's intranet and kept up to date.

Q35. Do you have evidence to suggest that data subjects do or do not read fair processing notices?

See response above. We have no actual evidence. We note in this context that compliance should not however depend on whether the employee has read the policy if the employer has taken sufficient steps to draw it to the employee's attention.

EXEMPTIONS UNDER THE DPA

Q36. Do you have evidence to suggest that the exemptions are fair and working adequately?

Comments:

Q37. Do you have evidence to suggest that the exemptions are not sufficient and need to be amended or improved?

Comments:

INTERNATIONAL TRANSFERS

Q38. What is your experience of using model contract clauses with third countries?

In general, the trans border dataflow rules were designed for a different age when it

was not so easy to transfer data around. Nowadays, you can process data at the click of a mouse. The two systems which are designed to deal with transfers of data (.e. Model Contracts and binding corporate rules) now look rather clunky and out of date.

The vast majority of businesses now rely on information flows via the internet. As expressed some time ago by the Information Commissioner, use of the internet, under the principles of least cost routing, means that every communication using the internet could be an international transfer - it makes use of the most efficient route to transmit a communication and this may be via multiple geographic locations where there is public electronic communications network capacity.

Thus many internet communications may be international transfers of some sort or another. In this context, ensuring adequate security for personal data transfers outside the EEA must be a consideration for all personal data communications. For multinational businesses, authorisation within the UK is flexible, allowing self-certification of transfers between their own group companies or to third party suppliers in EEA countries and onward transfers to non EEA countries. The same cannot be said of other EEA countries and the process of registration for a multinational employer becomes an administrative minefield.

The disparity of approach is evident in the information demanded of the data controller for exactly the same transfer. Fees will differ; procedural steps differ and timetables for handling such applications, notifications or registrations will differ. Where the transfer may involve sensitive personal data, in many instances, a different process will be required, and more detailed information will be required.

It is acknowledged that personal data must be handled appropriately. However, when large organisations may have millions of databases performing multiple functions, it is not entirely clear what each regulator will do with the vast detail requested on each database, its physical location, how personal data is handled within the database and what security is in place over each file. The registrations procedures also ignore the fact that many organisations have internal communications networks that render geographic location irrelevant, as all employees in one company are connected to the same corporate network and will have access to information that may be held on global databases held in the cloud, not in one physical location, but on multiple servers with dynamically allocated storage space. The practical reality of information being held as a piece of paper does not exist in these types of environments.

The possibility to register with one European wide data protection registrar or even one registration process with each registrar rather than each company in each country having to register with their own local data protection registrar would certainly ease the current bureaucratic challenge.

The EU Model Clauses do offer a pragmatic way through this minefield although in practice it can be confusing to know which version should be used. They are not as cumbersome as the alternatives and in practice employers know that if they do not diverge from them registration can be a comparatively straightforward process across Europe. They do fix responsibility firmly with the data controller. The benefit of this is to make it transparent who has responsibility for protecting personal data and how the data subject can obtain redress in the event of suffering damage. It is also of benefit to the data controller, as it sets out a common starting point for the contractual protections that must be offered as a basis for interacting with any customers or suppliers. This clarity and consistency drives a common understanding of the rights that are being protected. The challenge for each organisation handling personal data is to ensure it meets the common standard, but gives it flexibility to build on the standard to develop its own framework.

More could be done to reduce the bureaucracy required to comply. As an example, the new Model Clauses for Controller to Processor and sub-processor transfers require a list of sub-processors to be provided annually. In a high tech environment where suppliers may be brought on board to address short term capacity issues and then released in a matter of hours, but be available throughout the year on such a call off basis, maintenance of a list becomes a full time job. There will also be any number of such processor transactions occurring on a second by second basis in each geographic location where personal data may be processed.

More could also be done more generally to ensure that there is a global standard because the absence of such a standard can lead to complexity. [An example would be that some EEA countries have added more classes of data to the definition of sensitive personal data and as a result when an employer wishes to set up an international personnel database it will have to apply a different test in each country to whether it can process certain classes of data and transfer them outside the EEA.]

Q39. Do you have evidence to suggest that the current arrangements for

transferring data internationally are effective or ineffective?

See above.

Members of ELA Working Party

Ellen Temperton, Lewis Silkin LLP (Chair)

Ivor Adair, Russell Jones & Walker LLP
Daniel Aherne, Olswang LLP
Nina Barakzai, Dell
Ann Bevitt, Morrison & Foerster LLP
Daniel Ellis, Baker & McKenzie LLP
Paul Seath, Bates Wells & Braithwaite LLP
Khurram Shamsee, Beachcroft LLP
Catrina Smith, Linklaters LLP
Andrea Ward, Hogan Lovells LLP

About you

Please use this section to tell us about yourself

Full name	
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	
Date	6 October 2010
Company name/organisation (if applicable):	Employment Lawyers Association
Address	P.O. Box 353 Uxbridge
Postcode	UB10 0UN
If you would like us to acknowledge receipt of your response, please tick this box	☐ x (please tick box)
Address to which the acknowledgement should be sent, if different from above	lindseyw@elaweb.org.uk