Consultation Response to Article 29 Working Party Working Document on Draft Ad Hoc Contractual Clauses “EU data processor to non-EU sub-processor”

July 2014

1. INTRODUCTION

Hunton & Williams and the Centre for Information Policy Leadership at Hunton & Williams ("Centre") appreciate the invitation to respond to the Article 29 Working Party ("WP") Working Document 01/2014 on a set of draft ad hoc contractual clauses ("clauses") to be applied between an EU data processor and a non-EU sub-processor. Hunton & Williams has a leading global privacy and data protection practice with offices in the US, Belgium, China, and the UK. The Centre is a leading global privacy and security think tank, with members that are global businesses and committed to using personal data responsibly. This response has been prepared jointly by lawyers from Hunton & Williams and Centre leadership ("we" or "the team"). One of our team had the benefit of attending a workshop on the topic organised by the Research Centre Information, Law and Society ("CRIDS") in Belgium. We have also consulted clients of Hunton & Williams and Centre members and this response includes their feedback. Nothing in this response should be construed as representing the views of any individual client of Hunton & Williams or Centre member.

2. GENERAL COMMENTS

We generally welcome the concept of developing standard clauses for the transfer of personal data from processors in the EU to processors outside the EU. Standard form clauses are an important tool in delivering compliance for businesses and supporting the rights of individuals. In the modern information age with ubiquitous data flows, businesses need a spectrum of different legal mechanisms and tools to legitimise transfers of personal data across borders to controllers, processors and sub-processors in accordance with European data protection law. It is also important that such legal mechanisms remain flexible in order to cater for many different scenarios of data transfers and that they remain commercially and legally viable in order to be widely adopted by all organisations (controllers, processors and sub-processors). Finally, it is essential that these mechanisms also result in real and effective protection for individuals on the ground.

However, we consider that many important issues of policy and approach need to be considered, debated and resolved before further drafting is undertaken. We therefore recommend that a transparent public consultation process is organized to explain the issues and decision points to all relevant stakeholders. It is particularly important that any consultation material should be accessible to consumer groups, interested individuals and SME representative organisations.

Although we understand that the Working Document only captures the state of play of the current reflections of the WP, we have been mindful of the perspective of individuals as well as businesses. The rights of individuals to privacy and data protection are guaranteed by the EU Charter of Fundamental Rights. It is important for reasons of transparency and good regulation that individuals are able to understand the mechanisms by which their rights are being protected. Among other benefits this ensures that they are empowered to exercise
those rights where appropriate. We consider it should be a touchstone of any draft contract of this nature that it should be accessible to and understandable by individuals and not just legal experts in data protection.

3. POLICY CONTEXT

The EU is currently going through the legislative process of updating the European data protection regime. The General Data Protection Regulation (“GDPR”) and the Directive on Data Protection (“Directive”) have been approved by the European Parliament. It is anticipated that the Counsel will achieve agreement on its approach in the coming months and it is forecast that package should be agreed in 2015. The GDPR and the Directive will bring significant changes to the relationship of data controller and data processor. Any work on new standard clauses at this point in time should take account of the provisions of the GDPR and the relevant Directive. In particular, the new regime will impose significant new and broader direct statutory obligations on all processors. This is likely to change the rationale for making use of the existing controller-processor Model Clauses and will certainly impact the content of the proposed clauses.

It is apparent from our analysis that the clauses would:

a. Place data controllers and data processors within the EU under contractual obligations (via the proposed Framework Contract) which are far in excess of those required in order to comply with Article 17 of Directive 95/46/EC, as transposed (differently) into EU Member State law. The proposed clauses thus introduce a higher standard for controllers and processors, which is likely to open the door to extensive legal debate; and

b. Create a new type of Model Clauses which impose obligations that are more onerous than those imposed under the current Commission-approved Model Clauses for the export of personal data outside the EU.

These are challenging outcomes that will likely be a disincentive for businesses (both controllers and processors) to start using the proposed clauses. While the clauses will be unattractive to many businesses, regulators may bring pressure to bear on businesses to make use of the clauses. The clauses could therefore have far-reaching impacts.

4. STRUCTURE OF THE CLAUSES

It is a condition of use of the clauses that the controller and the head processor enter into a new form of standard contract, referred to as the “Framework Contract.” Although the Framework Contract seems to be based on the existing Model Clauses for the transfer of personal data outside the EU, it is structured differently and incorporates further and more onerous obligations.

Under Directive 95/46/EC clear obligations are imposed on controllers in the EU who use the services of processors in the EU to enter into written contracts which include stipulations that the processor shall act only on the instructions of the controller and shall meet the appropriate security standards. There is no requirement on such controllers to use a standard form contract. Under the proposed clauses, however, the controller and processor within the
EU would have to contract using a standard form Framework Contract. We believe there is really no need to have such a Framework Contract, as controllers are already legally obliged to make sure that they have a written agreement with their processors in accordance with Art. 17 of Directive 95/46/EC.

Directive 95/46/EC does not impose an obligation on a processor who uses a sub-processor to engineer a direct contractual relationship between the data controller and the sub-processor, nor is such an obligation imposed under the existing Model Clauses for the transfer of personal data outside the EU. Under the Framework Contract, a wholly new obligation is imposed on the head processor that it make the clauses “binding towards” the data controller through a specific reference to the clauses in the Framework Contract. The obligations of the parties under the Framework Contract (both those which apply to the controller and those which apply to the head processor) are recited fully in the clauses under a provision that the head processor “agrees and warrants” to the sub-processor that it has entered into a Framework Contract on such terms. The aim appears to be to create direct contractual relationships between all the parties in the processing chain. This gives rise to a number of issues as follows:

a. We do not consider that the aim has been achieved. At least in UK law a reference to a set of clauses in a contract will not have the effect to bind a party to such clauses; in the clauses the head processor is providing a simple warranty that it has entered into a contract as described. There is not even a warranty that the contract remains in existence, has not been terminated and will be maintained, which could have some value;

b. The benefit of a direct contractual relationship between the controller and the sub-processor is not apparent, particularly given that the sub-processing contract will cascade down all the relevant obligations and that third party rights are provided for in the draft;

c. Commercially we can see no justification for creating a direct contractual relationship in every case. If there are specific commercial reasons in particular situations to justify a direct contractual relationship one can be created by the parties. There is no reason to build it into the structure; and

d. It is not practicable given that head contracts and sub-contracts are likely to be entered into at different times and may be of different duration.

The Framework Contract is based on existing Model Clauses, which impose significant contractual obligations on the parties because they are designed to be used where personal data are being transferred from the EU to jurisdictions where the law does not offer adequate protection. By contrast the Framework Contract would be used within the EU by parties subject to EU law. We do not consider that the provisions of the existing Model Clauses are appropriate for use between parties subject to EU law. We further wish to express serious concern that controllers and processors who are fully compliant with existing law would be unable to benefit from the clauses because their contractual agreements do not meet the stringent standards of the Framework Contract.
5. COMMERCIAL ISSUES

As noted above, the proposed clauses are not coherent with commercial reality considering that:

a. They sanction unwarranted intrusion into business confidentiality by forcing the parties to disclose commercial information even when it is not necessary to support the rights of individuals;

b. The structure, under which a direct contractual relationship is envisaged between all the parties in the chain, would introduce uncertainty and room for dispute between the parties. A processor could well seek to shift responsibility for a sub-processor on to the data controller on the grounds that the data controller has a direct relationship with the sub-processor;

c. The requirement for the provision of information about the controller in Appendix 1 will often be impossible to complete, particularly in cloud computing environments where often agreements will already be in place between processor and sub-processors before the data controller enters the picture;

d. The complexity of the clauses and the lack of flexibility mean that they will not be acceptable as part of wider commercial contractual negotiations.

6. DRAFTING ISSUES

The proposed clauses as they are currently drafted are unnecessarily complex, making them inaccessible even to specialist lawyers. Moreover, there are some technical concerns, for instance:

- Substantive standards have been incorporated into the definition of “technical and organisational security measures”. This copies out Article 17 of Directive 95/46/EC, but the substantive obligation should be included as an obligation and not as part of the definition;

- Some terms are confusing, for example “data exporter” has one meaning in the existing Model Clauses but a different meaning in the proposed clauses;

- The definition of sub-processor is qualified by requirements around written contracts etc. The definition should cover all sub-processors who process personal data. The substantive obligations to enter into contracts etc. should not be in the definition;

- Under clause 1(f) it is provided that in the event of a “conflict” between the security requirements of the law of the country where the head processor is based and that of the country where the controller is based then the sub-processor must comply with the law of the head processor’s jurisdiction. We do not consider that this is in accord with Directive 95/46/EC and the relevant law should be that of the controller.

This document is not intended for publication or distribution
A number of clauses recite that one party or another has complied with very specific provisions of national law which implement Directive 95/46/EC, for example, over the submission of contracts. A general warranty that the party has met and will continue to meet all the requirements of national data protection law would cover this.

7. THIRD PARTY RIGHTS

Under the existing Model Clauses data subjects have rights against the data controller as third party rights under contract terms as well as having direct rights under national law. They also have third party rights against the processor under the contract where the controller has disappeared and rights against subsequent sub-processors which have become parties to the clauses. The Model Clauses also provide that if a sub-processor is appointed who does not become a party to the contract the data subject should be given third party rights against the sub-processor under the subcontract between the head processor and the sub-processor. The controller is not given any third party rights against the sub-processor.

Under the proposed clauses, however, the third party rights are more complex:

a) Under the Framework Contract (as recited in the clauses) data subjects will have rights against the data controller for any breach of the obligations under the Framework Contract, including any breach of the contract attributable to the head processor or any sub-processor;

b) Under the clauses data subjects have third party rights against the head processor and subsequent sub-processors if the controller has disappeared. This could only be effective if the controller is made party in some way to the contract between the head processor and the sub-processor. However, this approach is not workable in multi-processor arrangements where sub-processors may be processing personal data for a vast number of controllers;

c) It is implicit (but by no means clear) that the data subjects are also intended to have rights against the controller under the clauses, although again this would require the controller to be a party to the contract;

d) The structure of third party rights is not clear. For example, it is not clear why the controller requires third party rights against the head processor under the clauses as the controller and head processor will be in a direct contractual relationship.

We strongly recommend that any further draft clauses should be accompanied by a clear explanation of the desired outcome in respect of the third party beneficiary provisions.

8. PRECEDENTS

We have not been able to trace any precedents adopted for the draft other than the existing Model Clauses. However, at least one supervisory authority in the EU (the Spanish DPA) has produced standard form clauses for use between EU based head processors and non-EU based sub-processors. We would recommend that any further work should take account of
this precedent, how it has been used and the experience of businesses and the DPA in using them.

* *

*   *

This document is not intended for publication or distribution