Model contract terms - to use or not to use?

Model contracts are one route for complying with the EU's requirements on data transfers. But **Bridget Treacy** questions whether they are practical from a business perspective.

It is now some three years since the European Commission issued its model contract terms governing cross-border transfers of data between EU-based data controllers or controllers and data processors based elsewhere in the world. Initially met by a barrage of criticism from practitioners and businesses alike, the model contract terms are rarely mentioned in the press these days.

So have they come of age as the acceptable standard for cross-border data transfers, or are they simply being disregarded by the business community? And if organisations choose not to use model contracts, on what bases are their data transfers being undertaken? In this article we consider, from a UK business perspective, how the model contract terms bear up to scrutiny.

Model contracts

The principal advantage of the Commission's model contracts lies in the fact that they have been officially recognised as providing an adequate basis for data transfers and those who use them can rely on this fact. It is also helpful that model contract terms address both controller-controller and controller-processor transfers.

However, in the UK, casual observation suggests that the model contract terms are not greatly used in practice. Instead, a significant number of UK businesses tend to use model contracts as a starting point, but then amend and extend their terms. In seeking to understand why businesses are adopting this approach, it is relevant to consider the circumstances in which UK businesses are seeking to transfer personal data abroad. There appear to be three such circumstances:

1. Offshore outsourcing transactions
2. Day-to-day operations of multinational businesses; and
3. One-off transfers (eg. for corporate restructuring or merger activity)

The common feature of the first two circumstances is that they are likely to involve regular transfers of personal data over a sustained period of time, rather than a single transfer, and in those dynamic relationships many businesses regard the model contract terms as being too rigid to accommodate their commercial objectives.

An outsourcing perspective

To illustrate some of the concerns expressed by businesses when dealing with the model contract terms, it may be helpful to consider the context of an outsourcing transaction. Views in this

The legal basis for cross-border transfers

As data protection practitioners will know, the cross-border transfer of personal data from EU to non-EU countries may be undertaken on one of several legal bases.

The starting point is that the country to which the data is to be exported must have an "adequate" level of data protection. Several countries have been officially recognised as providing an adequate level of data protection, such as Argentina, Canada, Switzerland, Isle of Man, and Guernsey.

In addition, Article 26(1) of the EU Data Protection Directive contains several exemptions to the requirement of adequacy. For example:

- where the individual has provided unambiguous consent to the proposed transfer;
- where the transfer is necessary for the performance of a contract between the data controller and the individual;
- where the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the individual between the controller and a third party.

There is also the recognition in Article 26(2) of the directive that an EU member state may authorise a transfer to a country which does not ensure an adequate level of protection where the data controller adduces adequate safeguards. These safeguards may include contractual clauses, but may also involve the assessment of other considerations. In the UK, this process of assessment is promoted by the Information Commissioner's Office as the "Good Practice Approach" to cross-border transfers.

The Safe Harbor arrangements with the US provide a means of ensuring adequacy for certain US businesses. Further, binding corporate rules are yet another mechanism for adducing adequate safeguards.

Additionally, Article 26(4) of the directive expressly contemplates the adoption by the European Commission of standard contract clauses to ensure sufficient safeguards for such transfers. To date, the Commission has published two sets of model contracts, one for controller-controller data transfers, and one for controller-processor transfers.

Further information: http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm.

context can differ significantly, depending upon whether one speaks to an outsource supplier or to an outsource customer. Frequently (and for understandable reasons) suppliers tend to characterise themselves as data processors and then to deal with cross-border data flows on the more limited (and for them less risky) basis of a controller-processor transfer.

On occasions the processor-controller analysis is incorrect, but even where it is correctly applied, frequently UK parties are reluctant to use the model contract terms and are prepared to forgo the legal certainty they provide in return for terms which reflect the commercial reality of their transaction. Let us look now at some of the concerns expressed by businesses in the context of these transactions.

A significant number of UK businesses tend to use model contracts as a starting point, but then amend and extend their terms.

Liability issues

Almost without exception, the liability clause of the model contract terms is the clause to which most UK businesses object. The principal objection is not so much the fact that individuals may seek damages from either the data exporter or the data importer, but the fact that the parties are required to accept joint and several liability to individuals. This is contrary to the basis upon which parties to an outsourcing (or other) transaction will otherwise agree to share risk. It is frequently the clause parties will seek to deal with on a different basis while still preserving the rights of individuals to pursue a remedy for a breach.

Typically, parties expect to be responsible only for the consequences of their own breaches. Further, where a party has sub-contracted or procured the provision of certain services from a third party, the prime contractor would expect (and would be expected) to reach agreement (often privately) with the sub-contractor as to how liability will be apportioned. In an offshore outsourcing transaction, individuals (who may be customers, other suppliers or employees of the data exporter) generally would not wish to pursue a remedy from an outsource supplier based in another jurisdiction. The fact that the model contract terms permit individuals to initiate proceedings from his/her own jurisdiction may not greatly assist from a practical perspective.

A related concern expressed by UK businesses in this context is that the liability clause in the model contract terms (clause 6) refers simply to "damage". From a UK perspective, liability for exemplary damages would typically be excluded by a service provider. Accepting joint and several liability for "damages" can expose both the data exporter and the data importer to the risk of an award of exemplary damages in a jurisdiction where such awards are more common than in the UK.

Termination and exit

A further key issue in outsourcing situations concerns termination and exit provisions. From experience, outsourcing customers are frequently reluctant to consider termination issues in any depth when negotiating an outsourcing agreement, particularly when energies are focused on transition-in and service commencement. Against this wider issue, the parties may give insufficient thought at the outset to how personal data will be protected and transitioned away from the outsource supplier when the contract comes to an end. This omission has been a particular feature of the early wave of offshore outsourcing contracts, many of which deal inadequately with transfers of personal data. Indeed, some institutions have already had their fingers burnt when these early contracts have come to an end, or come up for renewal.

In dealing with termination, the model contract terms simply provide that termination does not exempt the parties from their obligations relating to the processing of transferred data. There is no consideration of the circumstances in which the wider contract may be terminated, nor do the model contract terms seek to deal with any consequences which might flow from termination in particular circumstances, such as fundamental breach or force majeure. Specifically, the model contract terms do not contemplate a suspension of data transfers in this context, although suspension is contemplated in other circumstances (eg. in clause 5 in the context of legislative change having a substantial adverse effect on guarantees provided by the model contract terms).

In practical terms, businesses often require the model contract terms to be supplemented in this area to provide additional flexibility, particularly in relation to the onward transfer of personal data to a new or interim supplier.

The reach of the regulator

Many outsource customers operate in regulated sectors, particularly the financial services sector. Regulators such as the Financial Services Authority in the UK have issued guidance for regulated entities in order to deal with some of the risks arising from the outsourcing of material activities. One of the issues with which such regulators are concerned, is the extent to which they may exert influence directly over the outsource supplier. For a number of reasons, the

Key issues

The European Commission's model contracts contain a number of mandatory requirements that businesses would find difficult to reconcile with commercial reality.

Liability - The requirement of joint and several liability means that either party to the transfer may be sued for the other party's breaches of data protection regulations.

Exit clauses - Lack of detail in the termination clause mean that vital business issues can be overlooked.

Regulatory control - Offshore service providers are reluctant to agree to abide by the 'advice' of foreign regulators.

Governing law - Creates complexity and potential confusion when transfers involve data from multiple EU jurisdictions.

Audits - Outsource service providers will try to avoid committing to the model contract's broad auditing requirements.

Disclosure risks - Individuals are entitled to a copy of the contractual terms that deal with data protection - increasing the risk of commercially sensitive data being disclosed .

Processor-processor relationships - Model contracts terms do not deal expressly with processor to processor transfers.

preferred route is to require the regulated entity to exercise appropriate controls over the outsource supplier.

In the context of data protection, the model contract terms require the data importer to agree to not only cooperate with a relevant data protection supervisory authority, but to abide by its "advice". Aside from the ambiguity as to the meaning of "advice", many offshore suppliers are reluctant to agree to accept what is, in effect, a degree of regulation by an unknown, foreign regulator.

Governing law

The model contract terms require that the governing law is that of the EU member state from which personal data is exported. In the context of an outsourcing transaction for a multinational business, data may be transferred from a number of EU member states to a single offshore destination. While under English law it is possible for different parts of a contract to be governed by differing laws, this requirement adds unnecessary complexity and the potential for confusion in the context of a global outsourcing transaction.

Auditing

Clause 5(d) of the model contract terms requires the data importer to submit its data processing facilities for audit, either by the exporter or by independent auditors. From experience, while recognising that outsource customers will insist on having such audit rights, suppliers are reluctant to accept such broad ranging audit provisions and will typically insist on these provisions being supplemented with caveats and safeguards. Outsource customers, on the other hand, will frequently wish to link data protection audit rights to more general audit rights under the contract, and consider these in the round with benchmarking provisions.

Dealing with individuals

Clause 5 of the model contract terms governing controller-controller transfers requires the data importer to accept a number of obligations in relation to enquiries from individuals. Usually the data exporter will wish to control the provision of information to individuals, even where it acts as a data controller. Frequently this is consistent with the wishes of individuals who may prefer to make enquiries via their locally-based employer or supplier, rather than having to contact the outsource provider direct.

In addition, the model contract terms require both the exporter and the importer to make available upon request to individuals a copy of the contractual terms dealing with data protection. In practice - particularly where model contract terms have been supplemented by other provisions - consideration needs to be given as to how these requests can be accommodated as a matter of course without risking the disclosure of other, more sensitive, commercial terms.

Frequently UK parties are reluctant to use the model contract terms and are prepared to forgo the legal certainty they provide in return for terms which reflect the commercial reality of their transaction.

Processor-processor transfers

It is also relevant to mention that in an outsourcing context, the initial transfer of personal data may be to a locally (or EU) based supplier who then wishes to transfer such data abroad as part of a sub-contract arrangement, either to an unrelated entity or to one of its group companies. The model contract terms do not deal adequately with such processor-processor transfers. It is arguable that such transfers require a data transfer agreement between the outsource customer and the sub-contractor. Parties generally seek to deal contractually with this issue by requiring the outsource supplier to impose equivalent terms on any subsequent sub-contractor, and also to obtain the prior consent of the outsource customer.

Intra-group transfers

Many of the issues which businesses raise by way of objection to the model contract terms arise equally where cross-border transfers are undertaken in an intra-group context. Again, casual observation suggests that multinational organisations prefer to use means other than the model contract terms in order to facilitate these transfers.

The risks associated with cross-border transfers are generally regarded as lower in situations where transactions take place between subsidiaries of a multinational corporation. Often it is the case that multinational groups will have a US dimension and sometimes parties utilise the Safe Harbor regime. Frequently, however, such corporations tend to implement a set of internal guidelines and procedures to govern data transfers.

To date, most of these procedures would not strictly satisfy the requirements for the EU's binding corporate rules scheme but many represent a position which provide adequate safeguards for individuals. In this context, many businesses regard the model contract terms as too onerous and inappropriate for intra-group transfers. Again, and for reasons already explained, the liability clause is one of the key stumbling blocks in this context.

Conclusion

The comments made in this article are based on observation, rather than on any empirical research, and are made from a UK perspective. Although consequently general in nature, what they serve to highlight is the fact that cross-border transfers of personal data are increasingly a significant issue for businesses, particularly as the global trends towards offshore outsourcing and globalisation continue.

Many businesses do not consider that the model contract terms best serve their interests in providing a basis for data transfer, but certainly where businesses decide to depart from their terms, they tend to do so against a background of having considered the provisions of the model contract terms and using them as a starting point for drafting modified contractual terms.

AUTHOR:

Bridget Treacy, Partner, Commercial & Technology Group, Barlow Lyde & Gilbert

CONTACT:

btreacy@blg.co.uk