Model clauses and alternative routes: global vendors

The European Commission adopted a Decision in February introducing a new set of model clauses for transfers of data to processors based outside the European Economic Area (EEA). Eduardo Ustaran, Partner at Field Fisher Waterhouse, examines the key obligations and discusses possible alternatives to model contracts.

When, in 2004, the European Commission approved the alternative model clauses for transfers of data to controllers based outside the EEA, this was hailed as a victory for common sense data protection. The alternative controller-to-controller clauses were regarded as a blueprint for pragmatism in the area of international transfers of personal data. Not surprisingly, the momentum created by this development was quickly seized by those involved in international outsourcing and a project to devise an EU approved set of clauses for transfers to processors started to take shape.

In October 2006, a consortium led by the International Chamber of Commerce (ICC) and supported by the American Chamber of Commerce to the European Union in Brussels (AmCham EU), the Federation of European Direct and Interactive Marketing (FEDMA), and the Japan Business Council in Europe submitted a formal proposal for a second set of alternative model clauses to the European Commission. Four years later, and despite the efforts that have taken place behind the scenes, the standard contractual clauses for transfers of data to processors based outside the EEA approved by the Commission have failed to meet expectations. Whilst the 2004 controller to controller clauses introduced some significant changes to the scope of the parties' obligations compared to the original version, the new controller to processor clauses do not include any discernible changes in that regard.

The big novelty in the new standard clauses is the recognition that a modern outsourcing relationship does not involve just two parties, but a chain of service providers that perform different roles. That alone deserves some credit, as it legitimises the power of a processor to subcontract its services and ends an unhelpful taboo.

However, 21st century outsourcing relies on flexible relationships and constant transformation. Unfortunately, this is not supported by the rigid approach of the model clauses and, as a result, the new clauses are nowhere near the commercially balanced position that the outsourcing industry was hoping for.

Exporter's obligations

The exporter's obligations essentially follow the requirements of the original 2001 model clauses. For example, the exporter must warrant that:

- The processing will continue to be carried out in accordance with the relevant provisions of the exporter's data protection law.
- After assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against all types of risks.
- If the transfer involves sensitive personal data, individuals will be informed before, or as soon as possible after, the data is transferred to a third country not providing adequate protection.

Although there is nothing in those obligations that is more onerous than before, they are far from the easy going amendments of the 2004 controller to controller clauses. Whilst it is understandable that the exporter of the data will have to ensure compliance with the relevant security measures, the wording of the clauses suggests that the controller has to keep a very close eye on the level of protection afforded by the processor. In practice, these are difficult obligations to comply with.

Importer's obligations

A similar pattern – if not worse – can be found in the importer's obligations. So, whilst the controller to controller alternative model clauses included toned down requirements in respect of adverse local legislation and audit rights, the new controller to processor clauses retain the full severity of the original version.

For instance, the importer must process the personal data only on behalf of the data exporter and in compliance with its instructions and the clauses. Furthermore, if the processor cannot provide such compliance for whatever reasons, it must promptly inform the controller of its inability to comply, in which case the controller is entitled to suspend the transfer of data and/or terminate the contract. The reality is that there may be situations when a global vendor may not be able to comply with every obligation under the contractual clauses at all times and therefore, the possibility of immediate termination seems to be a very drastic consequence.

On top of that, the importer's obligations include very strict rules concerning the processor's ability to subcontract some of its services. These rules are part of the different conditions that must be met by the parties to make sub-processing lawful. Under the model clauses,

there are 13 specific circumstances that must take place every time that some aspect of the outsourced service is flowed down to a sub-processor.

Subcontracting

As a result, the jewel of the crown of the new model clauses – the ability to subcontract – is so cumbersome that it hardly solves the problem that it was meant to address. Here is how the process works:

- Before subcontracting any of its processing operations, the importer must inform the controller and obtain its written consent.
- The processor and sub-processor must enter into an agreement with the same obligations as the model clauses and this agreement must be sent to the exporter and, where requested, made available to individuals.
- Then the importer must accept liability for the sub-processor's actions whilst the sub-processor must remain subject to the third party beneficiary clause and to the law of the exporter.
- The exporter must then keep a list of all of the sub-processing agreements and that list must be available to the data protection authority, who will also be entitled to audit the sub-processor.
- Finally, on termination, the sub-processor must return or destroy the data and allow the controller to audit compliance with this obligation.

Needless to say, this approach is unlikely to be accepted straightaway by the majority of global outsourcing service providers. In the context of complex data processing arrangements involving chains of service providers, for example, the step-by-step process of the standard contractual clauses is entirely at odds with the ability to engage different vendors for different aspects of the service without direct involvement of the customer.

The jewel of the crown of the new model clauses – the ability to subcontract – is so cumbersome that it hardly solves the problem that it was meant to address

Alternatives to model clauses

Why the European Commission has gone for the belt and braces approach is not difficult to understand. After 15 years of European data protection law and its prohibition on unsafe data transfers, now it is not the time to start lowering its guard. For that reason, the new model clauses will now fill the gap traditionally occupied by the 2001 controller to processor standard contractual clauses. However, the most sophisticated organisations are likely to move away from standard contractual clauses and explore other more suitable solutions.

One route that may take off in response to the cumbersome nature of the model clauses is the tailored data processing and transfer agreement. Under this approach, the parties negotiate the data protection provisions of their international data processing agreement and rely on their own judgment to procure an adequate level of protection. This may of course work fine in jurisdictions like the UK, where there is no obligation to evidence the arrangement in place by providing a copy of the contract to the data protection authority. Whether that route will work as well in more stringent jurisdictions – where, for example, the authority's authorisation is required – is a different matter. However, many organisations may regard that as preferable to an unsigned and unworkable model contract.

Binding Safe Processor Rules

Whilst the European Commission's decision on the new model clauses makes life difficult for outsourcing services providers, it is encouraging to see that the data protection authorities are prepared to consider other alternatives. In recent years, the EU data protection authorities have encouraged multinationals to adopt internal Binding Corporate Rules (BCRs) based on European standards as a more flexible way of legitimising their global data processing operations. However, the current BCR model has only been applied to cases where companies are 'controllers' of the personal data they process, and not to cases where they are 'processors'.

Now, the Article 29 Working Party is considering extending the BCR concept to processors through Binding Safe Processor Rules (BSPR) – a set of legally binding internal data protection rules that apply to clients' data processed by service providers. Unlike the model clauses, the BSPR can be tailored to the data protection practices of the service provider and, as long as they include the appropriate adequacy standards, they can become a very useful tool for the benefit of international data protection and the outsourcing industry alike.

Eduardo Ustaran Partner
Field Fisher Waterhouse
eduardo.ustaran@ffw.com