HUNTON& WILLIAMS

RESPONSE TO MINISTRY OF JUSTICE REVIEW OF THE BALANCE OF COMPETENCES IN INFORMATION RIGHTS

HUNTON & WILLIAMS

1. INTRODUCTION

Hunton & Williams appreciates the invitation to respond to the UK Ministry of Justice ("MoJ") review on the balance of competences in information rights (the "Review"). Hunton & Williams has a leading global privacy and data protection practice, of which our UK office is a part.

This response has been prepared by lawyers from our London team ("we" "the team") from the UK and EU perspective and represents the view of team members. The response is made from our position as legal experts in the field having a knowledge of common practices in industry and business. One of our team also had the benefit of attending a workshop on the topic organised by the MoJ in April 2014. We have not conducted any surveys on the questions posed in the consultation.

In responding to the Review we have taken into account the perspective of individuals as citizens as well as consumers. Rights to access information are important for citizens to exercise democratic choices and participate in public decision-making; rights to protect the personal privacy of individuals are important to support their autonomy and dignity.

2. OVERVIEW ON EXISTENCE AND EXERCISE OF COMPETENCE

The specific questions raise two separate issues: the existence of EU competence and the exercise of that competence.

For the reasons set out below we consider that the current allocation of competence in the two focus areas is the appropriate one. We do not consider that there are grounds on which to seek the "repatriation" of data protection to national competence. Equally we consider that there are no cogent reasons to extend EU competence to rights of access to information held by UK public bodies. We do, however, voice some concerns about the exercise of EU competence in the area of data protection, particularly the movement towards more prescriptive rules in the General Data Protection Regulation ("GDPR").

3. EXISTENCE OF EU COMPETENCE

We would suggest that the more consensus there is across the EU on a topic, the more acceptable EU legislation is likely to be to all Member States, including the UK. If EU legislation echoes national attitudes and values we are likely to be more accepting of EU rules in the area. Conversely, where there are wide differences between norms and attitudes in different Member States, any EU legislation will be unacceptable to some countries.

In our experience there is a higher degree of commonality between norms and attitudes in Member States in relation to the protection of informational privacy than there is in the area of access to information (outside the specific obligations imposed by the access to environmental information regime).

Some Member States have strong traditions of openness, for example Scandinavian countries, whereas others have traditions of secrecy in public administration. There are also significant differences in the way that privacy and openness are balanced where there is a tension between these two values, for example where subject access requests are made for information which includes personal data or in the application of exemptions in national data protection legislation to protect freedom of expression.

In relation to informational privacy we consider that there is a particularly strong consensus in relation to those provisions which deal with "information rights" proper, by which we mean the rights given to individuals and the mirror obligations on data controllers; a stronger consensus than there is on other issues such as cross-border transfers.

This may be attributable to the influence of supra-national instruments which have been in place for a long time, in particular the right to respect for private and family life in Article 8 of the ECHR and the individual rights enshrined in Council of Europe Treaty 108 ("Treaty 108"). The fact that most of the individual rights are long-standing and pre-date Directive 95/46/EC ("the Directive") can be seen by comparing the specific information rights under the Directive and under Treaty 108. Treaty 108 includes rights to subject access and to rectification of incorrect information. The "additional" rights provided by the Directive, i.e. which arise specifically as a result of the exercise of EU competence, are relatively limited. On our analysis they cover the following:

- Coverage of some manual information;
- Specific requirements to give data protection notices (Articles 10 and 11 of the Directive) (although Treaty 108 includes a general obligation to be fair which has been interpreted as a requirement to give adequate information);
- Right to know the logic of decision-making by automated means as part of the right of subject access;
- Rights to object to processing, both generally and in the context of direct marketing;
- Rights to object to automated decision-making; and
- The right to compensation for processing causing loss/distress

None of these rights appear to be particularly contentious across the EU. The right to object to processing for particular purposes has been given some prominence and is giving rise to debate following the decision of the CJEU in *Costeja*[1] but we suggest there remains a solid core of rights which are broadly supported across the EU.

[1] Case C 131/12, Preliminary ruling of the CJEU on *Google Spain SL, Google Inc.v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

Clearly the obligation to comply with the Directive means all Member States have data protection laws with a high degree of commonality but laws operate in wider national contexts; they operate in a context of values. Our perception is that there is a shared recognition across the EU that the protection of the privacy of personal information is important. There are strong differences of view around how that is best achieved but the principle is accepted as a European value.

In the area of access to information, apart from the specific provisions on access to environmental information, there appears to be less uniformity. Scandinavian attitudes to the availability of information appear to be very different from those of some of the Member States in the south and east of the EU. There is not the same sense of a shared value as exists in respect to the protection of privacy, let alone commonality of approach to supporting that value in practice.

A further issue of relevance to the appropriate allocation of competence is the relationship with other areas of regulation. Online commerce and other online activities give rise to increasingly complex issues, many of which have an international element. These intersect with data protection regulation, for example the regulation of e commerce raises questions about the security of applications, the uses of customer data, the extent of information obligations to customers and rights of remediation. These have synergies with aspects of data protection law. There are advantages in having a common level of competence for these areas. The possibility of overlapping or contradictory requirements would be increased if some linked areas rested in national competence and some at EU level.

In the area of access to information, however, there appears to be less risk of overlap with other areas of regulation. It is also our experience that businesses are far more impacted by data protection legislation than by rights of access to information, the burden of which tends to fall mainly on the public sector. We recognise that access rights in respect of environmental information can impact private sector organisations but these tend to be in specific sectors and of limited numbers. Businesses which operate across multiple jurisdictions are particularly impacted by differences in data protection laws in different Member States.

For all these reasons we would support the current allocation of competences as the correct one.

4. EXERCISE OF EU COMPETENCE

The question of the exercise of EU competence only applies to data protection regulation. Although we take the view that EU competence is appropriate in this field we would voice concerns over aspects of the exercise of that competence.

The first concern is that, in some areas of activity, under the current Directive the rules are applied differently in different Member States. These differential impacts do not derive from different interpretations of the Directive but arise because of national administrative arrangements. The most straightforward example is the different way model clauses are handled in different jurisdictions. These are contracts entered into by businesses in the EU and businesses outside the EU to govern the standards that will apply to protect the personal data sent outside the EU. They are standard form

contracts which have been approved by the EU. The Directive does not mandate any administrative requirements for the use of these contracts. Several Member States, including the UK, impose no additional administrative obligations, but others require prior approval, registration or subsequent ratification by local regulators. Businesses have to work out which rules apply in which jurisdictions and ensure that they are followed. It is a time-consuming and often costly exercise which does not improve the protection of individuals' personal data..

The difficulties this presents for business are caused by national requirements and not the Directive. They reflect different attitudes towards regulation, risk and control. We are conscious that, if data protection were repatriated to national competence, businesses could face significant additional administrative burdens in dealing with data uses and transfers from some EU jurisdictions.

The second area of concern is the approach taken in the GDPR. The development of international instruments in the field has demonstrated a steady movement from reliance on high level principles to reliance on detailed specific rules. Both the OECD Guidelines and Treaty 108 are short texts which focus on setting the guiding principles at a high level. The Directive added more specific rules to the principles e.g., Articles 10 and 11 on notice to data subjects, but the high level principles remained the core of the text. Under the GDPR, although there are differences between the two texts, both the Commission draft and the Parliament-approved text have shifted decisively towards process-focussed regulation. There are some areas in which the GDPR includes a risk based approach, where a level of risk to individuals' privacy determines the level of compliance, or the applicability of certain provisions of the law. Nevertheless, taken as a whole, the GDPR increases the level of detailed rules on process, for example in relation to record-keeping, documenting developments, providing specified detail in notices to individuals, submitting new initiatives for prior inspection or approval.

This gives rise to a number of concerns:

- it will be increasingly difficult for SMEs to understand and comply with their obligations – the exemptions for SMEs are in reality minimal;
- data protection may become a "tick-box" exercise of compliance in which the details will obscure the fundamental principles;
- regulators with limited resources will be forced to concentrate on the process requirements rather than focussing on serious problems;
- the regime will struggle to be responsive as it will become increasingly difficult to interpret the law to deal with the unknown changes technology will bring (the *Costeja* case demonstrates that generally drafted provisions can be applied to deal with changing technology);
- individuals will find the regime difficult and hard to understand/access; and
- the critical importance of the proportionality test will become obscured by the burdens of the process.

The different attitudes to the imposition of additional formalities and the different positions taken in negotiations over the GDPR illuminate the differences between attitudes of regulators and legislators from different jurisdictions.

Our comments, of necessity, have to become increasingly tentative. This is the domain of the social scientist not the law firm, but we hazard that one of the features of the UK regulatory approach is a willingness to trust organisations to follow a degree of self-regulation. Organisations are allowed to take a risk based approach and arrange their own affairs as long as they comply with the law, deliver the right outcomes and take responsibility for their actions, including the possibility of enforcement. In other words they must be accountable.

In the past several years, significant progress has been made in data protection debates to recognise the accountability principle. However, in our opinion, the GDPR has not moved sufficiently towards this approach. Effective compliance and prioritisation is in the interest of organisations, individuals and regulators, too. In the era of digitalisation and ubiquitous information, Big Data and the Internet of Things, data protection regulation needs to be supplemented by flexible tools and concepts, such as organisational accountability and risk-based approach to regulation, implementation and enforcement.

5. RESPONSE TO SPECIFIC QUESTIONS

In responding to these questions we have dealt with the entire data protection regime, not only those aspects that apply to information rights properly understood.

5.1 *What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?*

Impact of the Data Protection Act 1998

Overall we would comment that data protection regulation has provided a societal benefit by the imposition of standards of governance which support a balanced, fair and democratic society. All data is important to our post-industrialised society and personal data has become increasingly important. Its regulation has fostered an environment in which business or public sector bodies cannot use the power of data unfairly or inappropriately or without accountability. It has helped to create and maintain trust. It is not perfect and there are circumstances in which its workings are problematic but this is the case with all human laws and systems.

Advantages to business and public sector

- Recognition of the importance of security and focus on ensuring that outsourced arrangements have appropriate security provisions built-in;
- Focus on quality of records and records/information management leading to efficiencies and improved services;
- Recognition of the value of data as an asset and part of the relationship with consumers/customers; and

- Increase in transparency and resulting consumer/customer/public trust.

Advantages to individuals

- Rights to see/correct information, for example, incorrect credit records or records of convictions;
- Increased understanding of the way that information is used;
- Rights to object to being sent marketing materials; and
- The imposition of some restrictions on the unfettered disclosure or use of personal data about individuals.

Disadvantages to business and public sector

- The use of statutory rights to make subject access requests by claims firms and other "ambulance chasers". Business are obliged to deal with such requests and cannot refuse to deal with them or limit the impact, causing significant costs to business;
- The creation of a risk-averse approach to data uses which might be beneficial in the public sector, although this must be balanced against the benefit of restraining inappropriate disclosures; and
- Restrictions on the international flow of personal data where there is no evidence of harm through the requirement for the adoption of expensive, bureaucratic rules such as Binding Corporate Rules. While, we support BCR as an accountability mechanism, we note that the current approval system carries too much administrative burden. It is not scalable for the future, when many organisations may want to use this mechanism including SMEs.

Disadvantages to individuals

- The misuse of data protection by some businesses to hide behind, "Can't tell you that, it's data protection";
- The difficulty of using the right to object to processing (other than in relation to direct marketing) because of the threshold imposed by the UK implementation of the Directive (although recent case law from the CJEU has altered the position, at least in a limited range of cases); and
- The difficulty of claiming compensation for misuse of personal data because of the requirement to prove actual damage before a claim may be made (although recent judgments from UK courts have indicated that this may not be interpreted as strictly in the future as it has in the past).

5.2 *What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals' data protection rights and the pursuit of economic growth?*

This raises a difficult question of balance. There is no simple dichotomy or trade-off between the protection of individuals and the pursuit of economic growth. Regulation may be seen as a brake on development or a barrier to it in the short term but this can

be a false perception and, in reality, the absence of regulation/standards can lead to significant costs in the future, whether economic costs or societal costs. Examples are industrial developments that leave poisoned earth, air or rivers or cause disease or disfigurement, or working hours that put intolerable strains on families.

As noted earlier our evaluation is that there are sound justifications in favour of EU competence in this area. The question of whether the way it has been used to date has been appropriate is more nuanced.

We have already marked the growing tendency towards imposing detailed rules rather than relying on high-level principles and the absence of accountability mechanisms. We would repeat the example given of the way that the transfer of personal data outside the EU is handled. We have referred to this in Section 4 above. We are wholly supportive of the need to protect the security of personal information and to restrict its inappropriate dissemination. However, the mechanism adopted by the Directive, which is to impose a block on transfers unless they can fall under specified grounds or are subject to specific safeguard processes, such as the use of model clauses as described earlier, is not proportionate to the risk of transfer in most cases. We would draw attention to a paper published by the US Chamber of Commerce and available on our website www.huntonprivacyblog.com, Business without Borders, which highlights some of the problems that inappropriate restrictions on data transfers cause for businesses.

A focus of economic growth is in the digital economy and in the increased use of big data to drive developments (often not personal data but we concentrate on personal data for these purposes). It is doubtful if the current rules (or indeed the GDPR) are well equipped to deal with the challenges of Big Data. It is not clear how far the emphasis on consent and purpose limitation will impact on Big Data, how far the use of anonymisation will facilitate proper use of personal data and whether we will be able to strike the right balance to help achieve the societal and economic benefits promised by Big Data.

5.3 *What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?*

In order to respond to the question it is necessary to formulate the nature of the challenges posed by the list of developments. A glance at the challenges shows that the Directive is only one piece of legislation which contributes to dealing with these challenges and in the case of online commerce is not the most significant one. This illustrates a point made earlier which is the inter-relationship between data protection legislation and other areas of regulation.

Increased international flow of data – challenges are to the security of the data in transit, the control of the data, the need to ensure that traffic in data can flow smoothly and swiftly but with adequate security and control. The current regime imposes controls on transfers of personal data outside the EEA which place unnecessary burdens on business (see comments Section 5.2 above)

Technological developments – by the very nature of the term these are not known quantities. The challenges are that the law should be able to provide adequate protection for privacy and security while allowing the development and implementation of new business models/technologies. The development of mobile services, online services and services based on location data have proved particularly difficult to control and police. Control of electronic communications data including location data is exercised under the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR")[2]. While we understand this is because historically the regulation of e communications has been part of the regulation of telecommunications, we are concerned that the regulation of mobile privacy sits outside the core data protection legislation. It is moreover difficult to enforce and there appears to have been little enforcement through the EU.

Online commerce – particular challenges are the international nature of online commerce and the need for security of transactions. In our view the regulation of online commerce within the EU has been effective from a consumer perspective. The challenge of controlling dishonest or fraudulent behaviour taking place outside the EU is not one that data protection law can be expected to tackle.

Social networks - the disclosure of information outside groups of friends, rights to remove information, harassment and misuse e.g. trolls, revenge porn, abusive images, use for grooming. This is an area in which there is huge interplay between privacy concerns and other areas of regulation. There are deficiencies in our view in the control of abuse, grooming and harassment, all of which are within national competence. Data protection has only a limited role to play in this field, largely limited to rights to supress information. Historically the right to remove information has been limited but recent case law from the CJEU has changed the picture.

Overall our view is the regulation of these areas involves many different areas of law and social challenges. The regulation of data protection is only one small part of that bigger picture. It is difficult to gauge the extent to which the Directive and PECR can contribute to effective regulation. They appear to have been little used enforcement mechanisms but this may be due to the difficulty of enforcement across national boundaries.

5.4 *What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?*

This is by its nature a speculative question. The final text of the GDPR is not fixed, the matter is still under negotiation. The mechanism for cross-border enforcement has not been agreed nor have the controls on cross border transfer of personal data. These have the potential to impact significantly on business. There is no evidence to which we can usefully point in relation to this question.

5.5 *What evidence is there that the right to access documents of the EU institutions has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?*

[2] SI 2003/2426

We would start from the presumption that all rights of access to information held and used as part of public administration are positive, assuming that there are proper exemptions to protect legitimate areas of public interest in place and that these are properly applied in practice.

5.6 *How would UK citizens' ability to access official information benefit from more or less EU action?*

The UK's Freedom of Information Act appears to set a higher standard of openness and transparency for the public sector than the provisions that cover the EU institutions. It would be desirable for the standards in the EU to be raised to those in the UK. It would be undesirable for the UK standards to be lowered to those of the EU.

5.7 *How could action, in respect of information rights, be taken differently at national, regional or international level and what would be the advantages and disadvantages to the UK?*

This is a substantial question. We can make only the most brief response. As noted in earlier responses, we do not consider that the regulation of data protection in the connected world should, or indeed could, be moved to national, let alone a regional level. The major challenges facing international regulation of data protection are the differential standards of protection which are applicable and the barriers which this can present to legitimate and appropriate transfer of data[3]. The current initiative of dialogue between the US and the EU is an area to be encouraged.

5.8 *Is there any evidence of information rights being used indirectly to expand the competence of the EU? If so, is this advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?*

The GDPR would expand the territorial reach of EU law in the area of data protection to cover those organisations based outside the EU which target or offer services to residents in the EU. The effect of this will be to give regulators in the EU competence to regulate data controllers based outside the EU. It will also enable residents in the EU to take legal action against data controllers based outside the EU. This has potentially a beneficial effect on UK citizens and businesses. It provides UK citizens with remedies that they would not otherwise have and contributes to a more level playing field between UK and non EU businesses. While it may not technically be an expansion of competence, it strikes us it would be politically difficult for the UK alone to claim such an extension of territorial scope by using purely national legislation.

5.9 *What is the impact on EU competence of creating an entirely new legal base for making data protection legislation that is not expressly linked to the EU's single market objectives?*

The new basis in Article 16 of the GDPR is oddly worded and we consider that there remains a possible argument that it does not provide a basis for the regulation of data

[3] APEC Privacy Guidelines, OECD Guidelines, Treaty 108, Directive 95/46/EC

protection in the private sector. We have queried it with the Commission's legal service. There is a firm view in the Commission that Article 16 is a sufficient ground and the point appears to have been accepted without challenge by Member States. We remain of the view however, that it leaves some room for uncertainty on competence and it would have been reassuring to have a clearer basis.

5.10 *What future challenges or opportunities in respect of Information Rights might be relevant at a UK, EU or international level; for example cloud computing?*

We would highlight the threat of "cyberinsecurity" as the most daunting challenge facing all data owners and users internationally.

5.11 *Is there any other evidence in the field of EU Information Rights that is relevant to this review?*

In our response to this question we have made some general comments on the areas covered by the Review.

We appreciate that any consultation on competence must in some way limit the boundaries of the exercise or it will become impossibly unwieldy. Nevertheless in this case we question whether a more suitable boundary could have been drawn or the exercise could have been given a more generic title.

The term "information rights" is generally applied to the rights which are exercised in relation to information and to the mirror obligations to which organisations are subject to as a result of those rights. The rights include the right to respect for private and family life as far as that right touches upon information, rights to freedom of expression and rights to the privacy of electronic communications. It can also cover rights to protect against defamation or the misuse of private information. We have noted that the review has not addressed the question of confidentiality of communications or of retention of personal data. We have completed the specific questions by reference to the data protection regime but would flag that it would perhaps have been more useful to have included the wider area of information law in the review, particularly in relation to interception of communications and retention of communications data.

……..

Disclaimer

This material is provided by Hunton & Williams' London Data Protection and CyberSecurity Practice. It represents the views of lawyers in the practice with experience in this area. The response is not made on behalf of any clients nor does it represent the view of any clients. It does not comprise legal advice and should not be regarded as such.

Hunton & Williams

Hunton & Williams is a full-service international law firm of more than 800 attorneys. The firm's Global Privacy and Data Security practice is a leader in its field. It has been ranked by Computerworld magazine for four consecutive years as the top law

HUNTON& WILLIAMS

firm globally for privacy and data security. In the UK, Hunton & Williams' is recognised in Chambers UK as a leader for data protection.

We have a leading privacy blog (www.huntonprivacyblog.com) and a site dedicated to the European Commission's proposed Data Protection Regulation (www.huntonregulationtracker.com).

Hunton & Williams is recognised as a "thought leader" on international privacy issues through its Centre for Information Policy Leadership. The Centre provides strategic leadership and consulting on all aspects of global information policy, privacy and security and is internationally-recognised with active participation by more than 40 leading multinational corporations, see www.informationpolicycentre.com.

The firm's 19 offices in Europe, the United States, and Asia serve clients in more than 100 countries. Further information about our firm can be found at www.hunton.com.

London Data Protection and Privacy Practice Contacts

Bridget Treacy – Partner

Rosemary Jay – Senior Attorney

Anita Bapat – Associate

Telephone - 0207 220 5700 30 St Mary Axe, London EC3A 8AP

……..