RESPONSE TO THE "CALL FOR EVIDENCE" FROM THE MINISTRY OF JUSTICE IN CONNECTION WITH THE DATA PROTECTION REGULATION

(From Amberhawk Training Limited)

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LIMITED
DR. C. N. M. POUNDER, MARCH 2012

Response to the "Call for Evidence" from the Ministry of Justice in connection with the Data Protection Regulation

Table of Contents

About Amberhawk.

Amberhawk Training Limited is a company established in 2009 to provide information law training; collectively, its Directors have over 40 years experience in the data protection field. I make several points about the Regulation, most of which are aimed at improving the Regulation from the data subject perspective.

I make no apology for this focus. I am aware that the MoJ Consultation was largely targeted at data controller organisations, and any comment that I would make from the data controller perspective is likely to have been made already (e.g. about the Regulation's overtly prescriptive nature in some areas especially re Data Breach notification provisions; data protection officer post, and information given to data subjects, or in relation to a child's age being 18 years, or in relation to the processing of sensitive/special personal data re suspected criminal activity by child protection charities or private sector auditors in relation to fraud etc).

I do not object to our views being published.

1. The wider definition of "personal data" should not cause problems.

When is an IP address personal data? The current position under the UK Act is that an IP address is personal data if identifying information about a living individual is in the possession of the data controller or likely to come into the possession of the data controller. The Regulation widens this position; if identification of an individual is reasonably likely by the data controller *or by another person* then there is a "data subject" and the information is "personal data".

The consideration of identifying details held by *another person* is not an alien concept for data controllers in the UK, ***as it already exists*** in section 8(7) of the current DP Act in the context of subject access. (It occurs when there is a subject access request made by the data subject and the issue is whether the data controller can release personal data that identifies another individual). In this case section 8(7) states that if the "other individual" can be identified by the data subject from the personal data that are released or from the personal data ***plus*** "any other information which, ***in the reasonable belief of the data controller***, is likely to be in, or to come into, the possession of the data subject making the request", then the data controller might redact any information that could identify the other individual.

I conclude therefore, that such a change to the definition of personal data as proposed by the Regulation is unlikely to hold many difficulties for data controllers as they do it already, albeit in a more limited context. ***If there were practical problems or difficulties concerning the identification being held by another person, these would have been aired in the context of subject access.***

I am sure that many data controllers will oppose the change because it would mean more compliance work; by contrast, data subjects are likely to be in favour this change because it means more protection. As there is no evidence of difficulty with the inclusion of identification by another person, this in turn means there is only one question for Government to resolve: "which side it is on?".

If the Government's position favours the wider reach of personal data, I think the word "identifiable", as used in Recital 23 of the Regulation, should be brought into the main definition of "data subject". See next section and section 11, re other comments about the definitions.

2. Consider the "joint data controllers" rather than the "data subject" definition?

I am **not** convinced that using the definition of "data subject" is the best way to widen the scope of personal data – if that is what the Government decides to do. This comment is by way of suggestion.

The Regulation states that an individual is a data subject if a holder (organisation 1) of an IP address has reasonable cause to believe that another organisation (organisation 2) is likely to obtain the identifying details of that individual. In such a case, the holder of the IP address (organisation 1) will be processing personal data and will be a data controller. Organisation 2 should also be a data controller because it holds the identifying details, but that is implied.

I would argue that there is a much better strategy. That is to drop the identification that requires "reasonable means...of another person etc " from the definition of "data subject" but expand the definition of "joint controller" so that if one organisation holds linkable details where an individual is not identifiable and another organisation holds the relevant identifiable or identification details (or is likely to hold the such details), then **together both organisations** become "joint data controllers".

The advantage of this is that **as joint data controllers**, they are both expressly responsible for compliance; they are explicitly linked together and no doubt, will come to contractual arrangements for this. I also think that this will be far more acceptable to the data controller community, as they will see that the provision closes an obvious loophole when one organisation holds the "anonymous data" works with another organisation that holds the identifiability/identification details. It also means that you have far more natural definitions for "data subject" and "personal data".

To make this clear, Article 24 (re joint data controllers) could look something like:

> *"Where the purposes, conditions and means of the processing of personal data*
>
> - *are shared between more than one person, or*
> - *are the result of the processing, by one person, of details that make, or are likely to make, data subjects identifiable in combination with other details held, or made available, by another person,*
>
> *then the persons that are responsible for the processing to occur are "joint controllers".*
>
> *Each controller shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular, as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them".*

3. The Regulation excludes confidential personal data already subject to the DPA

The Regulation applies to personal data held in a structured "filing system" (Article 4(4)) and the rights of access (Article 15) are to personal data (e.g. in a structured filing system). Recital 13 of the Regulation confirms that manual personal data that are not in a structured file are not subject to the Regulation.

An Accessible Record under the DPA contains personal data that does not need to possess any structure (section 1, definition of "data"). Thus Accessible Records could well be excluded from the Regulation if they are not held in a structured filing system. This exclusion could be **from** all Principles and all rights whereas currently such personal data is **subject** to **all** principles and **all** rights in the Act.

Similarly "Unstructured personal data", as used in section 9A of the DPA (introduced as a result of FOIA) is subject to the right of access and correction. By implication the Regulation is stating that "Unstructured personal data" can't be personal data (not in a structured filing system) so it follows that there is no right of access nor correction. The concept of "Unstructured personal data" does not exist in the Regulation.

In this context, the Regulation could thus reduce rights and protection of personal data in the area of Social Work, Housing, Education services supplied by a local authority, in the area of health personal data produced by a registered health professional, and in the rights of access and correction when a data subject seeks "unstructured personal data" from **any public authority**.

The Regulation should be changed to maintain the protection of those personal data that are already subject to the UK's data protection regime.

4. The need for a prohibition on enforced subject access

There needs to be a provision that stops enforced subject access in the Regulation. Such provision exists in the Data Protection Act 1998 but has not been commenced; employers, in the UK for instance, can thus gain access to criminal records for employment purposes without the need to bother with the rules or Code of Practice promulgated by the Criminal Records Bureau.

The technique is being used by Legal and General (and possibly others in insurance industry in relation to health). This undermines the Access to Health Records Act (see "Enforced Subject Access to medical data raises its ugly head in the insurance industry" on http://amberhawk.typepad.com/amberhawk/2012/02/enforced-subject-access-raises-its-ugly-head-in-the-context-of-medical-insurance.html)

As the right of access to personal data is free, then other data controllers could be encouraged to misuse a right targeted at protecting the individual; the UK experience shows that the right can be perverted to protect a data controller's interest.

It would help promote understanding of "free access to personal data", if there was a link to Privacy by Design objectives in Article 23 so that "free access" is an integral part of the design.

5. Switch from the right to be forgotten to the right to object to the processing

My general view is that the many aspects of the "right to be forgotten" in Article 17 is best dealt with by "right to object" in Article 19, possibly by an amendment linked to Article 82 if the context is employment. The switch to the "right to object" has the same effect as the "right to be forgotten" but it avoids any "attack on freedom of expression" criticism, and is more effective as it targets the ***use*** of personal data by a data controller within the EU (and not the ***hosting*** of the personal data anywhere in the world). ***This effectiveness is especially important in the context of employment***.

It is best to explain this by example.

For instance, suppose an embarrassing fact about a data subject is posted on a USA web-site, but is used in the UK by an organisation (which by definition has to be by a data controller) to make an employment decision. If the controller is situated in the UK, then even the current Data Protection Act would apply – let alone the Regulation.

Such a data controller under the existing UK Act has to apply three Data Protection Principles (1st, 3rd and 4th). He has to demonstrate that the personal data are relevant to the purpose (e.g. employment purpose), that they are accurate and up to date (e.g. the personal data relate to the actual individual under examination and not someone who happens to have the same name) and ensure that the data subject knows of their use for a specific purpose. The data subject also has the right of access to personal data used to make that decision. The same will go for the Regulation.

I would also argue that it is not fair to the data subject to use personal data extracted from, say Facebook, without explaining what and why personal data were used by the data controller to make an employment decision (e.g. perhaps augmented by providing a copy of the personal data used especially as there is free subject access as proposed by the Regulation). Any failing in this area can already be enforced by the supervisory authority.

Instead of the "right to be forgotten", I would extend the existing "right to object" to the processing (as is proposed in Article 19 of the Regulation) to apply the "right to object" to those circumstances where the processing is "**necessary for an employment contract with the data subject**" or with "a view to entering into **an employment contract** with the data subject" (e.g. an employment contract with a prospective employee). That is why I suggested this change might better stand as a part of Article 82.

In this way, data controllers can argue that they should be able to scour the internet for background details about an individual but that data subject will be able to argue the exact opposite. This provides a structure where the facts of each case can be independently examined to identify whether the data controller's or the data subject's position should prevail. Following such examinations, advice on best practice will emerge.

Currently in the UK the right requires the processing to cause "unwarranted substantial distress" or "unwarranted substantial damage" to the data subject; a requirement which heavily tips the scales in favour of the data controller. The Regulation drops the "substantial" element of this threshold test; this means the test of the balance of interests between a data subject's interest and a data controller's interest is assessed on a level playing field. I therefore support the Commission's rebalancing proposal in Article 19.

I should conclude by saying that I am not sure of the reasoning extending the right to object in the context of that processing in "the vital interests of the data subject" ***in all circumstances***. Could this right be used by someone who wanted their life-support system in a hospital turned off? Could a mentally ill or suicidal patient object to that processing which keeps him alive? I suspect that the extension goes too far, and may need some further clarification as to what the Commission has in mind.

6. Recognise a form of notification to the supervisory authority will re-emerge

I think the "headline grabbing" provisions re the scrapping of red-tape notification to the Commissioner have not been thought through (although I acknowledge that notification in the UK in its current form is 95% useless). The reason why I think it has not been thought through is because supervisory authorities can be expected to require data controllers to inform them of something or other, and this is a form of notification.

Under Article 28, most of the detail that is the subject of registration in the UK have still to be collected by data controllers (e.g. the name and contact details of the controller, or

any joint controller or processor, and of the representative; the purposes of the processing, including the legitimate interests pursued by the controller; description of the category or categories of data subjects and of the personal data or categories of data relating to them; the recipients or categories of recipients of the personal data).

So in practice notification to the UK's Information Commissioner is replaced by the data controller keeping the same registration/notification detail as well as other items. So when the European Commission claims that "notification is gone", it is a statement that is arguably "economic with the truth". The expense for a data controller of collecting these details is still there; what's gone in the UK is the £35/£500 fee.

The question then turns to whether it is reasonable for such details as specified in Article 28 to be published? Article 28 is silent on whether such details should be published and so I think the Regulation should be amended to ensure that some of these details are published.

A publishing requirement exists for **public authority data controllers** in the UK as such details can be subject to FOI requests; so for these public sector controllers, notification has not really disappeared. So why should private sector data controllers not be obliged to publish the same level of detail as their public sector colleagues?

Notification has a bad reputation because its history relates to a description of the processing of personal data by mainframe computers in the 1970s. It thus contains far too much detail about the processing. In the UK, it is costly to maintain and is impenetrable. I have no doubt that this system of notification should be scrapped.

However, the concept of notification has several advantages; it provides a formal address for Subject Access and the use of enforcement powers, it lists those who need to comply with the Act, and, in the UK, provides a source of revenue which funds the Information Commissioner. Notification is also a public acknowledgement by the data controller that he recognises that there are data protection obligations.

In the UK, for instance, the public register is used to identify data controllers who are public authorities. So, assuming the Regulation is in force, how is an applicant to know whether a body called "The UK Consultative Committee on Potato Blight" is a public authority or not? With respect to the "main establishment", how do data subjects know where this is? Are they supposed to keep their fair processing notice for later reference? Article 37(h) requires the data protection officer to be the contact point for the supervisory authority. No doubt, some supervisory authorities will require data controllers to identify their data protection officer to it. (I think the CNIL does this already).

In all these cases, any list of data controller names plus other details requested by the supervisory authorities is a form of notification.

I just wonder whether some kind of quick study should be undertaken of data protection authorities to see whether or not the benefits identified above can be maintained by some kind of public domain detail having to be published on an annual basis (e.g. name and address of data controller, contact details for data protection problems, a list of Codes of Practice/Conduct (see Article 38), whether Binding Corporate rules apply to the data controller, identity of the main data controller establishment, number of reportable security breaches in the last year etc etc).

Such a study can be delivered quickly from existing supervisory authorities and should identify the kind of detail that could be listed in a simple public register whose prime objective is to be a source of information for data subjects. In a sense, the study is to ensure the baby is not thrown out with the bathwater**.**

In practice, it should be recognised that some system of "ad-hoc" notification to a data protection authority will re-emerge (but of course, data protection authorities will never call it "notification").

7. The need for a link between Article 8 and the concept of lawful processing

The Regulation has broken the very explicit link to Article 8 of the European Convention of Human Rights that appeared in Directive 95/46/EC. The Regulation has replaced the "*right to privacy*" found in Directive 95/46/EC with "*the right to the protection of personal data*" (which I will shorten to the "*right to data protection*").

This link should be reinstated. ***The proposal is that Article 52 tasks of a supervisory authority should explicitly include an assessment whether "lawful processing" includes lawful processing in accordance with Article 8 of ECHR.*** This would allow supervisory authorities, who often claim that some processing is "disproportionate", to assess Article 8 compliance.

Article 1 of Directive 95/46/EC to be replaced, defines its purpose in these words: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy* with respect to the processing of personal data" (my emphasis).

Recital 10 of Directive 95/46/EC then amplifies what is meant by the "*right to privacy*". It states that "... the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the *right to privacy*, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms". Recital 11 then adds that "*the right to privacy*" in the Directive is intended to "give substance to and amplify those (provisions) contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data".

Compare this position with the Regulation which does not use the word "privacy" (except in the context of "privacy by design" or "data loss"). In the Regulation, there is no mention of the "right to privacy", no mention of Article 8 of the Human Rights Convention, nor the Council or Europe Convention No 108 (which drove most European States to have data protection legislation in the first place).

The lack of such references is very disappointing. Is this decoupling from Article 8 deliberate? Answer has to be "yes". Why is there decoupling? So far, no reason has been given by the Commission.

The "*right to data protection*" is found in Article 8 of the Charter of Fundamental Rights of the European Union (and Article 16(1) of "The Treaty on the Functioning of the European Union"). The three parts to Article 8 state:

1. “Everyone has the right to the protection of personal data concerning him or her”.

2. “Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

This reference replaces, I assume, the Human Rights Article 8 emphasis of the Directive which relates to a “Right to respect for private and family life". This Article states that:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

So what is worrying about “*a right to data protection*?”.

Well, I think the term doesn’t mean anything and if one “Google’s” the term, it is clear nobody on the planet has published a view. Whereas there is a detailed literature, legal precedence and more than 100 year history of debate surrounding the term “*privacy*” (or 50 years in terms of Article 8), there has none surrounding “a *right to data protection*”. Yes, I know there are several different expressions of what “*privacy*” or *Article 8* should mean in practice, and these have been compared, criticised and compared and still people argue. However, such involvement and debate is a far cry from a Regulation that refers to a right which is not even been defined or subject to any debate.

Without such debate, there is a great risk that the “*right to data protection*” will mean different things to different people. For example, individuals might see it as equivalent to “*data privacy*” (which clearly it is not, in my opinion) whereas data controllers might see it as just an expression that they have to comply with the law (which I suspect it is). If it is the latter, the "*right to data protection*" is a right that possesses the same characteristics as “a right not to be mugged or murdered”.

In fact, I would say that if the “*right to data protection*” means as little as “data controller compliance” then it is not a right at all and to promote it as such is clearly misconceived. In short, the “*right to data protection*” is currently a confused, ill-defined and unknown concept. That is why the link to Article 8 of ECHR should be inserted in Article 52.

8. The centralization of power by the Commission is unbalanced and unacceptable

In about 50 circumstances, the Commission reserves the powers to modify the data protection outcome. For example, in Article 32(5) you have the following:

“The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data .breach is likely to adversely affect the personal data referred to in paragraph 1”.

Essentially this type of provision makes the Commission the ultimate arbiter of the data protection rules as these powers can overturn the actions of any supervisory authority.

There are several circumstances when the European Commission has determined that there is an adequate level of data protection, when most data protection authorities have formed the opposite view. The PNR agreement with the USA is a good example of this divergence of view, and any reading of the output from the European Data Protection Supervisor will provide a host of other examples.

Put simply, the European Commission appears to have a track record of putting political considerations above those of data protection; so my first comment is that there is a significant risk that this approach will continue. Secondly, the issue is quite serious in the context of the Commission as the Regulation will eventually apply to the Commission itself. This means the Commission is to be given powers to modify how the Regulation would apply to its own processing of personal data.

In my view, the Commission should not be given untrammeled powers to achieve either prospect as both are equally unacceptable.

The Regulation establishes a powerless European Data Protection Board whose function is to help establish consistency re data protection compliance by providing commentary and advice. I therefore suggest the powers that the Commission is seeking in the Regulation involve the Board so that they can establish the correct balance of interests between data controllers and data subjects.

My suggestion only applies to the Commission’s reserved powers deal with the determination of a data protection issue (see example above). I suggest two ways how the involvement of the Board could be achieved:

(a) the Board could exercise the powers the Commission identify in the Regulation. The Commission could raise an issue with the Board who then determines a suggested data protection solution. The Commission can then be given the power to overrule the Board in cases where this is deemed necessary – this would require the Board to “try again”. In this way, the Commission still possesses all the trump cards (as in the Regulation).

(b) an alternative is to leave the Commission’s powers where they are, but state that the exercise of the power is subject to Board approval on data protection grounds. This again provides a check on the misuse of Commission’s powers but gives the Board an ultimate veto.

Whatever happens, there needs to be a counterbalance to the Commission taking political decisions re data protection in its own interests that set aside the data protection rules the Regulation is supposed to establish.

9. The apparent absence of a criminal sanction

I am not sure whether criminal sanctions exist under the Regulation. If not, they should exist. If criminal sanctions are absent, a tier of enforcement options for the Regulator is removed.

The absence of a criminal sanction leaves the application of the law in a very unbalanced position. For instance if an employee sets out to deliberately flout the data protection law, a panoply of offences, some outside the data protection regime, could apply (e.g. Section 55 of the DPA, Official Secrets Act, Computer Misuse Act, Census Act, Regulation of Investigatory Powers Act re phone hacking or even the common law offence of "malfeasance in public office). The MoJ knows that the ICO has called for the weak penalties incurred under offences in the DPA to be put in line with the more serious offences in the Computer Misuse Act.

However, if a data controller sets out to deliberately flout the data protection law, then there may be no offence. Of course, there are Monetary Penalty type options. However, if the data controller then goes into bankruptcy, these Monetary Penalties and administrative sanctions become rather redundant.

For instance in the ACS law case, the ICO told Parliament that "Were it not for the fact that ACS:Law has ceased trading so that Mr Crossley now has limited means, a monetary penalty of £200,000 would have been imposed, given the severity of the breach". The actual penalty was £1,000 fine. (see http://www.bbc.co.uk/news/technology-13358896).

The imbalance I identify above should be corrected. Having offences that apply to **everybody** sends a consistent message to all who may be tempted to deliberately set out to flout data protection law take a serious risk.

10. Unclear use of "information" or "data" in the definitions

Because the Regulation is to be directly transposed into UK law, there may be a lack of precision in the use of definitions which could cause interpretational issues.

I recommend that the Regulation should be scanned to make sure the use of "data", "information", "personal information" or "personal data" will have a consistent interpretation, to avoid problems should a matter come to the Courts in the UK.

For example, the terms found in the definitions (Article 4) include:

1. "personal data" means any information relating to a data subject....
2. "genetic data" means all data....
3. "data concerning health" means any information...

When these terms are used in the Regulation, it is sometimes unclear whether:

1. "data" means the same thing as "information"?
2. "data" means "personal data" or not?
3. "information" needs to be recorded; can it include non-recorded information?

4. "information" is different to "data" or "personal data"?

All these terms are used interchangeably in different contexts. For example

1. The term "Information" is used in Article 5(c), Article 10 etc appear to give the impression that the "information" has to be recorded in some way and that the "information" is not personal data
2. In Articles 11, 12 and 14 the use "information" is different to that above (information given to data subject –could the information be verbal or has it to be a written notice (i.e. fair processing notice)?
3. Article 8 uses "information society services" should be defined in Article 4 to avoid confusion over the use of "information".
4. In Article 15(2) "information" in question is "personal data" but in Article 15(1) "information" does not mean personal data (its use is like that in Articles 11, 12 and 14)
5. Article 18(2) suggests that "information" is not "personal data"
6. In Article 28, "information" relates to "documentation"

I think this is enough detail to show the Regulation should be scanned to make sure the use of data, information, personal information or personal data is consistent.

11. Some contributions are devalued because they relate to a "defective" DPA

According to the Commission, the Directive definition of "personal data" has not been implemented properly by the UK Government. FOI requests now in the public domain show this clearly (see the attachment linked under the heading "*Privacy: new Government revelations amplify concerns surrounding deficiencies in UK's Data Protection Act*"; http://amberhawk.typepad.com/amberhawk/2011/05/privacy-new-government-revelations-amplify-concerns-surrounding-deficiencies-in-uks-data-protection-.html).

One reason for this is that the consideration of what information might be in the hands of "other persons" ***is also found in Directive 95/46/EC***, when Recital 26 is taken into account (e.g. ".....whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person...). ***In the UK transposition of the "personal data" definition in the Directive, Recital 26 has been ignored.***

This means that the views of data controllers opposing the Regulation's change to a wider reach for "personal data" might have been made in the mistaken belief that the UK definition of "personal data" is derived from a correct transposition of the Directive 95/46/EC, when in fact this transposition is disputed.

For example, the Hogan Lovells submission to the MoJ (available from their web-site), calls for the *Durant* judgment to be maintained and a narrow view of personal data to be adopted. Yet *Durant* is another of the reasons why the European Commission thought about infraction proceedings against the UK.

I believe that these comments may not have been made by Hogan Lovells, if the MoJ had stated, in its "Call for Evidence" that the definition of "personal data" in the UK Act was being challenged as being defective. This position also relates to all respondent comments made in respect of the Regulations modifications to Articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 and 28 of the Directive 95/46/EC (i.e. all Articles in the Directive that are changed by the Regulation where the Commission claim that there has been a defective transposition).

I do not want to labour this point – but this is a case where the absence of transparency about the European Commission's concerns about the UK's Data Protection Act has rebounded to the detriment of all those contributing to your "Call for Evidence".

In fact one can make the case, that if we assume the Commission's view is correct about the transposition of Directive 95/46/EC, then any comment from a data controller in support of the incorrect transposition in the UK's DP Act should be discarded as being irrelevant. I would say that this could apply to Hogan Lovells' comments on *Durant*.