Article

complinet

Lessons from SWIFT: the 'controller' v 'processor' dilemma

Jan 09 2008 Bridget C. Treacy

Bridget Treacy

Data protection issues dominated the news at the end of 2007 after the UK government admitted that it lost the data of 25 million individuals. Since then, the Information Commissioner has recommended that chief executives should be required to certify formally that they are satisfied that appropriate data security safeguards are in place within their organisations and proposed that reckless or repeated data breaches should become criminal offences.

Throughout the year, however, regulators had been noticeably more active in enforcing data protection laws. One of the most significant examples of this was SWIFT, a decision which considered the most fundamental of issues, namely, the capacity in which an organisation handles personal data. Which party is the processor, and which is the controller? What are the main features which distinguish one from the other? The increasingly collaborative manner in which businesses operate, particularly in the financial services sector, raises uncertainty as to where the line between controller and processor should be drawn. SWIFT has demonstrated that far-reaching commercial consequences may follow if the regulators disagree with the organisation's analysis.

Controller or processor: the law

The characterisation of a party as controller or processor determines the nature and scope of that party's data protection obligations. The controller remains accountable, to both the regulators and to individuals, for the data it processes. It is the controller that must register its processing activities with the data protection authorities, ensure that the data is processed in compliance with data protection principles, determine the appropriate level of security by which the data should be protected and ensure that it exercises sufficient control over any third parties to whom it has subcontracted or outsourced the processing of the data.

It is often difficult to determine in practice which party is the controller and which is the processor, although it is a fundamental issue. The Data Protection Directive (EC/95/46) characterises the test of a controller in terms of the degree of discretion or decision-making authority exercisable by that party in relation to the data it processes. The party which decides the purposes and means of the processing will be the controller.

The difficulty many organisations face in practice is that their business operations are dynamic. Businesses operate in an increasingly collaborative manner and the nature of relationships changes over time. A party that was once merely a processor might, over a period, assume a greater degree of responsibility in relation to the data. This might occur as a result of additional services being added or new technology being deployed. More subtly, as the relationship develops, the processor may simply be entrusted with greater discretion in relation to the data.

SWIFT analysis: controller or processor?

The decision of the EU data protection regulators (acting together as the Article 29 Working Party) that SWIFT, an intermediary which facilitates the international transfer of funds between financial institutions, was a controller and not a processor brought into sharp focus the fact that the "controller v processor" analysis is difficult in practice, yet can have far-reaching effects.

SWIFT had considered itself to be merely a processor, operating a messaging service. As part of its data back-up arrangements, SWIFT had a mirror database in the US which, ultimately, the United States Department of the Treasury gained access to via subpoenae issued as part of its post-9/11 anti-terrorism initiatives. This access brought SWIFT's processing arrangements to the attention of the Article 29 Working Party which concluded that SWIFT was a controller and that the manner in which data was made available to the UST contravened the EU Data Protection Directive.

The Working Party's characterisation of SWIFT as a joint controller (together with individual financial institutions) in relation to the personal data of the banks' customers and counterparties was crucial to its analysis. The Working Party pointed to several factors which, in its view, meant that SWIFT's role extended beyond that of a mere processor:

- SWIFT took on specific responsibilities which, by their nature and scope, went beyond the usual set of instructions and duties for execution by a processor.
- SWIFT's management was able to determine the purposes and means of processing by developing, marketing and altering SWIFT's services (e.g., by determining the form and content of payment orders).
- SWIFT provided additional value to the processing.
- SWIFT's management had the autonomy to take decisions (e.g., determining the security standard to be applied to the data and the location of the data centres).

Many of these factors are commonplace in a variety of commercial arrangements.

Wider implications of SWIFT

The characterisation of SWIFT as a controller meant that it had to comply with the more onerous compliance obligations of a data controller. Considered by many to be harsh, the decision has wider implications for many existing commercial relationships, particularly outsource relationships where the majority of outsource vendors characterise their role as that of a data processor.

Typically, the vendor's analysis is that the financial institution must take responsibility for its own legal compliance, including data protection compliance. If the processing of this data is to be outsourced, then it is for the financial institution, as controller, to warrant that the data has been properly collected and processed within the business prior to the outsource and that the financial institution is legally permitted to outsource the processing. Vendors then expect financial institutions to take the lead in specifying compliance requirements for the relevant data processing.

At a practical level, there is usually some uncertainty as the parties attempt to define the services, determine what personal data will be affected by the outsourcing of those services, and allocate responsibility. Careful analysis is required so that an informed judgement may be made as to whether the financial institution will continue to determine the purposes and means of the processing of the data, notwithstanding the fact that the performance of the services has been outsourced. Once the position has been agreed, the contractual risk is apportioned between the parties with warranties and, frequently, indemnities being agreed. The contract price may be adjusted to reflect the allocation of risk.

What then will be the consequences for the contract if, at some later point in time, a regulator characterises the outsource vendor as a joint controller? Clearly the balance of risk and reward will have changed and may well need to be addressed by amendment to the contract.

A new conservatism

Unsurprisingly, there is growing evidence of a new conservatism in the way in which banks, insurers, intermediaries and other financial institutions deal with personal data. SWIFT provides a timely reminder of the importance of carefully analysing the capacity in which parties process personal data, not just at the outset, but throughout the life of the contract.

This article does not provide a complete statement of the law. It is intended merely to highlight issues which may be of general interest and does not constitute legal advice.

• ***Bridget Treacy*** *is a partner in the Hunton & Williams Global Sourcing and Privacy practices. Tel: +44 (0)20 7220 5731*

This article first appeared on Complinet on www.complinet.com *on January 09 2008. For a free trial of Complinet's services, please contact client support on* client.support@complinet.com *or* +44 (0) 870 042 6400.