ENERGY METER DATA AND EU PRIVACY LAWS
A ROAD MAP

By Bridget Treacy

There is a growing media frenzy in Europe focused on data security breaches. Last year, the UK government was in the media spotlight, following the loss of 25 million records by HM Revenue and Customs; currently it is the turn of Deutsche Telecom and its subsidiary T-Mobile, following the loss of 17 million customer records.

Irrespective of market sector, organisations which collect and process the personal data of customers, staff and vendors must take their data protection obligations seriously. Recent data breaches demonstrate that data breaches are costly to respond to and quickly erode customer trust. As data protection regulators adopt a proactive approach to enforcement, data protection risk is moving up the corporate risk agenda.

WHAT ARE "DATA PROTECTION" LAWS ABOUT?

Data protection laws seek to strike a balance between the commercial interests of organisations in processing the personal data of individuals and the rights of those individuals to know that their data are being processed and to exert some control over that processing.

"Irrespective of their content, most data protection laws developed in a world in which computing power and data volumes were a mere shadow of what we now regard as standard."

Data protection laws exist in many countries but not all data protection laws are the same. In some countries, the focus is on the right to determine who may use personal data for commercial purposes (eg electronic marketing practices); in other countries, the laws may incorporate the human rights concept of "privacy", as well as rights to informational self-determination. In countries such as the US, privacy laws have developed on a piecemeal basis, in response to specific commercial needs. In other parts of the world, such as the EU, data protection laws form a comprehensive legal framework.

Irrespective of their content, most data protection laws developed in a world in which computing power and data volumes were a mere shadow of what we now regard as standard. Consequently, many commentators argue that the legal framework is in need of a radical overhaul to reflect both the advances in technology and the fact of our globally networked environment.

There is also a change in focus becoming apparent as organisations focus less on "data protection" as such and more on the concept of "information management". This change in focus reflects the fact that data is now central to everything we do and is increasingly becoming a valuable corporate asset for business.

Europe is widely regarded as having the most restrictive data protection laws. Although the laws of individual EU jurisdictions differ, they are all based on the EU Data Protection Directive (EC/95/46). This Directive is used as the reference point for the remainder of this article.

HOW ARE DATA PROTECTION LAWS RELEVANT TO ENERGY METERING?

Any business which collects and processes information about consumers will, in data protection terms, be processing "personal data" and is likely to be subject to data protection laws. It should be noted that personal data is not restricted to information about customers, but includes personal information about the organisation's staff and vendors as well.

The advent of the "smart" meter, plus increasingly sophisticated analytical research tools that rely on data collected by smart meters, means that companies operating within the energy distribution chain are increasingly likely to process personal data and will be subject to data protection laws.

KEY REQUIREMENTS OF EU DATA PROTECTION REGIME

To gain any useful insight into EU data protection laws, it is crucial to understand some key definitions. In essence, the Directive governs the processing of personal data by data controllers.

- "Processing" includes obtaining, recording, storing, amending, retrieving, disclosing and destroying the data. Even calling data up on a computer screen constitutes "processing". In fact, it is difficult to envisage any use of personal data which would not amount to "processing" under the Directive.
- "Personal data" is any information which relates to an identified or identifiable natural person. "Sensitive personal data" consists of special categories of data such as data relating to a person's racial or ethnic origin, religious beliefs or health, which are subject to additional safeguards.
- The Directive imposes obligations on "data controllers" who are the individuals or entities which determine the purposes for which and the manner in which personal data will be processed. The role of a data controller is distinct from that of a "data processor" which processes data in accordance with the instructions of a data controller.

Unlike the controller, the data processor does not have any obligations under the Directive, but will (or should) have contractual obligations imposed on it by the data controller.

In addition, the Directive recognises the rights of individuals to control how, when, for what purposes and by whom their personal data are processed. An individual can ask for details of their personal data held by an organisation (ie make a "subject access request"), require that their data are corrected and request that their data are no longer processed. In addition, an individual may be able to claim remedies in the event of infringement of their rights which can include damages for distress.

The Directive contains a set of eight "Data Protection Principles" which form an enforceable code of practice governing the processing of personal data. Organisations which process personal data as data controllers must ensure that all such use or processing is in accordance with these eight principles. In summary, the principles require that personal data are:

- processed fairly and lawfully
- processed only for the purposes specified to the individual
- adequate, relevant and not excessive
- accurate and up-to-date
- not retained unnecessarily
- processed in accordance with the individual's rights, including the right of subject access
- processed securely, and
- only transferred outside the EEA if adequate protections exist.

These principles may appear straightforward but care should be exercised in assessing compliance as many principles are expanded upon in domestic legislation and in fact require more compliance activity than their description might suggest.

At present, European data protection regulators appear to have a particular focus on the following key principles:

- Purpose limitation: ensuring that personal data are collected for specific, limited purposes and not used for other purposes. For example, consumers' home addresses which are collected for billing purposes by a gas distributor may not be used for more general marketing purposes.
- Data minimisation: collecting and processing only the minimum amount of data required for the particular purpose. For example, why does an electricity supplier require the date of birth of a retail customer? Where data are shared with sub-contractors for processing, only the minimum amount of data should be shared and not the entire database.
- Technical and organisational security: data breach is headline news in Europe and has been headline news for some time in the US. In the EU, controllers have an obligation to ensure that data are appropriately safeguarded. Some recent data breaches have resulted from serious operational oversight: for example, in the UK a junior clerk in a government department downloaded an entire database, comprising 25 million records, onto two CDs and sent them by post to the auditors. The CDs were lost. In other examples, vendors have downloaded data onto unencrypted data sticks and lost them.
- Cross-border transfers: the EU prohibits the transfer of personal data abroad, outside of Europe, unless adequate safeguards can be demonstrated. Several mechanisms exist for establishing adequacy, including entering into EC approved contractual clauses. Ignoring this restriction can result in EU data protection regulators prohibiting transfers of data abroad.

HOW CAN BUSINESSES IN THE ENERGY DISTRIBUTION CHAIN COMPLY WITH DATA PROTECTION LAWS?

Organisations at every level of the energy distribution chain should consider their data protection compliance obligations, particularly where part of the operation is in Europe or involves data obtained from Europe. Specific compliance obligations will differ from one country to another but the basic European requirement is that data controllers must process personal data in accordance with the eight Data Protection Principles set out above. Further specific obligations also apply. For example, if a third party is used to process personal data on behalf of another, the Directive requires specific contractual obligations to restrict the purpose of processing by the third party, and a positive obligation to safeguard the data using appropriate security.

"Organisations at every level of the energy distribution chain should consider their data protection compliance obligations, particularly where part of the operation is in Europe."

The practical issue of where to begin with a data protection compliance programme can sometimes be daunting. It may assist to visualise a compliance programme as an evolutionary process, rather than a "tick-the-box" or "off-the-shelf" solution. The programme will need to be developed to accommodate the particular needs and aspirations of the organisation and to take into account the specific risks or issues affecting the marketplace within which that organisation operates. Otherwise, as with any other audit or compliance project, the conventional stages of the project will involve:

1. identifying existing data protection procedures and practices within the business
2. understanding the relevant legal framework
3. assessing the extent to which the existing policies and procedures comply with the legal framework
4. determining the extent to which data is processed in accordance with compliant policies, and
5. developing remedial steps to address any identified shortcomings.

The challenge, particularly for large, global organisations, is to devise a compliance project which provides an appropriate level of comfort within a specified timescale and budget. A high-level scoping phase should assist with this planning by providing an overview of existing data protection policies and procedures and an indication of the extent to which they are followed in practice.

SCOPING THE PROJECT

It is usually helpful to begin with an overview of the organisation, on a country by country basis, and to gain a high level view of what personal data is processed, by whom, and for what purpose. Using the framework of the "data lifecycle" can assist here.

These initial investigations can easily be undertaken by someone within the organisation, although some businesses prefer to use an external advisor at this stage in order to gather more detailed information and to assist with scoping the project. From these investigations it should be possible to identify potential areas of risk, to which a greater part of the project budget should be allocated for further investigation.

LEGAL FRAMEWORK

Once a high level view has been obtained of what personal data is processed by the organisation globally, how and for what purpose, then a brief can be prepared for legal counsel in each of the relevant jurisdictions. Some organisations may be able to establish the legal framework using internal legal resource, but most will need to use external counsel.

ASSESS EXISTING POLICIES AND PROCEDURES

Existing policies and procedures will need to be reviewed in detail and analysed in light of the relevant legal framework. They should evidence detailed consideration of the nature and extent of the data gathering and processing activities of the business. Some organisations will undertake this activity using internal resources; others will turn to external advisers.

EVALUATE COMPLIANCE

This stage of the review involves an assessment of the extent to which personal data are in fact processed in accordance with compliant policies and procedures. There are many ways of undertaking this analysis. Some organisations will require a detailed compliance audit; others may be content with higher level assurance, perhaps using a form of statistical sampling or via interviews or questionnaires to gain a degree of comfort. It is crucial that this stage of the review is well planned and that the process and output are carefully documented.

"Within Europe, the number and size of recent data breaches has prompted calls for data protection regulators to have stronger powers of enforcement."

ADDRESS SHORTCOMINGS

The extent of the work required in this phase of the project will vary from superficial to extensive. It is important that resources are allocated to high risk areas. More significant issues are sometimes addressed as separate projects. Irrespective of the particular methodology used here, it is important that there is a sensible means of reporting back to senior level sponsors of the project in order to maintain visibility and support. Once serious shortcomings are remedied, an ongoing programme of review and exception monitoring can be helpful.

WHAT ARE THE RISKS OF NON-COMPLIANCE?

Data protection risk management has achieved a higher profile recently, not just within Europe but in countries such as the US which have strict data breach laws and a tough enforcement regime.

Within Europe, the number and size of recent data breaches has prompted calls for data protection regulators to have stronger powers of enforcement; however, even without stronger powers, these regulators' approach to enforcement has changed markedly during the past 18 months. In the UK, legislation has been passed this year to give the data protection regulator, the Information Commissioner, the power to impose substantial fines on an organisation which breaches the data protection principles deliberately or recklessly in a manner likely to cause substantial damage or distress. A broadly similar power is held by the Financial Services Authority in the UK and it has imposed fines in the region of £1 million to £1.26 million in the last year on organisations which have failed to safeguard personal data.

Further, the UK Information Commissioner has no hesitation in publicising its enforcement activity by issuing press releases. The regulator has also developed a practice of negotiating undertakings with companies in the context data breaches, securing a commitment from senior management to implement better data protection practices in exchange for the regulator not taking formal enforcement steps. Undertakings require execution by an officer of the company, typically the CEO, which ensures that these breaches are drawn to the attention of senior executives.

For businesses which are close to their customers, data protection compliance is fast becoming an issue that is addressed proactively. Many businesses are realising that individuals (both customers and staff) are concerned to know about and to control what happens to their personal data. Indeed, many instances of data protection infringement which have been highlighted by the media in Europe in the last year have featured individuals concerned about their personal data being transferred abroad. Whilst other reasons may explain why some of these instances attracted so much publicity (for example, the support of trade unions in highlighting issues which may help prevent the perceived loss of jobs to off-shore vendors), research carried out by the UK data protection regulator revealed in 2003 that a surprising 80% of individuals would not do business with an organisation which did not take data protection seriously. Data protection is now becoming a matter of enlightened self-interest for businesses.

CONCLUSION

Data protection is an increasingly significant aspect of regulation and one made more complex by the raft of data protection legislation with which global businesses need to comply. More proactive enforcement by European data protection regulators, often in the wake of data breaches, is ensuring that data protection moves up the corporate risk agenda. Companies now ignore data protection at their peril. MI

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.

ABOUT THE AUTHOR: Bridget Treacy is one of the UK's most experienced privacy lawyers. She advises multinational companies on the strategic use of personal data, particularly in the context of global outsourcing deals and the implementation of new technologies. She is a partner in the Privacy and Information Management Team at law firm Hunton & Williams.

A metering system head and shoulders above the rest.

Our advanced metering system, called Networked Energy Services, intelligently manages and controls energy all along the grid — shedding loads, detecting outages, managing streetlights, and enabling demand response programs in homes and buildings. No other advanced metering system offers a more integrated system to optimize energy, improve operations, reduce carbon emissions, and ensure customer satisfaction.

Call +1 408 938 5200 or visit www.echelon.com to see what NES can do for you.

ECHELON®