BIIA NEWS ON PRIVACY AND DATA PROTECTION

RegulatoryStrategies

A PRACTICAL GUIDE TO OUTSOURCING

With more organisations looking to outsource non-core activities it is critical that they understand the data protection and practical implications of doing so - and the ramifications of failing to.

Mike Bradford, *founder and director of Regulatory Strategies (www.regulatorystrategies.co.uk) and BIIA's Expert Advisor on Privacy and Regulatory Affairs* reports from his experiences in dealing with clients of all sizes and sectors that businesses still struggle with this. Some embed data protection requirements into their contracts but perform little due diligence; while others are thorough with the latter but have very weak contracts. And some do neither!

This article sets out what organisations need to do to comply with the Data Protection Act 1998 (DPA) - and sound commercial principles - when outsourcing the processing of personal information to a third party. It also draws on the Information Commissioner's guidance in this area.

WHAT IS 'OUTSOURCING'

Let's start in the real 'business' world. Yes there are strict DPA requirements around outsourcing. But not following these will not, in themselves, make any contract unenforceable unlike, for example, failing to comply with requirements under the Consumer Credit Act.

Similarly if no checks are undertaken on the third party 'processor', it doesn't automatically mean that they not capable of meeting the requirements of the organisation appointing them.

But if, or in reality when, something does go wrong, the lack of the requisite legal framework and evidence of due diligence will exacerbate what is a prima facie DPA breach - and one that will have legal, commercial and reputational impacts on the organisation concerned.

And if any incident involves loss or theft of personal data as is likely to be the case, the Information Commissioner will 'name and shame' and can now impose fines of up to £500k - not to mention what other regulators could do if the organisation is, for example, responsible to the FSA which imposed fines of £1.26m and £2.28m on Norwich Union and Zurich UK in 2007 and 2010 respectively, both for loss of customer data.

While it is obvious that an outsourcing relationship will be established when, for example, a UK organisation outsources some activity, be it a call-centre, IT processing or other support function to an unrelated organisation, it can also be established *within* a company.

Typically this could occur where a UK arm of a global organisation uses the capabilities of its US entity to undertake some processing on its behalf - perhaps because there is a specific skill set or technical infrastructure in their US operation. The principles outlined in this article equally apply albeit that in practice the due diligence requirements should be easier to evidence.

Indeed in the Zurich case mentioned above, Zurich UK outsourced processing to its South African subsidiary and a back-up tape was lost containing bank account, credit card and personal information. The resultant fine was the highest levied by the FSA on a single company for data security failings, even though none of the information had been misused or compromised.

And think across the organisation. Some processing may be less than obvious, but as the Information Commissioner considers 'processing' to cover everything from data acquisition to disposal, it is likely that there will be de facto outsourcing arrangements in place across the organisation - for example confidential waste disposal.

GENERAL AND CONTRACTUAL REQUIREMENTS

When an organisation (the 'data controller') outsources any processing of data it remains legally liable for any DPA breach even if it is the processor that is at fault. The 'data controller' cannot make the 'data processor' liable under the DPA, as a 'data processor' - acting in that capacity - has no DPA obligations in its own right.

This is a common misunderstanding in this area and the data controller should impose obligations on its data processor 'as if it were the data controller for the purposes of this agreement'

It is therefore critical to perform due diligence on any third party - either within the UK or abroad - the data controller appoints to undertake work on its behalf.

Commercially it is also critical to ensure there are 'back-to-back' warranties and indemnities to cover the data controller for any claims against it as a result of any failures of the processor.

The data processor should specifically have to take all 'appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data'. This effectively replicates the DPA obligation on IET as data controller.

Any potential appointment of a sub-processor by the data processor, perhaps an overseas office of their own organisation should always be caveated with the data controller having to approve any such appointment of a 'sub-processor' as again it will remain liable under the DPA for that processing and any breach. The due diligence it should perform on any processor would equally apply to any 'sub-processor.

As a final point, the contract should have a clause requiring the processor to immediately inform the data controller of any security breaches or other problems, including requests for information under foreign legislation. It follows that both parties should have procedures in place for managing such incidents or requests.

DUE DILIGENCE

The DPA requires the data controller to take **appropriate technical and organisational measures** to protect the personal information it processes, whether itself or through a third party.

Clearly any data breach or error resulting from the processor's actions could also damage the reputation of the organisation in the eyes of its customers and stakeholders and the consequences of failing to carry out due diligence are as much - if not more - reputationally and commercially damaging as any DPA breach.

As well as the contractual requirements outlined above, it is critical to have carried out due diligence on the third party ***and*** to be able to evidence this. The contract itself will not fulfil the data controller's DPA obligations without it being able to show it has vetted the data processor.

The processor should also be open to the data controller's right of audit at reasonable intervals.

The following is a useful checklist:

- What data are being processed? The more sensitive the data eg financial data (credit card details, bank account numbers, 'sensitive data' as defined by the DPA etc) the more security there should be around the data and the higher the data controller's requirements of the processor. However it is in practice always better to use the 'lowest common denominator' approach and protect even standard data to the same level as sensitive data.
- Financial and operational stability.
- Willingness to offer sufficient guarantees, warranties and indemnities.
- Track record of similar assignments.
- References.

- Reputation - market leader or small operator.
- Location and security of premises.
- Security of data storage and transfer facilities - physical and technical.
- Physical and organisational access controls - premises, databases, secure areas etc.
- DPA awareness and training within the organisation.
- Staff vetting procedures.
- How rigorous are their internal audit procedures?
- Ideally actually be on site for some of the time the processing is being carried out.

OUTSOURCING TO AN ORGANISATION OUTSIDE THE EEA

All the points above apply to outsourcing to a processor either in the UK or globally.

For any non UK processing the DPA requires that where personal information is transferred to any country or territory outside the European Economic Area (27 European Union Member States plus **Iceland, Norway and Liechtenstein)** there should be an adequate level of protection in place.

If an organisation were to outsource work on personal information to an organisation outside the EEA, for example, as is frequently the case to a data processing centre based in India or a processor (possibly even part of the same organisation) based in the USA, it will have to make sure that the information is adequately protected. This will apply to the method used to transfer the information to and from the processor as well as the work itself by the processor.

In practice there are two relatively simple ways to do this.

- If using an organisation based outside the EEA, as long as there are appropriate security measures in place, it is likely that there will be adequate protection for personal information.

  This is because the use of appropriate security measures, the selection of a reputable organisation and restrictions on the use of the information will all help ensure an appropriate level of protection for personal data.

-

- However, the data controller needs to be sure that the contract with the other organisation and its terms are enforceable in the country in which the processor is located.
- Use the model contract clauses approved by the European Commission and the Information Commissioner for transfers to organisations outside the EEA acting on the data controller's behalf. These contract terms can be used independently or incorporated into the data controller's main contract for services with the organisation.

Additional points in respect of overseas transfers are:

- What is meant by 'appropriate security measures' will depend on all the circumstances of the transfer. The data controller should consider the type of information, potential harm and available technology.

  Review the particular security and 'stability' risks (political, economic, social etc) associated with the recipient country, the existence of any data protection legislation in that country, or any other legislation that may affect the security of the data.
- The data controller should take into account the legislation in place in the country or territory where its chosen processor is located and any additional obligations this may impose.

A CLOSING MESSAGE

Established within a robust legal and commercial framework, outsourcing enables organisations to concentrate on their core activities and use the services of specialist providers, irrespective of geography, to add value to their business.

However, without following these legal and commercial protocols, outsourcing can be an accident waiting to happen with the potential for life-threatening consequences on the organisation concerned and its standing in the eyes of all stakeholders including customers, regulators and shareholders.

There's a very simple message here - get it right at the start of the relationship. No data processor will be too keen to have additional contractual obligations and warranties imposed on it 'after the event' (without using it as a negotiating lever on price!)

And with the new EU data Protection regulations on the not-too-distant horizon, with more onerous obligations and responsibilities on 'data processors', in other words our suppliers, watch this space for some really tough contracts discussions as they look to cover their exposures.

Posted June 25, 2012