DATA PROTECTION:

THE PROPOSED REFORMS

Aisling Duffy and Laurence Kaye

10 December 2014

DATA PROTECTION: THE PROPOSED REFORMS

1 WHY IS CHANGE NECESSARY?

1.1 The current Data Protection Directive (Directive 95/14/EC) (the "**Directive**") was implemented in the UK in the form of the Data Protection Act 1998 (the "**Act**"). In July 2009, the European Commission launched a consultation requesting feedback from the public and organisations on the Directive.

1.2 A number of criticisms were levied against the Directive. In particular, the Directive was considered to be outdated and requiring amendment, in the light of the introduction of new technologies and ongoing globalisation. In addition, it had become apparent that EU member states had implemented the Directive differently, resulting in inconsistent and sometimes conflicting approaches in relation to data protection across the EU, with different standards, regulators and added bureaucracy. This represented a significant challenge for organisations operating at that level.

2 CURRENT STATUS OF THE REFORMS

2.1 The European Commission published its initial draft proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the "**Regulation**") in January 2012.[1]

2.2 The Information Commissioner's Office ("**ICO**") and the Article 29 Working Party have subsequently published their views on the draft Regulation. In general, some provisions of the draft Regulation have been met with approval, whilst others have been criticised and therefore debated.

2.3 There have been a number of iterations of the draft Regulation now and its provisions are still the subject of discussion amongst the relevant EU institutions. Our comments in this note are therefore based on the current draft Regulation, which may be subject to further amendments.

2.4 The incoming President of the European Commission has said that the draft Regulation should be finalised in the first quarter of 2015. However, given the lengthy parliamentary process and the matters which remain outstanding, it may be that this is delayed until late 2015. The draft Regulation will be effective two years after it has been finalised and adopted by the European Parliament.

[1] The Commission's draft Regulation can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

3 WHAT IMPACT WILL THE PROPOSED NEW REGULATION HAVE?

3.1 Practical Implications:

3.1.1 *Increased accountability* - There are a number of provisions in the draft Regulation which will result in data controllers and processors taking on increased accountability. This represents a significant shift in approach. For example, data controllers and data processors will be required to maintain documentation relating to their processing activities in order to be able to "demonstrate compliance". In addition, data controllers will be required to carry out privacy impact assessments in certain circumstances. This may even involve consulting with Regulators and individuals concerned.

3.1.2 *Breach notification* – Organisations will be required to notify the Regulator of "every breach". Whilst discussions are ongoing regarding whether or not this obligation should incorporate some element of de minimis, current drafting suggests that the obligation to notify should apply regardless of how serious (or minor) the breach. In addition they must do so as soon as reasonably practicable and within 72 hours.

3.1.3 *The transparency principle* – The draft Regulation introduces the principle of transparency and requires that personal data be processed in a transparent manner[2]. Data controllers will be required to have easily accessible policies with regard to the processing of personal data and in relation to the exercise of data subjects' rights. For example, a comprehensive company wide data protection policy should be drafted, publicised and enforced and privacy policies should be easy to locate and not buried in the small print. These types of practices should be carried out already but the draft Regulation introduces transparency as a specific principle.

3.1.4 *Pro-active approach* – The draft Regulation is far more detailed and prescriptive in nature than the Directive, particularly concerning the measures it will require organisations to implement in order to achieve and demonstrate compliance. Data protection compliance will no longer be something that can be handled on a reactive basis. Organisations will need to take a pro-active approach to ensure that they can comply. It will be essential to maintain comprehensive and up to date records, policies and procedures and to continually monitor and verify the adequacy of those polices and procedures.

3.2 Increased risk profile

3.2.1 Under the current Directive, the ICO has the power to issue fines of up to £500,000 for a serious breach of the Act. In contrast, the draft Regulation will give the ICO the power to issue fines up to the greater of 5% of annual worldwide turnover of the organisation in breach or 100 million Euros. The risk profile associated with data protection compliance is therefore likely to increase and data protection compliance will become a key governance issue.

3.2.2 Because of the increasing trend for publishers to interact directly with consumers (rather than intermediaries) and to rely on their ability to collect and process personal data to develop their businesses, publishers will now, like retailers, need to see data protection compliance as a key risk area.

---

[2] See Article 5 of the Regulation (principles relating to personal data processing) under which personal data must be: "processed lawfully, fairly and in a transparent manner in relation to the data subject" (Article 5(a)).

3.3 Harmonisation

As mentioned, the instrument that will be used to implement the new laws will take the form of a Regulation, rather than a Directive. This means that it will have direct applicability across all EU member states without the need for local implementation. This should result in a more harmonised approach.

3.4 One-Stop-Shop

3.4.1 The current Directive requires each EU member state to ensure that its implementing legislation applies to the processing of personal data where a) the data controller is established within the territory of that member state b) national law applies by virtue of public international law or c) the data controller makes use of equipment situated within the territory of that member state. This means that currently, in the event of a breach, any one data controller may have to deal with data protection authorities across a number of member states.

3.4.2 In contrast, the draft Regulation will establish a 'one-stop-shop' mechanism. This will mean that organisations will only have to deal with one single supervisory authority, which will be decided by reference to the location of the main establishment of the data controller (for example, a company's head office). This should make it simpler and cheaper for companies to operate within the EU.

3.4.3 The 'one-stop-shop' will also make it simpler for individuals, who will only have to deal with the data protection authority in their member state if they have a complaint.

4 A REVIEW OF SOME OF THE KEY PROPOSED CHANGES

4.1 Definition of personal data

4.1.1 The definition of personal data is wider under the draft Regulation than it was under the Directive, and includes all data that can identify an individual, directly or indirectly (i.e. whether the data is held by the data controller or by a third party, which in combination with the data held by the controller, could identify the data subject).[3]

4.1.2 The present definition of personal data under the Act requires the *same* data controller to hold all the data that makes the data subject identifiable (this arguably was incompatible with the Directive in this respect, as the Directive included a similar definition to that proposed under the Regulation). The definition is therefore wider than it was under the Act, an approach which has been welcomed by the ICO, but both the ICO and Article 29 Working Party would prefer this to be widened further to include pseudonymised data.

4.1.3 In addition, the proposed definition under the draft Regulation specifically refers to identification numbers, location data and online identifiers (e.g. IP addresses). Under the Act, this information may constitute personal data but it would depend on the circumstances. The draft Regulation clears up any ambiguity over whether this data amounts to personal data.

[3] See Appendix for a comparison of the definitions of "personal data" between the Directive, the Act and the Regulation.

4.1.4 Whilst the definition of personal data under the draft Regulation is wider, it is likely that much of this information is already being treated as personal data in any event and so this may not have a significant impact in practice.

4.1.5 So, if a publisher had a consumer platform and collected personal details (e.g. contact details) by way of registration to the platform, and also used automated means to track user activity and location using cookies, all of this data would constitute the user's personal data.

4.2 **Scope of Regulation**

4.2.1 *Data processors* – The draft Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor within the EU. In contrast to the current Directive, data processors are specifically included within the scope of the draft Regulation.

However, the fact that the Regulation imposes obligations directly on data processors, will not necessarily make life easier for data controllers. In particular, the Regulation also imposes additional obligations on data controllers in circumstances where data processors process personal data on their behalf. By way of example, the draft Regulation requires data controllers to ensure that processors have implemented the necessary security measures to protect that data and requires both controllers and processors to enter into a contract which, amongst other things requires the processor to:

- act only on the controller's instructions;
- comply with equivalent security obligations;
- employ only staff who have committed themselves to confidentiality;
- hand over all results to the controller at the end of the processing; and
- enlist a sub-processor only with the prior permission of the controller.

This is wider than the Act which requires only that the controller enters into a written contract which requires the processor to act on the controller's instructions and implement appropriate technical and organisational measures.

Data controllers will therefore need to review (and where necessary, update) their contracts with data processors to ensure that the appropriate provisions are included.

In addition, there may be circumstances where companies act as both data controllers and data processors (for example, a marketing company may be a data controller in respect of its employee data and personal data which it uses for marketing activities on its own behalf, but a processor where it carries out marketing activities on behalf of clients). Such companies will also need to ensure that they are processing personal data in accordance with the Act where they carry out those processing activities and that they have entered into a contract incorporating the data processing obligations required by the draft Regulation.

4.2.2 *Territory* – The draft Regulation applies to controllers and processors who process data "…*in the context of the activities of an establishment"* in the EU. It will also apply to controllers and processors who do not have *an "establishment"* in the EU but target EU customers. The

Regulation is more explicit than the Directive as regards the targeting of EU customers.

In *Google Spain SL and Google Inc v Agencia Española de Protección de Datos and Mario Costeja González*[4] (the "Google Spain Decision"), the ECJ held that even though Google Spain's activities are confined to sales and marketing, and that all the "processing" (indexing, caching etc.) of personal data was undertaken by Google Inc, in the US, Google Spain's activities were sufficient to constitute processing "*in the context of an establishment in the EU*".

As noted, the Regulation is also more explicit about the activities of non-EU established controllers and processors which will bring them within the scope of the Regulation by *"…the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour."*

Accordingly, the Regulation could have a significant impact on controllers who are not established in the EU but offer goods or services to data subjects in the EU or monitor the behaviour of EU customers (e.g. online providers and ad networks placing cookies or other tracking devices on the equipment of EU data subjects for the purpose of tracking their online behaviour) as such non-EU controllers are also deemed to be within the scope of the Regulation.

For example, if a group company is based in the US and contracts online with EU customers in relation to the purchase of goods, or uses cookies on its website to track EU customers, the US company would need to ensure that it complies with the Regulation.

How organisations operating outside the EU are expected to be aware of the Regulation and indeed, how compliance with it would be enforced against a company operating outside the jurisdiction, is yet to be seen. An example often cited is of a small hotel in Alaska which offers services to customers (who may be based in the EU) – how could the hotel be expected to be even aware that the Regulation exists and to know what is required to comply with it?

4.3 New rights for data subjects

4.3.1 The draft Regulation includes and expands on existing rights available to data subjects. For example, in relation to the right to make a subject access request, the draft Regulation goes further than the Directive and requires the data controller to inform the data subject of the period for which their data will be stored and the existence of their rights to rectification and erasure of personal data. Requests made electronically must also be responded to electronically under the draft Regulation.

4.3.2 *Right to be forgotten*

The draft Regulation introduces new rights such as the "right to be forgotten", which has been the subject of much debate. This would entitle data subjects to request the data controller to erase all personal data relating to them and to abstain from further dissemination of that data. In practice, this means that (subject to certain exemptions) such data would have to be deleted entirely from the controller's system. This is likely to result in a huge administrative burden for many organisations.

---

[4] Case C-132/12 - http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5c27dd7414dea4cc9a92fc392d5e2ce10.e34KaxiLc3qMb40Rch0SaxuNbh90?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=380192

In fact, the Google Spain Decision earlier this year made clear that this 'right to be forgotten' already substantially exists under the Directive. The Court decided that the existing provisions of Article 12 of the Directive, which entitle a data subject to seek *"…rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive*" were sufficient for the Court to decide that this may include an obligation *"to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful."*

The ECJ held that individuals have the right to have search engine results removed where they affect privacy rights. This has huge implications, not just for search engines, but also for social media operators and many businesses with European operations (the EU's broad interpretation of "establishment" extends the jurisdictional reach of EU law to cover organisations outside the EU whenever users in the EU are targeted). This means that content providers may now find themselves with obligations to comply with data protection laws even where they are not involved in making decisions about the online content provided. The ECJ affirmed that publishers are still allowed to publish contested personal data for journalistic purposes. Therefore, whilst an individual may require a search engine operator to erase his data, the content of the webpage would be left unchanged.

The Google Spain Decision reflects a wide interpretation of the present Directive, which incorporates a right of erasure. The draft Regulation expands on this by strengthening and building on the right of erasure and introducing a formal "right to be forgotten". The draft Regulation also requires data controllers to take reasonable steps to ensure that any third party to whom it has passed the personal data, also deletes it.

4.3.3 *Right to data portability*

The draft Regulation also introduces a new right of data portability. This means that the data subject has the right to obtain from the data controller, on request, a copy of all personal data which the controller process by electronic means, in an electronic and structured format which is commonly used and which permits further use by the data subject. The key purpose of introducing this right is to enable data subjects to move their data seamlessly from one online provider to another, without losing any data previously disclosed to an online service or having to re-input such data.

4.4 **Consent requirements**

4.4.1 The draft Regulation requires consent to be "freely given, specific, informed and explicit". For consent to be explicit, it must involve a statement or clear affirmative action, such as clicking a tick box online. Under the current Directive, a distinction is drawn between the level of consent required in ordinary circumstances and where the processing relates to sensitive personal data. Only in the latter case will 'explicit' consent be required.

4.4.2 The requirement for all consents to be explicit will involve the introduction of significant changes by data controllers who will need to review all forms, documents and methods of collecting personal data and implement changes to ensure that all consents will be explicit.

4.4.3 "Consent" plays an important role in the personalisation of data.

4.5 **"Legitimate Interests"**

4.5.1 The first Data Protection Principle will continue to be the requirement that personal data is *"processed fairly and lawfully".* Furthermore, of the various criteria for "lawful" processing, consent will continue to be amongst – if not the – most important.

4.5.2 But it is worth remembering that other criteria include processing which is necessary for the performance of a contract and "….*for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject".*

4.5.3 This weighing of interests was an important feature of the Google Spain Decision. In this case, the Court gave greater weight to the interests of Mr Gonzalez and it has been criticised for that part of its decision by many. But it is worth remembering that in other cases the balance may well lie in favour of the controller or processor. This is what the Court said on this issue:

"*As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question."*

4.6 **Data personalisation**

4.6.1 A feature of 'big data' is the ability of organisations to personalise the user's experience online. The more an organisation knows about an individual and their preferences through that user's online history, the more that organisation can customise the user's experience e.g. "you liked xx, you may like yy".

4.6.2 There are three elements in data personalisation: Tracking > Profiling > Targeting:

- ***"Tracking"*** = the collection of data e.g. Web tracking (IP addresses, Cookies, Javascripts, Browser fingerprinting); location tracking e.g. CCTV, RFID cards for transportation tickets, GPS systems for car navigation; social network tracking e.g. personal data such as name, age, sexual orientation + preference/profile data such as "likes" and "shares";

- ***"Profiling"*** = analysis of those data; and

- ***"Targeting"*** = the activity facilitated by such collection and analysis e.g. via online advertising.

4.6.3 The draft Regulation seeks to limit the extent to which data subjects may be subjected to measures based on automated personal profiling (i.e. the use of personal characteristics or behaviour patterns to make generalizations about a person). Profiling is prohibited under the draft Regulation except in certain circumstances: profiling is permitted where it is necessary for the entering into or performance of a contract, where expressly authorised by law, or with the individual's consent. Individuals must be informed of their right to object to profiling in a highly

visible way.

4.6.4 This means that advertising networks could be prevented from creating extensive and detailed profiles of internet users based on their online behaviour, hence the importance of obtaining the consent of the data subject at the time those data are obtained.

4.7 **Exemptions for journalistic purposes**

4.7.1 Both the Directive and draft Regulation contain derogations from certain of their provisions *"..for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression"*.

4.7.2 The relevant exemption in the Act appears in section 32: "Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material; (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

4.7.3 Recital 121 of the Regulation calls for a broad interpretation of "journalistic" activities which make it clear that it can cover social media outlets as well as conventional press platforms:

"*Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited*
to media undertakings and may be undertaken for profit-making or for non-profit making purposes."

4.7.4 In the report of the Leveson Inquiry into the culture, practices and ethics of the press, Lord Justice Leveson recommended that the ICO should, in consultation with the industry, issue comprehensive guidelines and advice on appropriate principles and standards to be observed by the press in the processing of personal data. The ICO published its Guidance on Data Protection and Journalism in September 2014[5].

4.7.5 It was interesting to note that in the in Google Spain Decision, the Court observed that the exemption for journalistic purposes may have applied to the newspaper publisher but not to Google. The Court observed that "*Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page."*

[5] http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-protection-and-journalism-media-guidance.pdf

4.8 **Data relating to children**

4.8.1 The draft Regulation introduces a definition of "child" which is any person aged below 18 years. Children are given special protection through a number of provisions contained in the draft Regulation. In particular, the processing of personal data relating to a child below the age of 13 shall only be lawful if consent is given or authorised by the child's parent or custodian. The controller must make reasonable efforts to obtain verifiable consent. This is in line with provisions in The Children's Online Privacy Protection Act of 1998 ("COPPA") which requires verifiable consent from the children's parents (subject to certain, limited exceptions) where the child is aged below 13 years.

4.9 **Privacy Impact Assessments**

4.9.1 The draft Regulation impose a new obligation on controllers and processors to conduct an impact assessment before undertaking processing that presents a specific privacy risk due to its nature, scope or purposes. The draft Regulation sets out a non-exhaustive list of categories of processing that fall within this provision, including where organisations are carrying out profiling, an analysis of data on sensitive subjects or mass processing children's personal data.

4.9.2 The risk assessment must be documented and must contain a general description of the envisaged processing operations, an assessment of the risks to the rights of data subjects and a description of the measures envisaged to address those risks. As part of the risk assessment process, the data controller must also consult with the data subjects (or their representatives) in relation to the intended processing.

4.9.3 This provision has been welcomed by the Article 29 Working Party, however, it has criticised the current drafting for being too restricted and recommends that assessments should be required in all cases where processing operations "are likely to" present specific risks.

4.10 **Data minimisation**

4.10.1 Data controllers must only collect and process personal data to the extent that it is adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed. In particular, personal data must only be processed if the purposes could not be fulfilled by processing information that does not involve personal data.

4.10.2 This provision expands on the requirements under the Directive and introduces a more robust data minimisation principle. The intention is to ensure that data controllers do not engage in unnecessary processing activities for reasons of ease or convenience.

4.10.3 In the age of 'Open Data', where Government bodies and public institutions are making an increasing number of datasets available under open licensing terms, data minimisation techniques such as anonymisation are increasingly important. In that context, the ICO recently published its Code of Practice on Anonymisation in November 2012.[6]

4.10.4 The draft Regulation also introduces the concept that data protection measures should be "by design" and "by default", which are intended to support the new data minimisation principle to ensure that new technologies and business models are designed in a way which ensures that the

[6] https://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf

processing of personal data is limited to that data which is necessary to achieve the purpose for which it is collected.

4.11 **International transfers**

4.11.1 Under the Directive, personal data must not be transferred outside the European Economic Area ("**EEA**") without adequate protection. The draft Regulation reflects this position but proposes several changes to the existing regime. This includes introducing a one-stop-shop approval system for Binding Corporate Rules ("**BCRs**") (whereby all data protection authorities within the EU must recognise BCRs approved by any other authority as valid). This gives legal recognition for the first time to the role of BCRs, which, once in place, permit multinational groups of companies to transfer personal data between different members of the group.

4.11.2 The draft Regulation also enables national data protection authorities to pre-approve standard data protection clauses, subject to their being declared valid by the European Commission. Under the current Directive, only clauses approved by the European Commission can be used to establish safeguards in relation to the transfer of personal data outside the EEA.

4.11.3 The Regulation also proposes that a finding of adequacy by the European Commission may refer to a specific territory or processing sector within a non-EU country, rather than the country as a whole (as under the current Directive).

4.11.4 The Regulation also confirms that adequacy decisions made under the Directive, including the US-EU Safe Harbor framework, would remain in force unless amended, replaced or repealed by the European Commission. The Safe Harbor framework enables certified organisations to transfer personal data from the EU to the US in compliance with European data protection laws. Around 3.500 organisations are Safe Harbour certified. There have however been various criticisms of the Safe Harbor framework in recent years and so it remains to be seen whether this will be repealed.

5 OUR TOP 10 "PRACTICAL POINTERS"

(1) **It is not too early to start thinking about the proposed Regulation** - The Regulation is in draft form and is due to be finalised next year, hopefully coming into force in 2017. However, it is important for organisations to start considering the potential impact of the Regulation now and ensure data protection is given a more prominent and pro-active role in terms of compliance, to ensure a smooth transition when the Regulation does come into force. Conducting a data protection audit is an essential part of this process to identify current levels of compliance (or non-compliance) as well as an overview of data processing activities carried out within the business.

(2) **Data processors beware** – If your organisation processes personal data on behalf of another company, particular care needs to be taken as the draft Regulation will also apply to you.

(3) **Review your contracts** - If you permit third parties to access and process personal data, start reviewing your existing contracts to identify what contracts will need to be updated. Where data processing agreements are being entered into and will continue in force until 2017, consider future proofing them to avoid having to revisit them once the Regulations comes into effect.

(4) **It doesn't matter if your organisation is established the EU or not** – Non-EU data controllers offering goods and services to EU customers, or monitoring EU customers, will still be caught by the Regulation. This will also have an impact on group companies (for example where the

parent company is based outside of the EU).

(5) **Dealing with the expansion of the rights of data subjects** – Consider what changes will need to be made to your organisation's processes to take into account the changes relating to subject access, data portability and the right to be forgotten?

(6) **Are your consents adequate?** – Consider whether the consents which your organisation currently obtains in order to legitimize the processing personal data are "explicit". In particular, have you thought about subsequent uses of the personal data beyond those for which the data was originally collected? Care should be taken where consent from children is required.

(7) **Assess the risks** – Are you carrying out adequate risk assessments before processing personal data? This is required by the draft Regulation.

(8) **Consider how much personal data you are collecting and processing** – Is it adequate, relevant and limited to the minimum necessary in relation to the purpose for which it is processed?

(9) **Could you demonstrate compliance if requested?** – If you do not have adequate processes, policies and procedures in place to ensure compliance and to be able to demonstrate compliance with the Regulation, you will have a lot of work to do. Start now!

(10) **Board issue –** does your Board see your data protection strategy and policies as integral to your brand? If not, can you push it up the agenda?

Shoosmiths LLP

10 December 2014

t 03700 86 87 88 w www.shoosmiths.co.uk

APPENDIX

Definition of "personal data" under the Directive:

"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Article 2 (a)).

Definition of "personal data" under the Act:

"personal data" means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Section 1(1)).

Definition of "personal data" under the draft Regulation:

"personal data" means any information relating to a data subject; and

"data subject" means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (Article 4).

Aisling Duffy
Head of Data Protection
Senior Associate

T: 03700 865089
E: aisling.duffy@shoosmiths.co.uk

Laurence Kaye
Partner
Publishing & Digital Media

T: 03700 868335
E: laurence.kaye@shoosmiths.co.uk

Joanna Davis
Solicitor

T: 03700 865033
E: joanna.davis@shoosmiths.co.uk