A single law approach to global privacy compliance

By Jeroen Terstegge

MULTINATIONALS WHICH BASE their global privacy practices upon one EU country's national law, can ease the administrative burden while still maintaining high data protection standards, argues Philips' Jeroen Terstegge.

Multinational companies often operate unified data processing systems for their personnel (HR) data or customer data. They also have databases which are accessible by all employees or a number of them, such as personnel directories, books and Intranet web pages.

Complying with data protection laws often proves to be difficult – if not impossible – because of the differences in national data protection laws and regulations. These difficulties are exacerbated by the diverging opinions, interpretations and regulations of national data protection authorities, in addition to diverging opinions of national courts. Therefore, instead of lifting barriers to the free flow of personal data within the EU, the current European system of data protection tends to create barriers by imposing different obligations and procedures on organisations which operate in more than one member state.

In this article I will examine the possibility of creating a different system of control, one which should help in eliminating the distortions created by national implementations and interpretations of the EU Data Protection Directive. This system should also help to improve privacy compliance while at the same time facilitating supervision by data protection authorities of transborder data processing systems.

ANALYSING THE PROBLEM

Article 4 of the directive requires organisations to comply with the national data protection laws of the member states in which they process personal data. If an organisation has operations in different member states, it must ensure that each of its establishments complies with the laws of each member state.

This unwieldy system means that a multinational corporation could potentially be required to comply with up to 15 data protection laws within the EU. As organisations often adopt a unified approach to compliance, this obligation results in 'multi-jurisdictional' data processing systems, because each of the member states' data protection laws apply to these systems.

This problem will soon increase as new countries join the EU. Not only does this system create difficulties in complying with data protection obligations, it also creates a massive administrative burden for multinational companies. Often, these unified systems have to be registered with data protection authorities across several member states (referred to as the 'Tour d'Europe'). In cases where data is transferred to a non-EU country, multiple governmental authorisations have to be obtained, following procedures that vary in form, length and complexity. As a result, those member states that operate a system of permits or licences for transferring data have a right of veto over these systems.

Multinational corporations may wish to centralise or unify their data processing operations for a number of reasons. They may wish to have a harmonised marketing policy, which is best implemented by having one customer database and a single privacy policy. A multinational may wish to streamline its HR-procedures, such as headcount, hiring procedures, training and competence, rating employee performance, or awarding bonuses.

Sometimes these streamlining activities are implemented by creating central databases at the company's headquarters, but they may also include the mandatory use of computer networks, software and communication techniques which have been selected or are operated by the company's headquarters. Applying the directive's applicable law provisions to these situations is often difficult.

Often the division between the functional units of the company does not coincide with its legal structure. This often results in data processing operations with multiple data controllers within the company, or extensive third party data transfers. Where such data processing moves outside European borders (for example, online access to the directory of the functional unit), the data transfer provisions of the directive will prove to be particularly burdensome.

FINDING A WORKABLE SOLUTION

Since multinational companies are faced with difficulties regarding applicable law, as well as international data transfers, finding a proper solution must take into account an integrated corporate approach to privacy and data protection, and the applicable law and supervision.

In my view, a workable solution lies in the combination of the use of Privacy Codes of Conduct and a system

of 'Home Country Control'.

Privacy Code of Conduct

Unified data processing systems require an integrated corporate approach towards privacy and data protection. A privacy code of conduct would allow multinational companies to adopt a single policy on data protection issues such as the collection of and use of personal data, international data transfers, consent/opt-out and data security. Such a code – if implemented correctly – would provide a 'protective seal' around the company and could serve as a basis for legitimate data transfers to subsidiaries in non-EU countries, without the need for the additional governmental authorisation.

As it is near-on impossible to comply with the national data protection laws of all 15 EU member states, such a code could either be compliant with the directive itself or be compliant with the laws of a single member state. This leads me to the next topic.

Home Country Control

Within a multinational corporation, it is often the parent company that issues regulations or prescribes data processing systems that affect all or most of their subsidiaries. According to the definition of the directive, in such situations the parent company will be regarded as the data controller, because it wholly or partly determines the purposes or the means of the data processing. Examples of such determinations are: laying down a single privacy policy for customer data or running centralised marketing campaigns; setting up and maintaining a central computer network; creating central HR databases at a corporate level; prescribing customised software for customer or HR data for use by subsidiaries (often accompanied by central databases in which the data is stored).

However, in many cases, subsidiaries cannot be regarded as pure data processors (within the meaning of the directive). Often they have some degree of freedom to process the data concerned. Also, they have their own obligations under various national laws (for example, labour law), which influence their data processing activities.

For this reason, data processing carried out by a single database on a corporate or network level becomes 'multi-jurisdictional', meaning that the laws of more than one state regulate the same system at the same time. To comply with all national laws often proves to be difficult, if not impossible, through the lack of harmonised legal requirements.

A system of 'Home Country Control' would address the most pressing problems for transborder computer networks. Such a system would allow multinational companies to operate their unified system under the law of their home country only. Since this national data protection law will be based on the directive, it should be considered to provide an adequate level of protection even in other EU member states. To determine which location is the home country of a corporation, and therefore which law to apply, one should look at the location of the parent company (for EU companies) or the location of the European headquarters (for non-EU companies).

> ...finding a proper solution must take into account an integrated corporate approach to privacy and data protection...

However, not all legal requirements of the home country should be exported to other member states. The rights of the data subjects should at all times be addressed under the national law of the subsidiary which collected the personal data, or which is responsible for managing the relationship between the company and data subject.

This means that the right of access, correction, blocking and objection, as well as the obligation to inform the data subject, should be regulated by the national law of the country in which the subsidiary is based. Only if the subsidiary has no autonomy to control these obligations, its national law should not apply (eg. a privacy notice on the corporate website in accordance with the privacy laws of another member state would suffice).

Also, the provisions of the national law should apply to the autonomous actions of the subsidiary, such as the collection of the data or the use of the data.

These national laws should not apply, however, to those elements of data processing which are under the control of the parent company, such as the determination of the purposes and the means of the data processing in general, the design of the network or the database, the security of the personal data and the control and audit procedures.

The system can only work if the company assumes responsibility in a uniform manner, encompassing all its operations. This means that the data subject should always have the right to contact the subsidiary in their own country (or the one responsible for their country) for any access or correction request or complaint. If the subsidiary cannot act on this request or complaint itself, handling such a request will be the full responsibility of the entire company, meaning that the relevant entities of the company should assist this subsidiary in addressing the request or complaint. Such an obligation of mutual assistance and corporate responsibility would have to be part of the Privacy Code of Conduct mentioned earlier.

What would happen when a data subject files a complaint with its national data protection authority, with regard to the processing of its personal data in a transborder company database or network for which the parent company is responsible? In such a case, the data protection authority should seek the assistance of its counterpart in the country of the parent company to examine the claim and take corrective actions if necessary.

However, should the data processing be legitimate according to the laws of the country where the parent company is based (but not according to the laws of the country in which the sub-

sidiary is located), the law to which the parent company is subject should prevail. If this leads to undesirable results, it should be up to the European legislator to take actions to achieve the proper level of harmonisation desired.

Home country control also means that the database and the data processing operations should be subject only to the formal supervision procedures of the country in which the parent company is established. This would apply to the obligation to register the database or data processing and the governmental authorisation for international data transfers. The individual data processing actions of the subsidiaries – even partly autonomous – should not have to be registered in their own countries. Only in cases where the subsidiary has full control over the data processing system (full autonomy), should its national formal procedures apply. This would eliminate the 'Tour d'Europe', as well as a possible 'veto' on international data transfers by a particular member state.

Conclusion

Multinational companies often have a unified system to process customer and HR data. The current patchwork of national data protection laws in Europe makes it difficult, if not impossible, for multinational companies to comply. Even with a single EU Data Protection Directive, its implementation into national law, and the interpretations of the issues by the various data protection authorities, is failing to achieve a workable level of harmonisation.

The restructuring of the applicable law regime into a system of 'home country control' as well as the creation of a 'protective seal' would greatly benefit multinationals' ability to comply, and the supervision by national regulators.

Member states would, however, give up some sovereignty over the data processing occurring within their territory. They would need to recognise the adequacy of each other's data protection laws and trust each other's supervision and judicial control. But such 'weighty arguments' should not be an obstacle to improve the protection of personal data of their citizens.

Jeroen Terstegge is Legal Counsel for Privacy & Data Protection Law at Philips International B.V. (The Netherlands).
This article also appears in the December issue of Dutch Magazine "Privacy & Informatie"

Continued from page 7

3. The principles of "better regulation", with particular reference to legal clarity and legal security and to alleviating any unnecessary administrative burdens.

Bolkestein emphasised that the directive was approved for internal market purposes and that "divergences in data protection legislation and the way it is applied in the member states are in fact creating problems for the free movement of data. These difficulties damage the competitiveness of our enterprises because they are prevented from operating effectively on a European scale.

As most member states were late in transposing the directive into their national laws (Luxembourg had approved its law only in August this year and France and Ireland had still not done so) it would be "premature…to bring forward radical proposals for its amendment on the basis of so little experience with its application." Indeed the Commission would "hesitate before embarking on any kind of new legislative action" which can be slow to produce results. Instead, the Commission would exploit "more pragmatic possibilities." He would give priority to "ensuring a uniform and consistent application and interpretation of the directive" by changing national laws in some cases. His staff have already started a constructive dialogue with member states.

Priorities for future Community action include:

1. "the simplification of notification requirements"

2. "reduction of divergences in member state practices," helped by the Article 29 Data Protection Working Party

3. "a more determined effort to promote privacy enhancing technologies"

4. "more flexible arrangements for the transfer of personal data to third countries, together with a clearer and more uniform interpretation of the rules"

5. "promotion of self-regulatory approaches and in particular codes of conduct that can contribute to the free movement of personal data; the idea that approval by one data protection authority should in principle work in all member states needs to be pursued." (see p.8)

He concluded with an acknowledgement of the importance of privacy rights and the influence of the EU in the world: "Our readiness to conduct the review in this very open way is a measure of our underlying confidence in this piece of legislation which is setting a standard for many other countries in the world and symbolises the commitment of the European Union to strike the right balance between the interests of trade and competitiveness and the protection of the fundamental rights and freedoms of our citizens."

Stewart Dresner is the Editor & Publisher of PL&B newsletters, and Chief Executive of Privacy Laws & Business.

Speeches, consultation papers, and other commentary from the Brussels conference can be found at: http://europa.eu.int/comm/internal_market/en/dataprot/lawreport